PhD-FSTM-2024-039
The Faculty of Science, Technology and Medicine

DISSERTATION

Defence held on 03/06/2024 in Luxembourg

to obtain the degree of

DOCTEUR DE L'UNIVERSITÉ DU LUXEMBOURG

EN INFORMATIQUE

by

Tamara Heidi ROTH
Born on 27 November 1992 in Hof, Germany

INNOVATING WITH EMERGING IT IN HIGHLY STRUCTURED ENVIRONMENTS – AN ORGANIZING VISION PERSPECTIVE ON BLOCKCHAIN AND DIGITAL IDENTITY WALLETS

Dissertation defence committee

Dr. Gilbert Fridgen, dissertation supervisor
Professor, Université du Luxembourg

Dr. Amber Grace Young
Associate Professor, Sam M. Walton College of Business, University of Arkansas, United States of America

Dr. Andreas Hein, Chairman
Associate Professor, Université du Luxembourg

Dr. Djamila Aouada, Vice Chair
Assistant Professor, Université du Luxembourg

Dr. Andrew Burton-Jones,
Professor, The University of Queensland, Australia

“Reality is merely an illusion, albeit a very persistent one.”

Albert Einstein

Abstract

This cumulative thesis explores the challenges and institutional mechanisms of innovating with emerging information technologies (IT) in highly structured environments. Emerging technologies are often difficult to implement because they arrive on the market in an immature state and with unclear use cases. To make sense of the emerging IT, members of the innovation community develop various interpretations. These are typically replete with wishful and unbalanced claims, resulting in a vibrant IT discourse that is characterized by a plethora of discursive frames and value-laden buzz words. When this discourse becomes coherent, it often leads to contagion and motivates organizations to engage with the emerging IT. Such engagement is challenging even for the most flexible organizations with innovation-friendly structures – and it can be downright daunting in highly structured environments. The latter organizations often face high structural and cultural barriers that encumber digital innovation with emerging IT. Adopting the macro-level cognitive institutional perspective of organizing vision theory, this thesis sets out to investigate how organizations in these environments can nevertheless make sense of emerging IT and materialize it in applications that create organizational value. My thesis examines the challenges of surfacing a pertinent business problematic from the organizing vision and of unpacking the technologies' abilities and limitations. Moreover, it segues into pathways for navigating the aforementioned structural and cultural barriers. I develop four conjectures that provide practical guidelines for organizations in highly structured environments that are willing to engage with emerging IT. These insights build on 15 research papers, which are part of this thesis.

Acknowledgements

My gratitude goes to everyone who supported me in completing this doctoral thesis. First, I thank Prof. Dr. Amber Young for her unwavering support and mentorship, which helped me grow both as a person and a researcher. Her direction made me realize that "no goal is too high if we climb with care and confidence" (Cathy Truett). I look forward to even closer cooperation now that we are in the same department. I also want to thank my supervisor, Prof. Dr. Gilbert Fridgen, for helping me build bridges between my former and current discipline. You empowered me as an interdisciplinary researcher and encouraged me to constantly push my own boundaries. Thank you also to Prof. Dr. Djamila Aouada for your support as my CET board member. You are a role model for many female aspiring scientists.

Next, I extend a big thank you to my co-authors and colleagues at the University of Luxembourg; the University of Arkansas; the University of Bayreuth, together with the Research Center for Finance and Information Management; the University of Zurich; the University of Washington; and Leipzig University. I enjoyed our free and productive exchange of ideas. You always helped me to stay motivated. Third, I want to deeply thank my family and in-laws for their patience and support, and particularly, my beloved husband Alex – my biggest cheerleader, even in times when I could not see a way forward. My achievements would not have happened without you. I am also grateful for the warm welcome of Prof. Dr. Mary Lacity, Prof. Dr. Rajiv Sabherwal, and Prof. Dr. Shaila Miranda during my semester as a visiting scholar and, later, a visiting assistant professor at the University of Arkansas. I look forward to joining you as a tenure-track assistant professor in August.

A big shoutout also goes to my colleagues/friends Jana Gastineau and Justin Shipp. You make Fayetteville feel like home. Moreover, I thank the Luxembourg National Research Fund (FNR) and PayPal, PEARL grant reference 13342933/Gilbert Fridgen, grant reference NCER22/IS/16570468/NCER-FT, and grant reference 14783405; and the European Union (EU) within its Horizon 2020 program, project MDOT (Medical Device Obligations Taskforce) grant agreement 814654, for their support of my research.

Declaration

I, Tamara Heidi Roth, hereby declare that the thesis has been composed by myself and that the work has not been previously submitted to obtain any other degree or professional qualification. I confirm that the work is my own, except where publications have been created in larger authors teams. I have acknowledged any contributions made by other authors in jointly authored publications, and I have provided accurate citations and references throughout the thesis. AI tools, such as ChatGPT and Grammarly, were only used anecdotally to check grammar in individual sentences.

I have no financial interests to declare, and I adhere to the principles of transparency and integrity in both public and professional life. I fully understand and commit to ethical research practices and academic honesty. I have no other financial holdings, affiliations, or engagements that would require disclosure.

Luxembourg, 22/04/2024

Tamara Roth

Tamara Heidi Roth

Table of Contents

Abbreviations

EBP	European Blockchain Partnership
EBSI	European Blockchain Services Infrastructure
eIDAS	Regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market
EU	European Union
GDPR	General Data Protection Regulation
OV	Organizing Vision
PoC	Proof-of-Concept
PoW	Proof-of-Work
PoS	Proof-of-Stake
SSI	Self-sovereign Identity

Tables and Figures

1. Introduction

1.1. Innovating with Emerging IT in Highly Structured Environments

The constant demand for digital innovation keeps organizations on their toes across all sectors and industries (Fried, 2017; Gaspary et al., 2020). While digital innovation promises to foster positive organizational change – from better products and services to more efficient processes (Feller et al., 2011) – organizations in highly structured environments, i.e., formalized organizations with a clear set of rules for intra-organizational procedures and structures (Fredrickson, 1986), often struggle to realize digital innovation (Castagneto Gissey et al., 2018; Cinar et al., 2019; Fried, 2017; Meijer, 2015). They are shaped by complex legal frameworks that manifest in equally complex organizational processes and IT architectures, exacerbated by a culture of bureaucratic stewardship aimed at preserving the status quo (Goh & Arenas, 2020; Scott et al., 2016). The level of continuity enforced by such a culture can create stable and responsible governance. However, too much focus on preserving the status quo can also paralyze the organization and stall digital innovation (De Vries et al., 2016).

Digital innovation in these environments becomes particularly challenging when emerging technologies are involved (Shiller, 2020; Vinsel, 2023). Emerging ITs "often arrive on the marketplace in an immature state, puzzling as to its benefits, future prospects, and long-term form" (Swanson & Ramiller, 1997, p. 459). To make sense of the emerging IT, innovation community members usually construct various uses based on their interpretations of its potential (Barad, 2007; Miranda et al., 2015; Phillips et al., 2004). These interpretations are typically replete with wishful and unbalanced claims, resulting in an innovation discourse that is characterized by a plethora of discursive frames and value-laden buzzwords (Miranda et al., 2022; E. Swanson & Ramiller, 1997). While the initial frames and buzzwords can help spotlight expectations or organizational needs, and even create contagion for the technology (Shiller, 2020), they can also be a source of confusion for organizations eager to engage with the emerging IT (Gal et al., 2022; Wang, 2010). Specifically, "uncertainties concerning requirements, design, and use" (Swanson & Ramiller, 1997, p. 459) elevate the risk for organizations to invest time and resources in a technology they may not adopt.

To minimize this risk, organizations in the enactment field – i.e., those that materialize the discursive frames – usually embark on a process of organizational sense-making (Maitlis & Christianson, 2014; Miranda et al., 2022; Weick et al., 2005). This sense-making helps enacting organizations cut through the thicket of wishful and unbalanced claims and select discursive frames from the so-called organizing vision that best match their own organizational goals (E. Swanson & Ramiller, 1997). Organizing visions are defined as "focal community idea[s] for the application of information technology in organizations" (Swanson & Ramiller, 1997, p. 460). They usually encompass pertinent business problematics and institutional mechanisms for embedding the emerging IT into the organizational context. They serve three functions in the innovation process: interpretation, legitimation, and mobilization (Gorgeon & Swanson, 2011; E. Swanson & Ramiller, 1997). These steps dynamically combine sense-making of selected discursive frames from the IT organizing vision with their materialization in the organizational context (Currie, 2004; Gorgeon & Swanson, 2011). Such material-discursive practices typically facilitate the reduction of dissonance and establishment of resonance between the organizational context and the discursive frames surrounding the focal IT. Moreover, they help flesh out the concrete business problematics that the emerging IT can address (Miranda et al., 2015; E. Swanson & Ramiller, 1997; Wang & Swanson, 2007).

1.2. Research Goal

Since organizations in highly structured environments often have limited structural and cultural flexibility, reducing dissonance with the organizing vision of an emerging IT appears daunting (De Vries et al., 2016). Despite these challenges, an increasing number of such organizations – for instance, government agencies, financial service providers, or public utilities – are beginning to experiment with emerging IT, such as blockchain technology (Barbereau et al., 2023; Lüth et al., 2018; Mengelkamp et al., 2019; Rieger et al., 2019; Schlatt et al., 2022). However, these experiments often do not translate into the expected project progress, and consequently, many projects are abandoned after a proof-of-concept (PoC) or piloting phase. This motivated scholars to explore organizational innovation barriers, especially for government agencies and public utilities, when experimenting with the IT organizing vision and to envision potential mitigation strategies (Andoni et al., 2019; Fridgen et al., 2021; Glöckler et al., 2023; Rieger et al., 2019; Sedlmeir, Lautenschlager, et al., 2022). For public utilities, they focused particularly on technical challenges posed by emerging ITs (Ahl et al., 2020; Mengelkamp et al., 2019); for government agencies, they tried to find explanations for the successful or failed materialization of IT organizing visions in the investigation of human attitudes and behavior (Cinar et al., 2019; De Vries et al., 2016). These perspectives undoubtedly enrich the growing body of literature on IT innovation in highly structured environments. Yet, very few contributions have been made as to how organizations can navigate the plethora of discursive frames and value-laden buzzwords of emerging IT in an environment prone to embracing the status quo and resisting innovation even with conventional IT. Thus, this thesis sets out to answer the following main question:

How can organizations in highly structured environments facilitate innovation with emerging technologies?

We begin by exploring how organizations make sense of business problematics and focal technology in an emerging IT's organizing vision (Chapter 3), as well as how organizations navigate structural and cultural barriers during materialization of the organizing vision (Chapter 4). My analyses build on two emerging technologies: blockchain and digital identity wallets. I analyzed them by employing qualitative research. More specifically, I primarily followed two established methods in information systems (IS) – case study research (CSR) and systematic literature review (SLR) – that helped me structure the knowledge and gain deep project insights relevant to my analyses. The conclusion (Chapter 5) synthesizes the core insights of my analyses in the form of four conjectures that can offer guidance for practitioners in highly structured organizations who want to engage with emerging IT.

1.3. Thesis Structure

My cumulative thesis is structured as follows. After this introductory chapter is a brief conceptual background chapter that introduces organizing vision theory, the core theoretical frame of my dissertation (Chapter 2.1.) (E. Swanson & Ramiller, 1997). I then segue into the organizational particularities of IT innovation in highly structured environments (Chapter 2.2.) before introducing blockchain and digital identity wallets (Chapter 2.3.). Chapter 3.1. focuses on the sense-making processes related to identifying business problematics that emerging IT can address in highly structured environments. It draws on insights from four of my research papers (**RP1** Roth, Stohr, et al., 2023; **RP2** Roth, Utz, et al., 2022; **RP3** Lacity et al., 2023; **RP4** Rieger et al., 2024). After identifying the business problematics, Chapter 3.2. elaborates on the organizing visions for blockchain and digital identity wallets, and the sense-making of their technological capabilities. This chapter builds on four of my research papers (**RP5** Rieger et al., 2022; **RP6** Sedlmeir, Barbereau, et al., 2022; **RP7** Hoess et al., 2023; **RP8** Roth, Rieger, & Hoess, 2024). Both subchapters are primarily concerned with the initial sense-making stage – i.e., interpretation, in which organizations typically decide if an emerging IT is worth considering for adoption (Currie, 2004; E. Swanson & Ramiller, 1997).

Chapter 4 explores the structural and cultural innovation barriers in highly structured environments and introduces possible ways to navigate these barriers and materialize IT organizing visions. Chapter 4.1. focuses on navigating structural barriers and builds on three of my research papers (**RP9** Utz et al., 2023; **RP10** Amend et al., 2024; **RP11** Hartwich, Hoess, et al., 2023). Chapter 4.2. focuses on the navigation of cultural barriers; it is inspired by four of my research papers (**RP12** Roth, Rieger, et al., 2022; **RP13** Roth, Rieger, et al., 2023; **RP14** Hartwich et al., 2024; **RP15** Weigl et al., 2024). Chapter 5 summarizes the contribution of my thesis to research, outlines the limitations of my individual research papers and their further development, and acknowledges previous and related work. The structure of my thesis is summarized in Table 1, including the guiding research questions and papers.

Table 1. Thesis structure along research questions and research papers.

Chapter	Guiding research question	Sub-chapters	Research papers
III. Making Sense of the IT Organizing Vision	*How can organizations make sense of the business problematic and focal technology in an emerging IT's organizing vision?*	Making Sense of the Business Problematic	**RP1:** Blockchain as a Driving Force for Federalism: A Theory of Cross-Organizational Task-Technology Fit (Roth, Stohr, et al., 2023) **RP2**: Electricity Powered by Blockchain: A Review with a European Perspective (Roth, Utz, et al., 2022) **RP3**: The Quiet Corner of Web3 that Means Business (M. Lacity et al., 2023) **RP4**: Organizational Identity Management Policies (Rieger et al., 2024)
		Making Sense of the Focal Technology	**RP5**: We Need a Broader Debate on the Sustainability of Blockchain (Rieger, Roth, Sedlmeir, & Fridgen, 2022) **RP6**: Transition Pathways Towards Design Principles of Self-Sovereign Identity (Sedlmeir, Barbereau, et al., 2022) **RP7**: Managing Fashionable Organizing Visions: Evidence from the European Blockchain Services Infrastructure (Hoess et al., 2023) **RP8:** From Mutualism to Amensalism: A Case Study of Blockchain and Digital Identity Wallets (Roth, Rieger, & Hoess, 2024)
IV. Navigating the Materialization Process	*How can organizations navigate structural and cultural barriers during the implementation of emerging IT?*	Navigating Structural Barriers	**RP9**: From Ambivalence to Trust: Using Blockchain in Customer Loyalty Programs (Utz et al., 2023) **RP10**: Bringing Government into the Digital Age: Insights from Germany's Asylum Procedure (Amend et al., 2024) **RP11**: How Organizations Sustain and Navigate Between (De)centralization Equilibria: A Process Model (Hartwich, Hoess, et al., 2023)
		Navigating Cultural Barriers	**RP12**: The Role of Cultural Fit in the Adoption of Fashionable IT: A Blockchain Case (Roth, Rieger, et al., 2022) **RP13**: How IS Affect Social Justice Tensions: A Case Study of Asylum Management (Roth, Rieger, et al., 2023) **RP14**: Negotiation and Translation Between Discursive Fields: A Study on the Diffusion of Decentralized Finance (Hartwich et al., 2024) **RP15**: When Public Values and User-Centricity in e-Government Collide – A Systematic Review (Weigl et al., 2024)

2. Conceptual Background

2.1. Theoretical Frame: IT Organizing Vision

Organizing vision theory is a “macro-level cognitive institutional perspective on how IT innovations are adopted, used, and diffused within and across organizations” (Kim & Miranda, 2018). More specifically, it describes how innovation communities interpret the use and purpose of an emerging IT in an organizational context (E. Swanson, 2017). Organizing vision theory complements traditional rational-economic perspectives on innovation with emerging IT that describe the new technology as a tool whose adoption and diffusion depends solely on its inherent efficiency and effectiveness (Agarwal & Prasad, 1997; Kahneman & Tversky, 1979). While both certainly are important characteristics of a technology, IT innovation projects show that advances can be successful even when they are not inherently effective and efficient (Kim & Miranda, 2018). That is, other factors beyond the rational-economic appear to be at work, influencing how an emerging IT is embraced by the innovation community and potential adopting organizations (Inwood & Zappavigna, 2023; Miranda et al., 2015). Swanson & Ramiller (1997) position organizing vision as a theoretical lens to introduce a more holistic view of IT innovation that incorporates institutional factors, such as an organization’s culture and structure, as well as the environment in which an organization operates (Currie, 2004; Kim & Miranda, 2018). Organizing vision also enables a process-oriented analysis of the diffusion and adoption of emerging IT that often “arrives on the marketplace in an immature state, puzzling as to its benefits, future prospects, and long-term form” (Swanson & Ramiller, 1997, p. 459).

Members of the innovation community typically subject this immature state to extensive community sense-making, envisioning various uses and gauging its potential (Barad, 2007; Miranda et al., 2015; Phillips et al., 2004). The resulting interpretations can be replete with wishful and unbalanced claims that manifest in different discursive frames and value-laden buzzwords (Barrett et al., 2013; Miranda et al., 2022). These initial frames and buzzwords can help spotlight expectations or organizational needs and even create contagion for the technology (Shiller, 2020); however, they can also confuse organizations who might be eager to engage with the emerging IT (Gal et al., 2022; Wang, 2010). When frames become too distinct, the resulting frame diversity can further add to the confusion, effectively limiting the organizing vision’s coherence (Currie, 2004; Miranda et al., 2015; Wang & Ramiller, 2009). Yet, having a coherent and clear organizing vision is essential for its acceptance by adopting organizations (Kim & Miranda, 2018; Miranda et al., 2015). Coherence can be defined as the consistency in the meaning and interpretation of the vision, whereas clarity refers to “the transparency of a vision’s distinctive meanings” (Miranda et al., 2015, p. 593). That is, a vision can accommodate a certain level of flexibility and diversity, but the underlying meaning must remain consistent to avoid undermining the IT’s diffusion (Miranda et al., 2015; E. Swanson & Ramiller, 1997). Where organizing visions manage to establish coherence among the wishful and unbalanced claims surrounding the emerging IT, they gain relevance and impact, thus increasing their chances for adoption and diffusion. Should organizing visions not manage to establish coherence, the emerging IT becomes irrelevant (Miranda et al., 2015, 2022; E. Swanson & Ramiller, 1997).

Enactment fields – i.e., organizations that bring the discourse surrounding an emerging IT "into reality through action" (Suddaby & Foster, 2017, p. 28) – are key in tackling uncertainties and supporting the sense-making process of organizing visions (Miranda et al., 2022). They include all organizations, both private and public, that not only discursively engage with the emerging IT, but actively aim to materialize the organizing vision. Orlikowski & Scott (2014) describe this material enactment as a vital step toward better understanding which of the discursive frames in the IT organizing vision should be deemed true (Hardy & Maguire, 2016; Miranda et al., 2015). As a "focal lens [for] how organizational forms, structural components, and rules become institutionalized" (Currie, 2014, p. 240), organizing visions support this enactment through three major functions of IT innovation: interpretation, legitimation, and mobilization (Gorgeon & Swanson, 2011; E. Swanson & Ramiller, 1997). Interpretation is required to cut through the thicket of wishful and unbalanced claims and make sense of the emerging IT's capabilities. It allows for a first assessment of whether an emerging IT is worth considering for adoption (Davidson et al., 2015; B. E. Swanson & Ramiller, 2004). Legitimation, in turn, aims to explain why an organization should pursue the technology. It primarily focuses on identifying resonance between business needs and the emerging IT. This process allows for the abstraction of ideas and technical details to increase understanding and align the IT with the organizational culture and structures (Davidson et al., 2015; Parameswaran et al., 2023). Lastly, mobilization is concerned with inspiring a broader interest and creating a need for complementary products and services (Currie, 2004; E. Swanson & Ramiller, 1997).

The cultural meanings attributed to the emerging IT in the organizing vision can expedite especially the legitimation and mobilization phases, but they can also encumber the overall materialization and institutionalization process if they are too disparate from the organizational context (Shiller, 2020; Swanson & Ramiller, 2004; Berente et al., 2011). Thus, enactment fields are encouraged to engage in a process of organizational sense-making – specifically, cultural sense-making – at each of the three major IT innovation steps (Su, 2015; E. Swanson & Ramiller, 1997). This sense-making pays particular attention to cultural elements in the appropriation of the innovation community's IT organizing vision to the specific organizational context (Berente et al., 2011). The goal is to achieve resonance with the organizational culture, which appears to be a powerful linchpin for the successful adoption of the emerging IT (Alavi et al., 2005; Canato et al., 2013), especially in organizational contexts characterized as culturally-laden that are replete with ingrained beliefs, values, and behavioral norms. In such organizations, the establishment of cultural resonance can be the difference between successful and unsuccessful adoption (Alavi et al., 2005; Kappos & Rivard, 2008; Koch et al., 2013; Leidner & Kayworth, 2006).

2.2. Innovation Barriers in Highly Structured Environments

Highly structured environments typically come with structural innovation barriers (Cinar et al., 2019, 2021). These barriers trickle down from laws and policies that develop over decades and institutionalize organizational roles and responsibilities, providing a detailed script for the delivery of services (Meijer, 2015; Pahlka, 2023). Since highly structured environments are often organized hierarchically, the complexity manifests at all levels of organizing, creating a strict protocol of approval and oversight (Goh & Arenas, 2020; Pahlka, 2023) and limited flexibility at lower levels of organizing (Bozeman & Bretschneider, 1986; Heintze & Bretschneider, 2000). This protocol also informs the design of IT systems that have organically grown into a multi-layered, highly intertwined technical enigma, which is difficult to maintain and update (Benbunan-Fich et al., 2020; Iannacci, 2010). Innovating these systems typically involves adding new processes and systems to existing ones. This, of course, results in more complexity rather than real innovation (Benbunan-Fich et al., 2020; Caudle et al., 1991). The mounting digital debt that results from this incremental "grafting" is difficult to reduce and can be a root cause for failure of more comprehensive IT innovation projects (Pahlka, 2023).

In addition to structural barriers, organizations in highly structured environments are typically bound by a rigid set of laws, regulations, and organizational polices that institutionalize specific organizational values (McLaughlin & Sherouse, 2019). Being required to constantly monitor compliance with laws and regulations often fosters a culture of bureaucratic stewardship that is aimed at continuity rather than innovation (Goh & Arenas, 2020; Scott et al., 2016). Once such a culture is established, its underlying "pattern or system of beliefs, values, and behavioral norms […] come to be taken for granted as basic assumptions and eventually drop out of awareness" (Schein, 2017, p. 21), creating a cultural innovation barrier (de Vries et al., 2018). Where in other environments organizational culture is often an important invisible driver in developing, adopting, and using emerging IT (Alavi et al., 2005; Koch et al., 2013; Leidner & Kayworth, 2006), it tends to be a problem amid rigid structure. When organizational values conflict with those imbued in the emerging technology, organizational culture can readily cripple innovation (Canato et al., 2013; Leidner & Kayworth, 2006; Rinta-Kahila et al., 2023).

Public administration and the energy industry are examples of highly structured environments that are particularly vulnerable to structural and cultural innovation barriers – primarily due to their high level of regulation (Andoni et al., 2019; Goh & Arenas, 2020). Indicative of this vulnerability is a 2018 McKinsey study about innovation in public administration where, despite large IT investments, 80% of IT projects aimed at improving the delivery of public services failed to meet expectations (Allas et al., 2018). From a purely technical perspective, many emerging technologies would be well suited to achieve positive impacts. Yet, attempts at implementing them often do not progress beyond pilot projects (Carson et al., 2018; Thacher & Rein, 2004). Goh and Arenas (2020) provide a compelling overview of the structural and cultural barriers that feed these failures. Many of the challenges of public-sector innovation – such as system complexity (Avgerou & Bonina, 2020; Cordella & Willcocks, 2012; Wibbels, 2006), cooperation in a protected environment (Dawson et al., 2016; Deringer & Molnar, 1983) and organizational cultural values (Leidner & Kayworth, 2006; Seltsikas & O'Keefe, 2010) – are a direct result of federal organizing structures that, in turn, have their origin in shared federal values (Carter & Bélanger, 2005; Hughes et al., 2019; Scott et al., 2016).

These federal values are also a major barrier in the way of e-government innovation. With the advent of more user-centric technologies, such as digital identity wallets (Schlatt et al., 2022; Sedlmeir, Smethurst, et al., 2021), public administrations have embraced user centricity as a key concept in their digital transformation efforts (Dwivedi et al., 2011; Rudkin et al., 2019). However, treating citizens as users and prioritizing their needs and expectations can conflict with the strict protocols of public-service delivery (Alzahrani et al., 2017; Rana et al., 2012; Weigl et al., 2024). In addition to this structural barrier, the user-centric values introduced by the focal IT's organizing vision can conflict with established public values. Resulting IT-culture conflicts require careful management to allow for the materialization and adoption of the underlying technology (Leidner & Kayworth, 2006; van der Wal & van Hout, 2009). Weigl, Amard, et al. (2022), for instance, report that principles of user centricity are strongly aligned with values such as efficiency, innovation, transparency, or accountability to the public. These values reflect the general pursuit of legitimacy, reputation, and a democratic ethos in public administration; however, they introduce economic rationality, which is not typically at the core of public organizing (Mignerat & Rivard, 2015; Wiredu, 2012).

The energy industry faces similar cultural and structural barriers. Like public administration, it is governed by well-defined policies and regulations. These aim to ensure reliable energy supply – i.e., "Daseinsvorsorge" (services of general interest) – by allocating clear roles and responsibilities to all actors involved and delineating processes compliant with public and constitutional law (Ahl et al., 2020; Andoni et al., 2019; Bohne, 2011). At the same time, the energy industry follows a corporatist model of market coordination that allows for the definition of its own policies and regulations rather than being guided by industry associations and labor unions (Dyson, 1992). While this implies a certain degree of freedom, most energy utilities are subject to general directives by responsible ministries and state laws (Bohne, 2011; Theobald, 2010). The combination of different regulatory bodies with corporatist market principles creates an intricate patchwork of regulations and processes that needs to be mapped with IT. The resulting high level of specialization and evolutive growth of the IT system constrains more foundational IT innovation (Huenteler et al., 2016). That is, all IT innovation that targets actor roles or interferes with the carefully negotiated responsibilities in the delivery of energy will face insurmountable barriers to organizational innovation (Andoni et al., 2019; Diestelmeier, 2019).

2.3. Focal Technologies: Blockchain Technology and Digital Identity Wallets

The advent of blockchain technology and digital-wallet apps provides a very fruitful context for exploring these angles and studying organizational sense-making processes of emerging IT in highly structured environments. Blockchain in recent years has become known as a veritable hype technology, and its discourse has been defined by a variety of discursive frames and value-laden buzzwords (M. C. Lacity, 2022; Lichti & Tumasjan, 2023; Miranda et al., 2022). Digital identity wallets are a more recent development that has profited substantially from the initial hype surrounding blockchain technology (Sedlmeir, Smethurst, et al., 2021; Weigl et al., 2023).

2.3.1. Blockchain Technology

Blockchains are distributed databases that record transactional data in a chronological order on several blockchain nodes in a blockchain network (Ellinger et al., 2024; Halaburda et al., 2023). The basic ordering element are referred to as blocks that are connected with cryptographic hash functions – hence the name blockchain (Beck et al., 2018; Chong et al., 2019; Ziolkowski et al., 2020). To select the next block, blockchain networks employ consensus mechanisms that tie the right to propose the next block to a scare resource (Gallersdörfer et al., 2020; Sedlmeir et al., 2020). In proof-of-work blockchains, for instance, this scarce resource is the amount of energy required to solve a computational puzzle. In proof-of-stake blockchains, the scarce resource is a certain cryptocurrency balance that is put at stake to increase the odds of being selected as the next block proposer (Sedlmeir et al., 2020). Most blockchains also support the deployment of deterministic programming logic – or smart contracts – that make blockchain interesting for a range of business processes with clearly defined business rules (Halaburda et al., 2023). Blockchains are additionally characterized by their read-and-write permissions. While public blockchains can be freely accessed, private ones are only accessible to a set of preregistered users. Many private blockchains also limit write (and validation) rights to a subset of participants, making them permissioned blockchains. Permissionless blockchains do not have such limits (Beck et al., 2018; Rossi et al., 2019).

Blockchains originated in the cryptocurrency space, where they were envisioned as distributed ledger systems for tracking cryptocurrency transactions (Bakos & Halaburda, 2022; M. C. Lacity, 2022; Miranda et al., 2022; Rossi et al., 2019). They remained a niche technology for several years until the Ethereum blockchain went live in 2015. Ethereum offered the capability to process cryptocurrency transactions, as well as deploy smart contracts in a Turing-complete programming language. This enabled the automated execution of predefined logic and broadened the scope of blockchain applications to, for instance, supply chain management (Sarker et al., 2021). Over the next year, various industries saw a veritable blockchain hype (M. C. Lacity, 2022). The hype soon faded; however, blockchain enthusiasm still lingers in certain communities, to which Gartner offers testament with a special hype cycle for blockchain use cases (Leow et al., 2023).

Blockchain technology is usually associated with cultural values grounded in libertarian political ideologies (M. Lacity, 2022; Lichti & Tumasjan, 2023; Miranda et al., 2022). These values are variegated and often center around values of trust, cooperation, and empowerment. Specifically, blockchain has been marketed as being able to establish trust in contexts where parties do not trust each other (M. C. Lacity, 2022; Utz et al., 2023). This trustless trust – that is, trust in algorithms and not the cooperating party – has been a main driver of blockchain's contagion (Inwood & Zappavigna, 2023; Shiller, 2020). Moreover, blockchain systems are often described as enabling collaborative processes or as agents of disintermediation and empowerment (Beck et al., 2018; M. C. Lacity, 2022).

2.3.2. Digital Identity Wallets

Digital identity wallets represent a new paradigm for managing digital identity data (Glöckler et al., 2023; M. Lacity & Carmel, 2022; Sedlmeir, Smethurst, et al., 2021). These wallets allow users to collect digital attestations of identity attributes from different trustworthy issuers, such as governments and certified companies, and selectively disclose these attributes when required. Figure 1 provides an overview of the disclosure process.

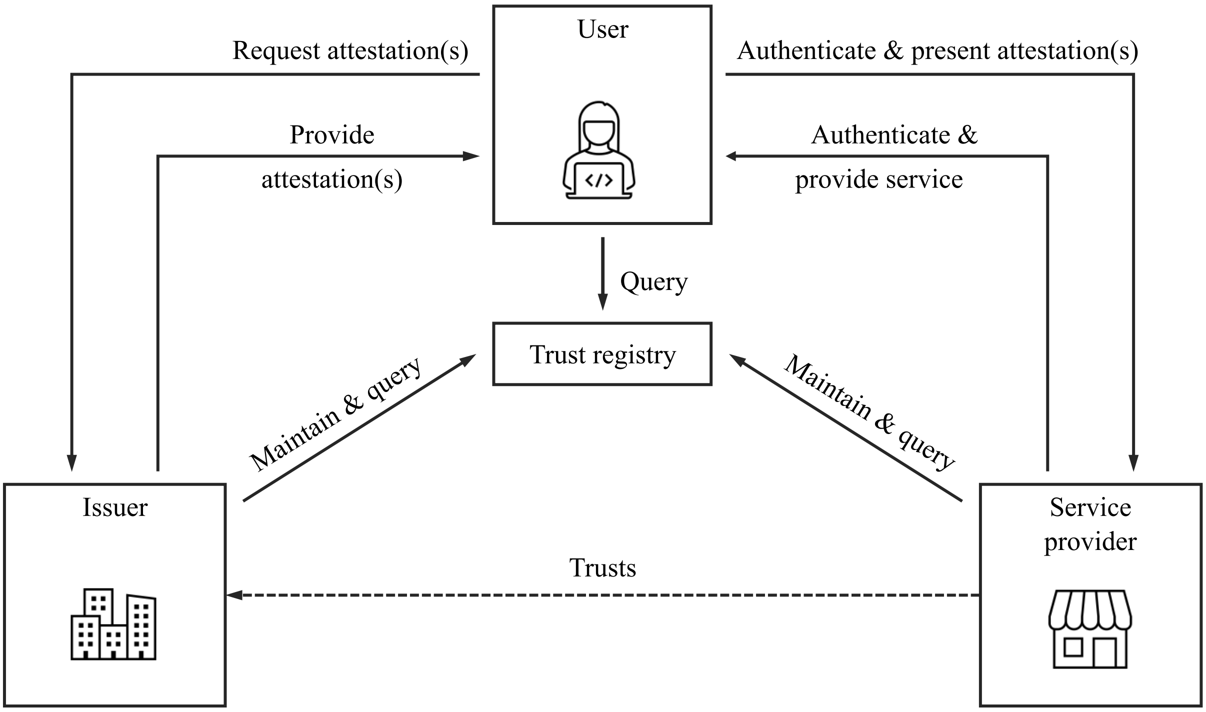


Figure 1. Roles and interactions in the wallet-based model.
(Kudra et al., 2024)

When a user wants to access a digital service, the service provider will send a so-called proof request that specifies a list of required identity attributes and a list of permissible attestations that these attributes can come with. The user's wallet will then respond by first checking the identity and access rights of the service provider, before creating the requested list of identity attributes, such as the user's name, from the required attestations. Once the user has confirmed this list, the wallet will forward it to the service provider, including cryptographic proofs of these attributes. The digital service provider, in turn, uses these proofs to validate the attributes' correctness, authenticity, and validity using public "trust" and "revocation" registries (Glöckler et al., 2023; Kudra et al., 2024; Sedlmeir, Smethurst, et al., 2021).

The idea for digital identity wallets originated in a libertarian online community with strong overlaps to the blockchain community (Narayanan, 2013). This community became concerned with weaknesses of the fragmented and federated identity-management models. In the fragmented model, users must keep a separate username-password combination for each digital service they use. Managing these combinations can be frustrating – especially when digital-service providers impose complex password rules to increase security (Kudra et al., 2024; Rieger et al., 2024). The fragmented accounts model can also be very costly for digital-service providers when they need to clearly identify new users either in-person or with video processes (M. Lacity & Carmel, 2022; Sedlmeir, Smethurst, et al., 2021). The federated model offers some remedies for these problems. Instead of maintaining hundreds of username-password combinations, users only need to manage those for their single sign-on (SSO) services. These services – offered by companies like Alphabet, Apple, or Meta – allow users to log into any digital service that supports sign-in with [this SSO service]. However, SSO services tie users to their providers, who may build detailed user profiles across various digital services – e.g., for targeted advertisement (Yeoh et al., 2023). These profiles are also attractive for hackers and state surveillance. Moreover, there have been several cases where SSO providers blocked their users, keeping them from accessing all digital services that were connected to their SSO account (Kudra et al., 2024).

Increasing awareness regarding the limits of both the fragmented and SSO models inspired libertarian-leaning parts of the digital identity community to seek an alternative model that puts the user center stage, ultimately leading to the wallet-based model. The resulting organizing vision was often referred to as decentralized or self-sovereign identity (SSI) (Kudra et al., 2024; M. Lacity & Carmel, 2022; Sedlmeir, Smethurst, et al., 2021). Given the strong overlap between this community and the blockchain group, the first digital identity wallets were implemented with blockchain-based trust and revocation registries (Sedlmeir, Smethurst, et al., 2021). These early-stage implementations soon inspired various identity-innovation projects across Europe, such as the European Blockchain Partnership (EBP) and its European Blockchain Service Infrastructure (EBSI) project (European Comission, 2024). However, as time progressed, it became apparent that blockchain-based registries were not essential for digital identity wallets (Kudra et al., 2024). On the contrary, many stakeholders in the digital identity community actively rejected the use of blockchain (Kudra et al., 2024; Sedlmeir, Smethurst, et al., 2021). This souring relationship between the two sibling technologies was notarized in mid-2021, when the European Commission proposed an updated version of its electronic identification, authentication and trust services (eIDAS) regulation. The revision enshrined the wallet-based model as the way toward a unified European approach for identity management, but it remained defensive on using blockchain as a desirable backbone for its digital identity wallets (European Comission, 2024).

3. Making Sense of the IT Organizing Vision

In the beginning of the sense-making process, the discursive frames inherent to the IT organizing vision tend to be diverse since they cater to the preferences and needs of different stakeholders (Hsu & Lim, 2014). However, for the IT organizing vision to be coherent and compelling, frame diversity needs to be reduced and the meaning of frames aligned to avoid contradiction and ambiguity (Barrett et al., 2013; E. Swanson & Ramiller, 1997). This is typically done by transferring the IT organizing vision from the discursive to the material (Miranda et al., 2022; Orlikowski & Scott, 2014; Wang & Ramiller, 2009). "Host" organizations willing to experiment with the emerging IT erect discourse walls (Wang & Ramiller, 2009) through the enactment of specific discursive frames from the IT organizing vision via institutional mechanisms (Miranda et al., 2022; Orlikowski & Scott, 2014). The initial institutional mechanism, referred to as *interpretation* (E. Swanson & Ramiller, 1997) will be examined in the following pages for both blockchain technology and digital identity wallets. Where possible, the thesis uses examples from government projects or industry collaborations to provide more depth to the sense-making processes.

3.1. Making Sense of the Business Problematic

IT organizing visions are usually shaped by and for organizations with a pronounced innovation culture (Miranda et al., 2015, 2022). These types of enacting organizations tend to have fewer structural and cultural innovation barriers than those in highly structured environments, which makes both "selling" the IT organizing vision to these organizations and materializing specific discursive frames easier (Goh & Arenas, 2020; Hueske & Guenther, 2015). However, with the emergence of blockchain technology and digital identity wallets, also highly structured organizations felt compelled to materially engage in the sense-making process (M. Lacity et al., 2023; Roth, Stohr, et al., 2023; Utz et al., 2023).

3.1.1. Surfacing a business problematic for public administration from the blockchain OV

One of the surprise enacting organizations I was able to study for this thesis was the Federal Office for Migration and Refugees in Germany. The Federal Office is responsible for Germany's asylum procedure, which is federally organized and requires close cooperation between various agencies for its completion (Roth, Stohr, et al., 2023). More specifically, the office manages and issues decisions on asylum applications, while state-level migration agencies are responsible for the initial registration of asylum seekers, along with their eventual integration or repatriation. Medical care is provided by health authorities, translation-service providers help with documents and the interview, and law enforcement agencies conduct background checks and support repatriations (Amend et al., 2024; Rieger et al., 2019; Roth, Stohr, et al., 2023). An exemplary overview of the first part of the procedure is provided in Figure 2.

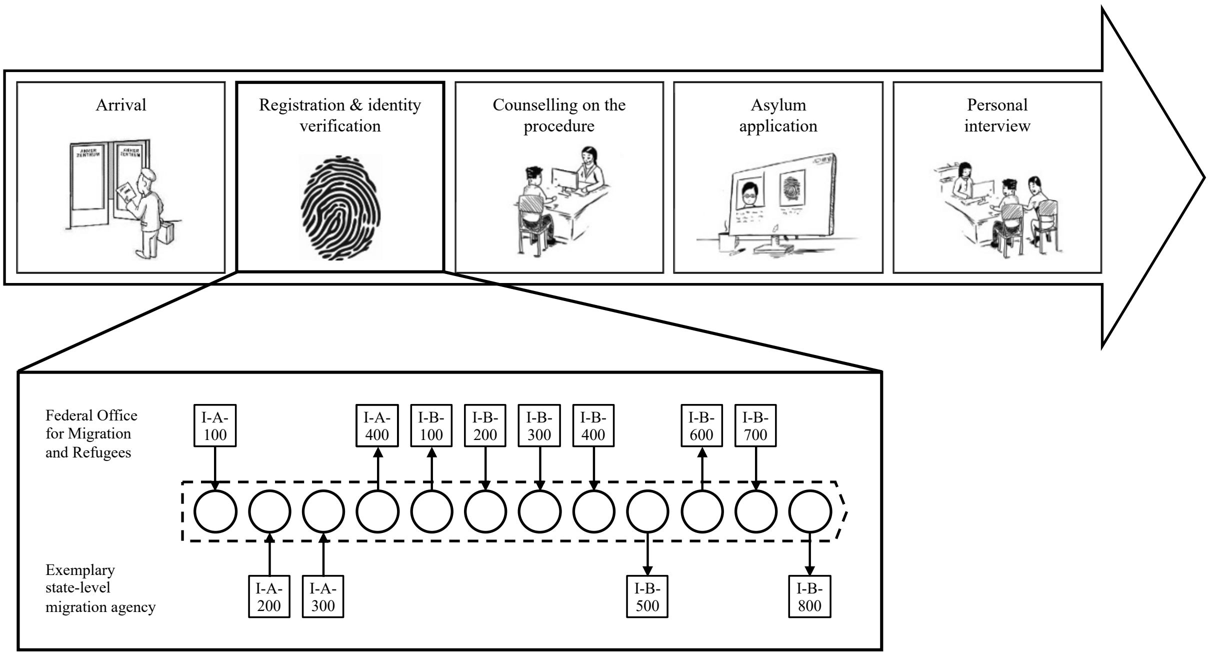

Arrival
Registration & identity verification
Counselling on the procedure
Asylum application
Personal interview
Federal Office for Migration and Refugees
I-A-100
I-A-400
I-B-100
I-B-200
I-B-300
I-B-400
I-B-600
I-B-700
Exemplary state-level migration agency
I-A-200
I-A-300
I-B-500
I-B-800

Figure 2. Drill-down Into the First Part of the Asylum Procedure.
(Based on Amend et al., 2024)

All involved organizations and providers are subject to a tight legal framework that defines the distribution of responsibilities and provides clear rules for every high-level step (Goh & Arenas, 2020; Roth, Stohr, et al., 2023). Moreover, this framework imposes four basic principles of federalism: *empowerment, separation of competencies, cooperation and coordination, and organizational flexibility* (Roth, Stohr, et al., 2023). *Empowerment* means that agencies across the various levels of organizing can develop their own low-level processes to complete their tasks (Egeberg, 2001; Grant & Tan, 2013; Roth, Stohr, et al., 2023). Agencies also do not need to engage with other agencies' tasks since the *separation of competencies* confines their responsibilities to their specific function (Conlan, 2006; Roth, Stohr, et al., 2023). As a consequence, *cooperation and coordination* occur exclusively where the involved agencies either deem an exchange of information useful or where they are legally required to cooperate (Amend et al., 2024; Rieger et al., 2019; Roth, Stohr, et al., 2023). Since the level of cooperation may need to be adapted over time, *organizational flexibility* is essential (Conlan, 2006; Roth, Stohr, et al., 2023).

While these four principles of federalism appear favorable for each individual agency in the asylum procedure, the resulting complex and multilayered process landscapes and IT systems do not only encumber the exchange of procedural information across agency and system boundaries, but also present a veritable IT innovation barrier (Amend et al., 2021). More specifically, the Federal Office used to exchange procedural information via Excel spreadsheets, which takes both a lot of time and is error prone, despite many technological alternatives (Amend et al., 2024; Roth, Stohr, et al., 2023).

With a thorough understanding of its structural limitations and a clear business goal in mind, the Federal Office launched the FLORA project to eliminate Excel-based information sharing. It began to engage with many different technologies but became hooked by blockchain's IT organizing vision in early 2018 (Amend et al., 2021, 2024). During the initial sense-making phase, the office saw substantial overlap between federal organizing and the IT organizing vision (see Figure 3). Moreover, it believed that blockchain could address many of the problems in the asylum procedure (Amend et al., 2024; Roth, Rieger, Utz, et al., 2024; Roth, Stohr, et al., 2023).

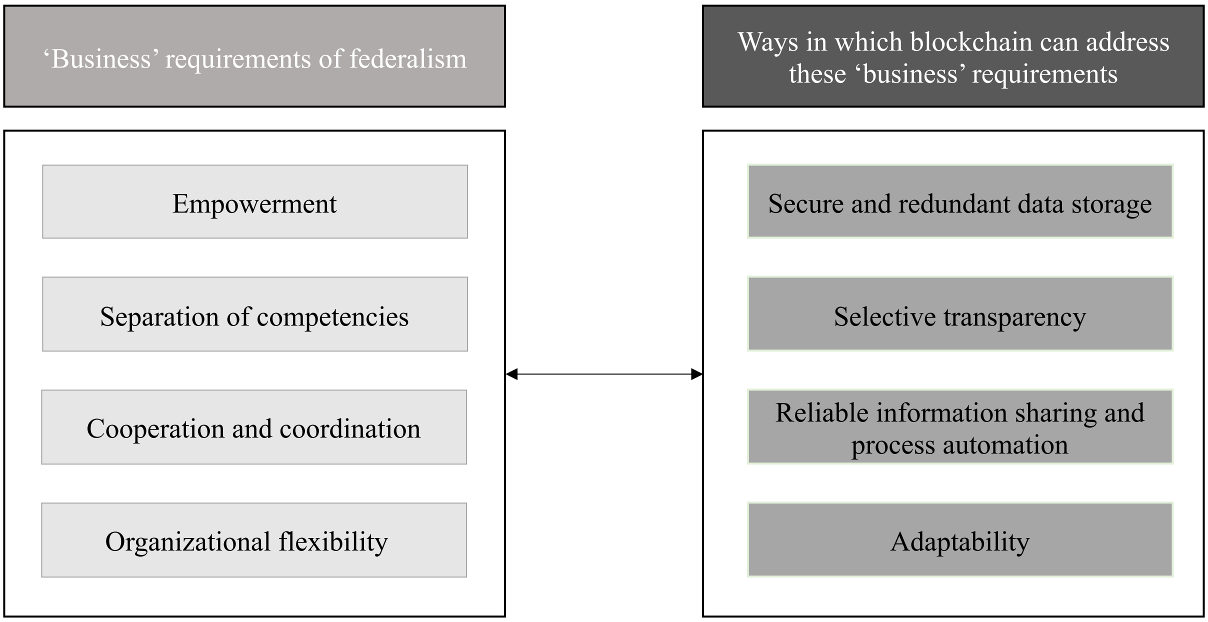

'Business' requirements of federalism
Empowerment
Separation of competencies
Cooperation and coordination
Organizational flexibility
Ways in which blockchain can address these 'business' requirements
Secure and redundant data storage
Selective transparency
Reliable information sharing and process automation
Adaptability

Figure 3. Result of the Federal Office's initial sense-making of the business problematic. (Based on Roth, Stohr, et al., 2023)

That is, the Federal Office was convinced that blockchain's *secure and distributed data storage* can help establish a common source of truth for all agencies involved – while retaining their autonomy. This would *empower* the respective agencies without negatively affecting the asylum procedure's quality (Amend et al., 2024; Roth, Rieger, Utz, et al., 2024). Blockchain may also conveniently accommodate the data-access requirements imposed by the procedure's legal framework in the form of *selective transparency* and maintain the *separation of competencies*. More specifically, a private blockchain based on the Hyperledger Fabric framework would allow the creation of "private data collections" that can be used to share procedural updates only with those agencies involved in handling a particular step in the asylum procedure. When responsibilities shift, procedural data could easily be copied to a new private data collection with a new set of responsible agencies (Rieger et al., 2019; Roth, Stohr, et al., 2023). In this sense, blockchain could facilitate *reliable information sharing* and a certain degree of *process automation.* Based on the capabilities of blockchain technology, the Federal Office envisioned status messages written on the blockchain to provide reliable updates on asylum applications for every agency involved in the asylum procedure. Since these messages would not contain any identifiable information for those without the relevant legal basis to access it, a common source of truth in keeping with the general data protection regulation (GDPR) could be maintained, which enables more targeted *cooperation and coordination* (Rieger et al., 2019; Roth, Stohr et al., 2023). However, this requires *adaptability* of the system when different authorities at different levels of organizing and cross-organization work together (Roth, Stohr, et al., 2023; Ziolkowski et al., 2020). The Federal Office also perceived blockchain to be quite versatile and was confident the technology could provide the desired *organizational flexibility* to meet local needs and changing requirements (Andersen & Bogusz, 2019; Roth, Stohr, et al., 2023).

This initial sense-making of the blockchain organizing vision led the Federal Office to conclude that blockchain would be a suitable technology. The identified business problematic in the organizing vision appeared to match the Federal Office's organizational needs and reflected its "Federal DNA." Perceived alignment with the four principles of federalism also created a sense of task-technology fit (Roth, Stohr, et al., 2023), i.e., "the degree to which a technology assists […] in performing [a] portfolio of tasks (Goodhue & Thompson, 1995). This considerably supported deeper engagement with the blockchain organizing vision in the Federal Office but also other projects (Liang et al., 2021).

3.1.2. Surfacing a business problematic for energy utilities from the blockchain OV

Where sense-making of a blockchain business problematic appeared comparatively easy in the Federal Office, energy utilities had a much harder time finding resonant elements with the blockchain organizing vision. More specifically, the business problematics they identified in the organizing vision were difficult, if not impossible, to reconcile with regulation (Ahl et al., 2020; Andoni et al., 2019; Roth, Utz, et al., 2022). Despite efforts in the European energy industry, regulatory barriers and technical immaturity led to slow progress, stagnation, or abandonment of projects (Andoni et al., 2019; Ahl et al., 2020; Roth et al., 2022). This thesis will focus on the four most commonly discussed business problematics: *peer-to-peer electricity trading*, *microgrid operation*, *e-roaming* for electric vehicles, and *machine identities* (Roth, Utz, et al., 2022) before turning to the "outlier," where an energy utility successfully used blockchain for *customer loyalty.*

Peer-to-peer (P2P) electricity trading was probably the most popular business problem for blockchain in the energy industry (Andoni et al., 2019; Roth, Utz, et al., 2022). Hooked by the discursive frames *decentralization* and *disintermediation*, different actors in European energy systems began to reconsider established roles and explore the use of blockchain to support peer-to-peer designs for retail and wholesale electricity markets based on automated transaction processing with smart contracts and blockchain-based registries (Thomas et al., 2019). From a retail perspective, P2P trading was argued to create markets that would be open to homeowners with distributed energy resources like solar panels, heat pumps, and energy storage units. From both a retail and wholesale perspective, automated transaction processing was believed to reduce transaction costs, lower market barriers, and level the playing field (Mengelkamp et al., 2018; Morstyn et al., 2018). However, these market designs proved difficult, if not impossible, to reconcile with the roles and responsibilities enacted by energy laws and regulation (Ahl et al., 2020; Andoni et al., 2019; Roth, Utz, et al., 2022). They were established to ensure a reliable energy supply, making them difficult to change or replace (Bohne, 2011; Roth, Utz, et al., 2022).

The *microgrid operation* problematic focused on the challenges associated with managing small units of the power grid that could, if necessary, be islanded. Smart contracts were promoted as ideal solutions for scheduling, balancing and settling production and consumption in these units, especially where centralized control was difficult to realize. Blockchain registries, in turn, could serve as tamper-evident proof for deviations from the schedule (Gao et al., 2020; Roth, Utz, et al., 2022). However, much like in P2P trading, the identified business problematic clashed with established and legally mandated roles. Moreover, management and transaction costs can be difficult to predict for microgrids, which makes approaches with conventional IT, where parameters are easier to predict, more attractive than with blockchain (Roth, Utz, et al., 2022).

Using blockchain to support *e-roaming* emerged as a business problematic when sales of electric vehicles increased dramatically, while access to charging points remained limited due to competing charging point operators and networks (Hoess et al., 2022; Zhang et al., 2018). Thus, enabling the exchange of driver, vehicle, and charging information across network boundaries was deemed essential. Blockchain appeared to be a suitable technology, since it could securely and transparently exchange the required data and facilitate transactions with third-party charging point operators (Hoess et al., 2022; Roth, Utz, et al., 2022). Moreover, blockchain could function as a registry for identity-related credentials so that drivers could easily identify themselves and their vehicles. Smart contracts could then be used to automatically validate the presented identity-related documents and issue invoices after the charging process (Hoess et al., 2022). Payment, however, was an unwelcome aspect due to the skepticism about cryptocurrencies. Although appealing, the *e-roaming* business came apart when it came to pass that new governance structures between charging networks would have to be negotiated to allocate responsibilities and protect customers (Roth, Utz, et al., 2022).

To dig deeper into blockchain-based identification, the German Energy Agency (dena) addressed a business problematic focused on *machine identities* (Djamali et al., 2021; Roth, Utz, et al., 2022). The idea was to equip power generation and storage units with machine-verifiable, digital credentials that would allow for their identification and authentication – and ultimately participation – in automated electricity markets (Anania et al., 2021; Roth, Utz, et al., 2022). As with e-roaming , these digital credentials would be anchored on a blockchain, allowing verification of accredited issuers, credential verification schemas, and credential validity (Rieger et al., 2024; Sedlmeir, Smethurst, et al., 2021). While *machine identities* can make for a compelling business problematic, limited technical maturity and technological know-how currently constrain their implementation. Moreover, compliance with regulation, such as the GDPR, would need to be established to prevent, for instance, the identification of a natural person based on a credential anchored on the blockchain (Roth, Utz, et al., 2022).

By the time the Stadtwerke Leipzig, a German energy utility, started looking into blockchain, many of its customers were dissatisfied with their green-electricity tariffs. These GET customers especially misunderstood the purpose of green-electricity certificates, which guarantee that their aggregated amount of electricity consumption was generated from sustainable sources. Instead, they feared becoming a victim of greenwashing (false "green" flagging) and felt betrayed by the Stadtwerke's insufficient provision of information (Utz et al., 2023). To appease customers and address their concerns, the Stadtwerke Leipzig considered ways to improve communication with its customers on the provenance of their electricity and green-electricity certificates (Roth, Rieger et al., 2022; Roth, Rieger, Utz et al., 2024). Their idea was to use blockchain for *customer loyalty*. More specifically, they aimed to use blockchain so that customers can reliably trace their energy consumption generated from sustainable sources. The Stadtwerke also enabled the automated setting of green-energy thresholds and consumption control via smart contracts. When customers behaved sustainably, they could gain and redeem additional loyalty tokens via the blockchain.

3.1.3. Surfacing a business problematic from the digital identity wallets OV

Making sense of a pertinent business problem for digital identity wallets may often be easier than with blockchain technology since its IT organizing vision is already more coherent (Miranda et al., 2022; E. Swanson & Ramiller, 1997). However, this level of coherence may also have led to a smaller business problematic (Kudra et al., 2024; Rieger et al., 2024). Digital identity wallets promise substantial cost savings for digital-service providers that require a high level of identity assurance for their users. Today, this level of assurance usually requires in-person or video identification during the enrollment process and complicated, multifactor authentication later in the process. Digital identity wallets and verifiable identity attributes promise to eliminate these costly processes. Moreover, they ensure high-quality identity data for organizational processes (Sedlmeir et al., 2021; Schlatt et al., 2022). However, there are few immediate business benefits for digital-service providers who are not subject to tight requirements for user identification and authentication, or who do not need high-quality identity data. The same holds true for issuers of variable identity attributes; and for users, digital wallets do not offer a breakthrough in convenience over single-sign-on services (Kudra et al., 2024; Rieger et al., 2024).

This rather one-sided distribution of benefits makes it difficult to approach digital identity wallets from a business problematic perspective. Sense-making has thus rather occurred on a policy level (Lacity et al., 2022). For the European Commission and many European member state governments, digital identity wallets are interesting in the sense that they resonate strongly with the digital sovereignty policy of the von der Leyen presidency (European Parliament, 2024). As such, sense-making about digital wallets is often more about privacy and user control rather than a business problem in the narrower sense (Lacity et al., 2022; Rieger et al., 2024).

However, this focus on *policy sense-making* creates a tricky chicken-or-egg problem (M. Lacity et al., 2023; Schlatt et al., 2022). Without a clear business benefit, few digital-service providers will want to adopt user identification and authentication with digital identity wallets. Users also will not want to use digital identity wallets when they support only a small set of digital services (Rieger, Roth, Sedlmeir, Weigl, et al., 2022). This limited demand will make it difficult to bring mobile phone manufacturers and operating-system providers on board. Broad adoption will only be possible if digital identity wallets have access to NFC chips for offline interactions and secure hardware components for services that require a high level of assurance (Kudra et al., 2024).

3.1.4. Summary

Regardless of how appealing and clear the pertinent business problem is in the IT organizing vision, organizations in enactment fields should critically engage with it early on. Especially for organizations in highly structured environments, this sense-making is key to (1) developing an understanding for how the emerging IT can address their own organizational needs and (2) gauging the business value the IT may create. For the Federal Office, for instance, it would have been impossible to simply transfer the business problematic advocated for organizations in the private sector. For the innovation community in the European energy industry, the organizing vision was full of compelling business problematics, but it did not manage to translate these into realistic use cases for blockchain technology. This leads me to my first conjecture for innovation with emerging IT in highly structured environments:

Conjecture 1: *Organizations in highly structured environments are more likely to achieve successful implementation if they cultivate the ability to craft their own realistic business problematic from the discursive repertoire of the community's vision.*

3.2. Making Sense of the Core Technology

"Tech people" may be an integral part of the IT discourse community and play a role in discursively constructing IT organizing visions (Miranda et al., 2022), but those visions are usually not designed for them. Instead, IT organizing visions target innovation managers with a strong business perspective. These managers are more focused on potential business opportunities an organizing vision presents than the actual capabilities of the underlying core technology. This often one-sided design of IT organizing visions can be challenging, especially when the emerging IT is still immature and has limited capabilities (Barrett et al., 2013; E. Swanson & Ramiller, 1997). Sense-making of an IT organizing vision should thus always go beyond discursive "business" frames, as placing all bets on one technology could be error prone or have only limited capabilities despite an otherwise catchy IT organizing vision

(Möhlmannn et al., 2023). The following part of this thesis focuses on understanding the technical capabilities and limitations of blockchains and digital identity wallets.

3.2.1. Technical capabilities and limitations of blockchain technology

As blockchain had matured substantially by the time I started my dissertation, it was relatively easy to identify capabilities and limitations – e.g., related to energy consumption, privacy, and performance (Hartwich, Rieger, et al., 2023; Schellinger et al., 2022; Sedlmeir, Lautenschlager, et al., 2022). One limitation I investigated in detail is energy consumption. Blockchain's energy use became a public concern when a Nature Climate Change comment authored by Mora et al. (2018) portrayed Bitcoin's proof-of-work consensus mechanism as a global climate threat. The comment claimed that if Bitcoin were to become a global currency, the emissions created from its use would increase the global temperature by 2°C. While this claim was debunked in a number of response articles (e.g., Dittmar & Praktiknjo, 2019), the belief that blockchain had a negative impact on the environment remained (Rieger, Roth, Sedlmeir, & Fridgen, 2022; Sedlmeir et al., 2020).

As part of my thesis, I tried to add more balance and nuance to this discussion. While it is indeed true that public blockchains that employ PoW consensus mechanisms are not environmentally friendly, the same does not apply for those that use a different consensus mechanism. For instance, using a proof-of-stake (PoS) consensus mechanism can reduce the energy consumption of a PoW blockchain by a factor of 10^6 (Rieger, Roth, Sedlmeir, & Fridgen, 2022; Sedlmeir et al., 2020). This enormous energy-saving potential is possible because PoW blockchains effectively employ power as a "scarce" resource to secure the consensus and block-building process. When security can be ensured with a different scarce resource, such as the staking of a certain cryptocurrency balance in PoS blockchains or "identity" in private blockchains, energy demand can be reduced to similar levels as conventional, distributed databases (Rieger, Roth, Sedlmeir, & Fridgen, 2022; Sedlmeir et al., 2020). In fact, blockchains can even be a source of sustainability where they prevent fresh produce from going to waste through extensive product monitoring across supply chains (e.g., IBM FoodTrust) or where it reduces paper- and airmail-based information exchange (e.g., IBM and Maersk's former TradeLens) (Rieger, Roth, Sedlmeir, & Fridgen, 2022).

Another misconception I looked into as part of my analysis of the Federal Office's blockchain project is blockchain's purported incompatibility with data-privacy requirments (Roth, Stohr, et al., 2023). These requirements typically include that personal data should be rectifiable and erasable (Rieger et al., 2019). At a first glance, these two requirements may conflict with blockchain's logic of append-only data storage. They can be adressed, however, by using pseudonymization techniques. Many of the other data-privacy requirements are also relatively easy to address, provided blockchains are employed in a way that each participant can be clearly identified (Akanfe et al., 2024; Guggenmos et al., 2020; Rieger et al., 2019; Roth, Stohr, et al., 2023).

3.2.2. Technical capabilities and limitations of digital identity wallets

The technical capabilities and limitations of digital identity wallets proved more difficult to unpack, as they were significantly less mature than blockchain technology when I began to investigate them. Moreover, their organizing vision was closely intertwined with that of blockchain, which made them a very interesting phenomenon to study, but also one that required a clear understanding of both technologies (Hoess et al., 2023; Roth, Rieger, & Hoess, 2024).

I began my investigation by analyzing the origins of digital identity wallets in a "technological niche" (Geels & Schot, 2007) of the digital identity community that was focused on "ownership" or "self-sovereignty" to empower users and give them more control over their identity attributes (Roth, Rieger, & Hoess, 2024; Tobin, 2018). This niche was guided by 10 principles that became known under the moniker "self-sovereign identity" (SSI) (Allen, 2016). Despite the "recipe" these principles provided, there were initially no clear technical building blocks to realize the SSI organizing vision (Sedlmeir, Smethurst, et al., 2021). Thus, interested organizations either had to wait for the successful completion of proof-of-concept and pilot projects, or act themselves. Some, like the European Blockchain Partnership with its European Blockchain Services Infrastructure project decided to take action (Roth, Rieger, & Hoess, 2024; Sedlmeir, Barbereau, et al., 2022; Smethurst, 2023).

One firm belief that emerged during this interpretation phase was that digital identity wallets are inextricably coupled with blockchain technology (Hoess et al., 2023; Roth, Rieger, & Hoess, 2024). More specifically, the innovation community originally positioned blockchain as the only technology that could deliver the "trust" infrastructures and revocation registries required for digital identity wallets (Hoess et al., 2023; M. C. Lacity, 2022; Sedlmeir, Barbereau, et al., 2022). In the beginning, this connection was indeed mutualistic, and both technologies benefitted equally (Coccia & Watts, 2020; Roth, Rieger, & Hoess, 2024). Digital identity wallets equipped blockchain with a business problematic in the identity space focused on security and user control (Hoess et al., 2023; Rieger et al., 2024; Sedlmeir, Smethurst, et al., 2021). Digital identity wallets, in turn, profited from the contagion surrounding blockchain and the ready availability of features required for issuer and credential verification (Hoess et al., 2023; Roth, Rieger, & Hoess, 2024).

However, once the various projects started to engage with digital identity wallets more deeply, they realized that blockchain may have been a good starting point but is no essential component (Roth, Rieger, & Hoess, 2024; Sedlmeir, Barbereau, et al., 2022; Sedlmeir, Smethurst, et al., 2021). Digital credentials, for instance, do not need to be stored on a blockchain to be verifiable and to ensure their integrity. In fact, storing credentials or identifiers of holders, even in encrypted form or a hash, may be a potential privacy threat, violating basic principles of the GDPR (Hoess et al., 2023; Roth, Rieger, & Hoess, 2024). While this realization did not immediately end the relationship between blockchain and SSI, it reduced their 'coupling'. The EBP, for instance, limited the use of EBSI to providing a trustworthy registry for digital credential issuers (Hoess et al., 2023; Roth, Rieger, & Hoess, 2024). The formerly mutualistic relationship between the technologies became commensalistic—i.e., one benefitted from the relationship, while the other experienced neither positive nor negative effects, with digital identity wallets benefitting in terms of scope and resources (Roth, Rieger, & Hoess, 2024).

When the blockchain discourse soured and certain groups like the eIDAS working groups actively opposed it, the relationship between the technologies took a turn for the worse (Hoess et al., 2023). This falling out of grace became evident when the European Commission's proposal for a revision of the eIDAS regulation and its complementary reference architecture framework did not contain any technical details that would institutionalize blockchain as a backbone technology (M. Lacity et al., 2023; M. Lacity & Carmel, 2022; Rieger et al., 2024; Roth, Rieger, & Hoess, 2024). Moreover, the European Commission pushed "citizen-centric, digital identity management based on digital identity wallets" (Hoess et al., 2023, p.9) instead of SSI (European Parliament, 2024), effectively moving a "child that has outgrown its parent [blockchain]'s home" (Hoess et al., 2023, p.10). The relationship in the EBSI project increasingly moved from commensalistic to amensalistic—i.e., one is neither positively nor negatively affected, while the other experiences negative effects (Coccia & Watts, 2020; Roth, Rieger, & Hoess, 2024). Yet, the increased decoupling between the two IT organizing visions also was beneficial in that it made the organizing vision for digital identity wallets more coherent and removed some of the cultural loadings associated with blockchain (Hoess et al., 2023; Roth, Rieger, & Hoess, 2024).

Besides understanding where digital identity wallets came from and how they developed, an important aspect of this thesis was also to scope the challenges that are associated with using such wallets for identification and authentication purposes. These challenges are numerous but can be grouped into three larger buckets: technical maturity, wallet usability and ecosystem development (Kudra et al., 2024; M. Lacity et al., 2023; Rieger et al., 2024; Rieger, Roth, Sedlmeir, Weigl, et al., 2022).

Technical maturity challenges exist, especially in terms of harmonization. The list of identity credentials that could be interesting for digital identity wallets is long, but so are the standards and data models for their representation and exchange. Moreover, many of these standards and models are not designed for selective disclosure of certain identity attributes or advanced privacy-enhancing techniques, such as zero-knowledge proofs. It will thus be important to define a core set of supported standards. Moreover, users will require solutions for the loss and theft of their digital wallets and credentials, as well as wallet synchronization across multiple devices (Babel & Sedlmeir, 2023; Kudra et al., 2024).

The second "elephant in the room" is usability. Although many prospective users are already familiar with Alphabet and Apple digital payment-wallet apps and their limited identity features, many do not fully understand how digital identity wallets work (Sartor et al., 2022). This pertains particularly to their unique privacy and security features. At first glance, there is little difference between the current payment-wallet apps and digital identity wallets since the underlying cryptography is in the backend and is rarely seen (M. Lacity et al., 2023). For users to see the difference and better understand digital identity wallets, those features would need to be visualized in the frontend (Sartor et al., 2022). However, even if the features became visible and users understood how digital identity wallets work, it is unclear how their current design can account for the needs of users who do not possess the skills or hardware to use them. What we refer to as the digital divide can have serious consequences regarding the inclusiveness of digital wallets – an essential requirement for government-service provision (M. Lacity et al., 2023; Rieger, Roth, Sedlmeir, Weigl, et al., 2022; Weigl et al., 2024).

3.2.3. Summary

Knowing the capabilities of an emerging technology and what it is can be instrumental in guiding the sense-making process (Orlikowski & Scott, 2014). It helps organizations better understand which of the conceptual frames surrounding the emerging IT should be deemed true (Hardy & Maguire, 2016; Miranda et al., 2022). This is particularly relevant for highly structured organizations enacting an IT organizing vision, as they need a nuanced understanding of the emerging IT to successfully navigate the substantial structural and cultural barriers posed by their environment (Goh & Arenas, 2020; Scott et al., 2016). Without this nuanced understanding, emerging ITs risk getting stuck in "pilot purgatory" and organizations will have a hard time materializing the organizing vision (Abbatemarco et al., 2022; Stohr et al., 2024). This leads to my second conjecture for innovation with emerging IT in highly structured environments:

Conjecture 2: *Organizations in highly structured environments are more likely to achieve successful implementation if they cultivate the ability to map their own business problematic to the capabilities and limitations of the focal IT.*

4. Navigating the Materialization Process

The second part of my thesis focuses on how organizations in highly structured environments can navigate the materialization process once they have successfully developed a realistic and actionable business problematic that the focal IT could address. Materialization in these environments is often difficult since organizations need to overcome complex structural barriers (Goh & Arenas, 2020; Meijer, 2015). These barriers can encumber the translation of the discourse surrounding an emerging IT "into reality through action" (Suddaby & Foster, 2017, p. 28) and impact the selection of suitable frames (Miranda et al., 2022; Weick et al., 2005). Moreover, the organizing vision can be imbued with cultural values to increase its appeal, but these values can create additional challenges in the materialization process when they do not resonate with the organizational culture (Roth, Rieger, Utz, et al., 2024; Shiller, 2020; Su, 2015; E. Swanson & Ramiller, 1997). Thus, organizations will often benefit from cultural sense-making to obviate cultural compatibility issues (Roth, Rieger, et al., 2022; Roth, Rieger, Utz, et al., 2024; Su, 2015). Given the limited maturity of digital identity wallets until the end of my dissertation, the following two sections primarily build on insights I could collect for blockchain technology.

4.1. Navigating Structural Barriers

Structural barriers in highly structured environments usually flow from complex legal frameworks that develop iteratively over time, institutionalizing organizational roles and responsibilities, as well as hierarchical decision making and oversight (Cinar et al., 2019, 2021; Meijer, 2015; Pahlka, 2023). This legal complexity tends to trickle down into equally complex processes and IT architectures, creating multilayered, highly intertwined digital debt (Benbunan-Fich et al., 2020; Iannacci, 2010; Rinta-Kahila et al., 2023). Maintenance and update work on this debt is difficult and real innovation is often sacrificed to workarounds (Benbunan-Fich et al., 2020; Iannacci, 2010; Pahlka, 2023). Hierarchical decision-making and oversight, in turn, are often in stark contrast to the agility and flexibility requirements of IT innovation projects (Bozeman & Bretschneider, 1986; Heintze & Bretschneider, 2000; Pahlka, 2023).

4.1.1. Innovating around multi-layered, highly intertwined digital debt

The Federal Office's FLORA project is again a rich case in point for unpacking how organizations can deal with multilayered, highly intertwined digital debt. Overall, the asylum procedure is well defined through laws and regulations, leaving little room for differences in high-level roles, responsibilities, and process steps (Roth, Stohr, et al., 2023). However, the devil is often in local subprocesses. Most agencies in the asylum procedure also run their own databases and workflow management systems, and many of these systems have developed intricate complexities over the years (Amend et al., 2021, 2024). Various attempts have been made to establish common design principles and standards for data exchange; however, these systems often still have a hard time talking to each other and exchanging procedural information (Amend et al., 2021, 2024).

In its implementation of the FLORA system, the Federal Office was thus mindful of the challenges of developing an IT system that would not only connect several agencies, but several levels of government. It carefully emphasized best practices for federal IT systems, such as putting user needs first, avoiding unnecessary data processing (the "once-only" principle), security and privacy by design, and a strong focus on modularity and interoperability (Amend et al., 2021, 2024; Roth, Stohr, et al., 2023). A key decision that resulted from these principles was to avoid top-down standardization of local variants of the procedure. Instead, FLORA usually implements these variants as they are, but their team strongly encourages experience-sharing between state-level migration agencies and supports process redesign, if required. Another was to develop a software-as-a-service model that allowed state-level migration agencies to immediately use the FLORA system and schedule integration with their legacy systems in line with already planned updates to these systems (Amend et al., 2024).

Similar insights ring true for the European energy industry and the NexoEnergy project. Public utilities in Europe are governed by well-defined laws and regulations that are designed to ensure reliable energy supply. As for Germany's asylum procedure, these laws lay out clear roles, responsibilities, and high-level process steps (Ahl et al., 2020; Andoni et al., 2019; Bohne, 2011). But again, local subprocess and IT systems are often markedly different (Huenteler et al., 2016; Roth, Utz, et al., 2022), which considerably complicates IT innovation (Andoni et al., 2019; Diestelmeier, 2019).

These structural barriers haunted many of the early blockchain projects in the European energy industry (Roth, Utz, et al., 2022). Blockchain often proved difficult to connect to legacy systems that used various data models or lacked standardized APIs. The Stadtwerke Leipzig was thus concerned about building a blockchain system that required integration with the legacy systems of other utilities, even though this decision defied a core belief in the blockchain-organizing vision, which framed blockchain as a technology for cross-organizational collaboration (Roth, Rieger, et al., 2022; Roth, Rieger, Utz, et al., 2024).

4.1.2. Innovating in an environment of hierarchal decision-making and oversight

The FLORA and NexoEnergy projects are also instructive for how organizations can successfully innovate in an environment of hierarchical decision making and oversight (Hartwich, Hoess, et al., 2023). What substantially benefitted the FLORA project were experiences the Federal Office had made as part of its accelerated digital transformation during the European migrant crisis in 2015 and 2016 (Amend et al., 2024; Roth, Rieger, et al., 2023). This period of forced innovation had created the necessary structures and processes for IT innovation projects (Amend et al., 2022, 2024). But the usual agile and DevOps approaches would take the Federal Office only half of the distance.

What these approaches assumed was a clear understanding of the challenges that needed to be addressed to implement a certain information technology (Amend et al., 2024; Roth, Rieger, et al., 2023). However, almost anything about blockchain was new and many of the solutions that reference projects in industry proved difficult to translate to the FLORA project (Roth, Rieger, et al., 2022; Roth, Rieger, Utz, et al., 2024; Roth, Stohr, et al., 2023). The Federal Office tried to overcome these uncertainties by assembling an interdisciplinary team with legal, process, and technical expertise. Where skills were unavailable in-house, the Federal Office brought in outside expertise. As a team, these project members managed to find creative and cross-disciplinary ways to navigate the asylum procedure's structural barriers (Amend et al., 2024). A second crucial decision was to articulate and frame these barriers as nonfunctional requirements rather than roadblocks. For instance, the FLORA team realized the importance of demonstrating that FLORA met all requirements of the EU's General Data Protection Regulation and did not require new any new legal bases for data processing (Rieger et al., 2019). It thus did not treat the GDPR's mandatory data protection impact assessment only as a costly compliance exercise. Instead, it framed the assessment as an opportunity to minutely lay out how FLORA's architecture and data flows could be mapped to requirements of the GDRP and the existing asylum laws and regulations. This proactive attention to potential concerns about data protection, in turn, proved to be instrumental in securing buy-in from many state-level migration agencies (Amend et al., 2024; Rieger et al., 2019).

The NexoEnergy project, in turn, had a more difficult time materializing its organizing vision for blockchain technology. Prior to the project, the business department had cooperated with the IT department on projects, but their cooperation followed strict structures and processes (Roth, Rieger, Utz, et al., 2024). Yet innovation with blockchain required more flexible, agile structures and processes than many centralized structures allowed (Hartwich, Hoess, et al., 2023). Introducing these took time. Another challenge was customer empowerment (Young et al., 2024). In the past, the Stadtwerke Leipzig had focused on creating products and services that required little customer involvement and shielded them from complexity. They would have also required more decentralized decision-making structures (Hartwich, Hoess, et al., 2023). However, the NexoEnergy project demanded more customer involvement, which again meant changes to the Stadtwerke Leipzig's product and design strategies. Similar changes were required in terms of including external partners in the development process (Roth, Rieger, et al., 2022; Roth, Rieger, Utz, et al., 2024). Prior to the project, it was common practice for the business and IT departments to develop products and services in internal projects. However, the NexoEnergy project challenged this closed approach and promoted a more open, co-development model. In particular, the NexoEnergy project began to involve external researchers and developers in the product and service development process (Roth, Rieger, et al., 2022; Roth, Rieger, Utz, et al., 2024). The Stadtwerke also partnered with a local university to organize a hackathon with computer science students. While the new co-development model required more time and effort, it greatly improved the NexoEnergy system and led to the creation of Leipzig Zero, a NexoEnergy-inspired product for a more sustainable and energy-efficient lifestyle in urban neighborhoods. Over time, the co-development model was also adopted in other IT projects (Roth, Rieger, et al., 2022; Roth, Rieger, Utz, et al., 2024). Although it put the Stadtwerke Leizig in a tension field between centralization and decentralization, the benefits from early-mover advances and quick innovation outweighed the challenges (Hartwich, Hoess, et al., 2023).

4.1.3. Summary

Innovation in highly structured environments is often weighed down by structural barriers, such as multilayered, highly intertwined digital debt (Benbunan-Fich et al., 2020; Iannacci, 2010; Rinta-Kahila et al., 2023) and hierarchical decision making and oversight (Bozeman & Bretschneider, 1986; Heintze & Bretschneider, 2000; Pahlka, 2023). But the FLORA and NexoEnergy projects show that these barriers can be overcome when innovation projects with emerging IT are aware of them and take the necessary steps to develop adapted IT architectures and assemble interdisciplinary teams (Amend et al., 2024; Hartwich, Hoess, et al., 2023; Utz et al., 2023). These insights lead me to my third conjecture:

Conjecture 3: *Organizations in highly structured environments are more likely to achieve successful implementation if they cultivate the ability to establish multi-disciplinary teams who translate structural barriers into actionable, non-functional requirements.*

4.2. Navigating Cultural Barriers

Organizational culture can be defined as a "a pattern or system of beliefs, values, and behavioral norms that come to be taken for granted as basic assumptions and eventually drop out of awareness" (Schein, 2017). It is typically conceived as a hierarchical construct with different levels that range from less-material basic assumptions or beliefs to more material cultural artifacts, such as behavioral norms and practices (Canato et al., 2013; Leidner & Kayworth, 2006; Schein, 2017). To balance observability and interpretability, studies of organizational culture typically focus on local and overarching organizational values (Alavi et al., 2005; Koch et al., 2013; Leidner & Kayworth, 2006).

These organizational values are often at the core of cultural barriers that can negatively affect IT innovation (Hueske & Guenther, 2015). Thus, organizations – especially those functioning as enactment fields – are encouraged to engage in cultural sense-making to mitigate emerging dissonances between the IT organizing vision and the organization's culture – both discursively and materially (Hartwich et al., 2024; Su, 2015). This sense-making can also help organizations identify resonant elements between the emerging IT and the adopting organization (Canato et al., 2013; Hartwich et al., 2024; Maitlis & Christianson, 2014; Miranda et al., 2022).

For cultural sense-making to be effective, Miranda et al. (2022) recommend four discursive processes, of which the first three are relevant for the current context. While these have initially been proposed to explain the trajectory of the general discourse surrounding a technology (Hartwich et al., 2024), they also contribute to better understanding of the interplay between organizational values and the IT organizing vision during the materialization phase (Hartwich et al., 2024; Roth, Rieger, Utz, et al., 2024). The three processes are: (1) frame imprinting – i.e., retaining elements from the original IT organizing vision following a process of sense-giving by or sense-taking from the innovation community; (2) frame imitating – i.e., copying elements from organizations that engage with the same IT following a process of sense-taking; (3) frame retracting – i.e., discarding elements from the original and other organizations' IT organizing vision following a process of sense-breaking; and (4) frame foreshadowing – i.e., anticipating elements of the IT organizing vision from other fields.

The first process, sense-making, is concerned with the "development of plausible images" (Weick et al., 2005) that support intersubjective meaning-making of dissonant elements. It typically follows a sense-giving process, whereby new elements are introduced to the organization from outside (Gioia & Chittipeddi, 1991; Miranda et al., 2022). Sense-taking describes the involvement of trusted stakeholders to support the meaning-making process. When plausibility cannot be achieved, sense-breaking initiates the removal of dissonant elements (Huemer, 2012; Miranda et al., 2022).

The following two chapters contain an overview of the cultural sense-making processes in the FLORA project of the Federal Office and the NexoEnergy project of the Stadtwerke Leipzig (Roth, Rieger, Utz, et al., 2024). I will provide an exemplary deep dive on one discursive frame extracted from the blockchain organizing vision for each project.

4.2.1. Cultural dissonance reduction in public administration

As the FLORA project team began to engage with blockchain technology, they were confronted with a blockchain organizing vision that was replete with wishful and unbalanced claims, represented by a plethora of discursive frames and value-laden buzzwords (Hartwich et al., 2024; Roth, Rieger, Utz, et al., 2024). To focus the project, the Federal Office's IT department initiated a sense-taking process by reaching out to other countries, such as India, that had already started working on blockchain systems for public services. Moreover, they asked consultants to collect success stories from innovation communities, supply chains, and identity-management efforts that could be imitated (Roth, Rieger, et al., 2022; Roth, Rieger, Utz, et al., 2024).

During the subsequent sense-making, the Federal Office primarily tried to find resonance with discursive frames in the blockchain organizing vision, becoming hooked with the discursive frame of transparent data storage (see detailed cultural sense-making process in Table 2) (Roth, Rieger, et al., 2022; Roth, Rieger, Utz, et al., 2024). The interest in this frame was owed to a long-held concern about the lack of transparency between authorities in the asylum procedure, which, in case of errors, made it difficult to determine where things had gone wrong (Roth, Rieger, et al., 2023). This initial resonance led to frame imprinting, and the Federal Office began to develop a prototype that would trace the asylum procedure across the boundaries and IT systems of three exemplary agencies (Roth, Rieger, et al., 2022; Roth, Rieger, Utz, et al., 2024).

While transparent data storage was a strong hook, it became evident that its materialization would require additional sense-making efforts (Roth, Rieger, et al., 2022; Roth, Rieger, Utz, et al., 2024). The organizing vision presented blockchain as a radical enforcer of transparency (Amend et al., 2021, 2024; Roth, Stohr, et al., 2023). Although transparency is also an espoused public value (Weigl et al., 2024), the level of transparency is constrained by legal mandates and data-minimization requirements (Amend et al., 2024; Rieger et al., 2019). That is, it was difficult to realize such radical transparency (Roth, Rieger, et al., 2022; Roth, Rieger, Utz, et al., 2024).

This frame retraction initiated a sense-breaking process, in which the FLORA team decided to switch from the proof-of-concept's Ethereum protocol to the Hyperledger Fabric protocol to allow for more flexibility in the degree of transparency (Roth, Rieger, et al., 2022; Roth, Rieger, Utz, et al., 2024). With Hyperledger's private data collections, the FLORA system could still achieve a higher degree of transparency but in a selective way (Rieger et al., 2019). The system only enables full transparency where authorities have the legal basis to share data (Amend et al., 2021, 2024; Guggenmos et al., 2020).

That is, on a material level, the selected transparency frame has resulted in the use of a different consensus mechanism and customization of the blockchain IT system to the organizational requirements (see Table 2). On a discursive level, the redefined selective transparency became an essential sense-giving element for the promotion of FLORA (see Table 2) (Roth, Rieger, et al., 2022; Roth, Rieger, Utz, et al., 2024; Roth, Stohr, et al., 2023).

Other discursive frames extracted from the blockchain organizing vision were, for instance, “distrust mediation” and “automated validation” (Roth, Rieger, et al., 2022; Roth, Rieger, Utz, et al., 2024). Since distrust mediation did not sit well with the Federal Office, the frame was retracted. Materially, the FLORA team opted for a simple ordering rather than a consensus mechanism to emphasize the value of blockchain for transparent information sharing, even in contexts where participants trust each other (Amend et al., 2021, 2024; Weigl et al., 2024). The frame ‘automated validation’ was also almost completely retracted. The associated exaggeration of efficiency at the cost of human decision making did not align well with the organizational values of accountability and employee empowerment (Roth, Rieger, et al., 2022, 2023; Roth, Rieger, Utz, et al., 2024; Weigl et al., 2024). Thus, the system was adapted to flag deviations from the default procedure but leave the final decisions to employees (Roth, Rieger, et al., 2022; Roth, Rieger, Utz, et al., 2024).

One instance where not the IT system and use was adapted, but the organizational culture was transformed, was the “cooperation” frame. While cooperation between agencies is an important value for the German asylum procedure, it is not always fully espoused (Roth, Rieger, et al., 2022; Roth, Rieger, Utz, et al., 2024; Roth, Stohr, et al., 2023). This became apparent during the FLORA rollout, as certain branches of the Federal Office had strained relationships with their state-level partner agencies (Roth, Rieger, et al., 2022; Roth, Rieger, Utz, et al., 2024). Promoting FLORA as an engine of cooperation proved instrumental in encouraging joint reflection and mending of these relationships (Amend et al., 2024). Moreover, the positive feedback by partner authorities iteratively cemented the identification of the FLORA system with the procedure’s “federal DNA,” which had a mobilizing effect on other authorities (Roth, Rieger, et al., 2022; Roth, Rieger, Utz, et al., 2024) and was important to establish legitimacy – especially as the initial blockchain hype began to dwindle.

Table 2. Cultural sense-making of blockchain's transparency frame.

Complete resonance is indicated by a full black circle with an R, while complete dissonance is signified by a full white circle with a D. Partial resonance is shown by a half black circle.

Discursive frame in the blockchain organizing vision	**Technical changes**	**Discursive changes**	**Pivotal blockchain value(s)**	**Affected organizational value(s)**	**Level of dissonance & resonance**
Transparency: On the blockchain, all transactions can be transparently viewed by participants in the network		Specification of the discursive frame: Agencies involved in the German asylum procedure require transparency to complete their tasks.	Transparency	Transparency Lawfulness	● R ○ D
	Changes to system design: Replacing the initial Ethereum framework with the Hyperledger Fabric framework	Specification of the discursive frame: Agencies involved in the German asylum procedure are not allowed to view all data	Transparency	Transparency Lawfulness	◗ ◗
Given back to the OV – Selective transparency: On the blockchains, transactions can only be transparently viewed by participants in the network if they have a legal basis.	Changes to system design: Establishment of private data collections so that only those with a legal basis can access data	Redefinition of the discursive frame: Agencies involved in the German asylum procedure are given full transparency if they have a pertinent legal basis.	Transparency	Transparency Lawfulness	● R ○ D

4.2.2. Cultural dissonance reduction in the energy industry

Much like the Federal Office, the Stadtwerke Leipzig was initially overwhelmed by the plethora of discursive frames and value-laden buzzwords when they started the NexoEnergy project (Hartwich et al., 2024; Roth, Rieger, et al., 2022; Roth, Rieger, Utz, et al., 2024). To support the initial sense-making phase, representatives of the Stadtwerke went to trade fairs, where they actively engaged in sense-taking to learn more about blockchain technology and its discursive frames, such as *transparency* for distrust mediation, *cooperation*, and *empowerment* (Utz et al., 2023). The first frame they imprinted required primarily adaptations to the IT system and its use, since the Stadtwerke had to adhere to the same privacy and data-minimization laws as the Federal Office (Rieger et al., 2019; Roth, Rieger, et al., 2022; Roth, Rieger, Utz, et al., 2024). More specifically, the NexoEnergy team made sense of this frame by creating a blockchain system that would enable customers to set thresholds for the share of "green" electricity in the overall electricity mix that would send alerts when reached or automatically switch on larger electronic devices, such as dishwashers and washing machines (Roth, Rieger, et al., 2022; Roth, Rieger, Utz, et al., 2024; Young et al., 2024). Customers could track if the green supply coincided with their demand via an aggregated user dashboard or by direct access to their blockchain (Utz et al., 2023).

The other two frames, *cooperation* and *empowerment*, were essential for cultural transformation processes to change organizational structures and values in the Stadtwerke Leipzig (Roth, Rieger, Utz, et al., 2024; Young et al., 2024). More specifically, when the Stadtwerke Leipzig started engaging with blockchain technology, they were in the process of rethinking their organizational culture, seeking inspiration in the blockchain organizing vision (Roth, Rieger, et al., 2022; Roth, Rieger, Utz, et al., 2024). What first caught their attention and led to frame imprinting was the required cooperation at eye level between participants in a blockchain network. The Stadtwerke have always had trouble establishing sustainable information exchange and joint innovation between the departments (Roth, Rieger, et al., 2022; Roth, Rieger, Utz, et al., 2024). However, working on improving customer service revealed that envisioned changes with the introduction of NexoEnergy could only be realized if the departments worked together more closely (Utz et al., 2023; Young et al., 2024). On a material level, the sense-making of the cooperation frame manifested in a restructuration of information exchange and cooperation practices between the departments. On a discursive level, cooperation was redefined to accommodate the organizational value of agility, which, in turn, also affected the amplification of this value (Roth, Rieger, et al., 2022; Roth, Rieger, Utz, et al., 2024).

Previously, the Stadtwerke Leipzig had focused on creating products and services that required little customer involvement and shielded them from complexity (Utz et al., 2022). However, the imprinting blockchain's empowerment frame led the NexoEnergy team to rethink customer interactions (Young et al., 2024). They first tried to give test customers more agency by turning them into active stakeholders, who could sell excess electricity from their solar panels. However, this idea could not be aligned with regulatory requirements and initiated frame retraction (Utz et al., 2023). To still engage customers after the retraction of this more radical empowerment frame, the Stadtwerke decided to create a rewards program based on consumption behavior as an add-on to NexoEnergy's electricity-tracing tool during the sense-breaking phase (Roth, Rieger, et al., 2022; Roth, Rieger, Utz, et al., 2024). Following test-customer feedback on the design, the NexoEnergy team doubled down on empowerment and decided to give customers full control over their rewards (Young et al., 2024).

The Stadtwerke liked the approach of giving customers more control and a voice in the organization. Thus, they asked the NexoEnergy team to also integrate customers in workshops, where they could give direct feedback on the development of the rewards program (Roth, Rieger, Utz, et al., 2024; Utz et al., 2023; Young et al., 2024). This new and radical frame of *customer empowerment* changed the position of customers within Stadtwerke Leipzig's culture (Roth, Rieger, et al., 2022; Roth, Rieger, Utz, et al., 2024). However, empowering customers by giving them more control and responsibility also caused dissonance with the organizational value of inclusion (Young et al., 2024). As an electricity supplier, the Stadtwerke needed to consider the inability of some customers to actively participate due to, for instance, digital-literacy issues (Young et al., 2024).

To keep the ensuing sense-breaking process to a minimum, the NexoEnergy team found a solution in offering simplified aggregated services for these functions (Roth, Rieger, et al., 2022; Roth, Rieger, Utz, et al., 2024; Utz et al., 2023). They tested these functions by engaging in a process of ethical grounding and evaluation. This approach focuses on five key activities essential for determining the emancipatory impacts of IS. The critical research methods of deconstruction and reconstruction, known from discourse analysis and sense-making, helped the team evaluate whether their design choices moved NexoEnergy closer to or further from the ethically grounded state of inclusion (Young et al., 2024).

Table 3. Cultural sense-making of blockchain's empowerment frame.

Complete resonance is indicated by a full black circle with an R, while complete dissonance is signified by a full white circle with a D. Partial resonance is shown by a half black circle.

Discursive frame in the blockchain organizing vision	Cultural changes	Discursive changes	Pivotal blockchain value(s)	Affected organizational value(s)	Level of dissonance & resonance
Empowerment: Blockchain enables users to take control of their data, assents, and transactions and grants them the relevant agency through the elimination of intermediaries		Specification of the discursive frame: NexoEnergy gives users full control over their rewards and gives them a voice in the organization	Control	Control Inclusiveness	R D
	Changes to the Stadtwerke Leipzig's organizational culture: Customer empowerment, i.e., giving customers voice and control, is desirable for product and service development	Specification of the discursive frame: NexoEnergy does not only need to empower customers with high digital skills, it also needs to include those with low digital skills	Control	Control Inclusiveness	R ◗
Customer Empowerment: The blockchain-based IT system enables customers to take control of their loyalty token, while enabling inclusivity through simplified services.	Changes to system design: NexoEnergy provides inclusion by offering control via simplified services, such as aggregated user dashboards.	Redefinition of the discursive frame: NexoEnergy balances customer empowerment with inclusivity and establishes the Stadtwerke as a reliable supplier of information and electricity	Transparency	Control Inclusiveness	R R

Since empowering customers yielded great results for the design and acceptance of NexoEnergy, the Stadtwerke Leipzig came to view this blockchain-inspired frame as an integral part of their revised organizational culture (Roth, Rieger, et al., 2022; Roth, Rieger, Utz, et al., 2024). That is, on a material level, the discursive frame of empowerment has changed how the Stadtwerke Leipzig treats customers. Customers not only became an integral part of the organization, but also a source of inspiration for future innovation projects (Utz et al., 2023). On a discursive level, the empowerment frame developed into customer empowerment and was redefined to accommodate the organizational value of inclusivity (Roth, Rieger, et al., 2022; Roth, Rieger, Utz, et al., 2024; Young et al., 2024).

4.2.3. Summary

Innovation in highly structured environments is often complicated by cultural barriers. Bureaucratic stewardship culture can be difficult to navigate (Amend et al., 2024; Cinar et al., 2019; Roth, Rieger, et al., 2023). These problems are often compounded for innovation with culturally loaded emerging IT (Miranda et al., 2022; Roth, Rieger, et al., 2022). For these technologies, it is especially important to establish cultural resonance (Hartwich et al., 2024; Roth, Rieger, Utz, et al., 2024). The FLORA project achieved this resonance mainly by changing the design and use of its blockchain system, while the NexoEnergy project changed the Stadtwerke Leipzig's organizational values and practices to capitalize on desirable discursive frames in blockchain's organizing vision (Roth, Rieger, et al., 2022; Roth, Rieger, Utz, et al., 2024). Overall, this translates into two recursive pathways along which cultural barriers can be mitigated: (1) the design and use of the emerging IT can be materially adapted to match the adopting organization's culture, which offers guidance for discursive reframing of the emerging IT's organizing vision; (2) organizational values and norms can be materially amplified or transformed when cultural meanings transported by the emerging IT are desirable, thus, adapting or refining the adopting organization's culture (Roth, Rieger, et al., 2022; Roth, Rieger, Utz, et al., 2024; Young et al., 2024). This leads to my fourth conjecture:

Conjecture 4: *Organizations in highly structured environments are more likely to achieve successful implementation if they enact cultural sense-making of emerging IT through non-discursive, material changes.*

5. Conclusion

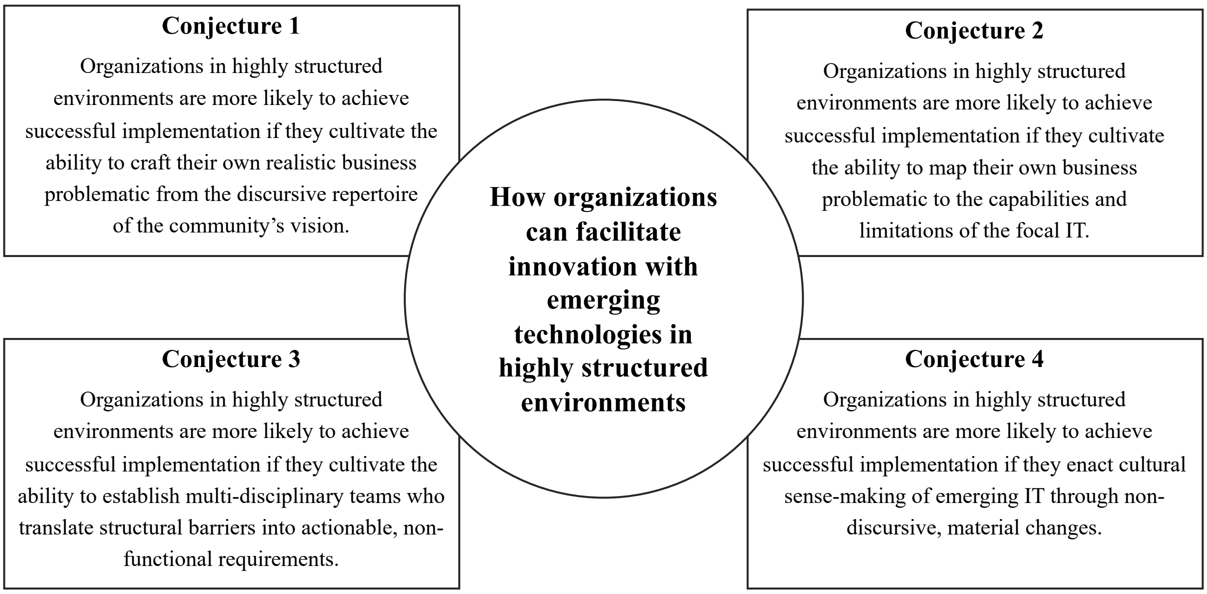
This cumulative thesis examined how organizations in highly structured environments can successfully innovate with emerging information technologies. These technologies are often difficult to appraise because the business problematics they can address are often not fully developed (Amend et al., 2024; Roth, Rieger, Utz, et al., 2024). Moreover, it is ambiguous what these technologies are capable of and what their limitations are (Miranda et al., 2022; E. Swanson & Ramiller, 1997). Organizations in highly structured environments are furthermore subject to a unique and often constraining set of structural and cultural innovation barriers that many times prove difficult to overcome (Amend et al., 2024; Hartwich et al., 2024; Hartwich, Hoess, et al., 2023) – even to innovation projects with established and well-understood information technologies (Cinar et al., 2019; Fried, 2017; Roth, Stohr, et al., 2023).

To structure my enquiry, I employed organizing vision theory as a theoretical framework that allowed me to unpack and connect the discursive sense-making and material implementation processes required for successful innovation in these environments. Throughout my investigation, I wrote 15 research papers that explored different aspects of these processes. I will next synthesize the contributions of these papers before discussing the limitations and outlook of my thesis. I will conclude with a short description of how this dissertation is embedded with the work of the FINATRAX research group and the Information Systems Department in the Sam. M. Walton College of Business at the University of Arkansas.

5.1. Contributions

I began this thesis with the observation that emerging IT is often surrounded by a thicket of stories about its transformative potential (Miranda et al., 2022; E. Swanson & Ramiller, 1997). These stories are often wishful and vague as is the IT organizing vision they create, which makes them difficult to navigate, especially for organizations in highly structured environments (Hartwich et al., 2024; Hartwich, Hoess, et al., 2023; Roth, Rieger, et al., 2022; Roth, Rieger, Utz, et al., 2024). To explore how these organizations engage with emerging IT and appropriate discursive frames from the IT organizing vision to their organizational context, I studied projects on blockchain and digital identity wallets in public administration and energy management (Roth, Rieger, et al., 2022; Roth, Rieger, Utz, et al., 2024; Roth, Stohr, et al., 2023; Roth, Utz, et al., 2022; Utz et al., 2023). The first overarching take-away from this analysis is that ‘buying into the hype’ surrounding these technologies usually does not pay off in the long term (Roth, Rieger, et al., 2022). Instead, organizations in highly structured environment are well advised to critically engage in sense-making of the IT organizing vision and identify selected discursive frames develop that can be made to fit with organizational context and requirements (see Figure 4) (Roth, Rieger, Utz, et al., 2024; Roth, Stohr, et al., 2023). The NexoEnergy case is a good example. The Stadtwerke Leipzig successfully managed to adapt the organizing vision of using blockchain for processing cryptocurrency transactions to one of tracing and trading green consumption credits (Roth, Rieger, et al., 2022; Roth, Rieger, Utz, et al., 2024; Utz et al., 2023).

However, this adapted organizing vision should not only focus on the business problematic, but also on the actual capabilities of the IT itself (Hoess et al., 2023; Rieger, Roth, Sedlmeir, & Fridgen, 2022; Roth, Rieger, & Hoess, 2024). Too often, these two seem separated. A sober look at the technology may take away some of its luster, but it will usually pave the way for applications that play on its emerging strengths (Hoess et al., 2023; Roth, Rieger, & Hoess, 2024). Germany’s use of the FLORA system is a good example. FLORA is not construed as an algorithmic mediator of trust, but as a simple application for the sharing of procedural data that leverages the strength of the Hyperledger Fabric framework (Amend et al., 2021, 2024; Roth, Rieger, et al., 2023).



Conjecture 1

Organizations in highly structured environments are more likely to achieve successful implementation if they cultivate the ability to craft their own realistic business problematic from the discursive repertoire of the community's vision.

Conjecture 2

Organizations in highly structured environments are more likely to achieve successful implementation if they cultivate the ability to map their own business problematic to the capabilities and limitations of the focal IT.

How organizations can facilitate innovation with emerging technologies in highly structured environments

Conjecture 3

Organizations in highly structured environments are more likely to achieve successful implementation if they cultivate the ability to establish multi-disciplinary teams who translate structural barriers into actionable, non-functional requirements.

Conjecture 4

Organizations in highly structured environments are more likely to achieve successful implementation if they enact cultural sense-making of emerging IT through non-discursive, material changes.

Figure 4. Contributions of this thesis.

When it's time to materialize the emerging IT, it is important to be mindful of the unique structural and cultural barriers that usually permeate highly structured environments (Hartwich et al., 2024; Hartwich, Hoess, et al., 2023; Roth, Rieger, et al., 2022; Roth, Rieger, Utz, et al., 2024). Many of these structural barriers will be rooted in complex and inflexible legal frameworks that define roles, responsibilities, and rules for these environments (Amend et al., 2024; M. Lacity et al., 2023; Roth, Stohr, et al., 2023; Roth, Utz, et al., 2022). Organizational processes and IT need to reflect these requirements, which typically translates into equally complex process landscapes and IT architectures (Hartwich, Hoess, et al., 2023; Roth, Rieger, & Hoess, 2024). Projects with emerging IT are thus well advised to be mindful of the "elephant in the room" (M. Lacity et al., 2023; Rieger et al., 2024). Such mindfulness will often be a crucial asset in user and stakeholder engagement. Again, the FLORA system is exemplary. The Federal Office was highly mindful of the legal requirements for the asylum procedure when designing and implementing the FLORA system (Rieger et al., 2019; Roth, Rieger, et al., 2023; Roth, Rieger, Utz, et al., 2024). This mindfulness was instrumental in securing the support of users and critical stakeholders within the Federal Office, as well as its partner authorities. The message of FLORA being an enabler for federalism was simple but effective (Roth, Rieger, Utz, et al., 2024; Roth, Stohr, et al., 2023).

Moreover, it pays to be mindful of potential clashes of IT and culture. IT organizing visions and their materialization often come with cultural loadings, such as beliefs on how certain business processes should be structured and how employees should work together (Hoess et al., 2023; Roth, Rieger, et al., 2022; Roth, Rieger, & Hoess, 2024; Roth, Rieger, Utz, et al., 2024). These loadings can be both boon and bane, either simplifying or complicating change management and use. It is thus important for organizations in highly structured environments to be aware of these loadings and their own organizational culture (Amend et al., 2024; Roth, Rieger, Utz, et al., 2024). Where there is resonance, consider putting emphasis (Hartwich et al., 2024; Roth, Rieger, et al., 2022). Where there is dissonance, it may be wise to change how the emerging IT is presented, implemented, and used – or to critically challenge organizational culture (Roth, Rieger, Utz, et al., 2024; Weigl et al., 2024; Young et al., 2024).

5.2. Limitations and Outlook

Like any research, my thesis is subject to limitations. Although I took great care in selecting rich and longitudinal cases for my analysis, the FLORA, NexoEnergy, and EBSI projects remain individual and, at times, highly specific cases. As such, caution is required in translating my insights to other organizations in highly structured environments or those of less structure. For instance, cultural sense-making processes may be less relevant for industries and organizations where organizational culture is less important or developed. Some of my insights may also be limited to the core technologies I investigated. Although I tried to improve generalizability and transferability by looking at two technologies—blockchain and digital identity wallets – both are considered cryptographic technologies (Sedlmeir, Barbereau, et al., 2022; Sedlmeir, Smethurst, et al., 2021). As such, the identified organizational sense-making mechanisms may look different from noncryptographic emerging IT, such as generative AI. Enacting these technologies may require other or additional discursive and material action to make sense of the IT organizing visions that form around them and materialize these technologies.

At the same time, the current limitations provide fertile ground for future work. For instance, it could prove interesting to more deeply investigate the co-development mechanisms between blockchain technology and digital-wallet apps (building on RP7: Hoess et al., 2023; and RP8: . It could be particularly interesting to unpack predictors for the development of “windows of co-development opportunity” and to mathematically formalize the unpacked mechanisms. Another opportunity for further research is to more closely study the linguistic mechanisms that appear to have played out during the negotiation and translation of the DeFi organizing vision into the organizational context (building on RP15: Hartwich et al., 2024). A third fruitful avenue may be to continue the work on decentralization equilibria in organizational and IT structures (RP 11: Hartwich, Hoess et al., 2023), extending the discussion to the literature on digital infrastructures.

5.3. Embeddedness in Previous and Related Work

For my research, I collaborated with colleagues from the FINATRAX GovTech and FinTech teams at the Interdisciplinary Centre for Security, Reliability and Trust (University of Luxembourg), colleagues from the Branch Business & Information Systems Engineering of the Fraunhofer FIT (University of Bayreuth), and colleagues from the Sam M. Walton College of Business (University of Arkansas). Naturally, many of the publications I co-authored were inspired by or built on the research of these colleagues and their predecessors.

My first forays into the socio-technical foundations of blockchain technology were guided by Schweizer et al. (2017), Fridgen et al. (2018), Fridgen et al. (2021), Hoess et al. (2021), Sedlmeir, Ross et al. (2021), Sedlmeir, Lautenschlager, et al. (2022), M. Lacity et al. (2023), and Bachmann et al. (2022). Frequent discussions with some of these authors have greatly advanced my understanding of the technology and its potential application in different industries. The respective groundwork for digital identity wallets was laid, in particular, by Sedlmeir, Smethurst, et al. (2021), Schlatt et al. (2022), Lacity & Carmel (2022), and Glöckler et al. (2023).

The core of my thesis is embedded into a vivid research stream at the FINATRAX GovTech team that is concerned with sense-making and the materialization of emerging technologies in different industries. My work builds on contributions such as Weigl, Barbereau et al. (2022), Weigl et al. (2023), and Codagnone & Weigl (2023) that explore the concepts of digital sovereignty and user centricity in e-government innovation. Smethurst (2023) was particularly inspirational regarding innovation discourse and organizational sense-making of emerging technologies. Moreover, my thesis connects to work of the FINATRAX FinTech team, such as Sedlmeir, Lautenschlager, et al. (2022), Hartwich, Ollig et al. (2023), Hartwich, Rieger et al. (2023), Álvarez et al. (2024), and Alt et al. (2024) that focus on the use of emerging technologies in different industries.

Furthermore, my work builds on the research of my colleagues in the Information Systems Department in the Sam M. Walton College of Business at the University of Arkansas. All of my papers on discursive mechanisms and IT organizing visions strongly benefitted from groundbreaking work by Prof. Dr. Amber Young and Prof. Dr. Shaila Miranda. Examples include but are not limited to Kane et al. (2021), Miranda et al. (2015), Miranda et al. (2016), Kim & Miranda (2018), and Miranda et al. (2022).

6. References

Abbatemarco, N., Gaur, A., & Meregalli, S. (2022). Stuck in Pilot Purgatory: Understanding and Addressing the Current Challenges of Industrial IoT in Manufacturing. *HICSS 2022 Proceedings*. http://hdl.handle.net/10125/80170

Agarwal, R., & Prasad, J. (1997). The Role of Innovation Characteristics and Perceived Voluntariness in the Acceptance of Information Technologies. *Decision Sciences*, *28*(3), 557–582. https://doi.org/10.1111/j.1540-5915.1997.tb01322.x

Ahl, A., Yarime, M., Goto, M., Chopra, S. S., Kumar, N. Manoj., Tanaka, K., & Sagawa, D. (2020). Exploring blockchain for the energy transition: Opportunities and challenges based on a case study in Japan. *Renewable and Sustainable Energy Reviews*, *117*, 109488. https://doi.org/10.1016/j.rser.2019.109488

Akanfe, O., Lawong, D., & Rao, H. R. (2024). Blockchain technology and privacy regulation: Reviewing frictions and synthesizing opportunities. *International Journal of Information Management*, *76*, 102753. https://doi.org/10.1016/j.ijinfomgt.2024.102753

Alavi, M., Kayworth, T. R., & Leidner, D. E. (2005). An empirical examination of the influence of organizational culture on knowledge management practices. *Journal of Management Information Systems*, *22*(3), 191–224. https://doi.org/10.2753/MIS0742-1222220307

Allas, T., Checinski, M., Dillon, R., Dobbs, R., Hieronimus, S., & Singh, N. (2018). *Delivering for citizens: How to triple the success rate of government transformations | McKinsey*. https://shorturl.at/VBpCo

Allen, C. (2016). *The path to self-sovereign identity*. Life with Alacrity. www.lifewith alacrity.com/2016/04/the-path-to-self-sovereign-identity.html

Alt, R., Fridgen, G., & Chang, Y. (2024). The future of fintech—Towards ubiquitous financial services. *Electronic Markets*, *34*(1), 3. https://doi.org/10.1007/s12525-023-00687-8

Álvarez, I. A., Gramlich, V., & Sedlmeir, J. (2024). *Unsealing the secrets of blockchain consensus: A systematic comparison of the formal security of proof-of-work and proof-of-stake*. https://doi.org/10.48550/ARXIV.2401.14527

Alzahrani, L., Al-Karaghouli, W., & Weerakkody, V. (2017). Analysing the critical factors influencing trust in e-government adoption from citizens' perspective: A systematic review and a conceptual framework. *International Business Review*, *26*(1), 164–175. https://doi.org/10.1016/j.ibusrev.2016.06.004

Amend, J., Arnold, L., Feulner, S., Fridgen, G., Köhler, F., Ollig, P., Rieger, A., & Roth, T. (2022). *Opportunities and challenges of using blockchain technology in public administration – Insights from the FLORA project of Germany's Federal Office for Migration and Refugees*. Federal Office for Migration and Refugees. https://shorturl.at/svlvI

Amend, J., Feulner, S., Rieger, A., Roth, T., Fridgen, G., & Guggenberger, T. (2024). Bringing Government into the Digital Age: Insights from Germany's Asylum Procedure. *MIS Quarterly Executive (Accepted)*.

Amend, J., Fridgen, G., Rieger, A., Roth, T., & Stohr, A. (2021). The Evolution of an Architectural Paradigm—Using Blockchain to Build a Cross-Organizational Enterprise Service Bus. *HICSS 2021 Proceedings*. http://hdl.handle.net/10125/71139

Anania, L., Le Gars, G., & van Kranenburg, R. (2021). Disposable Identities? Why Digital Identity Matters to Blockchain Disintermediation and for Society. In E. Kaili & D. Psarrakis (Eds.), *Disintermediation Economics: The Impact of Blockchain on Markets and Policies* (pp. 297–327). Springer International Publishing. https://doi.org/10.1007/978-3-030-65781-9_14

Andersen, J. V., & Bogusz, C. I. (2019). Self-organizing in blockchain infrastructures: Generativity through shifting objectives and forking. *Journal of the Association for Information Systems*, *20*(9), 1242–1273. https://doi.org/10.17705/1jais.00566

Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., McCallum, P., & Peacock, A. (2019). Blockchain technology in the energy sector: A systematic review of challenges and opportunities. *Renewable and Sustainable Energy Reviews*, *100*, 143–174. https://doi.org/10.1016/j.rser.2018.10.014

Avgerou, C., & Bonina, C. (2020). Ideologies implicated in IT innovation in government: A critical discourse analysis of Mexico's international trade administration. *Information Systems Journal*, *30*(1), 70–95. https://doi.org/10.1111/isj.12245

Babel, M., & Sedlmeir, J. (2023). *Bringing data minimization to digital wallets at scale with general-purpose zero-knowledge proofs* (arXiv:2301.00823). arXiv. https://doi.org/10.48550/arXiv.2301.00823

Bachmann, N. M., Drasch, B., Fridgen, G., Miksch, M., Regner, F., Schweizer, A., & Urbach, N. (2022). Tarzan and chain: Exploring the ICO jungle and evaluating design archetypes. *Electronic Markets*, *32*(3), 1725–1748. https://doi.org/10.1007/s12525-021-00463-6

Bakos, Y., & Halaburda, H. (2022). Overcoming the Coordination Problem in New Marketplaces via Cryptographic Tokens. *Information Systems Research*, *33*(4), 1368–1385. https://doi.org/10.1287/isre.2022.1157

Barad, K. (2007). Agential realism: How material-discursive practices matter. In *Meeting the universe halfway: Quantum physics and the entanglement of matter and meaning* (pp. 132–185). Duke University Press Durham NC.

Barbereau, T., Smethurst, R., Papageorgiou, O., Sedlmeir, J., & Fridgen, G. (2023). Decentralised Finance's timocratic governance: The distribution and exercise of tokenised voting rights. *Technology in Society*, *73*, 102251. https://doi.org/10.1016/j.techsoc.2023.102251

Barrett, M., Heracleous, L., & Walsham, G. (2013). A rhetorical approach to IT diffusion: Reconceptualizing the ideology-framing relationship in computerization movements. *MIS Quarterly*, *37*(1), 201–220. https://doi.org/10.25300/MISQ/2013/37.1.09

Beck, R., Müller-Bloch, C., & King, J. L. (2018). Governance in the blockchain economy: A framework and research agenda. *Journal of the Association for Information Systems*, *19*(10), 1020–1034. https://doi.org/10.17705/1jais.00518

Benbunan-Fich, R., Desouza, K. C., & Andersen, K. N. (2020). IT-enabled innovation in the public sector: Introduction to the special issue. *European Journal of Information Systems*, *29*(4), 323–328. https://doi.org/10.1080/0960085X.2020.1814989

Berente, N., Hansen, S., Pike, J. C., & Bateman, P. J. (2011). Arguing the Value of Virtual Worlds: Patterns of Discursive Sensemaking of an Innovative Technology. *MIS Quarterly*, *35*(3), 685–709. https://doi.org/10.2307/23042804

Bohne, E. (2011). Conflicts between national regulatory cultures and EU energy regulations. *Utilities Policy*, *19*(4), 255–269. https://doi.org/10.1016/j.jup.2011.05.003

Bozeman, B., & Bretschneider, S. (1986). Public Management Information Systems: Theory and Prescription. *Public Administration Review*, *46*, 475–487. https://doi.org/10.2307/975569

Canato, A., Ravasi, D., & Phillips, N. (2013). Coerced Practice Implementation in Cases of Low Cultural Fit: Cultural Change and Practice Adaptation During the Implementation of Six Sigma at 3M. *Academy of Management Journal*, *56*(6), 1724–1753. https://doi.org/10.5465/amj.2011.0093

Carson, B., Romanelli, G., Walsh, P., & Zhumaev, A. (2018). *Blockchain beyond the hype: What is the strategic business value?* https://shorturl.at/sI58H

Carter, L., & Bélanger, F. (2005). The utilization of e-government services: Citizen trust, innovation and acceptance factors. *Information Systems Journal*, *15*(1), 5–25. https://doi.org/10.1111/j.1365-2575.2005.00183.x

Castagneto Gissey, G., Dodds, P. E., & Radcliffe, J. (2018). Market and regulatory barriers to electrical energy storage innovation. *Renewable and Sustainable Energy Reviews*, *82*, 781–790. https://doi.org/10.1016/j.rser.2017.09.079

Chong, A., Lim, E., Hua, X., Zheng, S., & Tan, C.-W. (2019). Business on Chain: A Comparative Case Study of Five Blockchain-Inspired Business Models. *Journal of the Association for Information Systems*, *20*(9). https://doi.org/10.17705/1jais.00568

Cinar, E., Trott, P., & Simms, C. (2019). A systematic review of barriers to public sector innovation process. *Public Management Review*, *21*(2), 264–290. https://doi.org/10.1080/14719037.2018.1473477

Cinar, E., Trott, P., & Simms, C. (2021). An international exploration of barriers and tactics in the public sector innovation process. *Public Management Review*, *23*(3), 326–353. https://doi.org/10.1080/14719037.2019.1668470

Coccia, M., & Watts, J. (2020). A theory of the evolution of technology: Technological parasitism and the implications for innovation magement. *Journal of Engineering and Technology Management*, *55*, 101552. https://doi.org/10.1016/j.jengtecman.2019.11.003

Codagnone, C., & Weigl, L. (2023). Leading the Charge on Digital Regulation: The More, the Better, or Policy Bubble? *Digital Society*, *2*(1), 4. https://doi.org/10.1007/s44206-023-00033-7

Conlan, T. (2006). From Cooperative to Opportunistic Federalism: Reflections on the Half-Century Anniversary of the Commission on Intergovernmental Relations. *Public Administration Review*, *66*(5), 663–676. https://doi.org/10.1111/j.1540-6210.2006.00631.x

Cordella, A., & Willcocks, L. (2012). Government policy, public value and IT outsourcing: The strategic case of ASPIRE. *The Journal of Strategic Information Systems*, *21*(4), 295–307. https://doi.org/10.1016/j.jsis.2012.10.007

Currie, W. L. (2004). The organizing vision of application service provision: A process-oriented analysis. *Information and Organization*, *14*(4), 237–267. https://doi.org/10.1016/j.infoandorg.2004.07.001

Davidson, E. J., Østerlund, C. S., & Flaherty, M. G. (2015). Drift and shift in the organizing vision career for personal health records: An investigation of innovation discourse dynamics. *Information and Organization*, *25*(4), 191–221. https://doi.org/10.1016/j.infoandorg.2015.08.001

Dawson, G. S., Denford, J. S., Williams, C. K., Preston, D., & Desouza, K. C. (2016). An Examination of Effective IT Governance in the Public Sector Using the Legal View of Agency Theory. *Journal of Management Information Systems*, *33*(4), 1180–1208. https://doi.org/10.1080/07421222.2016.1267533

De Vries, H., Bekkers, V., & Tummers, L. (2016). Innovation in the Public Sector: A Systematic Review and Future Research Agenda. *Public Administration*, *94*(1), 146–166. https://doi.org/10.1111/padm.12209

de Vries, H., Tummers, L., & Bekkers, V. (2018). A stakeholder perspective on public sector innovation: Why position matters. *International Review of Administrative Sciences*, *84*(2), 269–287. https://doi.org/10.1177/0020852317715513

Deringer, D. K., & Molnar, A. R. (1983). University, Industry, Federal Cooperation—A Case Study. *Science, Technology, & Human Values*, *8*(4), 40–45. https://doi.org/10.1177/016224398300800407

Diestelmeier, L. (2019). Changing power: Shifting the role of electricity consumers with blockchain technology – Policy implications for EU electricity law. *Energy Policy*, *128*, 189–196. https://doi.org/10.1016/j.enpol.2018.12.065

Dittmar, L., & Praktiknjo, A. (2019). Could Bitcoin emissions push global warming above 2 °C? *Nature Climate Change*, *9*(9), 656–657. https://doi.org/10.1038/s41558-019-0534-5

Djamali, A., Dossow, P., Hinterstocker, M., Schellinger, B., Sedlmeir, J., Völter, F., & Willburger, L. (2021). Asset logging in the energy sector: A scalable blockchain-based data platform. *Energy Informatics*, *4*(Suppl 3), 22. https://doi.org/10.1186/s42162-021-00183-3

Dwivedi, Y., Williams, M., Mitra, A., Niranjan, S., & Weerakkody, V. (2011). Understanding Advances in Web Technolgies: Evolution from Web 2.0 to Web 3.0. *ECIS 2011 Proceedings*. https://aisel.aisnet.org/ecis2011/257

Dyson, K. (1992). Regulatory culture and regulatory change: Some conclusions. In K. Dyson (Ed.), *The Politics of German Regulation* (pp. 257–271). Dartmouth Pub Co.

Egeberg, M. (2001). How federal? The organizational dimension of integration in the EU (and elsewhere). *Journal of European Public Policy*, *8*(5), 728–746. https://doi.org/10.1080/13501760110083482

Ellinger, E. W., Gregory, R. W., Mini, T., Widjaja, T., & Henfridsson, O. (2024). Skin the the Game: The Transformational Potential of Decentralized Autonomous Organizations. *MIS Quarterly*, *48*(1), 245–272. https://doi.org/10.25300/MISQ/2023/17690

European Comission. (2024). *European Blockchain Services Infrastructure*. https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Home

European Parliament. (2024). *Regulation (EU) 2024/1183*. https://eur-lex.europa.eu/eli/reg/2024/1183/oj

Feller, J., Finnegan, P., & Nilsson, O. (2011). Open innovation and public administration: Transformational typologies and business model impacts. *European Journal of Information Systems*, *20*(3), 358–374. https://doi.org/10.1057/ejis.2010.65

Fredrickson, J. W. (1986). The Strategic Decision Process and Organizational Structure. *The Academy of Management Review*, *11*(2), 280–297. https://doi.org/10.2307/258460

Fridgen, G., Radszuwill, S., Schweizer, A., & Urbach, N. (2021). Blockchain Won't Kill the Banks: Why Disintermediation Doesn't Work in International Trade Finance. *Communications of the Association for Information Systems*, *49*(1). https://doi.org/10.17705/1CAIS.04932

Fridgen, G., Radszuwill, S., Urbach, N., & Utz, L. (2018). Cross-Organizational Workflow Management Using Blockchain Technology—Towards Applicability, Auditability, and Automation. *HICSS 2018 Proceedings*. http://hdl.handle.net/10125/50332

Fried, N. (2017). Innovating in a Highly Regulated Industry Like Health Care. *Harvard Business Review*. https://hbr.org/2017/06/innovating-in-a-highly-regulated-industry-like-health-care

Gal, U., Berente, N., & Chasin, F. (2022). *Technology Lifecycles and Digital Technologies: Patterns of Discourse across Levels of Materiality*. *23*(5), 1102–1149. https://doi.org/10.17705/1jais.00761

Gallersdörfer, U., Klaaßen, L., & Stoll, C. (2020). Energy Consumption of Cryptocurrencies Beyond Bitcoin. *Joule*, *4*(9), 1843–1846. https://doi.org/10.1016/j.joule.2020.07.013

Gao, H., Xu, S., Liu, Y., Wang, L., Xiang, Y., & Liu, J. (2020). Decentralized optimal operation model for cooperative microgrids considering renewable energy uncertainties. *Applied Energy*, *262*, 114579. https://doi.org/10.1016/j.apenergy.2020.114579

Gaspary, E., Moura, G. L. D., & Wegner, D. (2020). How does the organisational structure influence a work environment for innovation? *International Journal of Entrepreneurship and Innovation Management*, *24*(2–3), 132–153. https://doi.org/10.1504/IJEIM.2020.105770

Geels, F. W., & Schot, J. (2007). Typology of sociotechnical transition pathways. *Research Policy*, *36*(3), 399–417. https://doi.org/10.1016/j.respol.2007.01.003

Gioia, D. A., & Chittipeddi, K. (1991). Sensemaking and sensegiving in strategic change initiation. *Strategic Management Journal*, *12*(6), 433–448. https://doi.org/10.1002/smj.4250120604

Glöckler, J., Sedlmeir, J., Frank, M., & Fridgen, G. (2023). A Systematic Review of Identity and Access Management Requirements in Enterprises and Potential Contributions of Self-Sovereign Identity. *Business & Information Systems Engineering*. https://doi.org/10.1007/s12599-023-00830-x

Goh, J. M., & Arenas, A. E. (2020). IT value creation in public sector: How IT-enabled capabilities mitigate tradeoffs in public organisations. *European Journal of Information Systems*, *29*(1), 25–43. https://doi.org/10.1080/0960085X.2019.1708821

Goodhue, D. L., & Thompson, R. L. (1995). Task-Technology Fit and Individual Performance. *MIS Quarterly*, *19*(2), 213–236. https://doi.org/10.2307/249689

Gorgeon, A., & Swanson, E. B. (2011). Web 2.0 according to Wikipedia: Capturing an organizing vision. *Journal of the American Society for Information Science and Technology*, *62*(10), 1916–1932. https://doi.org/10.1002/asi.21612

Grant, G., & Tan, F. B. (2013). Governing IT in inter-organizational relationships: Issues and future research. *European Journal of Information Systems*, *22*(5), 493–497. https://doi.org/10.1057/ejis.2013.21

Guggenmos, F., Lockl, J., Rieger, A., Wenninger, A., & Fridgen, G. (2020). How to Develop a GDPR-Compliant Blockchain Solution for Cross-Organizational Workflow Management: Evidence from the German Asylum Procedure. *HICSS 2020 Proceedings*. https://doi.org/10.24251/HICSS.2020.492

Halaburda, H., Levina, N., & Semi, M. (2023). Digitization of transaction terms as a shift parameter within TCE: Strong smart contract as a new mode of transaction governance. *MIS Quarterly (Forthcoming)*. https://doi.org/10.25300/MISQ/2023/17818

Hardy, C., & Maguire, S. (2016). Organizing Risk: Discourse, Power, and "Riskification." *Academy of Management Review*, *41*(1), 80–108. https://doi.org/10.5465/amr.2013.0106

Hartwich, E., Hoess, A., Rieger, A., Roth, T., Fridgen, G., & Young, A. (2023). How Organizations Sustain and Navigate Between (De)centralization Equilibria: A Process Model. *ICIS 2023 Proceedings*. https://aisel.aisnet.org/icis2023/itadopt/itadopt/10

Hartwich, E., Ollig, P., Fridgen, G., & Rieger, A. (2023). Probably something: A multi-layer taxonomy of non-fungible tokens. *Internet Research*, *34*(1), 216–238. https://doi.org/10.1108/INTR-08-2022-0666

Hartwich, E., Rieger, A., Sedlmeir, J., Jurek, D., & Fridgen, G. (2023). Machine economies. *Electronic Markets*, *33*(1), 36. https://doi.org/10.1007/s12525-023-00649-0

Hartwich, E., Roth, T., Rieger, A., Zavolokina, L., & Fridgen, G. (2024). Negotiation and Translation Between Discursive Fields: A Study of the Diffusion of Decentralized Finance. *ECIS 2024 Proceedings*. https://aisel.aisnet.org/ecis2024/track20_adoption/track20_adoption/4

Heintze, T., & Bretschneider, S. (2000). Information Technology and Restructuring in Public Organizations: Does Adoption of Information Technology Affect Organizational Structures, Communications, and Decision Making? *Journal of Public Administration Research and Theory*, *10*(4), 801–830. https://doi.org/10.1093/oxfordjournals.jpart.a024292

Hoess, A., Rieger, A., Roth, T., Fridgen, G., & Young, A. (2023). Managing Fashionable Organizing Visions: Evidence from the European Blockchain Services Infrastructure. *ECIS 2023 Proceedings*. https://aisel.aisnet.org/ecis2023_rp/337

Hoess, A., Roth, T., Sedlmeir, J., Fridgen, G., & Rieger, A. (2022). With or Without Blockchain? Towards a Decentralized, SSI-based eRoaming Architecture. *HICSS 2022 Proceedings*. http://hdl.handle.net/10125/79899

Hoess, A., Schlatt, V., Rieger, A., & Fridgen, G. (2021). The Blockchain Effect: From Inter-Ecosystem to Intra-Ecosystem Competition. *ECIS 2021 Proceedings*. https://aisel.aisnet.org/ecis2021_rp/36

Hsu, D. H., & Lim, K. (2014). Knowledge Brokering and Organizational Innovation: Founder Imprinting Effects. *Organization Science*, *25*(4), 1134–1153. https://doi.org/10.1287/orsc.2013.0863

Huemer, L. (2012). Organizational identities in networks: Sense-giving and sense-taking in the salmon farming industry. *240-253*. https://biopen.bi.no/bi-xmlui/handle/11250/93704

Huenteler, J., Schmidt, T. S., Ossenbrink, J., & Hoffmann, V. H. (2016). Technology life-cycles in the energy sector—Technological characteristics and the role of deployment for innovation. *Technological Forecasting and Social Change*, *104*, 102–121. https://doi.org/10.1016/j.techfore.2015.09.022

Hueske, A.-K., & Guenther, E. (2015). What hampers innovation? External stakeholders, the organization, groups and individuals: a systematic review of empirical barrier research. *Management Review Quarterly*, *65*(2), 113–148. https://doi.org/10.1007/s11301-014-0109-5

Hughes, L., Dwivedi, Y. K., Misra, S. K., Rana, N. P., Raghavan, V., & Akella, V. (2019). Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda. *International Journal of Information Management*, *49*, 114–129. https://doi.org/10.1016/j.ijinfomgt.2019.02.005

Iannacci, F. (2010). When is an information infrastructure? Investigating the emergence of public sector information infrastructures. *European Journal of Information Systems*, *19*(1), 35–48. https://doi.org/10.1057/ejis.2010.3

Inwood, O., & Zappavigna, M. (2023). Ideology, attitudinal positioning, and the blockchain: A social semiotic approach to understanding the values construed in the whitepapers of blockchain start-ups. *Social Semiotics*, *33*(3), 451–469. https://doi.org/10.1080/10350330.2021.1877995

Kahneman, D., & Tversky, A. (1979). Prospect Theory: An Analysis of Decision under Risk. *Econometrica*, *47*(2), 263–291. https://doi.org/10.2307/1914185

Kane, K., Young, A., Majchrzak, A., & Ransbotham, S. (2021). Avoiding an Oppressive Future of Machine Learning: A Design Theory for Emancipatory Assistants. *MIS Quarterly*, *45*(1), 371–396. https://doi.org/10.25300/MISQ/2021/1578

Kappos, A., & Rivard, S. (2008). A three-perspective model of culture, information systems, and their development and use. *MIS Quarterly*, *32*(3), 601–634. https://doi.org/10.2307/25148858

Kim, I., & Miranda, S. (2018). 20 Years Old but Still a Teenager? A Review of Organizing Vision Theory and Suggested Directions. *PACIS 2018 Proceedings*. https://aisel.aisnet.org/pacis2018/23

Koch, H., Leidner, D. E., & Gonzalez, E. S. (2013). Digitally enabling social networks: Resolving IT–culture conflict. *Information Systems Journal*, *23*(6), 501–523. https://doi.org/10.1111/isj.12020

Kudra, A., Rieger, A., Roth, T., Sedlmeir, J., Fridgen, G., & Young, A. G. (2024). Digital Identity Wallets. *University of Arkansas Working Paper*.

Lacity, M. C. (2022). Blockchain: From Bitcoin to the Internet of Value and beyond. *Journal of Information Technology*, *37*(4), 326–340. https://doi.org/10.1177/02683962221086300

Lacity, M., & Carmel, E. (2022). Self-Sovereign Identity and Verifiable Credentials in Your Digital Wallet. *MIS Quarterly Executive*, *21*(3). https://aisel.aisnet.org/misqe/vol21/iss3/6

Lacity, M., Carmel, E., Young, A. G., & Roth, T. (2023). The Quiet Corner of Web3 That Means Business. *MIT Sloan Management Review*, *64*(3). https://sloanreview.mit.edu/article/the-quiet-corner-of-web3-that-means-business/

Leidner, D. E., & Kayworth, T. (2006). A review of culture in information systems research: Toward a theory of information technology culture conflict. *MIS Quarterly*, *3*(20), 357–399. https://doi.org/10.2307/25148735

Leow, A., Litan, A., Farahmand, H., & Valdes, R. (2023). *Gartner Hype Cycle for Blockchain and Web3, 2023*. https://www.gartner.com/en/documents/4594099

Liang, T.-P., Kohli, R., Huang, H.-C., & Li, Z.-L. (2021). What Drives the Adoption of the Blockchain Technology? A Fit-Viability Perspective. *Journal of Management Information Systems*, *38*(2), 314–337. https://doi.org/10.1080/07421222.2021.1912915

Lichti, C. W., & Tumasjan, A. (2023). "My Precious!": A Values-Affordances Perspective on the Adoption of Bi" by Constantin W. Lichti and Andranik Tumasjan. *Journal of the Association for Information Systems*, *24*(3), 629–663. https://doi.org/10.17705/1jais.00790

Lüth, A., Zepter, J. M., Crespo del Granado, P., & Egging, R. (2018). Local electricity market designs for peer-to-peer trading: The role of battery flexibility. *Applied Energy*, *229*, 1233–1243. https://doi.org/10.1016/j.apenergy.2018.08.004

Maitlis, S., & Christianson, M. (2014). Sensemaking in Organizations: Taking Stock and Moving Forward. *Academy of Management Annals*, *8*(1), 57–125. https://doi.org/10.5465/19416520.2014.873177

McLaughlin, P. A., & Sherouse, O. (2019). RegData 2.2: A panel dataset on US federal regulations. *Public Choice*, *180*, 43–55. https://doi.org/10.1007/s11127-018-0600-y

Meijer, A. (2015). E-governance innovation: Barriers and strategies. *Government Information Quarterly*, *32*(2), 198–206. https://doi.org/10.1016/j.giq.2015.01.001

Mengelkamp, E., Gärttner, J., Rock, K., Kessler, S., Orsini, L., & Weinhardt, C. (2018). Designing microgrid energy markets: A case study: The Brooklyn Microgrid. *Applied Energy*, *210*, 870–880. https://doi.org/10.1016/j.apenergy.2017.06.054

Mengelkamp, E., Schlund, D., & Weinhardt, C. (2019). Development and real-world application of a taxonomy for business models in local energy markets. *Applied Energy*, *256*, 113913. https://doi.org/10.1016/j.apenergy.2019.113913

Mignerat, M., & Rivard, S. (2015). Positioning the institutional perspective in information systems research. In L. P. Willcocks, C. Sauer, & M. C. Lacity (Eds.), *Formulating Research Methods for Information Systems: Volume 2* (pp. 79–126). Palgrave Macmillan UK. https://doi.org/10.1057/9781137509888_4

Miranda, S. M., Kim, I., & Summers, J. D. (2015). Jamming with Social Media: How Cognitive Structuring of Organizing Vision Facets Affects IT Innovation Diffusion. *MIS Quarterly*, *39*(3), 591–614. https://doi.org/10.25300/MISQ/2016/40.2.02

Miranda, S. M., Wang, D. D., & Tian, C. A. (2022). Discursive Fields and the Diversity-Coherence Paradox: An Ecological Perspective on the Blockchain Community Discourse. *MIS Quarterly*, *46*(3), 1421–1452. https://doi.org/10.25300/MISQ/2022/15736

Miranda, S. M., Young, A., & Yetgin, E. (2016). Are social media emancipatory or hegemonic? Societal effects of mass media digitization in the case of the Sopa discourse. *MIS Quarterly*, *40*(2), 303–330. https://doi.org/10.25300/MISQ/2016/40.2.02

Möhlmannn, M., Salge, C. A. de L., & Marabelli, M. (2023). Algorithm Sensemaking: How Platform Workers Make Sense of Algorithmic Management. *Journal of the Association for Information Systems*, *24*(1), 35–64. https://doi.org/10.17705/1jais.00774

Mora, C., Rollins, R. L., Taladay, K., Kantar, M. B., Chock, M. K., Shimada, M., & Franklin, E. C. (2018). Bitcoin emissions alone could push global warming above 2°C. *Nature Climate Change*, *8*(11), 931–933. https://doi.org/10.1038/s41558-018-0321-8

Morstyn, T., Farrell, N., Darby, S. J., & McCulloch, M. D. (2018). Using peer-to-peer energy-trading platforms to incentivize prosumers to form federated power plants. *Nature Energy*, *3*(2), 94–101. https://doi.org/10.1038/s41560-017-0075-y

Narayanan, A. (2013). What happened to the crypto dream?, part 1. *IEEE Security and Privacy*, *11*(2), 75–76. https://doi.org/10.1109/MSP.2013.45

Orlikowski, W. J., & Scott, S. V. (2014). What Happens When Evaluation Goes Online? Exploring Apparatuses of Valuation in the Travel Sector. *Organization Science*, *25*(3), 868–891. https://doi.org/10.1287/orsc.2013.0877

Pahlka, J. (2023). *Recoding America: Why government is failing in the digital age and how we can do better*. Metropolitan Books.

Parameswaran, S., Kishore, R., Yang, X., & Liu, Z. (2023). Theorizing about the Early-Stage Diffusion of Codependent IT Innovations. *Journal of the Association for Information Systems*, *24*(2), 379–429. https://doi.org/10.17705/1jais.00789

Phillips, N., Lawrence, T. B., & Hardy, C. (2004). Discourse and Institutions. *The Academy of Management Review*, *29*(4), 635–652. https://doi.org/10.2307/20159075

Rana, N. P., Williams, M. D., Dwivedi, Y. K., & Williams, J. (2012). Theories and Theoretical Models for Examining the Adoption of E-Government Services. *E-Service Journal*, *8*(2), 26–56. https://doi.org/10.2979/eservicej.8.2.26

Rieger, A., Lockl, J., Urbach, N., Guggenmos, F., & Fridgen, G. (2019). Building a blockchain application that complies with the EU General Data Protection Regulation. *MIS Quarterly Executive*, *18*(4), 7. https://doi.org/10.17705/2msqe.00020

Rieger, A., Roth, T., Sedlmeir, J., & Fridgen, G. (2022). We Need a Broader Debate on the Sustainability of Blockchain. *Joule*, *6*(6), 1137–1141. https://doi.org/10.1016/j.joule.2022.04.013

Rieger, A., Roth, T., Sedlmeir, J., Fridgen, G., & Young, A. G. (2024). Organizational Identity Management Policies. *Journal of the Association for Information Systems*, *25*(3), 522–527. https://doi.org/10.17705/1jais.00887

Rieger, A., Roth, T., Sedlmeir, J., Weigl, L., & Fridgen, G. (2022). Not Yet Another Digital Identity. *Nature Human Behaviour*, *6*(1), 3–3. https://doi.org/10.1038/s41562-021-01243-0

Rinta-Kahila, T., Penttinen, E., & Lyytinen, K. (2023). Getting Trapped in Technical Debt: Sociotegetting Trapped in Technical Debt: Sociotechnical Analysis of a Legacy System's Replacement1chnical Analysis of a Legacy System's Replacement. *MIS Quarterly*, *47*(1), 1–31. https://doi.org/10.25300/MISQ/2022/16711

Rossi, M., Mueller-Bloch, C., Thatcher, J. B., & Beck, R. (2019). Blockchain research in information systems: Current trends and an inclusive future research agenda. *Journal of the Association for Information Systems*, *20*(9), 1390–1405. https://doi.org/10.17705/1jais.00571

Roth, T., Rieger, A., Fridgen, G., & Young, A. (2023). How IS Affect Social Justice Tensions: A Case Study of Asylum Management. In B. Shishkov (Ed.), *Business Modeling and Software Design* (pp. 268–277). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-36757-1_18

Roth, T., Rieger, A., & Hoess, A. (2024). From Mutualism to Amensalism: A Case Study of Blockchain and Digital Identity Wallets. In B. Shishkov (Ed.), *Business Modeling and Software Design (Minor revisions)*. Springer Nature Switzerland.

Roth, T., Rieger, A., Utz, M., Fridgen, G., & Young, A. G. (2024). Cultural Sensemaking of Emerging IT in Enactment Fields. *MIS Quarterly (Under Preparation for Re-Submission)*.

Roth, T., Rieger, A., Utz, M., & Young, A. (2022). The Role of Cultural Fit in the Adoption of Fashionable IT: A Blockchain Case Study. *ICIS 2022 Proceedings*. https://aisel.aisnet.org/icis2022/blockchain/blockchain/17

Roth, T., Stohr, A., Amend, J., Fridgen, G., & Rieger, A. (2023). Blockchain as a driving force for federalism: A theory of cross-organizational task-technology fit. *International Journal of Information Management*, *68*, 102476. https://doi.org/10.1016/j.ijinfomgt.2022.102476

Roth, T., Utz, M., Baumgarte, F., Rieger, A., Sedlmeir, J., & Strüker, J. (2022). Electricity powered by blockchain: A review with a European perspective. *Applied Energy*, *325*, 119799. https://doi.org/10.1016/j.apenergy.2022.119799

Rudkin, J.-E., Kimbell, L., Stoermer, E., Scapolo, F., & Vesnic-Alujevic, L. (2019). *The future of government 2030+: A citizen centric perspective on new government models*. Publications Office of the European Union. https://data.europa.eu/doi/10.2760/145751

Sarker, S., Henningsson, S., Jensen, T., & Hedman, J. (2021). The use of blockchain as a resource for combating corruption in global shipping: An interpretive case study. *Journal of Management Information Systems*, *38*(2), 338–373. https://doi.org/10.1080/07421222.2021.1912919

Sartor, S., Sedlmeir, J., Rieger, A., & Roth, T. (2022). Love at First Sight? A User Experience Study of Self-Sovereign Identity Wallets. *ECIS 2022 Research Papers*. https://aisel.aisnet.org/ecis2022_rp/46

Schein, E. H. (2017). *Organizational culture and leadership* (5th ed.). John Wiley & Sons.

Schellinger, B., Völter, F., Urbach, N., & Sedlmeir, J. (2022). Yes, I do: Marrying blockchain applications with GDPR. *HICSS 2022 Proceedings*. http://hdl.handle.net/10125/79900

Schlatt, V., Sedlmeir, J., Feulner, S., & Urbach, N. (2022). Designing a Framework for Digital KYC Processes Built on Blockchain-Based Self-Sovereign Identity. *Information & Management*, *59*(7), 103553. https://doi.org/10.1016/j.im.2021.103553

Schweizer, A., Schlatt, V., Urbach, N., & Fridgen, G. (2017). Unchaining Social Businesses – Blockchain as the Basic Technology of a Crowdlending Platform. *ICIS 2017 Proceedings*. https://aisel.aisnet.org/icis2017/TransformingSociety/Presentations/8

Scott, M., DeLone, W., & Golden, W. (2016). Measuring eGovernment success: A public value approach. *European Journal of Information Systems*, *25*(3), 187–208. https://doi.org/10.1057/ejis.2015.11

Sedlmeir, J., Barbereau, T. J., Huber, J., Weigl, L., & Roth, T. (2022). Transition Pathways towards Design Principles of Self-Sovereign Identity. *ICIS 2022 Proceedings*. https://aisel.aisnet.org/icis2022/is_implement/is_implement/4

Sedlmeir, J., Buhl, H., Fridgen, G., & Keller, R. (2020). The Energy Consumption of Blockchain Technology: Beyond Myth. *Business & Information Systems Engineering*, *62*(6), 599–608. https://doi.org/10.1007/s12599-020-00656-x

Sedlmeir, J., Lautenschlager, J., Fridgen, G., & Urbach, N. (2022). The transparency challenge of blockchain in organizations. *Electronic Markets*, *32*(3), 1779–1794. https://doi.org/10.1007/s12525-022-00536-0

Sedlmeir, J., Ross, P., Luckow, A., Lockl, J., Miehle, D., & Fridgen, G. (2021). The DLPS: A New Framework for Benchmarking Blockchains. *HICCS 2021 Proceedings*. http://hdl.handle.net/10125/71443

Sedlmeir, J., Smethurst, R., Rieger, A., & Fridgen, G. (2021). Digital Identities and Verifiable Credentials. *Business & Information Systems Engineering*, *63*(5), 603–613. https://doi.org/10.1007/s12599-021-00722-y

Seltsikas, P., & O'Keefe, R. M. (2010). Expectations and outcomes in electronic identity management: The role of trust and public value. *European Journal of Information Systems*, *19*(1), 93–103. https://doi.org/10.1057/ejis.2009.51

Shiller, R. J. (2020). *Narrative economics: How stories go viral and drive major economic events*. Princeton University Press.

Smethurst, R. (2023). Digital Identity Wallets and their Semantic Contradictions. *ECIS 2023 Proceedings*. https://aisel.aisnet.org/ecis2023_rp/288

Stohr, A., Ollig, P., Keller, R., & Rieger, A. (2024). Generative mechanisms of AI implementation: A critical realist perspective on predictive maintenance. *Information and Organization*, *34*(2), 100503. https://doi.org/10.1016/j.infoandorg.2024.100503

Su, N. (2015). Cultural sensemaking in offshore information technology service suppliers. *MIS Quarterly*, *39*(4), 959–984. https://doi.org/10.25300/MISQ/2015/39.4.10

Suddaby, R., & Foster, W. M. (2017). History and Organizational Change. *Journal of Management*, *43*(1), 19–38. https://doi.org/10.1177/0149206316675031

Swanson, B. E., & Ramiller, N. C. (2004). Innovating Mindfully with Information Technology. *MIS Quarterly*, *28*(4), 553–583. https://doi.org/10.2307/25148655

Swanson, E. (2017). Theorizing Information Systems as Evolving Technology. *Communications of the Association for Information Systems*, *41*(1). https://doi.org/10.17705/1CAIS.04101

Swanson, E., & Ramiller, N. (1997). The Organizing Vision in Information Systems Innovation. *Organization Science*, *8*(5), 458–474. https://doi.org/10.1287/orsc.8.5.458

Thacher, D., & Rein, M. (2004). Managing Value Conflict in Public Policy. *Governance*, *17*(4), 457–486. https://doi.org/10.1111/j.0952-1895.2004.00254.x

Theobald, C. (2010). The Transformation of German Energy Regulation: Struggling with Policy Legacy. In B. Eberlein & G. B. Doern (Eds.), *Governing the Energy Challenge: Canada and Germany in a Multilevel Regional and Global Context* (pp. 259–284). University of Toronto Press. https://doi.org/10.3138/9781442697485-012

Thomas, L., Zhou, Y., Long, C., Wu, J., & Jenkins, N. (2019). A general form of smart contract for decentralized energy systems management. *Nature Energy*, *4*(2), 140–149. https://doi.org/10.1038/s41560-018-0317-7

Tobin, A. (2018). *Sovrin: What goes on the ledger?* https://sovrin.org/wp-content/uploads/2018/10/What-Goes-On-The-Ledger.pdf

Utz, M., Johanning, S., Roth, T., Bruckner, T., & Strüker, J. (2023). From ambivalence to trust: Using blockchain in customer loyalty programs. *International Journal of Information Management*, *68*, 102496. https://doi.org/10.1016/j.ijinfomgt.2022.102496

van der Wal, Z., & van Hout, E. Th. J. (2009). Is Public Value Pluralism Paramount? The Intrinsic Multiplicity and Hybridity of Public Values. *International Journal of Public Administration*, *32*(3–4), 220–231. https://doi.org/10.1080/01900690902732681

Vinsel, L. (2023). Don't Get Distracted by the Hype Around Generative AI. *MIT Sloan Management Review*, *64*(3), 1–3. https://sloanreview.mit.edu/article/dont-get-distracted-by-the-hype-around-generative-ai/

Wang, P. (2010). Chasing the hottest IT: Effects of information technology fashion on organizations. *MIS Quarterly*, 63–85. https://doi.org/10.2307/20721415

Wang, P., & Ramiller, N. C. (2009). Community learning in information technology innovation. *MIS Quarterly*, 709–734. https://doi.org/10.2307/20650324

Wang, P., & Swanson, E. B. (2007). Launching professional services automation: Institutional entrepreneurship for information technology innovations. *Information and Organization*, *17*(2), 59–88. https://doi.org/10.1016/j.infoandorg.2007.02.001

Weick, K. E., Sutcliffe, K. M., & Obstfeld, D. (2005). Organizing and the Process of Sensemaking. *Organization Science*, *16*(4), 409–421. https://doi.org/10.1287/orsc.1050.0133

Weigl, L., Amard, A., Marxen, H., Roth, T., & Zavolokina, L. (2022). User-centricity and Public Values in eGovernment: Friend or Foe? *ECIS 2022 Proceedings*. https://aisel.aisnet.org/ecis2022_rp/15

Weigl, L., Barbereau, T., & Fridgen, G. (2023). The construction of self-sovereign identity: Extending the interpretive flexibility of technology towards institutions. *Government Information Quarterly*, *40*(4), 101873. https://doi.org/10.1016/j.giq.2023.101873

Weigl, L., Barbereau, T., Rieger, A., & Fridgen, G. (2022). The Social Construction of Self-Sovereign Identity: An Extended Model of Interpretive Flexibility. *HICSS 2022 Proceedings*. http://hdl.handle.net/10125/79649

Weigl, L., Roth, T., Amard, A., & Zavolokina, L. (2024). When Public Values and User-Centricity in e-Government Collide—A Systematic Review. *Government Information Quarterly (Minor Revisions)*.

Wibbels, E. (2006). Madison in Baghdad: Decentralization and federalism in comparative politics. *Annual Review of Political Science*, *9*, 165–188. https://doi.org/10.1146/annurev.polisci.9.062404.170504

Wiredu, G. O. (2012). Information systems innovation in public organisations: An institutional perspective. *Information Technology & People*, *25*(2), 188–206. https://doi.org/10.1108/09593841211232703

Yeoh, W.-Z., Kepkowski, M., Heide, G., Kaafar, D., & Hanzlik, L. (2023). Fast IDentity Online with Anonymous Credentials (FIDO-AC). *32nd USENIX Security Symposium*. https://www.usenix.org/system/files/usenixsecurity23-yeoh.pdf

Young, A. G., Syed, S., Roth, T., Zhu, Y., & Hevner, A. R. (2024). Ethical Design through Ground and Evaluate (EDGE) Information Systems to Achieve Social Impacts. *Journal of Information Technology (Major Revisions)*.

Zhang, T., Pota, H., Chu, C.-C., & Gadh, R. (2018). Real-time renewable energy incentive system for electric vehicles using prioritization and cryptocurrency. *Applied Energy*, *226*, 582–594. https://doi.org/10.1016/j.apenergy.2018.06.025

Ziolkowski, R., Miscione, G., & Schwabe, G. (2020). Decision problems in blockchain governance: Old wine in new bottles or walking in someone else's shoes? *Journal of Management Information Systems*, *37*(2), 316–348. https://doi.org/10.1080/07421222.2020.1759974

7. Appendices

7.1. Appendix A: Research papers included in this thesis

RP1: Roth, T., Stohr, A., Amend, J., Fridgen, G., & Rieger, A. (2023). Blockchain as a Driving Force for Federalism: A Theory of Cross-organizational Task-technology Fit. *International Journal of Information Management*, *68*, 102476. https://doi.org/10.1016/j.ijinfomgt.2022.102476
Journal Rating: 41.9 (CiteScore); 5.266 (SNIP)

RP2: Roth, T., Utz, M., Baumgarte, F., Rieger, A., Sedlmeir, J., & Strüker, J. (2022). Electricity Powered by Blockchain: A Review with a European Perspective. *Applied Energy*, *325*, 119799. https://doi.org/10.1016/j.apenergy.2022.119799
Journal Ranking: 21.1 (CiteScore); 2.758 (SNIP)

RP3: Lacity, M., Carmel, E., Young, A. G., & Roth, T. (2023). The Quiet Corner of Web3 That Means Business. *MIT Sloan Management Review*, *64*(3), https://sloanreview.mit.edu/article/the-quiet-corner-of-web3-that-means-business/
Journal Rating: 4.9 (CiteScore); 1.100 (SNIP)

RP4: Rieger, A., Roth, T., Sedlmeir, J., Fridgen, G., & Young, A. G. (2024). Organizational Identity Management Policies. *Journal of the Association for Information Systems*, *25*(3*)*, 522–527. https://doi.org/10.17705/1jais.00887
Journal Rating: 9.0 (CiteScore); 2.244 (SNIP)

RP5: Rieger, A., Roth, T., Sedlmeir, J., & Fridgen, G. (2022). We Need a Broader Debate on the Sustainability of Blockchain. *Joule*, *6*(6)*,* 1137–1141. https://doi.org/10.1016/j.joule.2022.04.013
Journal Rating: 60.6 (CiteScore); 4.950 (SNIP)

RP6: Sedlmeir, J., Huber, J., Barbereau, T. J., Weigl, L., & Roth, T. (2022). Transition Pathways Towards Design Principles of Self-Sovereign Identity. *ICIS 2022 Proceedings*. https://aisel.aisnet.org/icis2022/is_implement/is_implement/4
Conference Ranking: 2 (GGS Class); A- (GGS Rating)

RP7: Hoess, A., Rieger, A., Roth, T., Fridgen, G., & Young, A. (2023). Managing Fashionable Organizing Visions: Evidence from the European Blockchain Services Infrastructure. *ECIS 2023 Proceedings*. https://aisel.aisnet.org/ecis2023_rp/337
Conference Ranking: 3 (GGS Class); B (GGS Rating)

RP8: Roth, T., Rieger, A., & Hoess, A. (2024). From Mutualism to Amensalism: A Case Study of Blockchain and Digital Identity Wallets. In B. Shishkov (Ed.), *Business Modeling and Software Design (forthcoming)*. Springer Nature Switzerland.

RP09: Utz, M., Johanning, S., Roth, T., Bruckner, T., & Strüker, J. (2023). From Ambivalence to Trust: Using Blockchain in Customer Loyalty Programs. *International Journal of Information Management*, *68*, 102496. https://doi.org/10.1016/j.ijinfomgt.2022.102496
Journal Rating: 41.9 (CiteScore); 5.266 (SNIP)

RP10: Amend, J., Feulner, S., Rieger, A., Roth, T., Fridgen, G., & Guggenberger, T. (2024). Bringing Government into the Digital Age: Insights from Germany's Asylum Procedure. *MIS Quarterly Executive (Accepted)*.
Journal Ranking: 10.0 (CiteScore); 1.840 (SNIP)

RP11: Hartwich, E., Hoess, A., Rieger, A., Roth, T., Fridgen, G., & Young, A. (2023). How Organizations Sustain and Navigate Between (De)centralization Equilibria: A Process Model. *ICIS 2023 Proceedings*. https://aisel.aisnet.org/icis2023/itadopt/itadopt/10
Conference Ranking: 2 (GGS Class); A- (GGS Rating)

RP12: Roth, T., Rieger, A., Utz, M., & Young, A. (2022). The Role of Cultural Fit in the Adoption of Fashionable IT: A Blockchain Case Study. *ICIS 2022 Proceedings*. https://aisel.aisnet.org/icis2022/blockchain/blockchain/17
Conference Ranking: 2 (GGS Class); A- (GGS Rating)

RP13: Roth, T., Rieger, A., Fridgen, G., & Young, A. (2023). How IS Affect Social Justice Tensions: A Case Study of Asylum Management. In B. Shishkov (Ed.), *Business Modeling and Software Design (pp. 268–277)*. Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-36757-1_18

RP14: Hartwich, E., Roth, T., Rieger, A., Zavolokina, L., & Fridgen, G. (2024). Negotiation and Translation Between Discursive Fields: A Study of the Diffusion of Decentralized Finance. *ECIS 2024 Proceedings.* https://aisel.aisnet.org/ecis2024/track20_adoption/track20_adoption/4
Conference Ranking: 3 (GGS Class); B (GGS Rating)

RP15: Weigl, L., Roth, T., Amard, A., & Zavolokina, L. (2023). When Public Values and User-Centricity in e-Government Collide – A Systematic Review. *Government Information Quarterly (Minor Revisions).*
Journal Rating: 17.3 (CiteScore); 3.309 (SNIP)

7.2. Appendix B: Research papers not included in this thesis

Over the course of my dissertation, I also co-authored the following research papers. These works are not part of this thesis.

Journal Papers

- Sedlmeir, J., Rieger, A., Roth, T. & Fridgen, G. (2023). Battling Disinformation with Cryptography. *Nature Machine Intelligence*, *5*, 1056–1057. https://doi.org/10.1038/s42256-023-00733-2
- Rieger, A., Roth, T., Sedlmeir, J., Weigl, L., & Fridgen, G. (2022). Not Yet Another Digital Identity. *Nature Human Behaviour*, *6*(1), 3-3. https://doi.org/10.1038/s41562-021-01243-0
- Rieger, A., Roth, T., Sedlmeir, J., & Fridgen, G. (2021). The Privacy Challenge in the Race for Digital Vaccination Certificates. *Med*, 2(6), 633-634. https://doi.org/10.1016/j.medj.2021.04.018

Journal Papers in the Review Process

- Roth, T., Rieger, A., Utz, M., Fridgen, G., & Young, A. G. (2024). Cultural Sensemaking of Emerging IT in Enactment Fields. *MIS Quarterly (Under Preparation for Re-submission)*.
- Young, A. G., Syed, S., Roth, T., Zhu, Y., & Hevner, A. R. (2024). Ethical Design through Ground and Evaluate (EDGE) Information Systems to Achieve Social Impacts. Journal of Information Technology *(Major Revisions)*.
- Rieger, A., Hartwich, E., Höß, A, Roth, T., Fridgen, G., & Young, A. (2024). Balancing Centralization and Decentralization in Cross-Organizational Digital Infrastructures. *Journal of Information Technology (Major Revisions)*.

Conference Papers

- Brennecke, M., Jurek, D., Rieger, A., & Roth, T. (2024). Towards Social Justice in Energy Transitions: An Information Systems Perspective. *HICCS 2024 Proceedings*. https://hdl.handle.net/10125/107240
- Amard, A., Hartwich, E., Hoess, A., Rieger, A., Roth, T., & Fridgen, G. (2024). Designing Digital Identity Infrastructures: A Taxonomy of Strategic Governance Choices. *HICCS 2024 Proceedings*. https://hdl.handle.net/10125/106646
- Marxen, H., Chemudupaty, R., Fridgen, G., & Roth, T. (2023). Maximizing Smart Charging of EVs: The Impact of Privacy and Money on Data Sharing. *ICIS 2023 Proceedings.* https://aisel.aisnet.org/icis2023/iot_smartcity/iot_smartcity/5
- Lima Baima, R., Roth, T., Berto, L. (2023). Expanding the Scope – Cognitive Robotics Meets NeuroIS. In F. D. Davis, R. Riedl, J. vom Brocke, P-M. Léger, A. B. Randolph, G. R. Müller-Putz

(Eds.), *Information Systems and Neuroscience: NeuroIS Retreat 2023 (Forthcoming)*. Springer Cham.

- Ritchey, J., Dehaghani, Y., Roth, T. (2023). Design of an In-Class Virtual Calm Down Space for Neurodiverse Students. In F. D. Davis, R. Riedl, J. vom Brocke, P-M. Léger, A. B. Randolph, G. R. Müller-Putz (Eds.), *Information Systems and Neuroscience: NeuroIS Retreat 2023 (Forthcoming)*. Springer Cham.

- Weigl, L., Amard, A., Fridgen, G., Marxen, H., Roth, T., & Zavolokina, L. (2022). User-Centricity and Public Values in E-Government: Friend or Foe? *ECIS 2022 Proceedings.* https://aisel.aisnet.org/ecis2022_rp/15

- Sartor, S., Sedlmeir, J., Rieger, A., & Roth, T. (2022). Love at First Sight? A User Experience Study of Self-Sovereign Identity Wallets. *ECIS 2022 Proceedings*. https://aisel.aisnet.org/ecis2022_rp/46

- Amard, A., Hoess, A., Roth, T., Fridgen, G., & Rieger, A. (2022). Guiding Refugees Through European Bureaucracy: Designing a Trustworthy Mobile App for Document Management. In: Drechsler, A., Gerber, A., Hevner, A. (Eds.) *The Transdisciplinary Reach of Design Science Research. DESRIST 2022*. Lecture Notes in Computer Science, vol 13229.

- Höß, A., Roth, T, Sedlmeir, J., Fridgen, G., & Rieger, A. (2022). With or Without Blockchain? Towards a Decentralized, SSI-based eRoaming Architecture. *HICSS 2022 Proceedings*. http://hdl.handle.net/10125/79899

- Amend, J., Fridgen, G., Rieger, A., Roth, T., & Stohr, A. (2021). The Evolution of an Architectural Paradigm: Using Blockchain to Build a Cross-Organizational Enterprise Service Bus. *HICSS 2022 Proceedings*. http://hdl.handle.net/10125/71139

Whitepapers

- Hoess, A., Howard Maclennan, D., Rieger, A., Ermolaev, E., Fridgen, G., & Roth, T. (2022). Issuing and Verifying Digital Diplomas with the European Blockchain Service Infrastructure – Insight from the EBSILUX project. *Ministry for Digitalisation, Luxembourg.*

- Amend, J., Arnold, L., Feulner, S., Fridgen, G., Köhler, F., Ollig, P., Rieger, A., & Roth, T. (2022). Opportunities and Challenges of Using Blockchain Technology in Public Administration – Insights from the FLORA Project of Germany's Federal Office for Migration and Refugees. *Federal Office for Migration and Refugees, Germany.*

7.3. Appendix C: Author contribution statements

Please find below an outline of the author contributions for each research paper included in this thesis. I specifically focus on my individual contributions to the respective papers.

RP1: Blockchain as a Driving Force for Federalism: A Theory of Cross-Organizational Task-Technology Fit

I wrote this paper as a joint primary author together with three subordinate co-authors. I conceptualized the paper based on observations in previously coded project materials. Moreover, I helped with the data curation in the form of setting up the interview guide and co-conducting interviews together with the joint primary author. The third author and I coded all relevant interviews and project materials and I also wrote the first draft of the paper, notably the introduction, background chapter, results, and discussion. During the revision process, I supported the incorporation of the reviewer feedback and re-wrote parts of the manuscript. The other two authors supervised the research and provided feedback.

The following authors have contributed to this research paper: **Roth, Tamara; Stohr Alexander; Amend, Julia; Fridgen, Gilbert; Rieger, Alexander**

RP2: Electricity Powered by Blockchain: A Review with a European Perspective

I wrote this paper as a joint primary author together with four subordinate co-authors. I conceptualized the paper together with the fourth author. The other joint primary author and I curated and analyzed the data. That is, we not only conducted interviews and selected the papers for an in-depth literature review, but also iteratively coded all documents in MAXQDA. The third author supported the coding of some academic literature. I wrote most of the paper and helped visualize key findings. The fourth author edited both the text and visualizations. Authors five and six provided feedback on the technical details.

The following authors have contributed to this research paper: **Roth, Tamara; Utz, Manuel; Baumgarte, Felix; Rieger, Alexander; Sedlmeir, Johannes; Strüker, Jens**

RP3: The Quiet Corner of Web3 that Means Business

This research paper was written by four equal co-authors, including myself. We met frequently to conceptualize the paper based on project insights and develop a coherent storyline. The second author and I each contributed text to their specific projects based on collected and analyzed data, which the first author streamlined into a compelling story. The third author helped develop the background literature. All authors edited and gave feedback on the text for the first draft and subsequent revisions.

The following authors have contributed to this research paper: **Mary Lacity; Carmel, Erran; Young, Amber Grace; Roth, Tamara**

RP4: Organizational Identity Management Policies

This research paper was written by three equal co-authors, including myself, and one subordinate co-author. All three equal co-authors conceptualized the paper. The first author and I wrote the first draft and all three co-authors the revised drafts of the paper. The third author provided input on the technical underpinnings of digital identity management, while the first author and I elaborated on its organizational perspective. All three co-authors edited the research paper. The other subordinate co-authors reviewed the research paper and provided feedback.

The following authors have contributed to this research paper: **Rieger, Alexander; Roth, Tamara; Sedlmeir, Johannes; Fridgen, Gilbert**

RP5: We Need a Broader Debate on the Sustainability of Blockchain

This research paper was written by three equal co-authors, including myself, and one subordinate co-author. All three equal co-authors conceptualized and wrote the paper. I particularly contributed to the introduction, background on different public and private blockchains, and conclusion. The third co-author did the formal analysis relevant to calculating the electricity consumption of different blockchains. The first author validated his calculations and supported the visualization. All equal co-authors worked on the revisions and edited the paper. The other subordinate co-authors reviewed the research paper and provided feedback.

The following authors have contributed to this research paper: **Rieger, Alexander; Roth, Tamara; Sedlmeir, Johannes; Fridgen, Gilbert**

RP6: Transition Pathways Towards Design Principles of Self-Sovereign Identity

The research paper was written by five authors. Four authors, including myself, contributed equally and one author was subordinate. The second author introduced the theoretical frame and gave feedback on the implementation of DSR. The first two authors curated and jointly analyzed the data. I embedded the findings in the design science research cycle and, together with the first author, conceptualized the paper. Moreover, I wrote substantial parts of the paper, including the introduction, the chapters on the development of design principles during the DSR cycle, and discussion, and provided editing. The fourth author gave feedback and supported the second author with the theoretical frame.

The following authors have contributed to this research paper: **Sedlmeir, Johannes; Barbereau, Tom; Huber, Jasmin; Weigl, Linda; Roth, Tamara**

RP7: Managing Fashionable Organizing Visions: Evidence from the European Blockchain Services Infrastructure

This research paper was written by five co-authors, one primary and four subordinate, including myself. I conceptualized the paper idea together with the second author. We also introduced the core theories, that is fashionable IT and organizing vision, to see how our postulated theory in RP13 would behave

when co-dependent technologies are involved. The primary author was responsible for data curation and data analysis. She also wrote a large part of the first draft, which was edited by the second author and me. Moreover, I supported the data analysis as a second coder. The fifth author provided guidance for theory development and the fourth author provided general feedback on the paper.
The following authors have contributed to this research paper: **Hoess, Alexandra; Rieger, Alexander; Roth, Tamara; Fridgen, Gilbert; Young, Amber**

RP8: From Mutualism to Amensalism: A Case Study of Blockchain and Digital Identity Wallets
I wrote this paper as primary author together with two subordinate co-authors. That is, I conceptualized the paper and introduced the core theory, drawing on concepts of population ecology principles of species interaction, loose coupling of systems in organizations, and organizing vision theory. I wrote the research paper and addressed the revisions. The third author supported the data analysis, while the second author provided feedback on the paper.
The following authors have contributed to this research paper: **Roth, Tamara; Rieger, Alexander Hoess, Alexandra**

RP9: From Ambivalence to Trust: Using Blockchain in Customer Loyalty Programs
This research paper was written five co-authors, one primary author four subordinate. I was added to the project as a subordinate co-author in the first round of revisions to develop the theoretical contribution. Specifically, I used my knowledge of the institutional trust literature to establish the core theory and flesh out the paper's contribution and embeddedness in the trust literature. This included rewriting some parts of the theoretical background, results, and discussion chapters. I also helped streamline the DSR methods section and adherence to the method-specific wording in the data analysis chapter. During the second round of revisions, I helped incorporate the reviewer feedback and did some minor editing. The primary author conceptualized the paper and curated the data. He also wrote the first draft of the paper together with the second author and analyzed the data. The other two authors reviewed the research paper and provided feedback.
The following authors have contributed to this research paper: **Utz, Manuel; Johanning, Simon; Roth, Tamara; Bruckner, Thomas; Strüker, Jens**

RP10: Bringing Government into the Digital Age: Insights from Germany's Asylum Procedure
This research paper was written by six co-authors, four of which, including myself, contributed equally and two subordinate co-authors. I conceptualized the paper together with the third author. The two other equal co-authors curated and analyzed the relevant data. They also wrote a first draft of the paper and addressed subsequent revisions based on guidance provided by the third author and me. I also supported the feedback and editing process. The other two co-authors reviewed the research paper and provided feedback.

The following authors have contributed to this research paper: **Amend, Julia; Feulner, Simon; Rieger, Alexander; Roth, Tamara; Fridgen, Gilbert; Guggenberger, Tobias**

RP11: How Organizations Sustain and Navigate Between (De)centralization Equilibria: A Process Model

This research paper was written by six co-authors. Four authors, including myself, were subordinate co-authors. The first two authors were the joint primary authors of this paper, who curated and analyzed the data. They also wrote the first draft of the paper. The third author supervised the research and provided guidance. I also provided guidance, and together with the third author and two joint primary authors, developed the theory. The sixth author and I also edited the manuscript before submission. The fifth author provided general feedback on the paper.

The following authors have contributed to this research paper: **Hartwich, Eduard; Hoess, Alexandra; Rieger, Alexander; Roth, Tamara; Fridgen, Gilbert; Young, Amber**

RP12: The Role of Cultural Fit in the Adoption of Fashionable IT: A Blockchain Case Study

I wrote this paper as primary author together with three subordinate co-authors. That is, I conceputalized the paper and introduced as well as developed the core theory, drawing on concepts from fashionable management, fashionable IT, and the IT-culture conflict literature. I wrote most of the research paper and addressed the revisions. The second and third author provided the case background for their respective cases and supported data curation. The third author supported the data analysis for his case and I did most of the other data analysis. The fourth co-author provided feedback during the paper development and wrote a part of the introduction.

The following authors have contributed to this research paper: **Roth, Tamara; Rieger, Alexander; Utz, Manuel; Young, Amber Grace**

RP13: How IS Affect Social Justice Tensions: A Case Study of Asylum Management

I wrote this paper as primary author together with three subordinate co-authors. That is, I conceputalized the paper and introduced as well as developed the core theory, drawing on concepts from social justice literature. I wrote the research paper and addressed the revisions. Moreover, I curated and analyzed the relevant data (i.e., interviews, project materials). The second author supported this data curation and analysis, while the fourth author edited the paper before submission. The third author provided general feedback on the coherence of paper and logic of our reasoning.

The following authors have contributed to this research paper: **Roth, Tamara; Rieger, Alexander, Fridgen, Gilbert; Young, Amber Grace**

RP14: Negotiation and Translation Between Discursive Fields: A Study on the Diffusion of Decentralized Finance

The paper was written by five co-authors, one primary author and four subordinate, including myself. I conceptualized the paper idea. Moreover, drawing on my background in English linguistic, I introduced the core theory (translation theory and Grice's conversational and conventional implicatures as an expansion of organizing vision theory). This should allow for a deep dive into the negotiation and translation of discursive frames between discursive fields as introduced in RP14. The primary author was responsible for data collection (46 interviews with experts in finance) and we jointly, including the third author, analyzed the data. The primary author wrote the first and second draft, where I contributed to the theoretical background section, discussion, and editing. The third author also edited the paper before and after revision. The other two authors reviewed the research paper and provided feedback.

The following authors have contributed to this research paper: **Hartwich, Eduard; Roth, Tamara; Rieger, Alexander; Zavolokina, Liudmila; Fridgen, Gilbert**

RP15: When Public Values and User-Centricity in e-Government Collide – A Systematic Review

I wrote this paper as a joint primary author together with two subordinate co-authors. The first author conceptualized the paper and initiated the data curation, which was jointly executed by the entire author team. The primary data analysis and theory development was conducted by and iterated between the first author and me. I also wrote parts of the background section, methods section, discussion, and conclusion. Moreover, I reviewed and edited the entire paper before each submission. The third and fourth authors also contributed to the writing of the theory section and the theoretical and practical implications. The first author wrote the introduction, parts of the background section, results, and discussion.

The following authors have contributed to this research paper: **Weigl, Linda; Roth, Tamara; Amard, Alexandre; Zavolokina, Liudmila**

7.4. Appendix D: Appended research papers

RP1: Roth, T., Stohr, A., Amend, J., Fridgen, G., & Rieger, A. (2023). **Blockchain as a driving force for federalism: A theory of cross-organizational task-technology fit.** *International Journal of Information Management*, *68*, 102476. https://doi.org/10.1016/j.ijinfomgt.2022.102476

Journal Rating: 41.9 (CiteScore); 5.266 (SNIP)

International Journal of Information Management 68 (2023) 102476

Contents lists available at ScienceDirect

International Journal of Information Management

journal homepage: www.elsevier.com/locate/ijinfomgt

Research Article

Blockchain as a driving force for federalism: A theory of cross-organizational task-technology fit

Tamara Roth[a], Alexander Stohr[b], Julia Amend[b,c], Gilbert Fridgen[a], Alexander Rieger[a,*]

[a] *SnT - Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg, 29 Avenue John F. Kennedy, 1855 Luxembourg, Luxembourg*

[b] *Project Group Business & Information Systems Engineering of the Fraunhofer FIT, Alter Postweg 101, 86159 Augsburg, Germany*

[c] *FIM Research Center, University of Bayreuth, Wittelsbacherring 10, 95444 Bayreuth, Germany*

ARTICLE INFO

Keywords:
Blockchain
Public sector
Federalism
Organizing principles
Task-technology fit

ABSTRACT

Digital technologies play an important role for the delivery of many public services. However, selecting and adopting the ‘right’ digital technologies is often challenging, especially for federally structured governments. Universal factors for successful adoption are hard to establish, and the particularities of federalism, such as the separation of competencies, complicate technology selection. Nevertheless, blockchain technology seems to flourish in these environments. Through a single-case study on the blockchain project of Germany’s Federal Office for Migration and Refugees, we unpack one essential factor for this success: the fit between (cross-) organizational task structure and technological properties. This fit earns the Federal Office’s project considerable credit and traction with stakeholders and partner authorities – not least because it supports the argument that the digitalization of federal systems is possible without ‘digital centralization’ and redistribution of competencies. Our task-technology fit analysis contributes to a better understanding of the adoption of blockchain in the public sector. It also provides the foundation for an extended task-technology fit theory for federally structured, cross-organizational contexts.

1. Introduction

Digital innovation has come a long way in the public sector. Some small countries like Estonia – one of the world’s most digitally advanced societies (Reynolds, 2016) – already offer most of their public services online. Many larger countries have yet to make similar progress, but targets are ambitious. Germany’s Online Access Act (OZG), for instance, obliges its federal, state, and local governments to offer all public services digitally by the end of 2022 (Federal Ministry of the Interior, Building & Community, 2020). One essential aspect of these digitalization efforts is the selection of the ‘right’ digital technologies (Avgerou & Bonina, 2020; Fairclough, 2003; Goh & Arenas, 2020; Rose, Persson, Heeager, & Irani, 2015); however, selection often proves to be difficult (Avgerou & Bonina, 2020; Rose et al., 2015; Scott, DeLone, & Golden, 2016) due to complex decision-making and accountability systems (Perrons & Cosby, 2020; Rose et al., 2015; Tangi, Janssen, Benedetti, & Noci, 2021; Ziolkowski, Miscione, & Schwabe, 2020). It is particularly challenging in federally structured government systems, which are characterized by a complex separation of competencies and the equal distribution of power between various levels of government and authorities (Berman & Martin, 1983; Biela, Hennl, & Kaiser, 2012; Borriello & Crespy, 2015).

Contrary to general expectations, blockchain technology seems to flourish in this complex environment (Guggenmos, Lockl, Rieger, Wenninger, & Fridgen, 2020; Jensen, Hedman, & Henningsson, 2019; Ølnes, Ubacht, & Janssen, 2017; Rieger, Guggenmos, Lockl, Fridgen, & Urbach, 2019; Seebacher & Schüritz, 2017). This is surprising because federally structured governments typically do not exhibit the same lack of trust evident among organizations involved in many other applications of blockchain (Avgerou & Bonina, 2020; Ziolkowski et al., 2020). Quite the opposite, federally structured governments are characterized by a high-level of trustful cooperation (Amend, Fridgen, Rieger, Roth, & Stohr, 2021; Rieger et al., 2019).

It seems that other factors are at play in this environment that positively influence the adoption of blockchain. Recent research suggests that blockchain adoption is typically the result of contextual (technological, organizational, and environmental) factors and expected benefits, such as coordination and horizontal integration of data

[*] Corresponding author.
E-mail addresses: tamara.roth@uni.lu (T. Roth), alexander.stohr@fit.fraunhofer.de (A. Stohr), julia.amend@fim-rc.de (J. Amend), gilbert.fridgen@uni.lu (G. Fridgen), alexander.rieger@uni.lu (A. Rieger).

https://doi.org/10.1016/j.ijinfomgt.2022.102476
Received 30 December 2020; Received in revised form 15 January 2022; Accepted 17 January 2022
Available online 26 January 2022

Table 1
Extracted organizing principles of federal organizing structures.

Organizing principles of federalism	Definition	Number of papers mentioned in (of 51)
Empowerment	Delegation of decision-making powers to lower levels of government	35
Separation of competencies	Allocation of essential functions to different levels and units of government with the guarantee of autonomy in the responsibilities they perform	28
Cooperation and coordination	Working together and exchanging information to achieve a common goal	30
Organizational flexibility	Ability to adapt to local requirements and changing requirements over time	19

Table 2
Extracted technological properties of private blockchain frameworks.

Technological properties of blockchain	Definition	Number of papers mentioned in (of 52)
Secure and distributed data storage	Cryptographically secure data storage on several nodes resistant to failure and manipulation	46
Selective transparency	Ability to grant limited rights to write and access data in accordance with the role and attributed competencies of involved parties	29
Reliable information sharing and process automation	Secure transmission of data and automated, tamper-resistant execution of predefined process logic	45
Adaptability	Technological adjustability to local requirements and changing requirements over time	35

(Toufaily, Zalan, & Dhaou, 2021). In the financial services industry, for instance, blockchain adoption appears to be driven by technological and economic viability, symbolic benefits associated with a high degree of environment-technology fit, and functional benefits resulting from task-technology fit (Liang, Kohli, Huang, & Li, 2021). Yet, viability and symbolic benefits appear to provide limited explanatory power for federally structured government systems. Viability is a fundamental antecedent rather than a context-specific adoption factor, while symbolic benefits, such as improved social image or conformity with external pressures, appear plausible but not cogent. The same applies to profit maximization considerations (Cho et al., 2021), which are irrelevant for governments. In essence, blockchain adoption appears to be more context-specific (Toufaily et al., 2021) than general frameworks for blockchain adoption suggest (Janssen, Weerakkody, Ismagilova, Sivarajah, & Irani, 2020; Liang et al., 2021; Toufaily et al., 2021). In the analysis that follows, we thus adopt a context-aware perspective on federally structured governments and explore the following research question:

RQ: Why do organizations in federally structured government systems adopt blockchain?

To answer this research question, we conduct a single-case study of a project undertaken by Germany's Federal Office for Migration and Refugees (BAMF) to develop a Federal Blockchain Infrastructure for Asylum Procedures (FLORA). The purpose of FLORA is to improve cross-organizational coordination in Germany's national asylum procedure by ensuring the efficient and secure exchange of process information between all involved authorities. We begin our analysis with a comprehensive literature review that investigates the organizing principles of federally structured government systems and the key technological properties commonly attributed to private blockchain frameworks. We then examine the links between these principles and technological properties in the context of the FLORA project. For this analysis, we draw on task-technology fit (TTF) theory (Goodhue & Thompson, 1995; Zigurs & Buckland, 1998). In line with TTF theory, we find a close fit between the organizing principles of federalism and blockchain's technological properties to be essential for the adoption and use of FLORA. This close fit is also instrumental in securing support for the project among stakeholders and partner authorities.

By revealing how blockchain technology can be employed successfully for the delivery of public services, our study makes an important contribution to both blockchain research and practice. Specifically, our rich analysis unpacks an important driving factor of blockchain adoption in federally structured government systems while offering actionable references and guidelines for meaningful blockchain applications in public service delivery. Our analysis also provides the foundation for an extended TTF theory that is suitable for use at the cross-organizational, federal level. Specifically, we propose a broader perspective that examines tasks at a (cross-)organizational task structure level. Furthermore, we highlight how federal task structures can be shaped by federal values in the form of legal norms.

2. Literature review

In federally structured government systems, cooperation among authorities is difficult to achieve, even with the use of digital technologies (Goh & Arenas, 2020; Shevory, 2015). Different competencies (Egeberg, 2001; Jaeger, 2002; Moya Palencia, 1974), organization-specific procedures (Berman & Martin, 1983; Ebinger & Richter, 2015; Fossum & Jachtenfuchs, 2017; Keating, 2017; Watts, 1998), and established organizational identities (Jaeger, 2002; Tyworth, 2014) can hamper digital innovation efforts (Davis, 1989; Seltsikas & O'Keefe, 2010). From a purely technical perspective, there are various technologies capable of meeting the requirements of these contexts. Yet, many technological options do not progress beyond pilot projects (Carson, Romanelli, Walsh, & Zhumaev, 2018) because digital innovation in the public sector – and particularly in federally structured government systems – is driven by more complex considerations and challenges than just technological feasibility (Carter & Bélanger, 2005; Hughes et al., 2019; Scott et al., 2016). Goh and Arenas (2020) provide a valuable summary of these non-technical considerations and challenges. Many of them, such as system complexity (Avgerou & Bonina, 2020; Cordella & Willcocks, 2012; Wibbels, 2006), cooperation in a protected environment (Dawson, Denford, Williams, Preston, & Desouza, 2016; Deringer & Molnar, 1983), and organizational cultural values (Leidner & Kayworth, 2006; Seltsikas & O'Keefe, 2010), are a direct result of federal organizing structures that, in turn, have their origin in shared federal values.

To better understand these structures and values, we carefully reviewed a total of 51 political science papers on federalism, federal organization, and e-governance in federally structured organizations. Furthermore, we analyzed 52 computer science and IS papers on the use of blockchain technology. This analysis revealed four basic principles inherent to federally organized contexts (see Table 1) and four key technological properties of private blockchain frameworks (see Table 2). It also informed a summary of recent research on blockchain adoption, on which we build in arguing that blockchain adoption requires context-specific considerations. While adoption research provides various frameworks and theories for these considerations, we found Goodhue and Thompson's (1995) task-technology fit (TTF) theory to be particularly conducive to our investigation.

2.1. Federal values and organizing principles

Federalism has its roots in the Latin word *foedus* meaning 'league', 'treaty' or 'compact', and has come to represent an "[…] organization in which the activities […] are divided between [decentral] and a central government in such a way that each kind of government has some activities on which it makes final decisions" (Riker, 1964). Federalism is not simply a form of organizing but also an ideology that can be traced back to the teachings of Plato (Inman, 2007). Over time, it has been endowed with multiple fundamental values and become a veritable cultural heritage (Chemerinsky, 1995). These fundamental values encompass, for instance, shared authority and decision-making (Grant & Tan, 2013), political balance (Erk & Koning, 2009; Moya Palencia, 1974), security and protection, fairness (Smith & Fernandez, 2010), and individual as well as communal freedom (Fossum & Jachtenfuchs, 2017; Wibbels, 2006). They represent "a set of beliefs about how the social world operates" (Ingram & Simons, 2000). Federal values are typically enacted in legal norms "at all levels of government" (Jaeger, 2002). These legal norms are also the basis of federal organizing principles. These organizing principles, in turn, play an important role in the shaping of cross-organizational procedures (Goh & Arenas, 2020; Shevory, 2015). By way of a comprehensive analysis of 51 political science papers, we could characterize four such organizing principles (see Table 1; detailed results of our analysis can be found in Table A1).

The first principle is *empowerment*. It grants authorities at different hierarchical levels equal status in decision-making processes (Egeberg, 2001; Grant & Tan, 2013; Moya Palencia, 1974). Simultaneously, it helps to retain individual organizational identities and the independence of central bodies (Bormann et al., 2019; Erk & Koning, 2009; Jaeger, 2002; Mackenzie, 2010). In federal systems, authorities are given the "power to" rather than "power over" (Heeks & Stanforth, 2007). Chemerinsky (1995) describes this set-up as "the greatest beauty of federalism since multiple levels of organization share the same interests and have each the ability to act."

The second principle is the *separation of competencies* between authorities at different levels. It promotes a complex, balanced system of self-rule and shared rule (Auer, 2005; Mckay, 2005). In federal systems, each authority has specific, predefined functions (Berman & Martin, 1983; Biela et al., 2012; Borriello & Crespy, 2015), which are usually associated with the allocation of certain powers and the respective accountability for procedures related to organizational functions (Conlan, 2006; Erk & Koning, 2009). The *separation of competencies* is often complemented by an accessory principle of subsidiarity, which specifies that a given task be delegated to the level best equipped to deal with it. Only tasks that cannot be effectively processed at a lower level should be transferred to the next higher (Abels, 2019; Ebinger & Richter, 2015; Keating, 2017).

The third principle, *cooperation and coordination*, is a direct consequence of the *separation of competencies* between authorities at different hierarchical levels (Handy, 1996; Watts, 1998), as some tasks are jointly exercised or functionally organized (Benson & Jordan, 2014; Mackenzie, 2010; Springer, 1962). Authorities in federal systems often cooperate where they could act autonomously – for instance, to exchange information on legal questions or to handle joint procedures (Ebinger & Richter, 2015; Rieger et al., 2019). In general, these authorities coordinate their actions where it is deemed useful, emphasizing coordination from both a bottom-up and top-down approach (Heeks & Stanforth, 2007; Hegele & Behnke, 2017).

The fourth organizing principle is *organizational flexibility*. The fact that federal systems push essential functions to the lowest levels means that decisions can be made independently, quickly, and accurately (Biela et al., 2012; Conlan, 2006; Erk & Koning, 2009; Graham, 1980). Varying degrees of push and pull across the different levels likewise encourage diversity among authorities, providing opportunities for innovation and activism (Egeberg, 2001; Fossum & Jachtenfuchs, 2017; Nathan, 2006). This also includes the flexible design of organizational structures with different degrees of centralization or decentralization (Auer, 2005; Keating, 2017; Tiller, 2011). Such flexibility may help authorities respond to critical situations (Conlan, 2006).

2.2. Technological properties of blockchain

The four identified organizing principles make it notably more challenging to find suitable digital technologies for federally structured government systems (Benbunan-Fich, Desouza, & Andersen, 2020). Despite these challenges, blockchain technology appears to be successful in this environment (Abramowicz, 2020; Treiblmaier et al., 2021; Ziolkowski et al., 2020). Blockchains are databases that store transactions in a transparent, chronological, and tamper-resistant way in a distributed network (Carvalho, Merhout, Kadiyala, & Bentley, 2021; Upadhyay, 2020; Warkentin & Orgeron, 2020). A blockchain consists of a chronologically ordered chain of blocks. Each block contains information about valid network activities since the last addition of the previous block (Andoni et al., 2019; Sedlmeir, Buhl, Fridgen, & Keller, 2020; Upadhyay, 2020). In the past few years, blockchain technology has gained considerable traction due to its various possible applications both in the public and private sector (Benbunan-Fich et al., 2020; Mattke, Maier, Hund, & Weitzel, 2019; Upadhyay, 2020; Ziolkowski et al., 2020).

Blockchain technology is as versatile as its applications, and the same can be said of its technological characteristics. This is evident, for instance, in the list of 11 observed characteristics that Seebacher and Schüritz (2017) compiled to give a nuanced view of the nature (Weber, 2005) of blockchain technology. These characteristics include *trust*, *immutability*, *redundancy*, *versatility*, and *automation*. There is some disagreement, however, as to whether certain characteristics, such as *trust*, are characteristics in their own right or rather the by-product of other more fundamental characteristics (Amend, Kaiser, Uhlig, Urbach, & Völter, 2021; Marella, Upreti, Merikivi, & Tuunainen, 2020; Ostern, 2018). To steer clear of these debates, we decided not to focus on blockchain's general nature but instead describe the behavior of private blockchain frameworks, as typically used in federally organized contexts. To this end, we analyzed the aforementioned 52 IS and computer science papers for 'properties' of private blockchain frameworks that are not only relevant to cooperation in federally organized contexts but also uncontested. The four key properties we identified can be found in Table 2, and the detailed results of our analysis in Table A2.

The first of the four properties is *secure and distributed data storage* (Ahl et al., 2020; Andoni et al., 2019; Chapron, 2017; Kranz, Nagel, & Yoo, 2019). Transactions, such as the steps of a public procedure, can be grouped into "blocks" and cryptographically added to a data "chain" with copies stored on all participating "nodes" (Khaqqi, Sikorski, Hadinoto, & Kraft, 2018; Morstyn, Farrell, Darby, & McCulloch, 2018; Pedersen, Risius, & Beck, 2019; Thomas, Zhou, Long, Wu, & Jenkins, 2019). This minimizes vulnerability to failure and attacks and creates a highly tamper-resistant data structure wherein manipulations are easily identified (Hughes et al., 2019; Kranz, Nagel, & Yoo, 2019; Sedlmeir et al., 2020; Sousa et al., 2019).

Second, private blockchain frameworks enable *selective transparency*. This means that authorities can be granted limited rights to input and access data, dependent on their role in the respective procedures (Noor, Yang, Guo, van Dam, & Wang, 2018; Ølnes et al., 2017; Perrons & Cosby, 2020; Rieger et al., 2019). This reduces complexity by maintaining the common shared truth and necessary transparency without disclosing information that either should not or may not be accessed (Hawlitschek, Notheisen, & Teubner, 2018; Mattke et al., 2019; Rieger et al., 2019). *Selective transparency* depends on *secure and distributed data storage.* While the latter property enables cross-organizational cooperation and considers frequently changing procedural setups, desired levels of transparency may also change dependent on the responsibilities of involved organizations (Iansiti & Lakhani, 2017; Risius & Spohrer, 2017).

Third, private blockchain frameworks support *reliable information sharing and process automation* (Rossi, Mueller-Bloch, Thatcher, & Beck, 2019; Sikorski, Haughton, & Kraft, 2017; Sousa et al., 2019; Ziolkowski et al., 2020). *Reliable information sharing* builds on the previous two properties: While *secure and distributed data storage* guarantees the

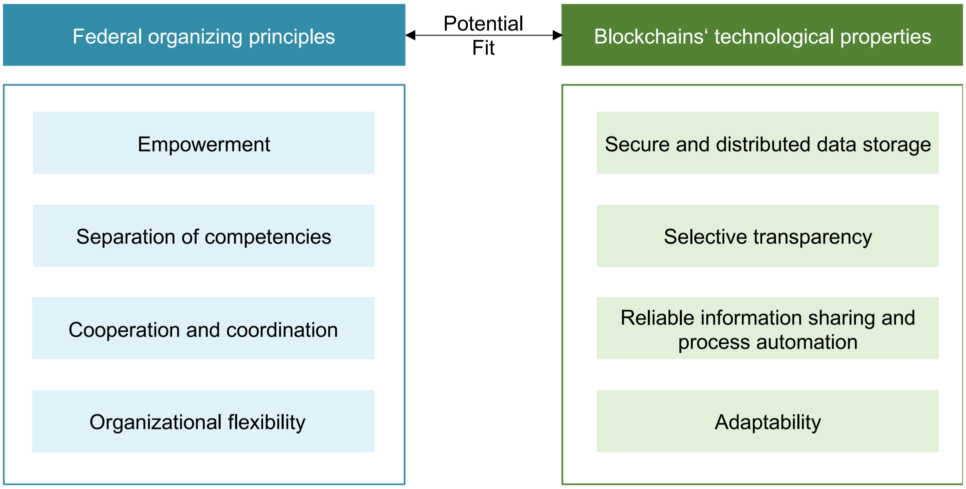

Federal organizing principles
Potential Fit
Blockchains‘ technological properties
Empowerment
Separation of competencies
Cooperation and coordination
Organizational flexibility
Secure and distributed data storage
Selective transparency
Reliable information sharing and process automation
Adaptability

Fig. 1. Apparent commonalties between the technological and organizational dimensions.

authenticity of shared information (Mattila & Seppälä, 2018; Perrons & Cosby, 2020; Sedlmeir et al., 2020), private blockchain frameworks can – depending on the allocated competencies – reliably disseminate important information in near real-time with *selective transparency*. That is, all actors involved in a particular procedure receive timely updates (Iansiti & Lakhani, 2017; Rieger et al., 2019; Risius & Spohrer, 2017). The use of smart contracts additionally permits *process automation* via the creation of automated triggers for certain steps of the process and extensive monitoring capabilities (Kranz et al., 2019; Lauslahti, Mattila, Hukkinen, & Seppälä, 2018; Rieger et al., 2019).

Fourthly, private blockchain frameworks ensure a certain degree of *adaptability* as the design of the network and the rules for information processing can differ locally and be adjusted over time to meet local particularities and changing requirements (Andersen & Ingram Bogusz, 2019). This *adaptability* is crucial in cross-organizational contexts, where one technological solution needs to suit various cooperation scenarios (Jensen et al., 2019; Kshetri, 2018; Ziolkowski et al., 2020).

2.3. Blockchain adoption

While most early blockchain research examined technological aspects, the focus is increasingly shifting toward studying blockchain's adoption and use (Janssen et al., 2020). Blockchain adoption research has identified certain factors as strong indicators of the desirability and viability of blockchain applications. These include the need for a shared common and immutable database or the avoidance of trusted third parties (Pedersen et al., 2019). Yet, blockchain adoption typically remains a case-specific phenomenon that can require an extensive experimentation phase to establish whether the technology is fit for purpose (Du, Pan, Leidner, & Ying, 2019).

In general, blockchain adoption is influenced by various interacting and mutually dependent contextual factors. These factors can be technological (e.g., technological complexity and readiness), organizational or institutional (e.g., governance, norms, and culture), and environmental or market-based (e.g., regulation and network effects) (Du et al., 2019; Janssen et al., 2020; Toufaily et al., 2021). Concerns about the maturity of blockchain technology, for instance, can significantly slow down its adoption (Jensen et al., 2019). When these concerns result in ambivalence or distrust, they can even be fatal (Bélanger and Carter, 2008). Successful blockchain adoption, in turn, requires organizations and their representatives to trust the technology (Marella et al., 2020; Ostern, 2018; Rossi et al., 2019) even though established IS trust signals may not be effective in this context (Völter, Urbach, & Padget, 2021).

Moreover, expected benefits and the (economic) viability of blockchain applications can vary substantially (Ostern, Rosemann, & Moormann, 2020; Sarker, Henningsson, Jensen, & Hedman, 2021; Toufaily et al., 2021). The expected benefits may be symbolic (e.g., image and reputation) or functional (e.g., efficiency and financial performance) (Grover, Chiang, Liang, & Zhang, 2018). Symbolic benefits may emerge from a close fit between contextual factors and blockchain technology. Functional benefits can result, for instance, from a close fit between organizational tasks and technology (Liang et al., 2021). Viability, in turn, determines whether the expected benefits can be realized (Liang et al., 2021; Ostern et al., 2020). Benefit and viability considerations can also differ between organization types. Companies typically evaluate blockchain applications based on their return on investment (Cho et al., 2021). Industry incumbents may seek this return from business process improvements and disintermediation, while start-ups may benefit from entirely new business model opportunities (Toufaily et al., 2021). Governments, on the other hand, may benefit from coordination and horizontal data integration as well as increased efficiency in delivering public services (Toufaily et al., 2021).

Contextualization is thus crucial for investigating blockchain adoption. This means that the particularities of each context – in our case, federalism - require a context-specific analysis (Toufaily et al., 2021) to identify relevant contextual factors and benefits (Guggenmos et al., 2020; Ølnes et al., 2017; Rieger et al., 2019; Toufaily et al., 2021). Insights and perspectives from other contexts may nevertheless provide a valuable starting-point. In our case, such a starting point is provided by task-technology fit.

2.4. Task-technology fit

IS research has a long tradition of studying technology adoption and, over time, many different frameworks and theories have been developed in these studies. Naturally, some of these frameworks are also used for blockchain research. Prominent examples are the technology-organization-environment (TOE) framework (Toufaily et al., 2021), diffusion of innovations (DOI) theory (Toufaily et al., 2021), and TTF (Liang et al., 2021). While the TOE framework focuses on the mutually dependent influence of technological, organizational, and environmental factors (Tornatzky & Fleischer, 1990), DOI theory emphasizes (perceived) aspects of the innovation itself, such as the speed of its diffusion, relative advantage, compatibility, and complexity (Rogers, 1995). TTF theory, in turn, builds on the idea that a technology's use or impact on performance depends on its fit or alignment with the tasks to be performed (Goodhue & Thompson, 1995). Insights from the financial services industry suggest that TTF can be an important driver for blockchain adoption (Liang et al., 2021). Our analysis of the organizing principles of federalism and the technological properties of private blockchain frameworks appears to support this notion for federally structured governments (see Fig. 1). Hence, we adopted TTF as the theoretical lens for our investigation.

Goodhue and Thompson (1995) originally introduced the concept of TTF as "the degree to which a technology assists an individual in performing his or her portfolio of tasks". Researchers have since refined and extended TTF theory in several studies (Furneaux, 2012; Howard & Rose, 2019; Zigurs & Buckland, 1998; Zigurs & Khazanchi, 2008). The fundamental premise of the theory, however, has remained constant (Furneaux, 2012). TTF theory argues that a technology's use or impact on performance depends on its fit or alignment with the task to be performed by an individual (Goodhue & Thompson, 1995) or a group (Zigurs & Buckland, 1998; Zigurs & Khazanchi, 2008). What this means is that TTF theory lends itself to multiple levels of analysis, individual or group, depending on the technology being studied (Furneaux, 2012). TTF theory is particularly useful for highlighting the interactive effects of tasks and technologies. In doing so, it accounts for the significance of the contexts in which technologies are applied (Howard & Rose, 2019).

TTF's basic constructs and links are very flexible in terms of adaptions and extensions. Trkman (2010), for instance, integrates contingency, dynamic capability, and TTF theory to postulate that continuous improvement alongside a good fit of business process tasks and information systems are critical success factors for business process management in organizations. Oliveira, Faria, Thomas, and Popovič (2014) combine TTF, the unified theory of acceptance and usage of technology (UTAUT), and the initial trust model (ITM) to better understand the facilitating conditions and behavioral intentions involved in the adoption of mobile banking. Huang, Zhang, and Liu (2017) use TTF theory to better understand how the technological characteristics of Massive Open Online Courses (MOOC) affect student revisits. Wang, Wang, Zhang, and Ma (2020) use an extended model of user-task-technology fit with two additional elements – job fit and professional fit – to discover that both elements are an integral part of the spillover mechanism between IT satisfaction and job satisfaction.

Although existing conceptualizations of TTF are rather organization-centric and lack consideration of cross-organizational aspects, we find TTF to be an interesting theoretical lens for our investigation. The apparent commonalities between federal organizing principles and blockchain's technological properties clearly indicate that TTF could help to better understand why organizations in federally structured government systems adopt blockchain. Moreover, recent research both demonstrates that TTF may be an interesting driver for blockchain adoption and explicitly calls for cross-organizational considerations (Liang et al., 2021).

When applying TTF, it is important to clearly conceptualize the 'tasks' and 'fit' in question, since both are abstract constructs with multiple potential conceptualizations (Zigurs & Buckland, 1998; Zigurs & Khazanchi, 2008). Tasks can be described and distinguished in various ways – for instance, by characteristics such as complexity, analyzability, and equivocality (Brown, Dennis, & Venkatesh, 2010; Zigurs & Buckland, 1998). Generally speaking, tasks can be conceptualized in four ways: *task qua task*, *task as behavior requirement*, *task as behavior description*, and *task as ability requirement* (Hackman, 1969). TTF theory typically draws on the first two conceptualizations (Zigurs & Buckland, 1998)*: task qua task* captures the task's specific attributes and the stimuli involved, and *task as behavior requirement* accounts for the 'what to do' and 'how to do' that are necessary to achieve particular goals (Hackman, 1969; Zigurs & Buckland, 1998). *Task as behavior description* and *task as ability requirement* are typically less relevant to TTF theory as they do not focus on the properties of the task itself but on outcomes and characteristics of the entities performing the task (Zigurs & Buckland, 1998).

Likewise, fit can assume many different forms (Venkatraman, 1989). Prior research on TTF theory has typically used three concepts of fit: *fit as moderation*, *fit as matching*, and *fit as profile deviation* (Cane & McCarthy, 2009). While *fit as moderation* refers to the interaction between certain technology, task, and individual/group characteristics, *fit as matching* conceptualizes fit as a more direct relationship between task and technology. The third of these conceptualizations, *fit as profile deviation,* treats fit as the adherence to an ideal task-technology profile and is particularly suitable for more theoretical analyses (Cane & McCarthy, 2009; Howard & Rose, 2019; Venkatraman, 1989).

3. Research design

To leverage the TTF lens in our investigation of the presumed fit between federal organizing principles and blockchain technology, we chose a qualitative-empirical research design. Such a design enables the development of an in-depth understanding of emerging phenomena (Bettis, Gambardella, Helfat, & Mitchell, 2015). More specifically, we conducted a single-case study based on the FLORA blockchain project of Germany's Federal Office for Migration and Refugees (BAMF). Thereby, we follow the recommendations of Yin (2014). According to these recommendations, a single-case study design is appropriate if the case is critical, unusual, common, longitudinal, or revelatory. A critical case is one that is key to a researcher's theory or theoretical proposition. An unusual case is one that deviates from certain theoretical norms or everyday events. A common case reflects everyday situations and aims to elicit social phenomena, whereas a longitudinal single-case study examines the same case at different points over time (Yin, 2014). We regard the BAMF's blockchain project as a revelatory case because it provides access to a phenomenon that researchers have previously been unable to study (Yin, 2014): the adoption of blockchain technology in a federally organized government context. Blockchain adoption has been studied in private sector settings, such as global shipping (Sarker et al., 2021), insurance (W. Zhang, Wei, Jiang, Peng, & Zhao, 2021), or financial services and health care (Liang et al., 2021) but using blockchain for cross-authority cooperation in the public sector is still a new phenomenon.

The BAMF and some of its partner authorities already use blockchain in day-to-day operations. This makes the project one of the most advanced of its kind. It offers detailed insights into why blockchain may be interesting to public authorities. At the same time, it reveals how these authorities can use blockchain for cross-organizational cooperation. As blockchain is an important technology both in Germany and the wider European Union (EU), the BAMF's project has also become a reference project, which creates added pressure of expectation. Accordingly, the 'phenomenon under investigation' is not only of notable interest in its own right but may also have complex ramifications for both scientific and political communities. These circumstances justify the use of a single-case study (Eisenhardt & Graebner, 2007; Eisenhardt, 1989; Yin, 2014).

3.1. Case description

The German asylum procedure involves close collaboration between various authorities at the local, state, and federal levels, with the BAMF playing a pivotal role in handling and issuing decisions regarding asylum applications. However, federal separation of competencies often prevents 'digital centralization' and redistribution of competencies to a central authority in the procedure. The BAMF thus often explores 'decentralized' technical alternatives that require neither the extension of centralized databases nor the delegation of control to a single authority. As part of these innovation exercises, the BAMF decided to also investigate blockchain technology.

The BAMF began with a proof-of-concept (PoC) in January 2018. Based on positive experiences from the PoC, the BAMF then initiated FLORA, a joint pilot project with Saxony's central immigration authority in Dresden. The objective of this project was to develop and evaluate a blockchain-based system for the coordination of asylum procedures. Upon successful completion of the pilot in the fall of 2021, the BAMF began to roll out the system to other German states. The overall goal is to ensure the efficient and secure exchange of process information between

Table 3
Coding examples from our data analysis process.

1st stage	2nd stage	Aggregate dimensions
- Getting more transparency (e.g., interviews 1, 3, 19, 24) - More substantiated decision-making (e.g., interview 9, 11, 13, 20)	Human control	Empowerment
- Respecting organizations' range of tasks (e.g., interviews 7, 8, 10, 25) - Limiting access to sensitive data (e.g., interviews 5, 6, 18, 22)	Separation of inter-organizational responsibilities	Separation of competencies
- Making processes more efficient (e.g., interviews 7, 13, 18, 25) - Reducing data disruption (e.g., interviews 1, 4, 7, 25)	Strategic coordination	Cooperation & coordination
- Supporting both micro- and macro flows (e.g., interviews 5, 7, 13, 17) - Adapting to organization's legacy systems (e.g., interviews 1, 2, 5, 7)	Changing procedures	Organizational flexibility

the relevant authorities.

To address these objectives, the BAMF developed an application with a multi-layered architecture that takes advantage of the benefits of blockchain and, at the same time, allows for the integration of existing IT applications and services (Amend, Fridgen, et al., 2021). For the blockchain part of the application, the BAMF uses Hyperledger Fabric, a private blockchain framework that emphasizes privacy as well as flexibility (Linux Foundation, 2017; Osterland & Rose, 2018). In particular, Hyperledger Fabric provides features that allow for compliance with the EU's General Data Protection Regulation (GDPR) (Guggenmos et al., 2020; Rieger et al., 2019). Besides being a private and permissioned framework wherein only authenticated and authorized participants can view, execute, and validate transactions (Beck, Müller-Bloch, & King, 2018), it enables the sharing of data with selected participants via so-called private data collections (PDCs). As a result, the BAMF's blockchain application provides relevant authorities with an efficient, secure, and GDPR-compliant means to exchange process information, which allows effective cross-organizational process coordination.

The success of the BAMF's blockchain application has attracted considerable attention on a national and international level. For instance, it won the award for best digitalization project at the federal and state level in the 2019 German eGovernment competition. Since the second half of 2020, the BAMF has also acted as the convening authority for the European Blockchain Partnership (EBP) and its working group on the use of the EBP's European Blockchain Service Infrastructure (EBSI) for cross-border asylum procedures.

3.2. Data collection and analysis

Case studies commonly draw on a combination of the following six sources of evidence: interviews, documentation, direct observations, participant-observations, archival records, and physical artifacts (Yin, 2014). To triangulate our findings, we built our case study upon three of these sources – namely interviews, documentation, and direct observations (Myers & Newman, 2007; Yin, 2014).

Our primary method of data collection was semi-structured interviews. These were conducted using an interview guide which helped to ensure comprehensive coverage of the subject area (Rubin & Rubin, 2005). Semi-structured interviews can generate rich data that provide deep, detailed, and authentic insights into the interviewees' inner worlds and their social realities (Leech, 2002; Schultze & Avital, 2011). The protocol of our semi-structured interviews involved a brief introduction followed by questions on interviewees' perceptions of cultural and organizational particularities in the public sector and the BAMF, and on the opportunities, challenges, and success factors for blockchain projects in this context. During the interviews, we adapted the questions to shift the focus depending on the respective interviewee's knowledge and actual expertise (Myers & Newman, 2007). We mirrored the interviewees' verbal posture and vocabulary and allowed the interviewees to go in directions that they found interesting (Orlikowski & Baroudi, 1991). In selecting our interviewees (Table B2), we focused on incorporating a broad variety of perspectives on the case. That is, we selected interviewees with technical expertise and in-depth knowledge of the asylum procedure. Likewise, we included the perspectives of BAMF employees as well as those of external consultants and IT service providers. Moreover, we chose interviewees from different hierarchical levels, such as higher management and case workers, and we balanced interviewees who were deeply involved in the project with interviewees with an outsider's perspective. At the end of each interview, we also asked the participants to suggest other potential interviewees. Overall, we conducted a total of 25 interviews. Our interviews lasted between 30 and 60 min, were audio-recorded and, afterward, fully transcribed. To establish consistency and comparability, all interviews were conducted by the same interviewer. In a few cases, another member of the author team, who the interviewee knew well, joined the interview to establish trust, but mainly remained in the background. In some cases, we approached the interviewee after the interview to clarify their statements and responses. To increase construct validity, we also obtained interviewees' feedback on the draft case study reports (Yin, 2014).

Some of the authors have accompanied and evaluated the BAMF's FLORA project since it began in January 2018. This meant that we could also draw from a comprehensive database of additional information to triangulate our findings (see Table B1). In particular, we analyzed over 400 pages of documentation on the collaboration software *Confluence* and over 200 pages of technical concepts and functional specifications. Moreover, we gathered field observations from bi-weekly sprint reviews, management meetings, and over 20 project workshops with different departments, authorities, and organizations.

We used qualitative analysis techniques and the analysis software MAXQDA to analyze our data (Mayring, 2014). We undertook three stages of data analysis: open, axial, and selective coding (Corbin & Strauss, 1990). First, we analyzed the data individually and assigned initial codes. During this stage, the research team met regularly to review emerging concepts and ensure the consistency of coding (Klein & Myers, 1999; Pan & Tan, 2011). In the second stage, we clustered the codes across data sources and assigned them to higher-level themes, which were either based on our theoretical lens (deductive coding) or emerged during data collection (inductive coding). In the final stage, we selected the core categories and related the established themes to these categories. This process led us to approximately 5000 codified statements, organized into four categories and seven sub-categories or themes. Table 3 provides an exemplary overview of our coding.

4. Findings

4.1. Replicability of federal organizing principles

From our analysis of the FLORA project, we identified various organizational characteristics that focus either on business requirements or on the intra- and inter-organizational specifics of the asylum procedure. These can be grouped into the same organizing principles outlined in our literature review of federalism, federal organization, and e-governance in federally structured organizations (see Fig. 2).

The interviewees and project documents repeatedly mentioned the organizing principles as crucial characteristics of organizations in federal contexts. The principles were either explicitly referenced or could be inferred from paraphrases. Most frequently mentioned by both

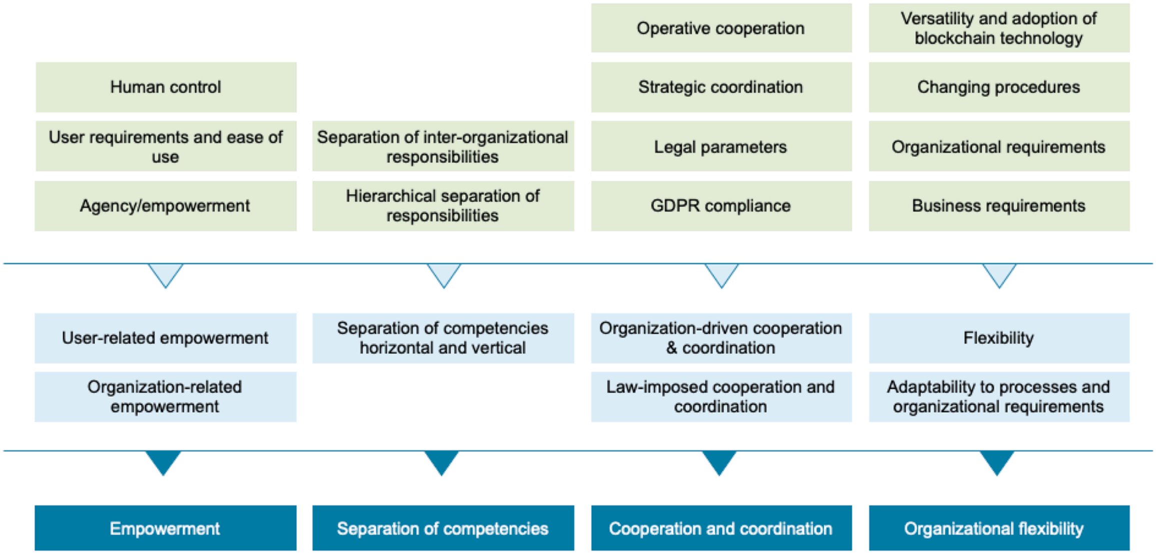

Operative cooperation
Versatility and adoption of blockchain technology
Human control
Strategic coordination
Changing procedures
User requirements and ease of use
Separation of inter-organizational responsibilities
Legal parameters
Organizational requirements
Agency/empowerment
Hierarchical separation of responsibilities
GDPR compliance
Business requirements
User-related empowerment
Separation of competencies horizontal and vertical
Organization-driven cooperation & coordination
Flexibility
Organization-related empowerment
Law-imposed cooperation and coordination
Adaptability to processes and organizational requirements
Empowerment
Separation of competencies
Cooperation and coordination
Organizational flexibility

Fig. 2. Organizing principles as replicated from interviews and project materials.

Table 4
Matches between federal organizing principles and technological properties of blockchain technology as identified in interviews (overall 25) and project materials (overall 30).

		Organizing principles of federalism			
		Empowerment	**Separation of competencies**	**Cooperation and coordination**	**Organizational flexibility**
		Number of Interviews + Number of Project Documents			
Technological properties of blockchain	**Secure and distributed data storage**	19 + 24	15 + 24	0 + 0	0 + 0
	Selective transparency	10 + 17	16 + 24	0 + 0	10 + 13
	Reliable information sharing and process automation	17 + 22	15 + 13	16 + 23	13 + 15
	Adaptability	16 + 16	16 + 14	13 + 12	13 + 14

interviewees and documents were the of principles of *empowerment* and *separation of competencies* followed by *cooperation and coordination* and *organizational flexibility*.

4.2. Matching of organizing principles and technological properties

Our analysis of the FLORA project also revealed that blockchain can effectively reflect, and even drive, the four organizing principles of federally structured governments. Our initial examination of relevant literature had already suggested that the technological properties of blockchain might match to the organizing principles of federally organized structures (and thus produce a close TTF), and our case study findings corroborate and substantiate this fit (see Table 4). Moreover, the recognition and presentation of blockchain as a technical agent of federalism encouraged the BAMF's partner authorities to support the project and adopt the technology. Apart from substantiating TTF, our findings also support the notion that organizing principles are reflections of legal norms based on federal values. That is, task in federally organized structures needs to be extended by a value-law-dimension that better reflects the origin of tasks.

To determine possible matches between blockchain and organizing principles, we examined the interview transcripts and project documents at those points where we had identified statements related to one or more of the four organizing principles. Where interviewees or project documents did not merely elaborate on organizing principles but referred to a fit between a specific technological property and organizing principles, we tagged this section and labeled the match accordingly. We then counted the interviews and project documents that mentioned a match between a particular organizing principle and a technological property (see Table 4). A higher number of mentions indicates a higher potency in the match. If neither the interviews nor the project documents indicated a match between a particular organizing principle and technological property, we report it as '0 + 0'.

4.2.1. Empowerment

Empowerment at both the organizational and user level is integral to the BAMF's FLORA project. *Empowerment* is supported by all four technological properties, as indicated in Table 4. Since many different organizations are involved in the German asylum procedure, an underlying technology should *"reflect the independence and autonomy of individual authorities and also […] address their needs"* (Interviewee 20).

Blockchain's *secure and distributed data storage* seems to meet this requirement at its most basic level. All participating authorities have access to a common ledger. This ledger contains cryptographic hashes of all status messages processed by the application for verification purposes. Moreover, the participating authorities have access to private ledgers: the *PDCs*. These *PDCs* allow data to be shared only between a subset of participants, which *"enables cooperation that facilitates data flow between organizations, while granting substantial freedom to individual organizations"* (Interviewee 15).

The distinction between common and private ledgers also highlights how blockchain's *selective transparency* can contribute to *empowerment*. Depending on their respective competencies, different authorities have access rights to different *PDCs*. As a result, the participating authorities can establish a common shared truth while emphasizing their autonomy and driving *empowerment*. In the words of Interviewee 1:

> "*Blockchain offers the possibility of mapping regional differences, leaves enough room for [individual changes], and still allows for standardization where appropriate. As a result, the technology strengthens autonomy at a local level, and federal structures are preserved and even driven.*"

Empowerment is also supported by *reliable information sharing and process automation* as well as *adaptability*. The FLORA application ensures that all competent authorities involved in a particular asylum procedure receive timely and often automated updates about important steps. These timely updates enable them to operate confidently and in a well-informed manner. As the participating authorities often have different regional structures, the *adaptability* of the Hyperledger Fabric framework also gives them the freedom to retain these structures while cooperating in various organizational scenarios. Interviewees 7 and 32 explain:

> *"Blockchain is the perfect technology to enable digital collaboration between the national and state governments. You can tell that this technology has been well received as it enables reliable and flexible collaboration not just between two agencies, or two groups, or two departments but at all different levels of organizing"*.

> *"What is usually discussed here is that blockchain technology can be used to directly and transparently execute processes between different actors in a tamper-proof manner; that individual processes can be automated, especially on the basis of smart contracts, which is expected to reduce potential errors and to increase process integrity by automatically integrating different process steps."*

4.2.2. Separation of competencies

The FLORA application supports the *separation of competencies* across the participating authorities. Particularly relevant in this regard is blockchain's *secure and distributed data storage*. Since *"[particularly] in Germany there is federalism and the separation of competencies, which – at a broader level – reflects the separation of powers"* (Interviewee 14), authorities value data control and tamper-resistance. Interviewee 19 explains that the FLORA application is:

> *"good for federal authorities because each authority has access to its data and it sees all [relevant] data, and [because FLORA] ensures that data has not been changed by somebody else. There are mathematic guarantees ensuring that data has not been changed."*

Separation of competencies also includes the individuality and rights of different authorities. FLORA addresses these expectations with *selective transparency*, as described by Interviewee 20:

> *"Authorities are very different in how they handle data that is stored on the blockchain, and which information is relevant to them. And they also want it that way. They want to be able to explicitly decide how specific connections should be made or how the data stored on the blockchain should be handled and into which system [the data] should be transferred in their own microcosm. That is, […] primarily the independence and autonomy of the individual authorities should be considered. You simply can't be cooperating 'too closely'."*

The authorities involved in the German asylum procedure place particular emphasis on their autonomy to implement new technologies for cooperation and realize the associated possibilities for action. Yet, at a cross-authority level, it is essential to maintain an adequate degree of *reliable information sharing and process automation*. To this end, authorities exchange large amounts of information, albeit often via spreadsheets and fax messages, which is cumbersome and error-prone. *"Blockchain is supposed to improve such [still paper-based] processes, especially in cross-organizational procedures, so that everything is digitalized and traceable" (Interviewee 11).* Specifically, Hyperledger Fabric's *PDCs* offer a technological solution that keeps relevant participants adequately informed without providing information to all authorities in the network. *PDCs* thus enable the sharing of data between a subset of authorities, but also enable the storing of data only on nodes of the authorities involved. All other authorities can only access the hash of the exchanged data as evidence of the transaction on the global ledger. In short, *PDCs* enable the reliable sharing of data and mapping of information with the specific organizations involved in handling a particular asylum procedure at a certain point in time. This, in turn, enables *reliable information sharing and process automation* while retaining the *separation of competencies.* In the words of Interviewee 11:

> *"In federal structures with decentralized coordination and asymmetric information, blockchain technology can distribute information to everyone simultaneously and automates intermediary procedural steps. That was one major selling point for decentralized coordination and automation of intermediary procedural steps. At the same time, of course, a certain transparency of available data [was mandatory]."*

Lastly, the *separation of competencies* principle is also supported by blockchain's *adaptability*. This property allows to reflect different allocations of competencies, depending on locally defined organizational procedures. Specifically, FLORA's *PDCs* have a modular and flexible design, enabling the desired plasticity and helping participating authorities adapt to locally distinct process logics using customized smart contracts. Interviewee 5 explains:

> *"We are not all in the same building. We are scattered all over the place. Information has to be shared in real-time. And, dependent on the process step, we have changing external collaborators: different state authorities, the federal police, state police, and various local authorities. That is, we often have to quickly and flexibly establish communication channels to enable immediate actions*".

4.2.3. Cooperation and coordination

To foster *cooperation and coordination* between authorities involved in the German asylum procedure, FLORA offers *reliable information sharing and automation of processes* by writing status messages to the blockchain. This provides all organizations involved in handling a specific asylum procedure with a 'shared truth' and timely updates. A statement by Interviewee 13 illustrates:

> *"It is particularly important that I can access data across different authorities, store crucial information, and accordingly improve processes. […] Especially in cross-organizational, federal contexts, wherein authorities usually work with their own databases and have, as a result, outdated information, [it is vital] that we developed a technological solution with only one shared truth that applies to all [authorities involved] in the procedure and is also traceable and accessible for all [authorities]."*

Working with many different backend systems and having *"locally distinct organizational procedures"* (Interviewee 15) also requires a high degree of *adaptability*. The BAMF's decision to use the Hyperledger Fabric framework ensures this *adaptability* at a technological level. The distinction between the common ledger and *PDCs* allows process coordination to be modified to suit local requirements and participating authorities. *PDCs* also help with adjustments to locally distinct process logics by using customized smart contracts. This is particularly important, as Interviewee 11 explains:

> *"Since, if you consider North Rhine-Westphalia, the processes are completely different [from Dresden] and the system cannot be transferred directly; instead, adjustments have to be made which, on the one hand, may be completely new, but on the other hand, are sometimes only minor adaptations."*

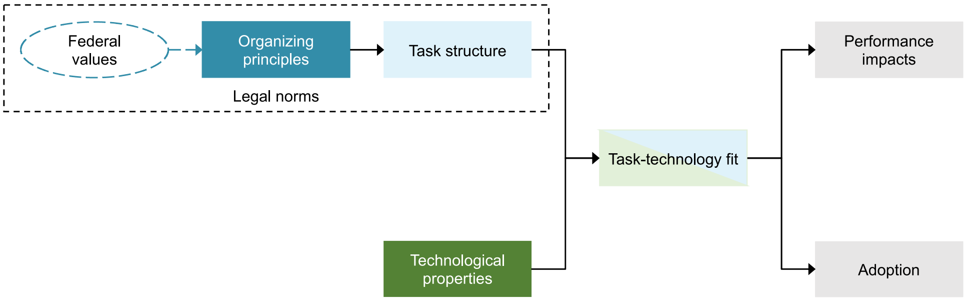


Fig. 3. An adapted and extended theory of task-technology fit in federally organized contexts.

4.2.4. *Organizational flexibility*

Organizational flexibility is supported by three technological properties of blockchain: *selective transparency*, *adaptability*, and *reliable information sharing and process automation*. Thanks to *selective transparency*, the exchange of information between authorities can be adapted to suit the authorities involved in a particular procedure. In federally organized contexts, various constellations of cross-organizational cooperation are encouraged, as Interviewee 32 explains:

> *"Federalism means that we have decentralized structures of organizing, that often run in parallel and need to be flexible. In such an environment, decentralized registers, decentralized databases - such as blockchain - with corresponding consensus mechanisms are an obvious choice."*

Selective transparency is also important to avoid jeopardizing the data sovereignty of participating authorities. As Interviewee 18 describes:

> *"If synchronization is not possible, although we have so many different processes between different agencies, data exchange can become very error-prone. Thus, data in different databases of agency one and agency two must somehow be reconciled and a synchronization process enabled. If you do this via a blockchain, you have the advantage that they have access to the same data but can only view certain data. Privacy is sort of guaranteed, but also that the data is the same. I find this distribution aspect very important, but also that you keep data secure and respect different responsibilities".*

FLORA's *adaptability* enables integration with various backend systems while providing a common framework for effective collaboration at the cross-organizational level. It also allows for *reliable information sharing and process automation* at various government levels while retaining authority-specific sovereignty. Interviewees 7 and 11 explain:

> *"We have many more collaborative processes than we had before. These collaborative processes mean that you are open and that you seek much more communication. This communication must be secure and assist cooperation, which is why we should not be afraid to use blockchain."*

> *"We have seen in the whole asylum procedure or mass migration, [that] this is not a problem only affecting Germany, it is a problem that affects Europe. And [it is crucial that] you can work together with a system that everyone can adapt individually but, in its entirety, is one system."*

5. Discussion

In this study, we explore the reasons why organizations in federally structured government systems adopt blockchain. As our analysis reveals, private blockchain frameworks can accommodate federal organizing principles, which results in a close task-technology fit. Certain blockchain properties, such as *secure and distributed data storage* and *adaptability* may even reinforce federal organizing principles by facilitating secure and distributed cross-organizational collaboration (Avgerou & Bonina, 2020; Fairclough, 2003; Goh & Arenas, 2020; Rose et al., 2015).

5.1. *A theory of task-technology fit in federally organized contexts*

In our analysis, we draw upon a task-technology fit (TTF) lens to illustrate that the successful adoption of blockchain in federally structured contexts is driven by a close TTF. In this way, we demonstrate that TTF theory is relevant and useful not only at the individual but also at the cross-organizational, federal level. Yet, we also propose adaptions and extensions for its use in these contexts (see Fig. 3). That is, we encourage the inclusion of task structure into the definition of tasks and the consideration of values and respective organizing principles as reflected in legal norms as mandatory prerequisites of tasks.

Consistent with prior research (Cane & McCarthy, 2009; Howard & Rose, 2019; Venkatraman, 1989; Zigurs & Buckland, 1998), we maintain the concept of *fit as matching*, which is to say that we are concerned with a direct relation between task and technology properties. Regarding our conceptualization of tasks in cross-organizational, federal contexts, we see them as a combination of *task qua task* and *task as behavior requirement*. More specifically, we look at all behavior relevant to achieving certain goals which are, for instance, linked to the federal organizing principles. Our results, however, suggest that the relevant unit of analysis at a cross-organizational level is less an individual task than the cross-organizational task structure. Moreover, we find that this task structure is the result of shared organizing principles, which, in turn, appear to be manifestations of shared values. In federally organized contexts, these values, and task structures are reflected in legal norms that ensure their implementation (Bozeman, 2007; Craig, 2010; Lindahl, 2000; Tobias, 1989). Thus, organizing principles are not simple antecedents of tasks and task structures but mandatory prerequisites stipulated by law (Bozeman, 2007; Lindahl, 2000). The FLORA application, for instance, is legally required to separate data from different authorities while facilitating its seamless exchange between all the authorities involved in the asylum procedure. As such, legal norms can function both as barriers to and boosters of technical innovation (Gil-Garcia, Chengalur-Smith, & Duchessi, 2007). While the function of legal norms as barriers to innovation has been examined at considerable length (Benbunan-Fich et al., 2020; Gil-Garcia et al., 2007), their role as boosters has not yet been established (Goh & Arenas, 2020). Consequently, our first proposition suggests an adaption and extension of TTF theory in federally organized contexts:

Proposition 1. In cross-organizational, federal contexts, tasks need to be conceptualized more broadly as task structure, which are the result of federal organizing principles and values as represented in legal norms.

In line with the fundamentals of TTF theory (Goodhue & Thompson, 1995; Zigurs & Buckland, 1998), we thus argue that an appropriate task-technology fit, encompassing organizing principles as well as their related values and legal norms, is the key to adopting a particular technology and securing positive performance impacts in federally organized contexts. It can also help to select the 'right' technologies for federally structured government systems. For instance, *separation of competencies* and *cooperation and coordination* provide clear indications of the technological aspects necessary to address the underlying organizational and business needs, such as the consideration of locally distinct organizational procedures (Berman & Martin, 1983; Biela et al., 2012; Borriello & Crespy, 2015; Rieger et al., 2019). In the FLORA case, *empowerment* and *organizational flexibility* appear to be equally important motivators for the selection of blockchain. Concerns about *empowerment* are prominent in federal contexts because organizations of various influence and scale need to cooperate in democratic, albeit hierarchical, structures (Bormann et al., 2019; Erk & Koning, 2009; Heeks & Stanforth, 2007; Mackenzie, 2010). Properties of private blockchain frameworks, such as *selective transparency* and *secure and distributed data storage*, can lead to *empowerment* at a technological level by supporting selective information access – where desired or required by law – while still maintaining a common 'shared truth' for all involved organizations (Guggenmos et al., 2020; Perrons & Cosby, 2020; Rieger et al., 2019). *Organizational flexibility* is crucial because federally organized procedures typically involve the participation of several organizations in constantly changing constellations (Ebinger & Richter, 2015; Heeks & Stanforth, 2007; Hegele & Behnke, 2017; Rieger et al., 2019; Ziolkowski et al., 2020). Private blockchain frameworks are interesting when it comes to these procedures because they can offer the necessary high degree of *adaptability* and *reliable information sharing and process automation* required (Hegele & Behnke, 2017). Which brings us to our second proposition:

Proposition 2. Private blockchain frameworks offer a close task-technology fit with federally organized governmental procedures, and this close fit is an important success factor for their adoption in a cross-organizational, federal context.

A close task-technology fit is not only key to adopting a particular technology and achieving positive performance impacts in federally organized contexts. It can also reinforce federal organizing principles and values. The presentation and recognition of blockchain as a socio-technical agent of federalism gave the FLORA project considerable traction with partner authorities. Its emphasis of task-technology fit convinced other national authorities to join the project and jointly adopt blockchain. Moreover, it was instrumental in the project's selection as a pioneer for the European Blockchain Partnership. This recognition is important since the impact of blockchain applications increases with the addition of further partners (Sedlmeir et al., 2020), especially when it comes to supporting cross-organizational cooperation (Fridgen, Radszuwill, Urbach, & Utz, 2018; Jensen et al., 2019; Kshetri, 2018; Ziolkowski et al., 2020). In effect, FLORA is highly successful in promoting not just blockchain but federal organizing principles. It demonstrates that digitalization of federal systems is possible without 'digital centralization' and redistribution of competencies. Moreover, it shows that blockchain can help reinforce and enhance the principle's underlying federal and cultural values (Duffy, Jeyaraj, Sethi, & Sethi, 2021; Salcedo & Gupta, 2021; Vos & Boonstra, 2022), which is why our third proposition is as follows:

Proposition 3. Blockchain technology can function as a socio-technical agent that strengthens federal organizing principles and the underlying federal and cultural values.

5.2. Theoretical contribution

Our study makes several contributions to research on blockchain adoption, digitalization in the public sector, and TTF theory. We contribute to research on blockchain technology and its adoption in three ways. First, we illustrate that the adoption of blockchain can be desirable and lead to positive performance impacts even when trust is not an issue. In particular, our research corroborates the suggestion that TTF can be an important driver for the adoption of blockchain technology. Second, we extend the body of rich case studies on blockchain adoption by providing a focused analysis of the technology's adoption in federally structured contexts (Toufaily et al., 2021). Third, our findings suggest that research on blockchain technology would do well to take a more practical perspective by focusing more on properties (Weber, 2005) rather than on characteristics of blockchain. To be clear, this approach does not ignore the characteristics of blockchain technology. Our identified properties, such as *secure and distributed data storage* and *selective transparency*, either reinforce characteristics such as *trust* (Amend, Kaiser, et al., 2021) or integrate characteristics such as *immutability* and *redundancy* (Seebacher & Schüritz, 2017).

Aside from blockchain adoption, our study contributes to research on digitalization in the public sector. As we have demonstrated, a fit between cross-organizational organizing principles and key technological properties can unlock the full potential of digitalization efforts in the public sector, particularly in federally structured government systems. Our research thus extends the work of recent studies that have attempted to identify non-technical challenges inherent to the adoption of new technologies in federally organized contexts (e.g., Goh & Arenas, 2020). Many of these challenges, such as system complexity (Avgerou & Bonina, 2020; Cordella & Willcocks, 2012; Wibbels, 2006), cooperation in a protected environment (Dawson et al., 2016; Deringer & Molnar, 1983), and organizational cultural values (Leidner & Kayworth, 2006; Seltsikas & O'Keefe, 2010), symbolize task characteristics. When these task characteristics are brought into close alignment with certain technological properties, adoption becomes more likely, as do positive performance impacts. As illustrated in our case study, this close alignment can be achieved by blockchain technology as it exhibits properties that fit many tasks associated with cross-organizational cooperation in the public sector – particularly in federally structured government systems. That being said, blockchain is certainly not the only solution for cross-organizational cooperation in the public or the private sector (Jensen et al., 2019; Jović, Tijan, Žgaljić, & Aksentijević, 2020; Tsiulin, Kristian, Hilmola, Goryaev, & Karam, 2020). Each case requires its own evaluation of task characteristics and underlying organizing principles in relation to the proposed technology and their fit (Vos & Boonstra, 2022).

Finally, our study contributes to TTF theory by demonstrating that TTF also plays an important role in cross-organizational, federally organized contexts. While the fundamental premises of TTF theory remain applicable – namely that adoption and performance depend on an appropriate fit between task and technology (Goodhue & Thompson, 1995) – we offer a new perspective on tasks and their cross-organizational structure as the result of shared organizing principles and values. Prior research has also indicated that TTF may be applicable beyond task conceptualization at an individual level (Furneaux, 2012; Zigurs & Buckland, 1998; Zigurs & Khazanchi, 2008), but what we demonstrate here is that a good fit between technology and tasks at an organizational and cross-organizational level is at least as important. At an individual level, poor TTF would lead to reduced usability and performance (Goodhue & Thompson, 1995; Howard & Rose, 2019), whereas poor TTF at an organizational and cross-organizational level would lead to high legal barriers, error-prone processes, and a significantly lower organizational readiness to adopt the technology in question. Moreover, our study demonstrates that, in federally organized contexts, tasks have to be considered on a more abstract level. That is, task structures are the result of federal organizing principles derived from federal values, all manifested in legal norms. In consequence, federal values are an important additional factor to be considered in technology selection and adoption. This suggestion aligns closely with recent studies by Salcedo and Gupta (2021), Duffy et al. (2021), and Vos and Boonstra (2022), who establish the importance of cultural values for technology selection and adoption in companies.

5.3. Practical implications

Aside from these theoretical contributions, our study also holds several practical implications. It can help decision-makers in authorities and other public institutions to identify the contexts in which blockchain technology can thrive. More specifically, it can guide technology selection and adoption in federally organized contexts. The core organizing principles we have identified, along with the matching blockchain properties, pinpoint some of the factors that drive successful technology adoption in the complex environment of federally structured governments. Furthermore, the deeper understanding of the underlying TTF that our study provides can help decision-makers improve the likelihood of successful adoption and positive performance impacts (Goodhue & Thompson, 1995; Zigurs & Buckland, 1998). This focus on TTF, if well communicated, can also help decision-makers encourage other organizations to participate in blockchain projects. Pointing out shared values and similar organizing principles should make the potential of TTF evident and spread the use of blockchain (Salcedo & Gupta, 2021). Since the benefit of a blockchain project increases with the size of the network, this acquisition of partners is very important (Sedlmeir et al., 2020), particularly when it comes to supporting cross-organizational cooperation (Fridgen et al., 2018; Jensen et al., 2019; Kshetri, 2018; Ziolkowski et al., 2020).

Another practical implication is the suggestion that governmental decision-makers should not focus exclusively on tasks and technology when assessing task-technology fit. Ideally, they would also look at task- and technology-related aspects. For instance, federal values and their manifestation as federal organizing principles can have a much higher priority than the potential benefits of applying a certain technology (Gil-Garcia et al., 2007; Jaeger, 2002; Salcedo & Gupta, 2021). Federally organized contexts may also require special frameworks for technology governance that are aligned both with technological properties and federalism's organizing principles. Centralized workflow-management systems are a case in point. Their 'centralized' governance frameworks often complicate adoption even though they are much easier to implement and maintain than blockchain applications (Rieger et al., 2019; Ziolkowski et al., 2020). With this in mind, governmental decision-makers should consider task- and technology-related aspects with the same rigorous attention to detail with which they consider a technical fit.

A third practical implication for decision-makers refers to the work of Trkman (2010), Zigurs and Buckland (1998), and Zigurs and Khazanchi (2008). TTF is typically dynamic, so organizations must continuously evaluate TTF and, if necessary, coordinate organizational or technological changes. Even if there is a good initial fit between task and technology, it is important to ensure organizational readiness for later changes. These may, for instance, be required due to the introduction of new procedures or partners in cross-organizational cooperation. Therefore, both the technology in use and the organization itself should be able to adapt to new circumstances and so retain TTF (Goodhue & Thompson, 1995; Zigurs & Buckland, 1998; Zigurs & Khazanchi, 2008).

Besides governmental decision-makers, this study also has practical implications for IT service providers and the technological, open-source community. For instance, IT service providers might want to define modularity or local adaptability as an important requirement for blockchain applications (Lockl, Schlatt, Schweizer, Urbach, & Harth, 2020; P. Zhang, White, Schmidt, Lenz, & Rosenbloom, 2018). In federal contexts, the degree of centralization and decentralization largely depends on the task at hand and the structure of the respective organization (Auer, 2005; Keating, 2017; Tiller, 2011). Blockchain applications should be able to accommodate these different degrees to ensure relevance beyond the German asylum procedure. The same is true of system complexity. The more organizations that join the blockchain network, the more value the network can create. Yet more organizations also mean more complex network management (Sedlmeir et al., 2020). Therefore, IT service providers might want to focus on reducing the complexities that come with an increasing number of participants, federal organizing structures, and legal requirements.

Closer collaboration between IT service providers, the open-source community, and governments could also drive the adoption of blockchain in the public sector. Insights from different pilot projects and the resulting adjustments to the blockchain frameworks would be readily available for other governmental and non-governmental organizations. This, then, would be a win-win scenario for all concerned, as IT service providers, open-source developers, and governmental decision-makers could avoid previous errors, and other organizations could profit from the current framework while also making valuable contributions to it (Mu, Bian, & Zhao, 2019).

5.4. *Limitations and future research directions*

While this study offers interesting insights into the adoption of blockchain technology in federally organized contexts, it is also subject to some limitations. First, the generalizability of single-case studies is often questioned (Walsham, 2006). Although we deem our single-case study design to be appropriate, our research could no doubt benefit from validation using other cases in a federal context, for instance, at the European level. A particularly interesting case could be the European Blockchain Service Infrastructure. At Germany's proposal, the European Blockchain Partnership has established a working group that will investigate options for using EBSI to support the management of cross-border asylum procedures. Although this application is still in an early phase, the organizing principles and respective technological properties identified in our study seem also to be relevant also at this cross-border, supranational level. For instance, the founding declaration of the EBP and documentation in the EBSI Confluence indicate that the EBP also considers features such as *separation of competencies* and *organizational flexibility* to be essential (Declaration: Cooperation on a European Blockchain Partnership, 2018; European Commission, 2021). As well as additional case studies, future research could also use quantitative methods to validate the identified TTF or to elaborate on how federal values affect organizing principles (Leidner & Kayworth, 2006).

Second, our study could benefit from cross-validation in other contexts. Specifically, equivalents of federal organizing principles may also be discovered in certain private sector cases. An interesting case in point could be the container shipping industry, where cooperation is similarly decentralized and separated according to competencies. We expect particularly valuable insights to emerge from an investigation of the TradeLens project. TradeLens is a blockchain application jointly developed by IBM and Maersk, the world's largest container shipping company, to track process data and documents across supply chains (Jensen et al., 2019). It would also be interesting to investigate the financial services industry where TTF also seems to be an important factor for the adoption of blockchain (Liang et al., 2021). Lastly, it could be worthwhile examining industries where centralized organizational structures dominate, such as the energy sector. In electric power systems, blockchain applications appear to be less successful (Mengelkamp et al., 2018; Ølnes et al., 2017; Sousa et al., 2019). This is particularly so for applications that involve the replacement of established market roles and, as such, face substantial regulatory challenges (Andoni et al., 2019; Li, Yang, He, Chen, & Wang, 2019; Thomas et al., 2019).

Third, it remains to be seen how TTF will impact performance in day-to-day operations and how it will combine with other success factors such as viability and symbolic benefits (Liang et al., 2021). The roll-out of the FLORA project to several of Germany's states and its selection as a trailblazer for the EBP have shown some propitious early signs that support our propositions and demonstrate viability. However, replicating our results with, for instance, EBSI will provide further feedback and a clearer indication of the importance of each factor as well as the relevance of symbolic benefits for federally structured governments.

6. Conclusion

In this study, we examine why organizations in federally structured government systems adopt blockchain. We draw on TTF theory to argue that adoption in these contexts is driven by a high degree of fit between cross-organizational task structure and blockchain's technological properties. In particular, we highlight four technological properties exhibited by private blockchain frameworks, each of which aligns closely with several of the four organizing principles of federalism. Accordingly, these blockchain frameworks can be powerful tools for facilitating cross-organizational cooperation between independent and heterogenous authorities. Our study contributes to a deeper understanding of the adoption of blockchain technology and of task-technology fit at the cross-organizational, federal level. Moreover, our insights can help researchers and practitioners – especially decision-makers in federally structured government systems – understand the circumstances in which blockchain technology can be a good fit.

CRediT authorship contribution statement

Tamara Roth: Conceptualization, Data curation, Formal analysis, Writing – original draft. **Alexander Stohr:** Investigation, Methodology, Validation, Writing – original draft. **Julia Amend:** Data curation, Formal analysis. **Gilbert Fridgen**: Supervision, Writing – review & editing. **Alexander Rieger**: Conceptualization, Project administration, Supervision, Writing – review & editing.

Declaration of interest

Since January 2018, Gilbert Fridgen and Alexander Rieger have been part of the scientific advisory team that supports and accompanies the FLORA blockchain project of Germany's Federal Office for Migration and Refugees (BAMF). Alexander Stohr has joined the team in August 2019 and Julia Amend in March 2020.

Acknowledgement

This work was supported by PayPal and the Luxembourg National Research Fund FNR (P17/IS/13342933/PayPal-FNR/Chair in DFS/Gilbert Fridgen).

Appendix A. Details of the literature review

see Appendix Table A1, Table A2.

Table A1
Results of the literature review on federalism.

#	Paper	Empowerment	Separation of competencies	Cooperation and coordniation	Organizational flexibility	Total of organizing principles mentioned
1	Auer (2005)	x		x	x	3
2	Avgerou and Bonina (2020)	x		x		2
3	Berman and Martin (1983)		x	x		2
4	Biela et al. (2012)	x	x		x	3
5	Borriello and Crespy (2015)	x	x		x	3
6	Bormann et al. (2019)	x	x		x	3
7	Carter and Bélanger (2005)	x		x		2
8	Christiaanse and Huigen (1997)			x		1
9	Conlan (2006)	x		x	x	3
10	Constantinides, Henfridsson, and Parker (2018)	x	x			2
11	Cordella and Willcocks (2012)	x		x		2
12	Davis (1989)	x				1
13	Dawson et al. (2016)	x		x		2
14	Deringer and Molnar (1983)			x		1
15	Dinan and Heckelman (2020)	x	x		x	3
16	Ebinger and Richter (2015)	x	x	x	x	4
17	Egeberg (2001)	x	x			2
18	Erk and Koning (2009)	x	x		x	3
19	Fossum and Jachtenfuchs (2017)	x	x	x	x	4
20	Gil-Garcia et al. (2007)			x		1
21	Goh and Arenas (2020)	x		x		2
22	Graham (1980)	x	x			2
23	Grant and Tan (2013)	x	x	x		3
24	Heeks and Stanforth (2007)	x	x			2
25	Hsueh and Prakash (2012)		x		x	2
26	Igira (2008)	x				1
27	Ingram and Simons (2000)		x	x		2
28	Irani, Love, Elliman, Jones, and Themistocleous (2005)			x		1
29	Jaeger (2002)	x	x	x	x	4
30	Keating (2017)	x	x		x	3
31	Leidner and Kayworth (2006)	x		x		2
32	Mackenzie (2010)		x	x	x	3
33	Mckay (2005)	x	x			2
34	Moya Palencia (1974)	x	x	x	x	4
35	Nathan (2006)	x	x			2
36	Pang, Lee, and DeLone (2014)			x	x	2
37	Parsons (2002)		x	x	x	3
38	Pencek (2008)		x	x		2
39	Rai and Tang (2010)				x	1
40	Ravishankar (2013)			x		1
41	Rodden and Wibbels (2002)	x	x			2
42	Scott et al. (2016)			x		1
43	Seltsikas and O'Keefe (2010)	x				1
44	Smith and Fernandez (2010)	x		x		2
45	Soss, Fording, and Schram (2008)	x				1
46	Springer (1962)			x		1
47	Trechsel (2005)	x	x	x		3
48	Tyworth (2014)	x			x	2
49	Watts (1998)	x	x	x	x	4
50	Wibbels (2006)	x	x	x		3
51	Ziblatt (2004)		x			1
		35	28 12	30	19	

Table A2
Results of the literature review on blockchain technology.

#	Paper	Secure and distributed data storage	Selective transparency	Reliable information sharing and process automation	Adaptability	Total of technological properties mentioned
1	Abramowicz (2020)	x	x		x	3
2	Ahl et al. (2020)	x	x	x	x	4
3	Andersen and Ingram Bogusz (2019)	x	x	x	x	4
4	Andoni et al. (2019)	x	x	x	x	4
6	Beck, Avital, Rossi, and Thatcher (2017)	x		x		2
7	Benbunan-Fich et al. (2020)	x			x	2
8	Chanson, Bogner, Bilgeri, Fleisch, and Wortmann (2019)	x	x	x	x	4
9	Chapron (2017)	x	x	x		3
10	Chong, Lim, Hua, Zheng, and Tan (2019)	x		x	x	3
11	Davidson, de Filippi, and Potts (2018)	x	x	x	x	4
12	di Silvestre et al. (2019)	x	x	x	x	4
13	Drummer and Neumann (2020)	x		x		2
14	Foti and Vavalis (2019)	x	x	x		3
15	Gomber, Kauffman, Parker, and Weber (2018)			x	x	2
16	Hawlitschek et al. (2018)	x	x	x		3
17	Howson (2019)	x	x	x		3
18	Iansiti and Lakhani (2017)	x	x	x	x	4
19	Jensen et al. (2019)	x	x	x	x	4
20	Khaqqi et al. (2018)		x			1
21	Kshetri (2018)	x	x	x	x	4
22	Lacity (2018)	x		x		2
23	Lauslahti et al. (2018)	x		x	x	3
24	van Leeuwen, AlSkaif, Gibescu, and van Sark (2020)	x	x	x	x	4
25	Li et al. (2019)	x		x	x	3
26	Lin, Pipattanasomporn, and Rahman (2019)	x				1
27	Lowitzsch, Hoicka, and van Tulder (2020)	x		x		2
28	Luo, Dong, Liang, Murata, and Xu (2019)	x			x	2
29	Lüth, Zepter, Crespo del Granado, and Egging (2018)	x		x		2
30	Mattila and Seppälä (2018)	x		x	x	3
31	Mattke et al. (2019)	x	x	x	x	4
32	Mendling, Pentland, and Recker (2020)			x		1
33	Mengelkamp et al. (2018)	x	x	x		3
34	Morstyn et al. (2018)	x			x	2
35	Noor et al. (2018)	x	x	x	x	4
36	Ølnes et al. (2017)	x	x	x	x	4
36	Pedersen et al. (2019)	x	x	x		3
38	Perrons and Cosby (2020)	x	x	x		3
39	Renwick and Gleasure (2021)		x	x	x	3
40	Riasanow, Burckhardt, Soto Setzke, Böhm, and Krcmar (2018)	x		x	x	3
41	Rieger et al. (2019)	x	x	x	x	4
42	Risius and Spohrer (2017)	x		x	x	3
43	Rossi et al. (2019)	x	x	x		3
44	Sedlmeir et al. (2020)	x	x	x	x	4
45	Shafiei Gol, Stein, and Avital (2019)	x		x	x	3
46	Sikorski et al. (2017)	x		x	x	3
47	Sousa et al. (2019)	x	x	x	x	4
48	Thomas et al. (2019)	x		x	x	3
49	Treiblmaier etal. (2021)	x		x	x	3
50	Ying, Jia, and Du (2018)			x	x	2
51	T. Zhang, Pota, Chu, and Gadh (2018)	x	x	x	x	4
52	Ziolkowski et al. (2020)			x	x	2
		46	29	45	35	

Appendix. B Case study evidence

see Appendix Table B1, Table B2.

Table B1
Overview of our case study evidence.

Type	Details
(1) Interviews	See Table B2
(2) Documentation	(1) 441 pages of documentation in Atlassian Confluence (2) Technical concepts on data privacy (89 pages) and IT security (81 pages) (3) 121 pages of functional specifications (4) Project presentations (5) Publicly available reports (Digitalization agenda, press clippings, blockchain strategy of Germany's federal government, reports of other organizations)
(3) Direct observations (with multiple observers)	(1) Bi-weekly sprint reviews and project management meetings (2) 20 + workshops with different directorates, authorities, and organizations

Table B2
Overview of the conducted interviews.

Interviewee	Role	Duration (min)
1	Head of division	50
2	Employee IT	50
3	Head of division	60
4	Employee IT	30
5	Head of group	40
6	Head of division	30
7	Head of group	50
8	Decision-maker	40
9	Case handler	30
10	Case handler	33
11	Researcher	42
12	Researcher	52
13	Researcher	56
14	Researcher	43
15	Researcher	43
16	Consultant	50
17	Consultant	60
18	Developer	30
19	Developer	50
20	Developer	60
21	Enterprise architect	60
22	External stakeholder	45
23	External stakeholder	32
24	External stakeholder	60
25	External stakeholder	51

References

Abels, G. (2019). Federalism and democracy in the European Union. In S. S. Krause (Ed.), *Theories of modern federalism* (pp. 283–300). Baden-Baden, DE: Nomos. https://doi.org/10.5771/9783845298320-283.

Abramowicz, M. (2020). The very brief history of decentralized blockchain governance. *Vanderbilt Journal of Entertainment & Technology Law, 22*(2), 273–298.

Ahl, A., Yarime, M., Goto, M., Chopra, S. S., Kumar, N., Manoj, … Sagawa, D. (2020). Exploring blockchain for the energy transition: Opportunities and challenges based on a case study in Japan. *Renewable and Sustainable Energy Reviews, 117*, Article 109488. https://doi.org/10.1016/j.rser.2019.109488

Amend, J., Fridgen, G., Rieger, A., Roth, T., & Stohr, A. (2021). The evolution of an architectural paradigm – Using blockchain to build a cross-organizational enterprise service bus. In *Proceedings of the 54th Hawaii international conference on system sciences*. 〈https://doi.org/10.24251/HICSS.2021.522〉.

Amend, J., Kaiser, J., Uhlig, L., Urbach, N., & Völter, F. (2021). What do we really need? A systematic literature review of the requirements for blockchain-based E-government services. In *Wirtschaftsinformatik 2021 proceedings*.

Andersen, J. V., & Ingram Bogusz, C. (2019). Self-organizing in blockchain infrastructures: Generativity through shifting objectives and forking. *Journal of the Association for Information Systems, 20*(9), 1242–1273. https://doi.org/10.17705/1jais.00566

Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., … Peacock, A. (2019). Blockchain technology in the energy sector: A systematic review of challenges and opportunities. *Renewable and Sustainable Energy Reviews, 100*, 143–174. https://doi.org/10.1016/j.rser.2018.10.014

Auer, A. (2005). The constitutional scheme of federalism. *Journal of European Public Policy, 12*(3), 419–431. https://doi.org/10.1080/13501760500091166

Avgerou, C., & Bonina, C. (2020). Ideologies implicated in IT innovation in government: A critical discourse analysis of Mexico's international trade administration. *Information Systems Journal, 30*(1), 70–95. https://doi.org/10.1111/isj.12245

Beck, R., Avital, M., Rossi, M., & Thatcher, J. B. (2017). Blockchain technology in business and information systems research. *Business & Information Systems Engineering, 59*(6), 381–384. https://doi.org/10.1007/s12599-017-0505-1

Beck, R., Müller-Bloch, C., & King, J. L. (2018). Governance in the blockchain economy: A framework and research agenda. *Journal of the Association for Information Systems, 19*(10), 1020–1034. https://doi.org/10.17705/1jais.00518

Bélanger, F., & Carter, L. (2008). Trust and risk in e-government adoption. *The Journal of Strategic Information Systems, 17*(2), 165–176. https://doi.org/10.1016/j.jsis.2007.12.002

Benbunan-Fich, R., Desouza, K. C., & Andersen, K. N. (2020). IT-enabled innovation in the public sector: Introduction to the special issue. *European Journal of Information Systems, 29*(4), 323–328. https://doi.org/10.1080/0960085X.2020.1814989

Benson, D., & Jordan, A. (2014). Explaining task allocation in the EU: 'Retooling' federalism for comparative analysis. *Journal of Common Market Studies, 52*(4), 794–809. https://doi.org/10.1111/jcms.12131

Berman, D., & Martin, L. (1983). The dynamics of federalism. *Policy Studies Journal, 11* (4), 718–721. https://doi.org/10.1111/j.1541-0072.1983.tb00576.x

Bettis, R. A., Gambardella, A., Helfat, C., & Mitchell, W. (2015). Qualitative empirical research in strategic management. *Strategic Management Journal, 36*(5), 637–639. https://doi.org/10.1002/smj.2317

Biela, J., Hennl, A., & Kaiser, A. (2012). Combining federalism and decentralization: Comparative case studies on regional development policies in Switzerland, Austria, Denmark, and Ireland. *Comparative Political Studies, 45*(4), 447–476. https://doi.org/10.1177/0010414011421767

Bormann, N.-C., Cederman, L.-E., Gates, S., Graham, B. A. T., Hug, S., Strøm, K. W., & Wucherpfennig, J. (2019). Power sharing: Institutions, behavior, and peace. *American Journal of Political Science, 63*(1), 84–100. https://doi.org/10.1111/ajps.12407

Borriello, A., & Crespy, A. (2015). How to not speak the 'F-word': Federalism between mirage and imperative in the euro crisis. *European Journal of Political Research, 54*(3), 502–524. https://doi.org/10.1111/1475-6765.12093

Bozeman, B. (2007). *Public values and public interest: Counterbalancing economic individualism*. Washington, D.C., US: Georgetown University Press.

Brown, S. A., Dennis, A. R., & Venkatesh, V. (2010). Predicting collaboration technology use: Integrating technology adoption and collaboration research. *Journal of Management Information Systems, 27*(2), 9–54. https://doi.org/10.2753/MIS0742-1222270201

Cane, S., & McCarthy, R. (2009). Analyzing the factors that affect information systems use: A task-technology fit meta-analysis. *Journal of Computer Information Systems, 50* (1), 108–123. https://doi.org/10.1080/08874417.2009.11645368

Carson, B., Romanelli, G., Walsh, P., & Zhumaev, A. (2018). *Blockchain beyond the hype*. McKinsey & Company. 〈https://www.mckinsey.com/~/media/McKinsey/Business_Functions/McKinsey_Digital/Our_Insights/Blockchain_beyond_the_hype_What_is_the_strategic_business_value/Blockchain-beyond-the-hype-What-is-the-strategic-business-value.pdf?shouldIndex=false〉.

Carter, L., & Bélanger, F. (2005). The utilization of e-government services: Citizen trust, innovation and acceptance factors. *Information Systems Journal, 15*(1), 5–25. https://doi.org/10.1111/j.1365-2575.2005.00183.x

Carvalho, A., Merhout, J. W., Kadiyala, Y., & Bentley, J., II (2021). When good blocks go bad: Managing unwanted blockchain data. *International Journal of Information Management, 57*, Article 102263. https://doi.org/10.1016/j.ijinfomgt.2020.102263

Chanson, M., Bogner, A., Bilgeri, D., Fleisch, E., & Wortmann, F. (2019). Blockchain for the IoT: Privacy-preserving protection of sensor data. *Journal of the Association for Information Systems, 20*(9), 1272–1307. https://doi.org/10.17705/1jais.00567

Chapron, G. (2017). The environment needs cryptogovernance. *Nature, 545*(7655), 403–405. https://doi.org/10.1038/545403a

Chemerinsky, E. (1995). Dunwody distinguished lecture in law: The values of federalism. *Florida Law Review, 47*(4), 499–540. 〈https://heinonline.org/HOL/P?h=hein.journals/uflr47&i=513〉.

Cho, S., Lee, K. (Kari), Cheong, A., No, W. G., & Vasarhelyi, M. A. (2021). Chain of values: Examining the economic impacts of blockchain on the value-added tax system. *Journal of Management Information Systems, 38*(2), 288–313. https://doi.org/10.1080/07421222.2021.1912912

Chong, A. Y. L., Lim, E. T. K., Hua, X., Zheng, S., & Tan, C.-W. (2019). Business on chain: A comparative case study of five blockchain-inspired business models. *Journal of the Association for Information Systems, 20*(9), 1308–1337. https://doi.org/10.17705/1jais.00568

Christiaanse, E., & Huigen, J. (1997). Institutional dimensions in information technology implementation in complex network settings. *European Journal of Information Systems, 6*(2), 77–85. https://doi.org/10.1057/palgrave.ejis.3000258

Conlan, T. (2006). From cooperative to opportunistic federalism: Reflections on the half-century anniversary of the commission on intergovernmental relations. *Public Administration Review, 66*(5), 663–676. https://doi.org/10.1111/j.1540-6210.2006.00631.x

Constantinides, P., Henfridsson, O., & Parker, G. G. (2018). Introduction—Platforms and infrastructures in the digital age. *Information Systems Research, 29*(2), 381–400. https://doi.org/10.1287/isre.2018.0794

Corbin, J. M., & Strauss, A. (1990). Grounded theory research: Procedures, canons, and evaluative criteria. *Qualitative Sociology, 13*(1), 3–21. https://doi.org/10.1007/BF00988593

Cordella, A., & Willcocks, L. (2012). Government policy, public value and IT outsourcing: The strategic case of ASPIRE. *The Journal of Strategic Information Systems, 21*(4), 295–307. https://doi.org/10.1016/j.jsis.2012.10.007

Craig, R. K. (2010). Comparative guide to the western states' public trust doctrines: Public values, private rights, and the evolution toward an ecological public trust. *Ecology Law Quarterly, 37*(1), 53–198.

Davidson, S., de Filippi, P., & Potts, J. (2018). Blockchains and the economic institutions of capitalism. *Journal of Institutional Economics, 14*(4), 639–658. https://doi.org/10.1017/S1744137417000200

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319–340. https://doi.org/10.2307/249008

Dawson, G. S., Denford, J. S., Williams, C. K., Preston, D., & Desouza, K. C. (2016). An examination of effective IT governance in the public sector using the legal view of agency theory. *Journal of Management Information Systems, 33*(4), 1180–1208. https://doi.org/10.1080/07421222.2016.1267533

, 2018Declaration: Cooperation on a European Blockchain Partnership, (2018). *Testimony of Austria, Belgium, Bulgaria, Czech Republic, Estonia, Finland, France, Germany, Ireland, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Slovakia, Slovenia, Spain, … Norway*. ⟨https://ec.europa.eu/newsroom/dae/redirection/document/50954⟩.

Deringer, D. K., & Molnar, A. R. (1983). University, industry, federal cooperation—A case study. *Science, Technology, & Human Values, 8*(4), 40–45. https://doi.org/10.1177/016224398300800407

Dinan, J., & Heckelman, J. C. (2020). Stability and contingency in federalism preferences. *Public Administration Review, 80*(2), 234–243. https://doi.org/10.1111/puar.13157

Drummer, D., & Neumann, D. (2020). Is code law? Current legal and technical adoption issues and remedies for blockchain-enabled smart contracts. *Journal of Information Technology, 35*(4), 337–360. https://doi.org/10.1177/0268396220924669

Du, W. (Derek), Pan, S. L., Leidner, D. E., & Ying, W. (2019). Affordances, experimentation and actualization of FinTech: A blockchain implementation study. *The Journal of Strategic Information Systems, 28*(1), 50–65. https://doi.org/10.1016/j.jsis.2018.10.002

Duffy, K., Jeyaraj, A., Sethi, V., & Sethi, V. (2021). Drivers of information technology choice by individuals. *International Journal of Information Management, 58*, Article 102320. https://doi.org/10.1016/j.ijinfomgt.2021.102320

Ebinger, F., & Richter, P. (2015). Decentralizing for performance? A quantitative assessment of functional reforms in the German Länder. *International Review of Administrative Sciences, 82*(2), 291–314. https://doi.org/10.1177/0020852315586916

Egeberg, M. (2001). How federal? The organizational dimension of integration in the EU (and elsewhere). *Journal of European Public Policy, 8*(5), 728–746. https://doi.org/10.1080/13501760110083482

Eisenhardt, K. M. (1989). Building theories from case study research. *Academy of Management Review, 14*(4), 532–550. https://doi.org/10.5465/amr.1989.4308385

Eisenhardt, K. M., & Graebner, M. E. (2007). Theory building from cases: Opportunities and challenges. *Academy of Management Journal, 50*(1), 25–32. https://doi.org/10.5465/AMJ.2007.24160888

Erk, J., & Koning, E. (2009). New structuralism and institutional change: Federalism between centralization and decentralization. *Comparative Political Studies, 43*(3), 353–378. https://doi.org/10.1177/0010414009332143

European Commission (2021). *EBSI documentation*. ⟨https://ec.europa.eu/cefdigital/wiki/display/EBSIDOC/EBSI+Documentation+Home⟩. Accessed 16.12.21.

Fairclough, N. (2003). *Analysing discourse: Textual analysis for social research* (1st ed.). London, UK: Routledge,.

Federal Ministry of the Interior, Building and Community (2020). *What is the online access act?* ⟨https://www.onlinezugangsgesetz.de/Webs/OZG/EN/home/home-node.html⟩. Accessed 16.12.21.

Fossum, J. E., & Jachtenfuchs, M. (2017). Federal challenges and challenges to federalism. Insights from the EU and federal states. *Journal of European Public Policy, 24*(4), 467–485. https://doi.org/10.1080/13501763.2016.1273965

Foti, M., & Vavalis, M. (2019). Blockchain based uniform price double auctions for energy markets. *Applied Energy, 254*, Article 113604. https://doi.org/10.1016/j.apenergy.2019.113604

Fridgen, G., Radszuwill, S., Urbach, N., & Utz, L. (2018). Cross-organizational workflow management using blockchain technology – Towards applicability, auditability, and automation. In *Proceedings of the 51st Hawaii international conference on system sciences*. ⟨https://doi.org/10.24251/HICSS.2018.444⟩.

Furneaux, B. (2012). Task-technology fit theory: A survey and synopsis of the literature. In Y. K. Dwivedi, M. R. Wade, & S. L. Schneberger (Eds.), Information systems theory: Explaining and predicting our digital society, *Vol. 1* (pp. 87–106). New York, NY: Springer New York. ⟨https://doi.org/10.1007/978-1-4419-6108-2_5⟩.

Gil-Garcia, J. R., Chengalur-Smith, I., & Duchessi, P. (2007). Collaborative e-Government: Impediments and benefits of information-sharing projects in the public sector. *European Journal of Information Systems, 16*(2), 121–133. https://doi.org/10.1057/palgrave.ejis.3000673

Goh, J. M., & Arenas, A. E. (2020). IT value creation in public sector: How IT-enabled capabilities mitigate tradeoffs in public organisations. *European Journal of Information Systems, 29*(1), 25–43. https://doi.org/10.1080/0960085X.2019.1708821

Gomber, P., Kauffman, R. J., Parker, C., & Weber, B. W. (2018). On the fintech revolution: Interpreting the forces of innovation, disruption, and transformation in financial services. *Journal of Management Information Systems, 35*(1), 220–265. https://doi.org/10.1080/07421222.2018.1440766

Goodhue, D. L., & Thompson, R. L. (1995). Task-technology fit and individual performance. *MIS Quarterly, 19*(2), 213–236. https://doi.org/10.2307/249689

Graham, L. S. (1980). Centralization versus decentralization dilemmas in the administration of public service. *International Review of Administrative Sciences, 46*(3), 219–232. https://doi.org/10.1177/002085238004600301

Grant, G., & Tan, F. B. (2013). Governing IT in inter-organizational relationships: Issues and future research. *European Journal of Information Systems, 22*(5), 493–497. https://doi.org/10.1057/ejis.2013.21

Grover, V., Chiang, R. H. L., Liang, T.-P., & Zhang, D. (2018). Creating strategic business value from big data analytics: A research framework. *Journal of Management Information Systems, 35*(2), 388–423. https://doi.org/10.1080/07421222.2018.1451951

Guggenmos, F., Lockl, J., Rieger, A., Wenninger, A., & Fridgen, G. (2020). How to develop a GDPR-compliant blockchain solution for cross-organizational workflow management: Evidence from the German Asylum procedure. In *Proceedings of the 53rd Hawaii international conference on system sciences*. ⟨https://doi.org/10.24251/HICSS.2020.492⟩.

Hackman, J. R. (1969). Toward understanding the role of tasks in behavioral research. *Acta Psychologica, 31*, 97–128. https://doi.org/10.1016/0001-6918(69)90073-0

Handy, C. (1996). *Beyond certainty: The changing worlds of organizations*. Boston, MA, US: Harvard Business School Press.

Hawlitschek, F., Notheisen, B., & Teubner, T. (2018). The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy. *Electronic Commerce Research and Applications, 29*, 50–63. https://doi.org/10.1016/j.elerap.2018.03.005

Heeks, R., & Stanforth, C. (2007). Understanding e-Government project trajectories from an actor-network perspective. *European Journal of Information Systems, 16*(2), 165–177. https://doi.org/10.1057/palgrave.ejis.3000676

Hegele, Y., & Behnke, N. (2017). Horizontal coordination in cooperative federalism: The purpose of ministerial conferences in Germany. *Regional & Federal Studies, 27*(5), 529–548. https://doi.org/10.1080/13597566.2017.1315716

Howard, M. C., & Rose, J. C. (2019). Refining and extending task–technology fit theory: Creation of two task–technology fit scales and empirical clarification of the construct. *Information & Management, 56*(6), Article 103134. https://doi.org/10.1016/j.im.2018.12.002

Howson, P. (2019). Tackling climate change with blockchain. *Nature Climate Change, 9*(9), 644–645. https://doi.org/10.1038/s41558-019-0567-9

Hsueh, L., & Prakash, A. (2012). Incentivizing self-regulation: Federal vs. state-level voluntary programs in US climate change policies. *Regulation & Governance, 6*(4), 445–473. https://doi.org/10.1111/j.1748-5991.2012.01140.x

Huang, L., Zhang, J., & Liu, Y. (2017). Antecedents of student MOOC revisit intention: Moderation effect of course difficulty. *International Journal of Information Management, 37*(2), 84–91. https://doi.org/10.1016/j.ijinfomgt.2016.12.002

Hughes, L., Dwivedi, Y. K., Misra, S. K., Rana, N. P., Raghavan, V., & Akella, V. (2019). Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda. *International Journal of Information Management, 49*, 114–129. https://doi.org/10.1016/j.ijinfomgt.2019.02.005

Iansiti, M., & Lakhani, K. R. (2017). The truth about blockchain. *Harvard Business Review, 95*(1), 118–127.

Igira, F. T. (2008). The situatedness of work practices and organizational culture: Implications for information systems innovation uptake. *Journal of Information Technology, 23*(2), 79–88. https://doi.org/10.1057/palgrave.jit.2000132

Ingram, P., & Simons, T. (2000). State formation, ideological competition, and the ecology of israeli workers' cooperatives, 1920–1992. *Administrative Science Quarterly, 45*(1), 25. https://doi.org/10.2307/2666978

Inman, R. P. (2007). Federalism's values and the value of federalism. *CESifo Economic Studies, 53*(4), 522–560. https://doi.org/10.1093/cesifo/ifm018

Irani, Z., Love, P. E. D., Elliman, T., Jones, S., & Themistocleous, M. (2005). Evaluating e-government: Learning from the experiences of two UK local authorities. *Information Systems Journal, 15*(1), 61–82. https://doi.org/10.1111/j.1365-2575.2005.00186.x

Jaeger, P. T. (2002). Constitutional principles and E-government: An opinion about possible effects of Federalism and the separation of powers on E-government policies. *Government Information Quarterly, 19*(4), 357–368. https://doi.org/10.1016/S0740-624X(02)00119-3

Janssen, M., Weerakkody, V., Ismagilova, E., Sivarajah, U., & Irani, Z. (2020). A framework for analysing blockchain technology adoption: Integrating institutional, market and technical factors. *International Journal of Information Management, 50*, 302–309. https://doi.org/10.1016/j.ijinfomgt.2019.08.012

Jensen, T., Hedman, J., & Henningsson, S. (2019). How tradelens delivers business value with blockchain technology. *MIS Quarterly Executive, 18*(4), 221–243. https://doi.org/10.17705/2msqe.00018

Jović, M., Tijan, E., Žgaljić, D., & Aksentijević, S. (2020). Improving maritime transport sustainability using blockchain-based information exchange. *Sustainability, 12*(21), 8866. https://doi.org/10.3390/su12218866

Keating, M. (2017). Europe as a multilevel federation. *Journal of European Public Policy, 24*(4), 615–632. https://doi.org/10.1080/13501763.2016.1273374

Khaqqi, K. N., Sikorski, J. J., Hadinoto, K., & Kraft, M. (2018). Incorporating seller/buyer reputation-based system in blockchain-enabled emission trading application. *Applied Energy, 209*, 8–19. https://doi.org/10.1016/j.apenergy.2017.10.070

Klein, H. K., & Myers, M. D. (1999). A set of principles for conducting and evaluating interpretive field studies in information systems. *MIS Quarterly, 23*(1), 67–93. https://doi.org/10.2307/249410

Kranz, J., Nagel, E., & Yoo, Y. (2019). Blockchain token sale. *Business & Information Systems Engineering, 61*(6), 745–753. https://doi.org/10.1007/s12599-019-00598-z

Kshetri, N. (2018). 1 Blockchain's roles in meeting key supply chain management objectives. *International Journal of Information Management*, vol. 39 (pp. 80–89). ⟨https://doi.org/10.1016/j.ijinfomgt.2017.12.005⟩.

Lacity, M. C. (2018). Addressing key challenges to making enterprise blockchain applications a reality. *MIS Quarterly Executive, 17*(3), 201–222.

Lauslahti, K., Mattila, J., Hukkinen, T., & Seppälä, T. (2018). Expanding the platform: Smart contracts as boundary resources. In A. Smedlund, & L. Mitronen (Eds.), *Collaborative value co-creation in the platform economy* (pp. 65–90). Singapore, SG: Springer. https://doi.org/10.1007/978-981-10-8956-5_4.

Leech, B. L. (2002). Asking questions: Techniques for semistructured interviews. *Political Science & Politics, 35*(04), 665–668. https://doi.org/10.1017/S1049096502001129

Leidner, D. E., & Kayworth, T. (2006). Review: A review of culture in information systems research: Toward a theory of information technology culture conflict. *MIS Quarterly, 30*(2), 357–399. https://doi.org/10.2307/25148735

Li, Y., Yang, W., He, P., Chen, C., & Wang, X. (2019). Design and management of a distributed hybrid energy system through smart contract and blockchain. *Applied Energy, 248*, 390–405. https://doi.org/10.1016/j.apenergy.2019.04.132

Liang, T.-P., Kohli, R., Huang, H.-C., & Li, Z.-L. (2021). What drives the adoption of the blockchain technology? A fit-viability perspective. *Journal of Management Information Systems, 38*(2), 314–337. https://doi.org/10.1080/07421222.2021.1912915

Lin, J., Pipattanasomporn, M., & Rahman, S. (2019). Comparative analysis of auction mechanisms and bidding strategies for P2P solar transactive energy markets. *Applied Energy, 255*, Article 113687. https://doi.org/10.1016/j.apenergy.2019.113687

Lindahl, H. (2000). Authority and representation. *Law and Philosophy, 19*(2), 223–246. https://doi.org/10.1023/A:1006466126333

Linux Foundation. (2017). Hyperledger. *Architecture, 1*. ⟨https://www.hyperledger.org/wp-content/uploads/2017/08/Hyperledger_Arch_WG_Paper_1_Consensus.pdf⟩.

Lockl, J., Schlatt, V., Schweizer, A., Urbach, N., & Harth, N. (2020). Toward trust in internet of things ecosystems: Design principles for blockchain-based IoT applications. *IEEE Transactions on Engineering Management, 67*(4), 1256–1270. https://doi.org/10.1109/TEM.2020.2978014

Lowitzsch, J., Hoicka, C. E., & van Tulder, F. J. (2020). Renewable energy communities under the 2019 European Clean Energy Package – Governance model for the energy clusters of the future. *Renewable and Sustainable Energy Reviews, 122*, Article 109489. https://doi.org/10.1016/j.rser.2019.109489

Luo, F., Dong, Z. Y., Liang, G., Murata, J., & Xu, Z. (2019). A distributed electricity trading system in active distribution networks based on multi-agent coalition and blockchain. *IEEE Transactions on Power Systems, 34*(5), 4097–4108. https://doi.org/10.1109/TPWRS.2018.2876612

Lüth, A., Zepter, J. M., Crespo del Granado, P., & Egging, R. (2018). Local electricity market designs for peer-to-peer trading: The role of battery flexibility. *Applied Energy, 229*, 1233–1243. https://doi.org/10.1016/j.apenergy.2018.08.004

Mackenzie, K. D. (2010). Turf disputes within federal systems: Leadership amidst enforceable checks and balances. *The Leadership Quarterly, 21*(6), 1050–1068. https://doi.org/10.1016/j.leaqua.2010.10.008

Marella, V., Upreti, B., Merikivi, J., & Tuunainen, V. K. (2020). Understanding the creation of trust in cryptocurrencies: The case of Bitcoin. *Electronic Markets, 30*(2), 259–271. https://doi.org/10.1007/s12525-019-00392-5

Mattila, J., & Seppälä, T. (2018). Distributed governance in multi-sided platforms: A conceptual framework from case: Bitcoin. In A. Smedlund, A. Lindblom, & L. Mitronen (Eds.), *Collaborative value co-creation in the platform economy* (pp. 183–205). Singapore, SG: Springer,. https://doi.org/10.1007/978-981-10-8956-5_10.

Mattke, J., Maier, C., Hund, A., & Weitzel, T. (2019). How an enterprise blockchain application in the U.S. pharmaceuticals supply chain is saving lives. *MIS Quarterly Executive, 18*(4), 245–261. https://doi.org/10.17705/2msqe.00019

Mayring, P. (2014). *Qualitative content analysis: Theoretical foundation, basic procedures and software solution*. Klagenfurt, AT.

Mckay, D. (2005). Economic logic or political logic? Economic theory, federal theory and EMU. *Journal of European Public Policy, 12*(3), 528–544. https://doi.org/10.1080/13501760500091810

Mendling, J., Pentland, B. T., & Recker, J. (2020). Building a complementary agenda for business process management and digital innovation. *European Journal of Information Systems, 29*(3), 208–219. https://doi.org/10.1080/0960085X.2020.1755207

Mengelkamp, E., Gärttner, J., Rock, K., Kessler, S., Orsini, L., & Weinhardt, C. (2018). Designing microgrid energy markets. *Applied Energy, 210*, 870–880. https://doi.org/10.1016/j.apenergy.2017.06.054

Morstyn, T., Farrell, N., Darby, S. J., & McCulloch, M. D. (2018). Using peer-to-peer energy-trading platforms to incentivize prosumers to form federated power plants. *Nature Energy, 3*(2), 94–101. https://doi.org/10.1038/s41560-017-0075-y

Moya Palencia, M. (1974). Federalism and administrative decentralization. *International Review of Administrative Sciences, 40*(1), 15–22. https://doi.org/10.1177/002085237404000103

Mu, W., Bian, Y., & Zhao, J. L. (2019). The role of online leadership in open collaborative innovation. *Industrial Management & Data Systems, 119*(9), 1969–1987. https://doi.org/10.1108/IMDS-03-2019-0136

Myers, M. D., & Newman, M. (2007). The qualitative interview in IS research: Examining the craft. *Information and Organization, 17*(1), 2–26. https://doi.org/10.1016/j.infoandorg.2006.11.001

Nathan, R. P. (2006). There will always be a new federalism. *Journal of Public Administration Research and Theory, 16*(4), 499–510. https://doi.org/10.1093/jopart/muj011

Noor, S., Yang, W., Guo, M., van Dam, K. H., & Wang, X. (2018). Energy demand side management within micro-grid networks enhanced by blockchain. *Applied Energy, 228*, 1385–1398. https://doi.org/10.1016/j.apenergy.2018.07.012

Oliveira, T., Faria, M., Thomas, M. A., & Popovič, A. (2014). Extending the understanding of mobile banking adoption: When UTAUT meets TTF and ITM. *International Journal of Information Management, 34*(5), 689–703. https://doi.org/10.1016/j.ijinfomgt.2014.06.004

Ølnes, S., Ubacht, J., & Janssen, M. (2017). Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. *Government Information Quarterly, 34*(3), 355–364. https://doi.org/10.1016/j.giq.2017.09.007

Orlikowski, W. J., & Baroudi, J. J. (1991). Studying information technology in organizations: Research approaches and assumptions. *Information Systems Research, 2*(1), 1–28. https://doi.org/10.1287/isre.2.1.1

Osterland, T., & Rose, T. (2018). Engineering sustainable blockchain applications. In *Proceedings of the ERCIM blockchain workshop 2018*. Reports of the European Society for Socially Embedded Technologies. ⟨https://doi.org/10.18420/blockchain2018_05⟩.

Ostern, N. (2018). Do you trust a trust-free technology? Toward a trust framework model for blockchain technology. In *Proceedings of the 39th international conference on information systems*.

Ostern, N., Rosemann, M., & Moormann, J. (2020). Determining the idiosyncrasy of blockchain: An affordances perspective. In *Proceedings of the 41st international conference on information systems*.

Pan, S. L., & Tan, B. (2011). Demystifying case research: A structured–pragmatic–situational (SPS) approach to conducting case studies. *Information and Organization, 21*(3), 161–176. https://doi.org/10.1016/j.infoandorg.2011.07.001

Pang, M.-S., Lee, G., & DeLone, W. H. (2014). IT resources, organizational capabilities, and value creation in public-sector organizations: A public-value management perspective. *Journal of Information Technology, 29*(3), 187–205. https://doi.org/10.1057/jit.2014.2

Parsons, C. (2002). Showing ideas as causes: The origins of the European Union. *International Organization, 56*(1), 47–84. https://doi.org/10.1162/002081802753485133

Pedersen, A. B., Risius, M., & Beck, R. (2019). A ten-step decision path to determine when to use blockchain technologies. *MIS Quarterly Executive, 18*(2), 99–115. https://doi.org/10.17705/2msqe.00010

Pencek, B. (2008). Book review: Transparency: The key to better governance?, In Christopher Hood, David Heald (Eds.), *Proceedings of the British academy*, 135. Oxford University Press, New York (2006), Published for the British Academy, Oxford. xiii, 231 pp. $60, £30 (cloth. Government Information Quarterly, vol. 25(3) (pp. 561–562). ⟨https://doi.org/10.1016/j.giq.2007.12.002⟩.

Perrons, R. K., & Cosby, T. (2020). Applying blockchain in the geoenergy domain: The road to interoperability and standards. *Applied Energy, 262*, Article 114545. https://doi.org/10.1016/j.apenergy.2020.114545

Rai, A., & Tang, X. (2010). Leveraging IT capabilities and competitive process capabilities for the management of interorganizational relationship portfolios. *Information Systems Research, 21*(3), 516–542. https://doi.org/10.1287/isre.1100.0299

Ravishankar, M. N. (2013). Public ICT innovations: A strategic ambiguity perspective. *Journal of Information Technology, 28*(4), 316–332. https://doi.org/10.1057/jit.2013.18

Renwick, R., & Gleasure, R. (2021). Those who control the code control the rules: How different perspectives of privacy are being written into the code of blockchain systems. *Journal of Information Technology, 36*(1), 16–38. https://doi.org/10.1177/0268396220944406

Reynolds, M. (2016). *Welcome to E-stonia, the world's most digitally advanced society*. ⟨https://www.wired.co.uk/article/digital-estonia⟩, Accessed 16.12.21.

Riasanow, T., Burckhardt, F., Soto Setzke, D., Böhm, M., & Krcmar, H. (2018). The generic blockchain ecosystem and its strategic implications. In *Proceedings of the 24th Americas conference on information systems*.

Rieger, A., Guggenmos, F., Lockl, J., Fridgen, G., & Urbach, N. (2019). Building a blockchain application that complies with the EU general data protection regulation. *MIS Quarterly Executive, 18*(4), 263–279. https://doi.org/10.17705/2msqe.00020

Riker, W. H. (1964). *Federalism: Origin, operation, significance*. Boston, MA, US: Little, Brown and Company.

Risius, M., & Spohrer, K. (2017). A blockchain research framework. *Business & Information Systems Engineering, 59*(6), 385–409. https://doi.org/10.1007/s12599-017-0506-0

Rodden, J., & Wibbels, E. (2002). Beyond the fiction of federalism: Macroeconomic management in multitiered systems. *World Politics, 54*(4), 494–531. https://doi.org/10.1353/wp.2002.0016

Rogers, E. M. (1995). *Diffusion of innovations* (4th ed.). New York, NY, US: The Free Press.

Rose, J., Persson, J. S., Heeager, L. T., & Irani, Z. (2015). Managing e-Government: Value positions and relationships. *Information Systems Journal, 25*(5), 531–571. https://doi.org/10.1111/isj.12052

Rossi, M., Mueller-Bloch, C., Thatcher, J. B., & Beck, R. (2019). Blockchain research in information systems: Current trends and an inclusive future research agenda. *Journal of the Association for Information Systems, 20*(9), 1388–1403. https://doi.org/10.17705/1jais.00571

Rubin, H., & Rubin, I. (2005). *Qualitative interviewing: The art of hearing data* (2nd ed.). Thousand Oaks, CA, US: SAGE Publications. https://doi.org/10.4135/9781452226651

Salcedo, E., & Gupta, M. (2021). The effects of individual-level espoused national cultural values on the willingness to use Bitcoin-like blockchain currencies. *International Journal of Information Management, 60*, Article 102388. https://doi.org/10.1016/j.ijinfomgt.2021.102388

Sarker, S., Henningsson, S., Jensen, T., & Hedman, J. (2021). The use of blockchain as a resource for combating corruption in global shipping: An interpretive case study. *Journal of Management Information Systems, 38*(2), 338–373. https://doi.org/10.1080/07421222.2021.1912919

Schultze, U., & Avital, M. (2011). Designing interviews to generate rich data for information systems research. *Information and Organization, 21*(1), 1–16. https://doi.org/10.1016/j.infoandorg.2010.11.001

Scott, M., DeLone, W., & Golden, W. (2016). Measuring eGovernment success: A public value approach. *European Journal of Information Systems, 25*(3), 187–208. https://doi.org/10.1057/ejis.2015.11

Sedlmeir, J., Buhl, H. U., Fridgen, G., & Keller, R. (2020). The energy consumption of blockchain technology: Beyond myth. *Business & Information Systems Engineering, 62* (6), 599–608. https://doi.org/10.1007/s12599-020-00656-x

Seebacher, S., & Schüritz, R. (2017). Blockchain technology as an enabler of service systems: A structured literature review. In *Proceedings of the 8th international conference on exploring service science*.

Seltsikas, P., & O'Keefe, R. M. (2010). Expectations and outcomes in electronic identity management: The role of trust and public value. *European Journal of Information Systems, 19*(1), 93–103. https://doi.org/10.1057/ejis.2009.51

Shafiei Gol, E., Stein, M.-K., & Avital, M. (2019). Crowdwork platform governance toward organizational value creation. *The Journal of Strategic Information Systems, 28* (2), 175–195. https://doi.org/10.1016/j.jsis.2019.01.001

Shevory, K. (2015). *Slowly, tech innovation makes inroads in government*. ⟨https://www.forbes.com/sites/techonomy/2015/06/26/slowly-tech-innovation-makes-inroads-in-government/?sh=645a1d31413b⟩, Accessed 16.12.21.

Sikorski, J. J., Haughton, J., & Kraft, M. (2017). Blockchain technology in the chemical industry: Machine-to-machine electricity market. *Applied Energy, 195*, 234–246. https://doi.org/10.1016/j.apenergy.2017.03.039

di Silvestre, M. L., Gallo, P., Ippolito, M. G., Musca, R., Riva Sanseverino, E., Tran, Q. T. T., & Zizzo, G. (2019). Ancillary services in the energy blockchain for microgrids. *IEEE Transactions on Industry Applications, 55*(6), 7310–7319. https://doi.org/10.1109/TIA.2019.2909496

Smith, C. R., & Fernandez, S. (2010). Equity in federal contracting: Examining the link between minority representation and federal procurement decisions. *Public Administration Review, 70*(1), 87–96. https://doi.org/10.1111/j.1540-6210.2009.02113.x

Soss, J., Fording, R. C., & Schram, S. F. (2008). The color of devolution: Race, federalism, and the politics of social control. *American Journal of Political Science, 52*(3), 536–553. https://doi.org/10.1111/j.1540-5907.2008.00328.x

Sousa, T., Soares, T., Pinson, P., Moret, F., Baroche, T., & Sorin, E. (2019). Peer-to-peer and community-based markets: A comprehensive review. *Renewable and Sustainable Energy Reviews, 104*, 367–378. https://doi.org/10.1016/j.rser.2019.01.036

Springer, H. W. (1962). Federation in the Caribbean: An attempt that failed. *International Organization, 16*(4), 758–775. https://doi.org/10.1017/S0020818300011619

Tangi, L., Janssen, M., Benedetti, M., & Noci, G. (2021). Digital government transformation: A structural equation modelling analysis of driving and impeding factors. *International Journal of Information Management, 60*, Article 102356. https://doi.org/10.1016/j.ijinfomgt.2021.102356

Thomas, L., Zhou, Y., Long, C., Wu, J., & Jenkins, N. (2019). A general form of smart contract for decentralized energy systems management. *Nature Energy, 4*(2), 140–149. https://doi.org/10.1038/s41560-018-0317-7

Tiller, S. R. (2011). Federalism and change. *Leadership and Management in Engineering, 11* (4), 297–301. https://doi.org/10.1061/(ASCE)LM.1943-5630.0000140

Tobias, C. (1989). Public law litigation and the federal rules of civil procedure. *Cornell Law Review, 74*(2), 270–346.

Tornatzky, L. G., & Fleischer, M. (1990). *The processes of technological innovation*. Lexington, MA, US: Lexington Books.

Toufaily, E., Zalan, T., & Dhaou, S. B. (2021). A framework of blockchain technology adoption: An investigation of challenges and expected value. *Information & Management, 58*(3), Article 103444. https://doi.org/10.1016/j.im.2021.103444

Trechsel, A. H. (2005). How to federalize the European Union … and why bother. *Journal of European Public Policy, 12*(3), 401–418. https://doi.org/10.1080/13501760500091117

Treiblmaier, H., Swan, M., de Filippi, P., Lacity, M., Hardjono, T., & Kim, H. (2021). What's next in blockchain research? *ACM SIGMIS DATABASE: The DATABASE for Advances in Information Systems, 52*(1), 27–52. https://doi.org/10.1145/3447934.3447938

Trkman, P. (2010). The critical success factors of business process management. *International Journal of Information Management, 30*(2), 125–134. https://doi.org/10.1016/j.ijinfomgt.2009.07.003

Tsiulin, S., Kristian, H. R., Hilmola, O.-P., Goryaev, N., & Karam, A. (2020). Blockchain-based applications in shipping and port management: A literature review towards defining key conceptual frameworks. *Review of International Business and Strategy, 30* (2), 201–224. https://doi.org/10.1108/RIBS-04-2019-0051

Tyworth, M. (2014). Organizational identity and information systems: How organizational ICT reflect who an organization is. *European Journal of Information Systems, 23*(1), 69–83. https://doi.org/10.1057/ejis.2013.32

Upadhyay, N. (2020). Demystifying blockchain: A critical analysis of challenges, applications and opportunities. *International Journal of Information Management, 54*, Article 102120. https://doi.org/10.1016/j.ijinfomgt.2020.102120

van Leeuwen, G., AlSkaif, T., Gibescu, M., & van Sark, W. (2020). An integrated blockchain-based energy management platform with bilateral trading for microgrid communities. *Applied Energy, 263*, Article 114613. https://doi.org/10.1016/j.apenergy.2020.114613

Venkatraman, N. (1989). The concept of fit in strategy research: Toward verbal and statistical correspondence. *Academy of Management Review, 14*(3), 423–444. https://doi.org/10.5465/amr.1989.4279078

Völter, F., Urbach, N., & Padget, J. (2021). Trusting the trust machine: Evaluating trust signals of blockchain applications. *International Journal of Information Management*. , Article 102429. https://doi.org/10.1016/j.ijinfomgt.2021.102429

Vos, J. F. J., & Boonstra, A. (2022). The influence of cultural values on enterprise system adoption, towards a culture – Enterprise system alignment theory. *International Journal of Information Management, 63*, Article 102453. https://doi.org/10.1016/j.ijinfomgt.2021.102453

Walsham, G. (2006). Doing interpretive research. *European Journal of Information Systems, 15*(3), 320–330. https://doi.org/10.1057/palgrave.ejis.3000589

Wang, W., Wang, Y., Zhang, Y., & Ma, J. (2020). Spillover of workplace IT satisfaction onto job satisfaction: The roles of job fit and professional fit. *International Journal of Information Management, 50*, 341–352. https://doi.org/10.1016/j.ijinfomgt.2019.08.011

Warkentin, M., & Orgeron, C. (2020). Using the security triad to assess blockchain technology in public sector applications. *International Journal of Information Management, 52*, Article 102090. https://doi.org/10.1016/j.ijinfomgt.2020.102090

Watts, R. L. (1998). Federalism, federal political systems, and federations. *Annual Review of Political Science, 1*(1), 117–137. https://doi.org/10.1146/annurev.polisci.1.1.117

Weber, C. (2005). CPM/PDD – An extended theoretical approach to modelling products and product development processes. In H. Bley, H. Jansen, & F.-L.S.M. Krause (Eds.), *Advances in methods and systems for development of products and processes, Proceedings of the 2nd German-Israeli symposium for design and manufacturing* (pp. 159–179). Stuttgart: Fraunhofer IRB Verlag.

Wibbels, E. (2006). Madison in Baghdad?: Decentralization and federalism in comparative politics. *Annual Review of Political Science, 9*(1), 165–188. https://doi.org/10.1146/annurev.polisci.9.062404.170504

Yin, R. K. (2014). *Case study research* (5th ed.). Thousand Oaks, CA, US: Sage Publications.

Ying, W., Jia, S., & Du, W. (2018). Digital enablement of blockchain: Evidence from HNA group. *International Journal of Information Management, 39*, 1–4. https://doi.org/10.1016/j.ijinfomgt.2017.10.004

Zhang, P., White, J., Schmidt, D. C., Lenz, G., & Rosenbloom, S. T. (2018). FHIRChain: Applying blockchain to securely and scalably share clinical data. *Computational and Structural Biotechnology Journal, 16*, 267–278. https://doi.org/10.1016/j.csbj.2018.07.004

Zhang, T., Pota, H., Chu, C.-C., & Gadh, R. (2018). Real-time renewable energy incentive system for electric vehicles using prioritization and cryptocurrency. *Applied Energy, 226*, 582–594. https://doi.org/10.1016/j.apenergy.2018.06.025

Zhang, W., Wei, C.-P., Jiang, Q., Peng, C.-H., & Zhao, J. L. (2021). Beyond the block: A novel blockchain-based technical model for long-term care insurance. *Journal of Management Information Systems, 38*(2), 374–400. https://doi.org/10.1080/07421222.2021.1912926

Ziblatt, D. (2004). Rethinking the origins of federalism: Puzzle, theory, and evidence from nineteenth-century Europe. *World Politics, 57*(1), 70–98. https://doi.org/10.1353/wp.2005.0013

Zigurs, I., & Buckland, B. K. (1998). A theory of task/technology fit and group support systems effectiveness. *MIS Quarterly, 22*(3), 313–334. https://doi.org/10.2307/249668

Zigurs, I., & Khazanchi, D. (2008). From profiles to patterns: A new view of task-technology fit. *Information Systems Management, 25*(1), 8–13. https://doi.org/10.1080/10580530701777107

Ziolkowski, R., Miscione, G., & Schwabe, G. (2020). Decision problems in blockchain governance: Old wine in new bottles or walking in someone else's shoes? *Journal of Management Information Systems, 37*(2), 316–348. https://doi.org/10.1080/07421222.2020.1759974

Tamara Roth is a researcher at the Interdisciplinary Center for Security, Reliability and Trust (SnT) at the University of Luxembourg. Her research interests include the effect of cultural values on the adoption of cryptographic technologies in the public sector as well as the design of solutions based on cryptographic technologies for the healthcare sector. Prior to joining the SnT, Tamara has been a research assistant at the University of Bayreuth at the Faculty of Biology, Chemistry & Earth Sciences.

Alexander Stohr is a researcher **at the Finance & Information Management (FIM) Research Center, University of Bayreuth, and the Project Group Business & Information Systems Engineering of the Fraunhofer FIT. His current research focuses on the adoption of emerging technologies, such as blockchain and artificial intelligence, and their socio-technical implications. Alex has worked as a consultant on a variety of industry projects before joining the BAMF's blockchain project in August 2019.**

Julia Amend is a is a researcher at the Finance & Information Management (FIM) Research Center and the Project Group Business & Information Systems Engineering of the Fraunhofer FIT, University of Bayreuth. Her current research focuses on blockchain technology in the public and private sector. Julia has worked as project

manager at Fresenius Medical Care before joining the BAMF's blockchain project in March 2020.

Gilbert Fridgen is full professor and PayPal-FNR PEARL Chair in Digital Financial Services in the Interdisciplinary Center for Security, Reliability and Trust (SnT) at the University of Luxembourg. His work focuses on smart grids, the machine economy, and blockchain technology in both the public and private sectors. Gilbert's work has been published in several prominent information systems, management, computer science and engineering journals. He has also managed various industry research projects and received multiple research grants. Gilbert has served as expert counsel to many German government bodies, including the Bundestag and six German federal ministries, and also to the European Commission through its European Blockchain Partnership.

Alexander Rieger is a research associate at the Interdisciplinary Center for Security, Reliability and Trust (SnT) at the University of Luxembourg. His research interests include innovative digital technologies such as blockchain, digital identities, and artificial intelligence, and, more specifically, their design, governance and strategic implications. Alex leads the scientific advisory team for the blockchain project of Germany's Federal Office for Migration and Refugees and acts as advisor to the European Blockchain Partnership and various public and private sector partners in Germany and Luxembourg. Prior to joining the SnT, he was the operational lead of the Fraunhofer Blockchain Lab.

RP2: Roth, T., Utz, M., Baumgarte, F., Rieger, A., Sedlmeir, J., & Strüker, J. (2022). **Electricity powered by blockchain: A review with a European perspective.** Applied Energy, 325, DOI: 10.1016/j.apenergy.2022.119799.

Journal Ranking: 21.1 (CiteScore); 2.758 (SNIP)

Contents lists available at ScienceDirect

Applied Energy

journal homepage: www.elsevier.com/locate/apenergy

Electricity powered by blockchain: A review with a European perspective

Tamara Roth [a], Manuel Utz [b], Felix Baumgarte [c], Alexander Rieger [a,*], Johannes Sedlmeir [c], Jens Strüker [c]

[a] *Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg, Luxembourg, Luxembourg*
[b] *Faculty of Law, Business & Economics, University of Bayreuth, Bayreuth, Germany*
[c] *Branch Business and Information Systems Engineering of the Fraunhofer FIT, FIM Research Center, University of Bayreuth, Bayreuth, Germany*

HIGHLIGHTS

- Many blockchain projects in Europe's energy systems fail.
- Technological, legal, and organizational challenges often outweigh benefits.
- Certificate trading and machine identities are increasingly hyped applications.
- Blockchain can best leverage its benefits when it takes a backseat.

ARTICLE INFO

Keywords:
Blockchain
Benefits
Challenges
Energy Systems
Machine Identities
Systematic Literature Review

ABSTRACT

Blockchain is no longer just a hype technology, and effective blockchain applications exist in many industries. Yet, few blockchain projects have been successful in Europe's energy systems. To identify the reasons for this slow progress, we reviewed the recent energy literature regarding the use of blockchain, analyzed industry reports, and interviewed experts who have conducted blockchain projects in Europe's energy systems. Our analysis reveals eight common use cases, their expected benefits, and the challenges encountered. We find that the expected benefits are often little more than generic hopes, largely outweighed by technological, organizational, and regulatory challenges. The identified challenges are significant and numerous, especially for peer-to-peer trading and microgrid use cases. The fact that few projects have yet provided robust evidence for profitable use suggests there is still a rocky road ahead. Moreover, many use cases appear to require more than just blockchain technology to succeed. In particular, privacy and scalability requirements often call for systems in which blockchains only take a backseat. This realization may be essential for the future use of blockchain technology in energy systems – in Europe and beyond.

1. Introduction

In the past few years, blockchain has attracted attention across many industries and become a veritable hype technology. In a predominantly technology-driven effort, various industries have initiated projects to test the prospects and limitations of blockchain applications. Success stories – such as some reported from logistics and retail, where blockchain enables the sharing of digital trade documents and improves the efficiency of supply chains [1,2] – have fueled similar expectations for the use of blockchain in energy systems [3,4]. In particular, blockchain's ability to enable intermediary-free transactions was expected to support the integration of an increasing number of distributed renewable energy sources (RES) that require more flexible, local concepts [5–7]. Accordingly, various research and pilot projects began to explore use cases for blockchain [5,8]. Many of these projects were concentrated in Europe, which could be considered a hotbed for the use of blockchain in energy systems [5,9].

Blockchains are primarily known for their use as registries for cryptocurrency transactions, such as Bitcoin or Ethereum, and for the enormous energy consumption of the Proof of Work (PoW) consensus mechanisms many of these cryptocurrencies use [10–12]. At the same time, blockchains have gained a reputation of being particularly secure and tamper-proof database systems. Every transaction written to a blockchain is cryptographically linked to the previous transaction,

* Corresponding author.
E-mail address: alexander.rieger@uni.lu (A. Rieger).

https://doi.org/10.1016/j.apenergy.2022.119799
Received 12 May 2022; Received in revised form 19 July 2022; Accepted 3 August 2022
Available online 19 August 2022

which creates a transparent and traceable record. Copies of this record are stored across various nodes in a blockchain network and authorized nodes continuously vet the validity of new transactions [5,12].

These origins and properties have made blockchain especially popular in the context of peer-to-peer concepts. The proposed use cases range from transaction processing at the retail level to supporting selected processes in wholesale and system services markets [13–15]. Blockchain was hyped for improving the balancing of generation and demand, and for facilitating more automated and secure transactions between the various actors [13,16,17]. Similar expectations emerged in the context of e-roaming. Blockchain was promoted as a means to mediate range anxiety by facilitating vehicle-to-vehicle transactions [16] or prosumer services [5,15]. More recent ideas include the labeling of electricity [16,17], the trading of certificates of origin or emission [18,19], and machine identities [20,21].

Despite this wide range of use case ideas, many projects have since been abandoned or are still at a pilot stage – especially in Europe [5,9]. Some publications, such as [5,14,22], have begun to identify challenges that might contribute to this slow adoption. These encompass, for instance, high barriers to market entry for smaller actors [5], legally required market actor roles [6], and scalability and interoperability issues [14,23]. Yet, it remains ambiguous how exactly these challenges impact the feasibility of the various blockchain use cases and what implications they may have for the future of blockchain technology in Europe's energy systems.

Thus, the aim of our paper is to provide a balanced, more practice-informed, and 'past-the-hype' overview on the use of blockchain technology in Europe's energy systems. Secondly, we aim to identify and rate the benefits and challenges related to the use of blockchain. Thirdly, we indicate avenues for further research where the use of blockchain appears promising. To inform our investigation, we reviewed academic papers, and in addition, studied industry reports and conducted expert interviews. From this consolidated analysis, we identified eight common use cases, their expected benefits, and the challenges encountered.

2. Background

Blockchain technology has its roots in the cryptocurrency industry [24], but over the last years it has also found its way into energy systems [6,22,25]. Simply speaking, blockchains are a particular type of database that groups data into a block structure [25,26]. More technically speaking, blockchains are distributed ledgers that are replicated, shared, and distributed across multiple servers in a blockchain network – so-called nodes [19,27]. A selection of these nodes can append new blocks using so-called consensus mechanisms that help select the node that can append the next block [19,26,28]. Each new block references the previous block using a hash-pointer [29]. These pointers typically make retrospective changes to the blockchain easy to detect, and together with data replication on several nodes, they create a highly secure, transparent, auditable, and robust transaction environment [30].

Dependent on the network design, any participant can host a blockchain node and add a new block [31]. Such a 'public', permissionless design is particularly attractive for residential peer-to-peer trading, as it permits any prosumer to participate [8]. Yet, there are also 'private', permissioned designs that limit participation, e.g., to certain companies or public organizations [32]. These designs are closer to the structure of many European energy systems and allow for the distribution of rights to write and access data on the blockchain in accordance with legally mandated roles and attributed competencies [5,6].

Beyond storing data and processing simple payments, blockchains may also execute programming logic with the help of so-called smart contracts [33,34]. These are redundantly executed scripts that enable participants to control how data is processed by the blockchain network. As such, they can considerably reduce dependencies on trusted third parties and enable reliable information sharing and process automation [35–37]. Moreover, they reduce the vulnerability to failures and attacks, which makes blockchain particularly attractive for applications in energy systems [38,39]. The avoidance of trusted third parties also prevents the aggregation of market power and mitigates lock-in effects [40].

Inspired by the technological capabilities of blockchains and their use across various industries, academic researchers have started to explore their potential benefits for energy systems. This research has quickly evolved into a plethora of different and often parallel discussions [26,34,35], ranging from conceptual aspects to empirical and analytical models [25,36]. Examples include prototypes with more accurate pricing mechanisms for peer-to-peer markets [39,40] and calculations of costs (reductions) [41,42]. While some studies try to capture benefits over the full range of possible applications [5], others focus on the 'disruptive potential' of the use of blockchain [35]. A prominent example for these 'disruptive' use cases is residential peer-to-peer trading [5,14,21]. Overall, discussions on the use of blockchain in energy systems are mostly theoretical and strongly focused on potential benefits [25,26].

Previous reviews also only selectively elaborate on the challenges of using blockchain technology in energy systems. One of the first reviews by Andoni et al. [5] aims to provide a comprehensive overview of technical aspects, such as different consensus mechanisms, and explores their application in 140 blockchain research and pilot projects. Based on their analysis of academic literature and project reports at the peak of the blockchain hype, they derive potential opportunities and challenges of blockchain technologies in diverse use cases. Another review by Ante et al. [22], past the initial hype, uses a bibliometric analysis to explore dominant research streams on the use of blockchain in energy systems. They identify overall six use case patterns and explore the extent to which the use cases focus on blockchain or on general improvements of the energy system without a specific technology. Based on the analysis of selected papers, Ante et al. [22] also discuss a roadmap for future research. The latest review by Choobineh et al. [14] aims to provide a more comprehensive overview of benefits and challenges of using blockchains in energy systems. Based on a literature review, they derive a plethora of vague benefits based on inherent characteristics of blockchain technology, five dominant challenges of blockchain applications in energy systems, and four emerging trends that may help blockchain thrive.

Although instructive, these reviews provide few indications of feasible applications, their actual benefits, or challenges associated with the use of blockchain technology. Moreover, they do not include 'past-the-hype' insights from pilot projects that might advance the understanding of drivers and inhibitors of blockchain applications in energy systems.

3. Materials and Methods

Here, we offer a balanced and empirically substantiated overview of common blockchain use cases in Europe, including the benefits and challenges of using blockchain technology. We selected three different data sources for our analysis: Academic literature, industry reports, and expert interviews. First, we searched for high-quality academic literature by conducting a systematic literature review. For our review, we followed Kitchenham's five-step approach [43], which involved (1) the identification of relevant publications, (2) their selection, (3) their quality assessment, (4) the extraction and evaluation of data, and (5) the aggregation and interpretation of data. Second, we identified industry reports from renowned agencies, research institutions, think tanks, start-ups, non-profit organizations, and consulting firms to add an industry perspective. Lastly, we conducted interviews with industry experts to gain in-depth insights into blockchain projects in Europe's energy systems. In total, we reviewed 89 academic papers, analyzed 42 industry reports, and conducted 45 interviews with academic, technical, legal, and business experts who have worked on blockchain projects in

Europe's energy systems.

3.1. Data collection

3.1.1. Academic literature selection

In line with Kitchenham's approach [43], we conducted a keyword search across five databases: IEEE Xplore, Scopus, Science Direct, Taylor & Francis, and SAGE Journals. To combine our keywords, we used the Boolean operators AND and OR:

1. "Blockchain" **AND** ("Energy Sector" **OR** "Energy System" **OR** "Power System" **OR** "Electric Power System")
2. "Blockchain" **AND** ("Power Markets" **OR** "Electricity Trading")
3. "Blockchain" **AND** ("Energy Management System" **OR** "Electricity Management System")

In addition, we applied a set of selection criteria regarding the year of publication, language, and publication type. That is, we focused on publications from 2018 onwards when blockchain projects in Europe's energy systems began to reach a level of maturity beyond conceptualization and proof of concepts. For additional quality assurance, we focused on published and peer-reviewed articles in journals with a 75 percentile or higher Scopus rating and only included articles written in English. To filter out academic contributions that did not focus on blockchain applications in energy systems, we restricted the search fields – dependent on the available filters for the different databases – to abstract, keywords, and introduction. All identified literature was transferred to the bibliographic manager Mendeley. We extracted overall 710 academic contributions with our initial keyword search after having removed duplicates.

We further refined the results of this pre-selection of relevant literature throughout Kitchenham's selection and quality assessment steps [43]. To illustrate these steps and our applied selection criteria, we used the Preferred Reporting Items for Systematic Reviews and meta-Analyses (PRISMA) protocol by [44]. The protocol afforded additional rigor and enabled transparency and replicability of our results (Fig. 1). During the screening and refinement phases, we reviewed titles and abstracts of the high-quality subset and narrowed down our body of literature to 89 academic publications that focused on the application of blockchain technology in energy systems (see Appendix A1).

3.1.2. Industry report selection

Industry reports were selected by identifying reports of renowned agencies, research institutions, think tanks, start-ups, non-profit organizations, and consulting firms from 2018 onwards. We only included reports that had a clear focus on the application of blockchain technology in energy systems. Regarding language, we primarily included reports that were either directly written in English or translated into English. After having reviewed the executive summaries and tables of content, we identified a total of 42 relevant industry reports, which are detailed in Appendix A2.

3.1.3. Interviews

Since literature and industry reports only provided a high-level overview of benefits and challenges in blockchain projects and often lacked a practice-informed perspective, our main method of data collection was interviews. More specifically, we contacted developers and employees of energy companies in key positions, who were directly involved in blockchain projects. Almost all interviewees were from Europe, where a large part of the ongoing blockchain projects in energy systems are located, such as Germany, Austria, Switzerland, and Spain. We conducted 45 semi-structured interviews using an interview guide (see Appendix A3) to ensure coverage of our focal topic while allowing the conversation to develop naturally [37,39]. This provided detailed and authentic insights into the interviewees' perspectives of their projects [40,41]. We conducted each interview with one or two interviewers, audio-recorded the discussion, and took notes. Audio recordings were later transcribed for further analysis.

The interviews consisted of overall three parts. We began with a brief introduction. We then asked the interviewees for their experience and perspective regarding the benefits and challenges of using blockchain technology in their project or related projects. Lastly, we asked for recommendations on how policy makers could contribute to the success of blockchain projects in energy systems. Dependent on the individual knowledge and expertise of our interviewees, we adapted the questions and changed the interviews' focus, allowing the interviewees to go into directions they found interesting [45]. We provide an overview of the interviews in Appendix A4.

3.2. Data analysis

From the identified academic literature, industry reports, and conducted interviews, we first extracted the most commonly discussed use cases. Those that were only mentioned in one or two studies, industry reports, or interviews, were excluded. This selection resulted in eight use cases, which we then analyzed regarding specific benefits and challenges of the use of blockchain technology. We based our review on a two-step coding process in line with Corbin and Strauss' [46] recommendations for grounded theory development. That is, we coded openly and focused on positively and negatively connotated statements regarding the implementation of blockchain technology for specific use cases. In a subsequent axial coding phase, we explored the relationship between different benefits and challenges and tried to find higher-level groups to summarize them. To support coding, we used the MAXQDA software toolkit. Our analysis led to overall 58 first-order themes and six second-order categories. More specifically, we identified three benefit and three challenge types: (1) efficiency benefits, (2) effectiveness gains, and (3) an added level of security as well as (1) organizational challenges, (2) technological challenges, and (3) regulatory challenges.

3.2.1. Use case analysis

To evaluate and rate the identified benefits and challenges for each use case, we employed established qualitative data analysis techniques

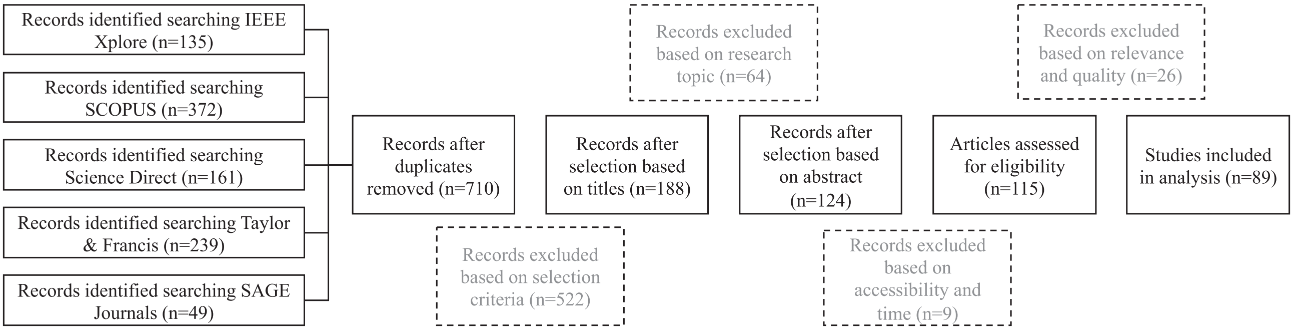

Records identified searching IEEE Xplore (n=135)
Records identified searching SCOPUS (n=372)
Records identified searching Science Direct (n=161)
Records identified searching Taylor & Francis (n=239)
Records identified searching SAGE Journals (n=49)
Records after duplicates removed (n=710)
Records excluded based on selection criteria (n=522)
Records after selection based on titles (n=188)
Records excluded based on research topic (n=64)
Records after selection based on abstract (n=124)
Records excluded based on accessibility and time (n=9)
Articles assessed for eligibility (n=115)
Records excluded based on relevance and quality (n=26)
Studies included in analysis (n=89)

Fig. 1. Overview of the academic literature selection.

[47,48]. In particular, we went through three additional rounds of coding. In a first round, we read again through all data sources – that is, we challenged and validated our initial annotations of "benefit" or "challenge" for relevant statements allocated to specific use cases.

In the second round, we looked for adjectives, adverbs, or other details in the sentences surrounding the respective statements, such as elaboration on a specific benefit or challenge, to better assess their overall relevance for the success or failure of blockchain projects. As this proved difficult on a verbal basis, we transferred the extracted insights into a Likert-scaled format. Specifically, we used a 7-point Likert scale ranging from 1 (not substantial) to 7 (very substantial). To achieve objectivity, we collected the annotated statements in a large table that listed the identified use cases on the horizontal axis and the benefit and challenge types on the vertical axis.

In a third round of coding, we went through the collected statements and conducted an initial rating of the importance of individual benefits and challenges. Throughout this process, we used the above-mentioned criteria and coded in two independent two-person groups. These two groups would go through the aggregated statements and assign a numerical value within the 7-point Likert scale for each of the identified challenges and benefits of every use case. Thereafter, the two groups compared their independently obtained assessments, discussed differences, and settled on a final rating. Where the two groups differed significantly in their rating, we additionally consulted the interviewed experts. To evaluate the third round of coding, we calculated intra-rater and inter-rater reliability using the Cohen's kappa coefficient [49]. Scores of 0.90 and 0.72 for intra-rater and inter-rater reliability indicated a substantial to "almost perfect" overlap between the two groups [50].

To increase the clarity of our results, we summarized our rating in a heatmap (Fig. 2). More specifically, we used color-codes based on the 7-point Likert scale to signify the importance of an identified benefit or challenge category. We used green to signal substantial benefits (5–7) and negligible challenges (1–2), yellow for uncertain benefits (3–4) and manageable challenges (3–4), and red for negligible benefits (1–2) and substantial challenges (5–7). We provide a list of the sources on which we based our use case analysis in Appendix A5.

4. Results

4.1. Common use cases

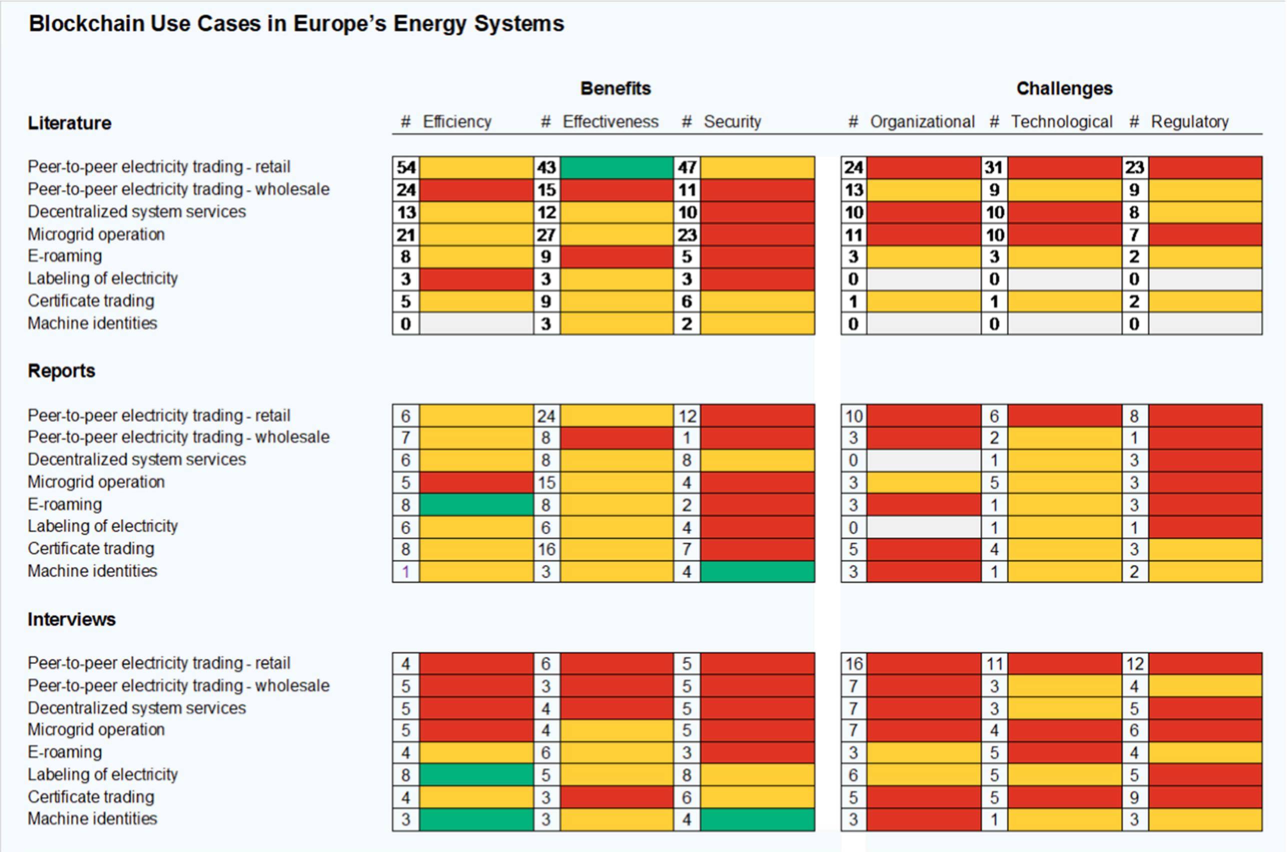
Our analysis revealed that blockchain projects in Europe commonly focus on a set of eight use cases (Table 1).

4.1.1. Peer-to-peer electricity trading and decentralized system services

Many projects explore the use of blockchain for *retail* or *wholesale peer-to-peer electricity trading* as well as *decentralized system services*. These applications are similar in that each uses blockchain to reduce dependence on centralized market operators [25]. They differ, however, in the addressed market inefficiencies.

Retail trading applications seek to facilitate trading between small actors that typically do not have access to wholesale electricity markets. Specifically, they try to reduce the costs of small transactions by automating transaction processing with blockchain-based registries and smart contracts [40,41,51]. Reduced processing costs, in turn, would enable small electricity producers to turn a profit from selling their power [52–54]. Moreover, they would increase the attractiveness of buying local and thus create a larger pool of potential customers for small producers [5,55,56].

Most wholesale trading applications try to improve the operation of wholesale electricity markets. Specifically, they explore the use of blockchain-based registries and smart contracts to reduce the cost of clearing and settlement processes, for instance, by reducing the number



Blockchain Use Cases in Europe's Energy Systems

	Benefits						Challenges					
Literature	#	Efficiency	#	Effectiveness	#	Security	#	Organizational	#	Technological	#	Regulatory
Peer-to-peer electricity trading - retail	**54**	🟨	**43**	🟩	**47**	🟨	**24**	🟥	**31**	🟥	**23**	🟥
Peer-to-peer electricity trading - wholesale	**24**	🟥	**15**	🟥	**11**	🟥	**13**	🟨	**9**	🟨	**9**	🟨
Decentralized system services	**13**	🟨	**12**	🟨	**10**	🟥	**10**	🟥	**10**	🟥	**8**	🟨
Microgrid operation	**21**	🟨	**27**	🟨	**23**	🟥	**11**	🟥	**10**	🟥	**7**	🟥
E-roaming	**8**	🟨	**9**	🟥	**5**	🟥	**3**	🟨	**3**	🟨	**2**	🟨
Labeling of electricity	**3**	🟥	**3**	🟨	**3**	🟥	**0**	⬜	**0**	⬜	**0**	⬜
Certificate trading	**5**	🟨	**9**	🟨	**6**	🟨	**1**	🟨	**1**	🟨	**2**	🟨
Machine identities	**0**	⬜	**3**	🟨	**2**	🟨	**0**	⬜	**0**	⬜	**0**	⬜
Reports												
Peer-to-peer electricity trading - retail	6	🟨	24	🟨	12	🟥	10	🟥	6	🟥	8	🟥
Peer-to-peer electricity trading - wholesale	7	🟨	8	🟥	1	🟥	3	🟥	2	🟨	1	🟥
Decentralized system services	6	🟨	8	🟨	8	🟨	0	⬜	1	🟨	3	🟥
Microgrid operation	5	🟥	15	🟨	4	🟥	3	🟨	5	🟨	3	🟥
E-roaming	8	🟩	8	🟨	2	🟥	3	🟥	1	🟨	3	🟥
Labeling of electricity	6	🟨	6	🟨	4	🟥	0	⬜	1	🟨	1	🟥
Certificate trading	8	🟨	16	🟨	7	🟥	5	🟥	4	🟨	3	🟨
Machine identities	1	🟨	3	🟨	4	🟩	3	🟥	1	🟨	2	🟨
Interviews												
Peer-to-peer electricity trading - retail	4	🟥	6	🟥	5	🟥	16	🟥	11	🟥	12	🟥
Peer-to-peer electricity trading - wholesale	5	🟥	3	🟥	5	🟥	7	🟥	3	🟨	4	🟨
Decentralized system services	5	🟥	4	🟥	5	🟥	7	🟥	3	🟨	5	🟥
Microgrid operation	5	🟥	4	🟨	5	🟥	7	🟥	4	🟥	6	🟥
E-roaming	4	🟨	6	🟨	3	🟥	3	🟨	5	🟥	4	🟨
Labeling of electricity	8	🟩	5	🟨	8	🟨	6	🟨	5	🟨	5	🟥
Certificate trading	4	🟨	3	🟥	6	🟨	5	🟥	5	🟥	9	🟥
Machine identities	3	🟩	3	🟨	4	🟩	3	🟥	1	🟨	3	🟨

Fig. 2. Evaluation of commonly implemented blockchain use cases in Europe's energy systems.

Table 1
Identified, commonly discussed blockchain use cases in energy systems and their definitions.

Use Case	Use Case Definition
Peer-to-peer electricity trading – retail	Processing of transactions in (local) energy markets for small actors
Peer-to-peer electricity trading – wholesale	Processing of transactions in large commercial markets for electricity
Decentralized system services	Processing of transactions in markets for system services and flexibility
Microgrid operation	Balancing of demand and supply in microgrids as well as processing of related transactions
E-roaming	Exchange of financial and identity-related data between charging point operators, e-mobility service providers, and e-mobility customers
Labeling of electricity	Tracing of feed-in levels for power generation and storage facilities as well as processing of related energy purchase agreements
Certificate trading	Processing of clearing and settlement for certificates that provide proof of origin or emission from specific generation and storage facilities
Machine identities	Authentication and validation of identity-related documents that confirm identity attributes of e.g., power generation and storage units

of warranties required [35,57]. Moreover, smart contracts are discussed as means to automate certain exchange trading activities such as escrow services [35,58]. These improvements are expected to reduce access barriers to exchange trading so that also smaller actors can participate in these markets [3,59]. Some wholesale trading applications also focus on over-the-counter (OTC) electricity trading [6,60–62]. These applications try to reduce the use of e-mails, instant messaging, or phone calls in the processing of OTC transactions. They use blockchains as tamper-resistant registries to verify transactions in case of misunderstandings or suspected fraud [35,63].

Like wholesale applications, *decentralized system services* applications seek to improve the operation of system service markets. They explore the use of smart contracts to decentralize and automate many control services including registration, verification, and approval required for participation in these markets [61,64]. Smart contracts could additionally automate the activation and settlement of system services [35,40]. Moreover, they may optimize billing processes where these are characterized by cumbersome manual paperwork and require a substantial amount of time [25,65,66].

4.1.2. Microgrid operation

Microgrid operation applications provide automated microgrid management where conventional, centralized management models and tools are not feasible or desirable [67,68]. They involve the use of smart contracts to schedule and manage production and consumption units in microgrids [22]. Blockchain-based registries are used to collect and track schedules and flexibility potentials for these units. Smart contracts then use this information to balance demand and supply, automatically activate flexibility potentials when required, and even potentially increase cyber-security [69,70]. The unit's actual power generation and consumption levels are again tracked in a blockchain-based registry to facilitate later settlement and allocation of flexibility costs. Microgrid applications are typically combined with peer-to-peer trading applications to cover both grid management and economic aspects.

4.1.3. E-roaming

E-roaming applications address the problem of limited access to charging points by enabling the free and secure exchange of relevant data regardless of charging network membership [41,57,71]. Some of these applications rely on blockchains to exchange electric vehicle charging data and settle transactions between charging point operators and mobility service providers. Others use blockchains as a registries for identity-related documents that enable easy and secure identification and authentication of e-mobility customers. The blockchain attests the authenticity and validity of these documents. Smart contracts are used to validate the credentials and automatically issue invoices after the charging process has been completed.

4.1.4. Labeling of electricity

Labeling of electricity applications use blockchain to track the share of power being fed into the grid by different sources at the time of consumption [72]. These applications are typically combined with RES generation facilities to create 'green' labels and reduce the risks of greenwashing but some projects also focus on creating 'local' labels [73,74]. Smart contracts can additionally be used to automate the processing of energy purchase agreements for the labeled electricity. The settled quantities can again be stored on the blockchain [57,75,76] to mitigate concerns regarding the sources of consumed electricity, accelerate data exchange, and reduce manual processes [58,77].

4.1.5. Certificate trading

Certificate trading applications employ blockchain to create and exchange certificates that provide a proof of origin or emission [78]. They can be seen as an extension of labeling of electricity applications as most use labeling data to create certificates that establish the origin or emissions for specific generation and storage facilities [79,80]. The certificates can be anchored or fully stored on the blockchain to create a validity registry as well as a transparent and unequivocal ownership history [5,81,82]. Smart contracts are used for issuing as well as processing and documenting certificate exchange [83].

4.1.6. Machine identities

Several projects have recently begun to explore *machine identity* applications [57,84,85]. The underlying idea is to package identity-related information about power generation and storage units as machine-verifiable, digital credentials [86–88]. These digital credentials can then be used for identification and authentication purposes. They are typically anchored on a blockchain, which stores essential cryptographic material and information on accredited issuers, schemas to verify credential authenticity, and revocation registries to verify credential validity. Blockchains are used because certain blockchains readily support digital credentials and because they reduce lock-in effects [89,90].

4.2. Expected benefits

Results from our analyses of the eight use cases could be attributed to three types of expected benefits (Table 2): efficiency, effectiveness, and security. Use cases that emphasize efficiency use blockchain to improve the output of a process. For instance, this can involve the reduction of overhead costs associated with traditional trading practices, or an increased speed of transactions [3,91,92].

Use cases that pursue effectiveness aim to achieve a desired output by improving the structure of processes. Such improvement approaches primarily focus on the empowerment of small actors by excluding intermediaries, who process transactions, and on the design of

Table 2
Identified benefits of using blockchain in energy systems.

Efficiency	Effectiveness	Security
• Digitalization and automation of processes, services, and transactions • Reduction of process, service, and transaction costs • Flexibility of processes, services, and transactions	• Decentralization and disintermediation • Autonomy from macro-grids • Empowerment of small actors within energy communities • Market flexibility • Reduction of complexity	• Transparency • Data security and data sovereignty • Creation of trust through tamper-resistant data storage • Resiliency and reliability

decentralized and self-sustaining energy infrastructures [4,6,60]. Expected security improvements include the protection of processes from failure and attacks, ensuring reliable output. Specifically, blockchain technology is understood to enable tamper-resistant data storage [5,72,93] and strengthen cyber-security [3,92], which is believed to enhance the robustness of energy systems [34,92] and ensure the security of supply. Additional transparency provides monitoring capabilities, which further enhances security [52,94].

All benefits in our analysis fit into one of the three benefit types. Security benefits were commonly identified as being of secondary importance because acceptable levels of security are often already provided by common database technologies. Although we expected benefits to differ between the various use cases and project settings, most sources did not progress beyond the mention of generic benefits, and we could identify only few specific benefits (Table 2). In many ways, the named benefits were variations of general attributes of blockchain, such as secure and redundant data storage or reliable information sharing and process automation [5,19,22,72]. They appear more as hopes of a fundamental change to energy systems, not as real benefits derived from blockchain technology. For instance, the expected cost savings from the use of blockchain technology are difficult to quantify. Specifically, cost estimates for developing, maintaining, and integrating blockchain applications are often fraught with uncertainty and reference costs are hard to establish. As a result, few blockchain applications have a clear ‘business case’, which reduces their economic attractiveness.

4.3. *Encountered challenges*

In addition to benefits, we also identified challenges commonly encountered in blockchain projects (Table 3). The challenges are far more specific and numerous than the identified benefits. Although many challenges are particular to the respective use case, they can be grouped into three types: organizational, technological, and regulatory.

Organizational challenges include all problems arising from changes to organizational structures, roles, or processes. They result especially from the desired replacement of essential mediating actors and the vague delegation of responsibilities in decentralized and disintermediated structures [5,35,95]. Moreover, many actors are deterred by the need for high levels of involvement and participation combined with unpredictable and hidden costs, particularly when they feel little regulatory and customer pressure to innovate [60,96].

Technological challenges result from difficulties in integrating blockchain with legacy systems and meeting functional requirements for successful application in energy systems. A lack of interoperability and technical standards, and the blockchain trilemma of decentralization, scalability, and security [5,71,96] are particularly salient technological challenges. Moreover, throughput can be a challenge, especially for ‘public’ blockchains [97]. The academic literature also often discusses the high energy consumption of PoW based ‘public’ blockchains [78,98]. Yet, energy consumption is manageable for ‘private’ blockchains and also for ‘public’ blockchains when alternative consensus mechanisms are used [26,99].

Regulatory challenges refer to conflicts with rules regarding the organization and the responsibilities of actors in energy systems. Perceived regulatory barriers include privacy laws – such as the General Data Protection Regulation (GDPR) [100] – or energy market regulation [59]. While compliance with privacy laws appears more manageable for ‘private’ blockchains [100], substantial challenges remain, especially when competing organizations participate in the same private blockchain network. Furthermore, many energy market regulations presuppose a need to involve mediating actors, which makes such actors very difficult to replace [6,22,95,101]. The same applies to critical market actor roles, such as Transmission System or Distribution System Operators. These actors often have well-defined responsibilities, and their replacement may jeopardize the stability of energy systems. Legal uncertainties pertaining to alternative market actor roles, especially in *peer-to-peer electricity trading* applications, further exacerbate such concerns. Overall, the proposed deviations from current regulatory frameworks and legally required market roles make the use of blockchain in energy systems cumbersome.

Table 3
Identified challenges of using blockchain in energy systems.

Organisational	Technological	Regulatory
• Low market pressure and need for substantial investments • Low stakeholder acceptance and usability • Complex infrastructural and technological requirements to enable productive applications • Unpredictable and hidden costs • Unpredictable revenues • High organizational complexity of distributed market structures • Difficulties replacing critical, established, and mediating energy actors • Vague market actor responsibilities • Substantial efforts of automating and decentralizing governance • High involvement and participation effort • Difficulties maintaining social justice principles • Difficulties encouraging behavioral change of consumers	• Volatility of transaction speed • Lack of interoperability and technical standards • Blockchain trilemma of decentralization, scalability, and security • Complex and nontransparent data management • Few plug-and-play hardware and software components • Difficulties controlling data quality and quantity • High programming effort • Trade-off between privacy and efficiency	• Risk of data concentration • Regulatory barriers (e. g., GDPR, antitrust regulation, energy market regulation, contractual agreement requirements, governance, or payment with tokens) • Slow adaptation of current regulations • Low investment security and incomplete, ambiguous legal frameworks • Legally required market roles

The analyzed industry reports and interviews strongly indicate that technical concerns appear to be the easiest to address (Fig. 2). This is in stark contrast to the analyzed literature, where technological challenges are particularly salient but where assessments of blockchain applications remain predominantly theoretical [5,27]. Specifically, challenges resulting from limited performance and high energy-consumption can often be addressed with ‘private’ designs. Moreover, literature only attaches minor importance to organizational and, in particular, regulatory challenges [6,19]. However, these appear to be important hurdles for many blockchain projects [102]. For certain use cases, such as those focused on *peer-to-peer electricity trading*, addressing the respective challenges would require fundamental changes in the roles and responsibilities of key actors as well as the adjustment of multiple laws. Both industry reports and the interviewed experts deem such changes and adjustments highly unlikely.

4.4. *Evaluation of the identified use cases*

We evaluated and compared the attributed benefits and challenges for each of the eight use cases using a Likert scale with seven levels (see the Methods section). To depict the evaluation result (Fig. 2), we employed two simple traffic light schemes. For benefits, the color ‘green’ indicated that literature, industry reports, or experts identified clear benefits of the particular type. We tagged benefits as ‘yellow’ if their existence was less evident and 'red' if no such benefits were identified for the use case. For challenges, we used a similar scheme to indicate the severity of challenges from manageable ('green') to substantial ('red'). Naturally, these schemes only provided a simplified snapshot of the status quo, but they help to identify quickly if a use case was promising and realizable.

The upper section provides the results from our evaluation of academic literature, whereas the mid-section focuses on industry reports, and the lower on the interviews we conducted. The first column (#) indicates the number of sources that discuss the specific type of benefit or challenge. The second column provides the evaluation of the statements made.

4.4.1. Peer-to-peer electricity trading, decentralized system services and microgrid operation

In terms of benefits, *peer-to-peer electricity trading, decentralized system services,* and *microgrid operation* applications are controversial. While literature, reports, and experts agree that wholesale peer-to-peer markets based on blockchain hardly offer any benefits, they are divided on retail trading, system services, and microgrid operation. This divide is most prominent for retail markets, where experienced experts see few actual benefits of blockchain, studies are ambiguous, and the literature is very positive but hypothetical.

In terms of challenges, there is little controversy. All but a few sources identify considerable challenges from the proposed reorganization of established structures, roles, and processes. For *peer-to-peer electricity trading,* such changes entail substantial challenges of all three types, particularly at the organizational and regulatory levels. The decentralization and disintermediation of trading processes conflict with established roles and regulations, which has slowed the further development of blockchain-based trading platforms. Many of these roles are associated with critical and mediating functions, and their responsibilities are defined by law, which makes them hard to change or replace.

This also applies to *microgrid operation*, where new transaction processes with blockchain would require significant modifications of existing regulations. Even where regulatory frameworks are less restrictive, such as in the US, Thailand, and some African countries, *microgrid operation* is not easy to adopt [5,22,52,103]. Besides, microgrid operators can already process microgrid transactions securely, cheaply, and without regulatory modifications using conventional energy management software [104,105]. Such conventional software solutions also come with predictable management efforts and costs [106]. In contrast, blockchain applications are often more complex and not profitable enough, especially for transactions below a certain value.

From a technological viewpoint, frequent, near-real-time transactions are still difficult to achieve with 'public' blockchains. Thus, decentralized energy markets and microgrid management based on these types of blockchains are also hard to establish technologically. 'Private' blockchains, in contrast, can often provide sufficient transaction speed but typically do not offer the desired level of openness [107].

Consequently, few *peer-to-peer trading* and *microgrid operation* applications have yet taken off. Successful projects exist, however, for *decentralized system services* that cannot be traded effectively on existing markets. One prominent such example is the Equigy platform [108]. The platform allows aggregators to register storage and electric vehicles of their residential customers in a blockchain-based registry. Once registered, these aggregators can use the platform to trade flexibility with transmission and distribution system operators. These transactions are again processed through the blockchain-based registry. The Equigy platform is in productive use since 2021 and has been rolled out in different countries, such as the Netherlands, Germany, and Italy.

4.4.2. E-roaming

E-roaming is an ambiguous use case with unclear efficiency benefits (Fig. 2). Literature, reports, and experts all expect efficiency gains from the automated and standardized transfer of data and the reduction of tedious manual exchanges [41]. Smart contracts and cryptocurrencies may also further automate and unify processes across national borders [109]. These efficiency gains are expected to entail considerable cuts in transaction fees for mobility providers and reduced costs for consumers. Yet, none of the sources provide a precise estimate of these gains.

In contrast, *e-roaming* applications come with various specific regulatory, technological, and organizational challenges. Primarily raised by the interviewed experts, these challenges make the use of blockchain-based charging systems unnecessarily complicated. For instance, cryptocurrency prices can be very volatile and only few users have crypto wallets. Both reasons have brought blockchain based e-roaming platforms to a halt in Germany. Also, governance frameworks need to be established between charging networks and consortia, resulting in costly and time-consuming negotiations. These are, however, necessary as legal uncertainty resulting from unclear governance frameworks and responsibilities may jeopardize customer safety. Another problem is interoperability with existing systems and a lack of standardized and secure interfaces [71,110]. Often, it may be easier to use non-blockchain-based solutions such as conventional platforms that are technologically more mature and easier to implement.

Consequentially, e-roaming applications have so far failed to make it beyond pilot projects. Those applications focusing on transaction processing are weighed down especially by the existence of alternative means of payment, such as credit cards, and those applications focusing on identification and authentication are still stuck at the conceptual level.

4.4.3. Labeling of electricity and certificate trading

Labeling of electricity applications build on expectations of efficiency gains and come with comparatively few challenges (Fig. 2). Blockchain-based labeling systems promise to mitigate concerns regarding the sources of consumed electricity. These systems are expected to reduce the risk of 'greenwashing', accelerate data exchange about fed-in and consumed electricity, and reduce manual processes [73,107]. While these efficiency gains are expected to substantially reduce costs, we were – once again – unable to establish specific estimates.

Specific challenges, in turn, are easier to identify. They include regulatory challenges, for instance, compliance with data privacy regulation, and technological challenges, such as limited usability. Few actors in the energy industry have the technological know-how required to effectively use blockchain technology. Another complex challenge is compliance with data privacy regulations, such as the GDPR. Data privacy regulation requires that data can be erased if it is either directly or indirectly attributable to a natural person, which is difficult to implement with blockchain [111]. As such, labeling systems have to prevent natural persons from being easily identifiable using data stored on the blockchain.

Given these uncertainties, electricity labeling is still at an early stage and most projects remain exploratory. Examples include the InDEED project [112], which explores the use of blockchain to create green and regional labels, and the SMECS project [113], which develops a blockchain-based registry to identify those power generation units from which a customer's electricity was purchased at a particular time.

Certificate trading applications are a new hype that takes the use of blockchain a step further than labeling applications. The idea of most of these applications is to use labeling data as the foundation of certificates of origin or emission for specific generation and storage facilities. Since every certificate is issued uniquely, its secure and redundant storage on the blockchain creates a transparent and unequivocal ownership history. However, quantifying these benefits is difficult. Moreover, the development of an industry-wide or cross-border trading system is highly complex, especially without established technical standards.

Despite these challenges, certain projects have started working on *certificate trading* applications. For instance, the start-up CarbonFuture develops a blockchain-based trading platform for ‘carbon removal credits’ [114]. Companies can use the platform to fund and trade contributions to carbon removal projects such as biochar sinks that offset their own emissions.

4.4.4. Machine identities

Machine identities are another new hype application; they are expected to generate benefits of all three types. They are argued to increase effectiveness by offering a more flexible, decentralized way of organizing public key infrastructures. Moreover, they are believed to increase the efficiency of processes associated with identifying, (de-) registering, and managing distributed energy resources. In terms of security, these applications could obviate centralized databases for identity information, which would reduce the risk of identity theft and undesirable monitoring by large companies. While these benefits sound promising, they are only hopes at this point and the respective projects have yet to demonstrate that they can be realized and outweigh their costs.

Moreover, *decentralized digital identity* applications are afflicted by many fundamental organizational, technological, and regulatory challenges. These include important governance issues, such as the definition of processes for accrediting issuers of machine identities and the agreement on joint standards for the format of identity credentials. Technological challenges result from limited maturity of technical building blocks as well as limited technological know-how. Regulatory challenges arise, for instance, from privacy requirements as the anchoring of a credential on a blockchain can lead to inadvertent attribution to a natural person.

A prominent example for *machine identity* is the Blockchain Machine Identity Ledger [115] project coordinated by the German Energy Agency (dena). The project investigates the potential of equipping distributed energy resources with machine identities. These identities are expected to enable automated and digital authentication and enable operators to market these resources in a range of electricity markets. Although promising, the Blockchain Machine Identity Ledger is still in the conceptual phase. Another example is a strategic partnership established by the Elia Group and the Energy Web Foundation to explore blockchain-based machine identities for a broad range of use cases in the energy industry [116].

5. Discussion

Blockchain technology has been hyped as a potentially disruptive technology for energy systems. Yet, our analysis of recent academic literature, in addition to practice-informed industry reports and expert interviews, indicates that there is still a long and rocky road ahead for blockchain in Europe. We reveal that expected benefits are often little more than unspecific hopes. Moreover, we find that applications focused on the reorganization of established structures, such as *peer-to-peer electricity trading* or *microgrid operation*, face significant organizational and regulatory barriers, especially in Europe. These barriers make such use cases very hard to realize. Promising projects exist, however, in less regulated areas, such as new markets for *decentralized system services*. These applications address clear and unmet needs in areas that require neither substantial reorganization nor significant regulatory change. Use cases that focus on increasing the efficiency of processes, such as *e-roaming and machine identities*, are feasible yet blockchain may not have enough to offer over alternative technologies. Moreover, such use cases require more than just blockchain technology to succeed. Blockchain may thus best leverage its benefits for energy systems when it takes a backseat.

When we asked the interviewed experts for their opinions on changes required for blockchain to flourish in energy systems, many were outspoken in their criticism of the perceived regulatory uncertainties and barriers. Yet, few could propose specific changes and, even fewer, unbiased recommendations that would not unduly favor blockchain over other technologies. This undifferentiated stance hinders a constructive dialogue with policymakers and regulators, especially when they strongly favor the use of blockchain. Some initiatives have begun to address this divide, particularly for *peer-to-peer electricity trading* applications [22,55]. Other noteworthy developments are the European Union’s ‘Markets in Crypto-Assets’ (MiCA) directive [117], which is expected to reduce regulatory uncertainties for applications that use blockchain for payment purposes, and the revision of the European eIDAS regulation, which will create a European Digital Identity framework [99,118]. Reducing legal uncertainties in highly regulated markets might enable digital innovations to evolve from pilot stages into products that can be safely used by end customers. This, in turn, could increase the number of commercially available products. However, it remains to be seen to what extent such developments will turn the tide.

We thus encourage research and industry to revisit their choice of blockchain applications, especially in Europe, where regulatory challenges are more significant than, for instance, in the US or African countries [5,52,103]. That is, blockchain projects are more likely to succeed when they require few to any regulatory modifications and when they provide competitive solutions for new requirements. Moreover, we encourage a more focused approach that only uses blockchain technology for very specific purposes and combines blockchain with other technologies where these are better suited. Successful applications of blockchain will likely be found in the context of *decentralized system services* but may also become apparent for *certificate trading* or *machine identities* [35,119]. *Microgrid operation* may be useful as well in geographically remote areas that are not connected to a central power grid, such as certain regions in the United States, Australia, or African countries [3,25].

Regarding the technical challenges, we see several promising approaches. Privacy concerns resulting from the replicated processing of transactions on blockchains may be tackled with privacy-enhancing technologies, such as zero-knowledge proofs (ZKPs) [101]. ZKPs allow to verify the validity of a payment or a smart contract call without requiring the distribution of corresponding raw data inputs or outputs to all nodes. Other approaches, such as secure multi-party computation or fully homomorphic encryption, may improve privacy where ZKPs appear infeasible. Yet, these approaches are arguably less mature and would require more research [120].

In addition to privacy issues, the scalability and performance challenges of blockchains may be addressed through incremental improvements or by using ’private’ blockchains. Novel concepts such as ’serverless distributed ledgers’ may allow for meeting exceptional throughput requirements in private networks [121]. For ’public’ blockchains, sharding in combination with scaling solutions like zk-rollups may substantially improve throughput as well [120]. Zk-rollups use ZKPs to compress the computational effort and the storage necessary for the validation of transactions [120]. Such an approach, however, increases system complexity. Moreover, these throughput-enhancing concepts come with a host of other challenges such as tradeoffs between, for instance, throughput and centralization or data availability.

Yet, these technical approaches may also help to address challenges at the regulatory and organizational level. Serverless distributed ledgers, for instance, may provide better cost structures and integration with legacy cloud systems, which often appears to be an acceptable trade-off with increased centralization [121]. Moreover, the use of private blockchains may allow for the retention of traditional market actor roles, which enhances compliance with regulatory frameworks and causes less organizational overhead. Private blockchains are often also better reconcilable with GDPR requirements as they facilitate selective transparency between involved actors [100].

6. Conclusion

Blockchain is no longer just a hype technology, and successful applications exist in various contexts, ranging from food supply chains [1] to public services [28]. However, adoption in energy systems is slow, especially in Europe. In this paper, we investigate the reasons for this slow up-take. Our analysis reveals a stark asymmetry between high hopes and low viability: blockchains expected benefits are often unspecific and hard to quantify, whereas the associated challenges are specific and difficult to resolve. Certain use cases, such as those focusing on peer-to-peer electricity trading, have vague benefits and are difficult to reconcile with regulation, established market structures, and technological requirements. Others, such as e-roaming, entail addressable challenges, yet blockchain fails to offer relevant advantages. Using blockchain to support markets for decentralized system services, certificate trading, or creating machine identities is feasible and promising, but blockchain may only be one part of an effective solution. Blockchain may thus very well have a future in Europe's energy systems – albeit one that is smaller than originally anticipated.

CRediT authorship contribution statement

Tamara Roth: Conceptualization, Methodology, Data curation, Formal analysis, Writing – original draft, Visualization. **Manuel Utz:** Conceptualization, Data curation, Formal analysis, Writing – review & editing, Visualization. **Felix Baumgarte:** Conceptualization, Data curation, Formal analysis, Writing – review & editing. **Alexander Rieger:** Conceptualization, Formal analysis, Project administration, Supervision, Writing – review & editing. **Johannes Sedlmeir:** Validation, Writing – review & editing. **Jens Strüker:** Validation, Writing – review & editing.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

The data that has been used is confidential.

Acknowledgements

This work was supported by PayPal and the Luxembourg National Research Fund FNR (P17/IS/13342933/PayPal-FNR/Chair in DFS/Gilbert Fridgen).

Analyzed academic literature

Appendix A1 *List of analyzed academic literature*

Here we list the academic literature that we analyzed to identify benefits and challenges of using blockchain in electric power systems.

Article	Authors	Year	Title	Journal
Ableitner et al. (2020)	Ableitner, L., Tiefenbeck, V., Meeuw, A., Wörner, A., Fleisch, E., & Wortmann, F.	2020	User behavior in a real-world peer-to-peer electricity market.	Applied Energy
Ahl et al. (2019)	Ahl, A., Yarime, M., Tanaka, K., & Sagawa, D.	2019	Review of blockchain-based distributed energy: Implications for institutional development.	Renewable and Sustainable Energy Reviews
Ahl et al. (2020)	Ahl, A., Yarime, M., Goto, M., Chopra, S. S., Kumar, N. M., Tanaka, K., & Sagawa, D.	2020	Exploring blockchain for the energy transition: Opportunities and challenges based on a case study in Japan.	Renewable and Sustainable Energy Reviews
Akter et al. (2020)	Akter, M. N., Mahmud, M. A., Haque, M. E., & Oo, A. M.	2020	An optimal distributed energy management scheme for solving transactive energy sharing problems in residential microgrids.	Applied Energy
Al-Obaidi et al. (2021)	Al-Obaidi, A., Khani, H., Farag, H. E., & Mohamed, M.	2021	Bidirectional smart charging of electric vehicles considering user preferences, peer to peer energy trade, and provision of grid ancillary services.	International Journal of Electrical Power & Energy Systems
AlAshery et al. (2021)	AlAshery, M. K., Yi, Z., Shi, D., Lu, X., Xu, C., Wang, Z., & Qiao, W.	2021	A blockchain-enabled multi-settlement quasi-ideal peer-to-peer trading framework.	IEEE Transactions on Smart Grid
An et al. (2020)	An, J., Lee, M., Yeom, S., & Hong, T.	2020	Determining the Peer-to-Peer electricity trading price and strategy for energy prosumers and consumers within a microgrid.	Applied Energy
Andoni et al. (2019)	Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., … & Peacock, A.	2019	Blockchain technology in the energy sector: A systematic review of challenges and opportunities.	Renewable and Sustainable Energy Reviews
Antal et al. (2021)	Antal, C., Cioara, T., Antal, M., Mihailescu, V., Mitrea, D., Anghel, I., … & Bellesini, F.	2021	Blockchain based decentralized local energy flexibility market.	Energy Reports
Ante et al. (2021)	Ante, L., Steinmetz, F., & Fiedler, I.	2021	Blockchain and energy: A bibliometric analysis and review.	Renewable and Sustainable Energy Reviews
Bandeiras et al. (2020)	Bandeiras, F., Pinheiro, E., Gomes, M., Coelho, P., & Fernandes, J.	2020	Review of the cooperation and operation of microgrid clusters.	Renewable and Sustainable Energy Reviews
Bhushan et al. (2020)	Bhushan, B., Khamparia, A., Sagayam, K. M., Sharma, S. K., Ahad, M. A., & Debnath, N. C.	2020	Blockchain for smart cities: A review of architectures, integration trends and future research directions.	Sustainable Cities and Society
Bian et al. (2022)	Bian, Z., & Zhang, Q.	2022	Combined compromise solution and blockchain-based structure for optimal scheduling of renewable-based microgrids: Stochastic information approach.	Sustainable Cities and Society
Bischi et al. (2021)	Bischi, A., Basile, M., Poli, D., Vallati, C., Miliani, F., Caposciutti, G., … & Desideri, U.	2021	Enabling low-voltage, peer-to-peer, quasi-real-time electricity markets through consortium blockchains.	Applied Energy
Choobineh et al. (2022)	Choobineh, M., Arab, A., Khodaei, A., & Paaso, A.	2022	Energy innovations through blockchain: Challenges, opportunities, and the road ahead.	The Electricity Journal
Christidis et al. (2021)	Christidis, K., Sikeridis, D., Wang, Y., & Devetsikiotis, M.	2021	A framework for designing and evaluating realistic blockchain-based local energy markets.	Applied Energy
Das et al. (2020)	Das, L., Munikoti, S., Natarajan, B., & Srinivasan, B.	2020	Measuring smart grid resilience: Methods, challenges and opportunities.	Renewable and Sustainable Energy Reviews

(*continued on next page*)

(*continued*)

Article	Authors	Year	Title	Journal
Di Silvestre et al. (2019)	Di Silvestre, M. L., Gallo, P., Guerrero, J. M., Musca, R., Sanseverino, E. R., Sciumè, G., … & Zizzo, G.	2019	Blockchain for power systems: Current trends and future applications.	Renewable and Sustainable Energy Reviews
Diestelmeier et al. (2019)	Diestelmeier, L.	2019	Changing power: Shifting the role of electricity consumers with blockchain technology–Policy implications for EU electricity law.	Energy Policy
Doan et al. (2021)	Doan, H. T., Cho, J., & Kim, D.	2021	Peer-to-peer energy trading in smart grid through blockchain: A double auction-based game theoretic approach.	IEEE Access
Dong et al. (2018)	Dong, Z., Luo, F., & Liang, G.	2018	Blockchain: a secure, decentralized, trusted cyber infrastructure solution for future energy systems.	Journal of Modern Power Systems and Clean Energy
Esfahani (2022)	Esfahani, M. M.	2022	A hierarchical blockchain-based electricity market framework for energy transactions in a security-constrained cluster of microgrids.	International Journal of Electrical Power & Energy Systems
Esmat et al. (2021)	Esmat, A., de Vos, M., Ghiassi-Farrokhfal, Y., Palensky, P., & Epema, D.	2021	A novel decentralized platform for peer-to-peer energy trading market with blockchain technology.	Applied Energy
Foti & Vavalis (2019)	Foti, M., & Vavalis, M.	2019	Blockchain based uniform price double auctions for energy markets.	Applied Energy
Fu et al. (2020)	Fu, Z., Dong, P., & Ju, Y.	2020	An intelligent electric vehicle charging system for new energy companies based on consortium blockchain.	Journal of Cleaner Production
Guerrero et al. (2020)	Guerrero, J., Gebbran, D., Mhanna, S., Chapman, A. C., & Verbič, G.	2020	Towards a transactive energy system for integration of distributed energy resources: Home energy management, distributed optimal power flow, and peer-to-peer energy trading.	Renewable and Sustainable Energy Reviews
Guerrero et al. (2021)	Guerrero, J., Sok, B., Chapman, A. C., & Verbič, G.	2021	Electrical-distance driven peer-to-peer energy trading in a low-voltage network.	Applied Energy
Hahnel et al. (2019)	Hahnel, U. J., Herberz, M., Pena-Bello, A., Parra, D., & Brosch, T.	2019	Becoming prosumer: Revealing trading preferences and decision-making strategies in peer-to-peer energy communities.	Energy Policy
Han et al. (2020)	Han, D., Zhang, C., Ping, J., & Yan, Z.	2020	Smart contract architecture for decentralized energy trading and management based on blockchains.	Energy
Hasankhani et al. (2021)	Hasankhani, A., Hakimi, S. M., Bisheh-Niasar, M., Shafie-khah, M., & Asadolahi, H.	2021	Blockchain technology in the future smart grids: A comprehensive review and frameworks.	International Journal of Electrical Power & Energy Systems
Hayes et al. (2020)	Hayes, B. P., Thakur, S., & Breslin, J. G.	2020	Co-simulation of electricity distribution networks and peer to peer energy trading platforms.	International Journal of Electrical Power & Energy Systems
Hirsch et al. (2018)	Hirsch, A., Parag, Y., & Guerrero, J.	2018	Microgrids: A review of technologies, key drivers, and outstanding issues.	Renewable and Sustainable Energy Reviews
Howson (2019)	Howson, P.	2019	Tackling climate change with blockchain.	Nature Climate Change
Hua et al. (2020)	Hua, W., Jiang, J., Sun, H., & Wu, J.	2020	A blockchain based peer-to-peer trading framework integrating energy and carbon markets.	Applied Energy
Jiang et al. (2020)	Jiang, Y., Zhou, K., Lu, X., & Yang, S.	2020	Electricity trading pricing among prosumers with game theory-based model in energy blockchain environment.	Applied Energy
Johnson & Mayfield (2020)	Johnson, R. C., & Mayfield, M.	2020	The economic and environmental implications of post feed-in tariff PV on constrained low voltage networks.	Applied Energy
Kanakadhurga et al. (2022)	Kanakadhurga, D., & Prabaharan, N.	2022	Demand side management in microgrid: A critical review of key issues and recent trends.	Renewable and Sustainable Energy Reviews
Khan et al. (2019)	Khan, F. A., Asif, M., Ahmad, A., Alharbi, M., & Aljuaid, H.	2019	Blockchain technology, improvement suggestions, security challenges on smart grid and its application in healthcare for sustainable development.	Sustainable Cities and Society
Khorasany et al. (2021)	Khorasany, M., Dorri, A., Razzaghi, R., & Jurdak, R.	2021	Lightweight blockchain framework for location-aware peer-to-peer energy trading.	International Journal of Electrical Power & Energy Systems
Kobashi et al. (2020)	Kobashi, T., Yoshida, T., Yamagata, Y., Naito, K., Pfenninger, S., Say, K., … & Hara, K.	2020	On the potential of "Photovoltaics + Electric vehicles" for deep decarbonization of Kyoto's power systems: Techno-economic-social considerations.	Applied Energy
Lei et al. (2021)	Lei, N., Masanet, E., & Koomey, J.	2021	Best practices for analyzing the direct energy use of blockchain technology systems: Review and policy recommendations.	Energy Policy
Li et al. (2018)	Li, Z., Shahidehpour, M., & Liu, X.	2018	Cyber-secure decentralized energy management for IoT-enabled active distribution networks.	Journal of Modern Power Systems and Clean Energy
Li et al. (2019)	Li, Y., Yang, W., He, P., Chen, C., & Wang, X.	2019	Design and management of a distributed hybrid energy system through smart contract and blockchain.	Applied Energy
Li et al. (2021)	Li, S., Pan, Y., Xu, P., & Zhang, N.	2021	A decentralized peer-to-peer control scheme for heating and cooling trading in distributed energy systems.	Journal of Cleaner Production
Lin et al. (2019)	Lin, J., Pipattanasomporn, M., & Rahman, S.	2019	Comparative analysis of auction mechanisms and bidding strategies for P2P solar transactive energy markets.	Applied Energy
Long et al. (2018)	Long, C., Wu, J., Zhou, Y., & Jenkins, N.	2018	Peer-to-peer energy sharing through a two-stage aggregated battery control in a community Microgrid.	Applied Energy
Lowitzsch et al. (2020)	Lowitzsch, J., Hoicka, C. E., & van Tulder, F. J.	2020	Renewable energy communities under the 2019 European Clean Energy Package–Governance model for the energy clusters of the future?.	Renewable and Sustainable Energy Reviews
Luo et al. (2018)	Luo, F., Dong, Z. Y., Liang, G., Murata, J., & Xu, Z.	2018	A distributed electricity trading system in active distribution networks based on multi-agent coalition and blockchain.	IEEE Transactions on Power Systems
Lüth et al. (2018)	Lüth, A., Zepter, J. M., del Granado, P. C., & Egging, R.	2018	Local electricity market designs for peer-to-peer trading: The role of battery flexibility.	Applied Energy
Maneesha & Swarup (2021)	Maneesha, A., & Swarup, K. S.	2021	A survey on applications of Alternating Direction Method of Multipliers in smart power grids.	Renewable and Sustainable Energy Reviews
Mehdinejad et al. (2022)	Mehdinejad, M., Shayanfar, H. A., Mohammadi-Ivatloo, B., … & Nafisi, H.	2022	Designing a Robust Decentralized Energy Transactions Framework for Active Prosumers in Peer-to-Peer Local Electricity Markets.	IEEE Access

(*continued on next page*)

(*continued*)

Article	Authors	Year	Title	Journal
Mengelkamp et al. (2018)	Mengelkamp, E., Gärttner, J., Rock, K., Kessler, S., Orsini, L., & Weinhardt, C.	2018	Designing microgrid energy markets: A case study: The Brooklyn Microgrid.	Applied Energy
Mengelkamp et al. (2019)	Mengelkamp, E., Schlund, D., & Weinhardt, C.	2019	Development and real-world application of a taxonomy for business models in local energy markets.	Applied Energy
Mika et al. (2021)	Mika, B., & Goudz, A.	2021	Blockchain-technology in the energy industry: Blockchain as a driver of the energy revolution? With focus on the situation in Germany.	Energy Systems
Milchram et al. (2020)	Milchram, C., Künneke, R., Doorn, N., van de Kaa, G., & Hillerbrand, R.	2020	Designing for justice in electricity systems: A comparison of smart grid experiments in the Netherlands.	Energy Policy
Neves et al. (2020)	Neves, D., Scott, I., & Silva, C. A.	2020	Peer-to-peer energy trading potential: An assessment for the residential sector under different technology and tariff availabilities.	Energy
Noor et al. (2018)	Noor, S., Yang, W., Guo, M., van Dam, K. H., & Wang, X.	2018	Energy demand side management within micro-grid networks enhanced by blockchain.	Applied Energy
Nour et al. (2022)	Nour, M., Chaves-Ávila, J. P., & Sánchez-Miralles, Á.	2022	Review of Blockchain Potential Applications in the Electricity Sector and Challenges for Large Scale Adoption.	IEEE Access
Paiho et al. (2021)	Paiho, S., Kiljander, J., Sarala, R., Siikavirta, H., Kilkki, O., Bajpai, A., … & Weisshaupt, T.	2021	Towards cross-commodity energy-sharing communities–A review of the market, regulatory, and technical situation.	Renewable and Sustainable Energy Reviews
Perrons et al. (2020)	Perrons, R. K., & Cosby, T.	2020	Applying blockchain in the geoenergy domain: The road to interoperability and standards.	Applied Energy
Prinsloo et al. (2018)	Prinsloo, G., Dobson, R., & Mammoli, A.	2018	Synthesis of an intelligent rural village microgrid control strategy based on smartgrid multi-agent modelling and transactive energy management principles.	Energy
Roberts et al. (2019)	Roberts, M. B., Bruce, A., & MacGill, I.	2019	Opportunities and barriers for photovoltaics on multi-unit residential buildings: Reviewing the Australian experience.	Renewable and Sustainable Energy Reviews
Saha et al. (2021)	Saha, S., Ravi, N., Hreinsson, K., Baek, J., Scaglione, A., & Johnson, N. G.	2021	A secure distributed ledger for transactive energy: The Electron Volt Exchange (EVE) blockchain.	Applied Energy
Soto et al. (2021)	Soto, E. A., Bosman, L. B., Wollega, E., & Leon-Salas, W. D.	2021	Peer-to-peer energy trading: A review of the literature.	Applied Energy
Sousa et al. (2019)	Sousa, T., Soares, T., Pinson, P., Moret, F., Baroche, T., & Sorin, E.	2019	Peer-to-peer and community-based markets: A comprehensive review.	Renewable and Sustainable Energy Reviews
Thomas et al. (2019)	Thomas, L., Zhou, Y., Long, C., Wu, J., & Jenkins, N.	2019	A general form of smart contract for decentralized energy systems management.	Nature Energy
Thukral (2021)	Thukral, M. K.	2021	Emergence of blockchain-technology application in peer-to-peer electrical-energy trading: a review.	Clean Energy
Tsao & Thanh (2021)	Tsao, Y. C., & Thanh, V. V.	2021	Toward blockchain-based renewable energy microgrid design considering default risk and demand uncertainty.	Renewable Energy
Tsao et al. (2021)	Tsao, Y. C., & Thanh, V. V.	2021	Toward sustainable microgrids with blockchain technology-based peer-to-peer energy trading mechanism: A fuzzy *meta*-heuristic approach.	Renewable and Sustainable Energy Reviews
Tsao, Thanh & Wu (2021)	Tsao, Y. C., Thanh, V. V., & Wu, Q.	2021	Sustainable microgrid design considering blockchain technology for real-time price-based demand response programs.	International Journal of Electrical Power & Energy Systems
Tushar et al. (2021)	Tushar, W., Yuen, C., Saha, T. K., Morstyn, T., Chapman, A. C., Alam, M. J. E., … & Poor, H. V.	2021	Peer-to-peer energy systems for connected communities: A review of recent advances and emerging challenges.	Applied Energy
van Cutsem et al. (2020)	Van Cutsem, O., Dac, D. H., Boudou, P., & Kayal, M.	2020	Cooperative energy management of a community of smart-buildings: A Blockchain approach.	International Journal of Electrical Power & Energy Systems
van Leeuwen et al. (2020)	van Leeuwen, G., AlSkaif, T., Gibescu, M., & van Sark, W.	2020	An integrated blockchain-based energy management platform with bilateral trading for microgrid communities.	Applied Energy
Vieira & Zhang (2021)	Vieira, G., & Zhang, J.	2021	Peer-to-peer energy trading in a microgrid leveraged by smart contracts.	Renewable and Sustainable Energy Reviews
Wang et al. (2019)	Wang, C. S., Yan, J. Y., Jia, H. J., Wu, J. Z., Yu, J. C., Xu, T., & Zhang, Y.	2019	Renewable and distributed energy integration with mini/microgrids.	Applied Energy
Wang et al. (2020)	Wang, L., Liu, J., Yuan, R., Wu, J., Zhang, D., Zhang, Y., & Li, M.	2020	Adaptive bidding strategy for real-time energy management in multi-energy market enhanced by blockchain.	Applied Energy
Wang et al. (2021)	Wang, B., Zhao, S., Li, Y., Wu, C., Tan, J., Li, H., & Yukita, K.	2021	Design of a privacy-preserving decentralized energy trading scheme in blockchain network environment.	International Journal of Electrical Power & Energy Systems
Warneryd et al. (2020)	Warneryd, M., Håkansson, M., & Karltorp, K.	2020	Unpacking the complexity of community microgrids: A review of institutions' roles for development of microgrids.	Renewable and Sustainable Energy Reviews
Wu & Zhang (2021)	Wu, Y., Zhang, X., & Sun, H.	2021	A multi-time-scale autonomous energy trading framework within distribution networks based on blockchain.	Applied Energy
Wu et al. (2019)	Wu, J., Hu, J., Ai, X., Zhang, Z., & Hu, H.	2019	Multi-time scale energy management of electric vehicle model-based prosumers by using virtual battery model.	Applied Energy
Wu et al. (2021)	Wu, Y., Wu, Y., Guerrero, J. M., & Vasquez, J. C.	2021	Digitalization and decentralization driving transactive energy Internet: Key technologies and infrastructures.	International Journal of Electrical Power & Energy Systems
Yan et al. (2022)	Yan, M., Gan, W., Zhou, Y., Wen, J., & Yao, W.	2022	Projection method for blockchain-enabled non-iterative decentralized management in integrated natural gas-electric systems and its application in digital twin modelling.	Applied Energy
Yazdanie et al. (2021)	Yazdanie, M., & Orehounig, K.	2021	Advancing urban energy system planning and modeling approaches: Gaps and solutions in perspective.	Renewable and Sustainable Energy Reviews
Yun et al. (2021)	Yun, G., Zhygulin, V., & Zheng, Q. P.	2021	Residential energy trading with blockchain technology.	Energy Systems
Zhang et al. (2018)	Zhang, T., Pota, H., Chu, C. C., & Gadh, R.	2018	Real-time renewable energy incentive system for electric vehicles using prioritization and cryptocurrency.	Applied Energy

(*continued on next page*)

(*continued*)

Article	Authors	Year	Title	Journal
Zhang et al. (2019)	Zhang, H., Wang, J., & Ding, Y.	2019	Blockchain-based decentralized and secure keyless signature scheme for smart grid.	Energy
Zhang et al. (2020)	Zhang, S., Rong, J., & Wang, B.	2020	A privacy protection scheme of smart meter for decentralized smart home environment based on consortium blockchain.	Journal of Electrical Power & Energy Systems
Zhang et al. (2022)	Zhang, Q., Su, Y., Wu, X., Zhu, Y., & Hu, Y.	2022	Electricity trade strategy of regional electric vehicle coalitions based on blockchain.	Electric Power Systems Research
Zhao et al. (2022)	Zhao, S., Zhu, S., Wu, Z., & Jaing, B.	2022	Cooperative energy dispatch of smart building cluster based on smart contracts.	International Journal of Electrical Power & Energy Systems

Analyzed industry reports

Appendix A2 *List of analyzed industry reports*

Here we list the industry reports that we analyzed to identify benefits and challenges of using blockchain in electric power systems.

Report	Organization	Year	Title
Accenture (2018)	Accenture	2018	Blockchain for Utilities: Beyond the Buzz
Adelphi (2019)	Adelphi Consult and Wuppertal Institute	2019	Smart power grids and integration of renewables in Japan. Current activities concerning smart grids implementation, energy system digitization and integration of renewables
Atlantic Council (2019)	Atlantic Council Global Energy Center	2019	Assessing Blockchain's Future in Transactive Energy
Bitkom (2020)	Bitkom e. V. Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.	2020	Self Sovereign Identity Use Cases – von der Vision in die Praxis
EU Blockchain Observatory and Forum (2019)	European Union Blockchain Observatory and Forum	2019	Blockchain and Digital Identity
BNetzA (2019)	German Federal Network Agency (Bundesnetzagentur)	2020	Die Blockchain-Technologie - Potenziale und Herausforderungen in den Netzsektoren Energie und Telekommunikation
Bundesblock (2019)	Blockchain Bundesverband	2019	Aktionspapier des Blockchain Bundesverband e.V. zur Blockchain-Strategie der Bundesregierung
Capgemini (2019)	Capgemini	2019	World Energy Markets Observatory 2019
CDC Canada (2019)	Chamber of Digital Commerce Canada	2019	Canadian Blockchain Census 2019. Part I: Measuring Canada's Blockchain Ecosystem
CLI (2019)	Climate Ledger Initiative	2019	Navigating Blockchain and Climate Action
Cognizant (2018)	Cognizant	2018	Blockchain for Power Utilities: A View on Capabilities and Adoption
Congressional Research Service (2019)	Congressional Research Service (USA)	2019	Bitcoin, Blockchain, and the Energy Sector
Council on Foreign Relations (2018)	Council on Foreign Relations (USA)	2018	Applying Blockchain Technology to Electric Power Systems
CSIS (2019)	Center for Strategic and International Studies	2019	Blockchain and Aggregating Microgrid Projects in Developing Nations in: New Perspectives in Foreign Policy
Deloitte (2019)	Deloitte	2019	Blockchain: A true disruptor for the energy industry. Use cases and strategic questions
DENA (2019)	German Energy Agency (DENA)	2019	Blockchain in the integrated energy transition
Detecon (2018)	Detecon	2018	Blockchain Disruptively Changing the Energy Industry
Energy Futures Initiative (2018)	Energy Futures Initiative	2018	Promising Blockchain Applications for Energy: Separating the Signal from the Noise
EnergyWeb (2019)	Energy Web Foundation	2019	The Energy Web Chain - Accelerating the Energy Transition with an Open-Source, Decentralized Blockchain Platform
Enisa (2022)	European Union Agency for Cybersecurity (ENISA)	2022	Digital Identity - Leveraging the Self-Sovereign Identity (SSI)Concept to Build Trust
EU Blockchain Observatory and Forum (2019)	European Union Blockchain Observatory and Forum	2019	EU Blockchain Observatory & Forum - Energy and Sustainability
European Commission (2019)	European Commission	2019	Blockchain Now and Tomorrow: Assessing Multidimensional Impacts of Distributed Ledger Technologies
EY (2019)	Ernst & Young	2019	Blockchain-basierte Erfassung und Steuerung von Energieanlagen mithilfe des Smart-Meter-Gateways: Machbarkeitsstudie und Pilotkonzept
FFE (2018)	Forschungsstelle für Energiewirtschaft	2018	Die Blockchain-Technologie - Chance zur Transformation der Energiewirtschaft? Berichtsteil: Anwendungsfälle
Fraunhofer FIT (2021)	Project Group Business & Information Systems Engineering of the Fraunhofer Institute for Applied Information Technology FIT, Bayreuth.	2021	Self-Sovereign Identity Foundations, Applications, and Potentials of Portable Digital Identities
FSR (2019)	German-Mexican Energy Partnership (EP) and Florence School of Regulation (FSR)	2019	Blockchain meets Energy - Digital Solutions for a Decentralized and Decarbonized Sector
Germanwatch (2018)	Germanwatch	2018	Blockchain – Opportunities and threats for the energy transition
GIZ Mexico (2019)	German Corporation for International Cooperation (Deutsche Gesellschaft für Internationale Zusammenarbeit - GIZ)	2019	Blockchain in the Mexican Energy Sector - Fostering digital transformation

(*continued on next page*)

(*continued*)

Report	Organization	Year	Title
IFC (2018)	International Finance Corporation	2018	Using Blockchain to Enable Cleaner, Modern Energy Systems in Emerging Markets
IRENA (2019)	International Renewable Energy Agency	2019	Innovation landscape brief: Blockchain
NERA (2019)	NERA Economic Consulting	2019	Blockchain in Electricity: a Critical Review of Progress to Date
Netherlands Innovation Network (2019)	Netherlands Enterprise Agency	2019	Blockchain - Netherlands Innovation Network
NITI Aayog (2019)	NITI Aayog	2019	Blockchain: The India Strategy
NREL (2020)	National Renewable Energy Laboratory	2020	The Evolving U.S. Distribution System: Technologies, Architectures, and Regulations for Realizing a Transactive Energy Marketplace
Renew Nexus (2019)	RENeW Nexus	2019	Enabling resilient, low cost & localized electricity markets through blockchain P2P & VPP trading
SAP (2018)	SAP	2018	Blockchain in the Energy Sector - The Potential for Energy Providers
Smart Service Welt (2020)	Smart Service Welt	2020	Energierevolution getrieben durch Blockchain
Solarplaza (2019)	Solarplaza	2019	Comprehensive Guide to Companies involved in Blockchain & Energy
Stanford (2019)	Stanford Graduate School of Business	2019	Blockchain for Social Impact - Moving Beyond the Hype
UTCID Report (2021)	The University of Texas at Austin Center for Identity	2021	Blockchain-Based Self-Sovereign Identity: Survey, Requirements, Use-Cases, and Comparative Study
Vise (2019)	Virtual Institut Smart Energy (VISE)	2019	Blockchain in der Energiewirtschaft
World Energy Council (2019)	World Energy Council	2019	The Developing Role of Blockchain

Interview guide

Appendix A3 *Interview guide*

1. **Presentation of the research project’s objectives (5 min)**
   a. **General information**
   o Explain the purpose and details of the interview and data processing
   o Request permission to record the interview
   o Restatement of the purpose of the agreement and acknowledgement of the interviewee.
   b. **Presentation of the research project**
   o We investigate promising blockchain use cases in the energy industry
   o We examine both benefits and challenges associated with blockchain applications
   o We want to identify where the use of blockchain technology makes sense
2. **Introduction of the interviewee (5 min)**
   o Ask the interviewee to briefly introduce their organization
   o Ask the interviewee to briefly their role in the organization and the length of their affiliation
   o Ask the interviewee to state how long they have been in their current role or field
   o Ask the interviewee to present their professional background
3. **Discussion of the use case or pilot project in which the interviewee was/is involved (35 min)**
   a. **General**
   o What is the use case or project scope?
   - What was done?
   - Which partners were involved?
   - How long did the project last?
   - What were the cost of the project?

   b. **Role of blockchain**
   o Why was blockchain used in the project / which added value did it bring to the table?
   o Which blockchain framework (Ethereum, Hyperledger, etc.) was used and why?
   o Which Blockchain components were adapted and which were used “out of the box”?
   o How were the blockchain components integrated into existing systems? (e.g., data transfer from existing systems, etc.).
   o What does an exemplary process of data processing, storage, and transfer look like for the use case / the pilot project?
   o Where did blockchain-specific challenges arise over the course of the project and how did you solve them?
   c. **Recommendations for action**
   o Based on the challenges identified, what do you expect from:
   - **political decision-makers?** (Adopt legislation to facilitate implementation? Create a new policy framework? What should this framework look like?)
   - the **scientific community?** (In which area would research need to be intensified? Are “sandboxes” useful? In which area would collaboration between research and industry need to be improved?)
   - other **companies/ the market?** (Is the competition too strong / too weak? Should there be more collaboration between start-ups and established companies)?

Interviewed experts

Appendix A4 *List of interviewed experts*

Here we list the interviews that we conducted to identify benefits and challenges of using blockchain in electric power systems. For privacy reasons, we do not list the names of the interviewed experts and their organizations.

Interview No.	Job Title	Organization Type	Organization No.	Discussed Use Cases
1	Product and Partner Manager	Non Profit Organization	1	Peer-to-peer electricity trading - retail, E-roaming, Certificate trading
2	CEO	IT Service Provider	2	Peer-to-peer electricity trading - retail, Peer-to-peer electricity trading - wholesale
3	Blockchain Engineer	Non Profit Organization	3	Decentralized system services, Labeling of electricity, Certificate trading
4	Lead Blockchain and Distributed Ledger Technologies	Energy Utility	3	Peer-to-peer electricity trading - retail, Labeling of electricity
5	Director Operations	IT Service Provider	4	Certificate trading
6	Chief Security Officer	IT Service Provider	5	Peer-to-peer electricity trading - retail
7	Product and Innovation Manager	IT Service Provider	6	Labeling of electricity, Certificate trading
8	Product Manager	IT Service Provider	5	Peer-to-peer electricity trading - retail
9	Head of Distributed Ledger Technologies	IT Service Provider	7	Peer-to-peer electricity trading - retail, Decentralized system services, E-roaming
10	Head of Business Relationship Management	Energy Utility	8	Peer-to-peer electricity trading - retail, Decentralized system services, Certificate trading
11	IT Project Manager	Distribution System Operator	9	Peer-to-peer electricity trading - retail, Decentralized system services
12	Head of Energy Data Lab	Energy Utility	10	Peer-to-peer electricity trading - retail, E-roaming
13	Distributed Ledger Software Engineer	Energy Utility	10	E-roaming
14	Team Leader Local Energy Platforms	Research Institute	11	Peer-to-peer electricity trading - retail
15	Researcher	Research Institute	12	Peer-to-peer electricity trading - retail, Certificate trading
16	Lawyer and Partner	Law Firm	13	Microgrid operation
17	Researcher	Research Institute	14	Peer-to-peer electricity trading - retail
18	Project Manager	Energy Think Tank	15	Peer-to-peer electricity trading - retail
19	Senior Technical Manager	IT Service Provider	16	Peer-to-peer electricity trading - retail
20	CEO and Founder	IT Management Consultancy	17	Peer-to-peer electricity trading - retail
21	Head of Technology Lab	Energy Service Provider	18	Peer-to-peer electricity trading - retail
22	Software Developer	Research Institute	19	Peer-to-peer electricity trading - wholesale, Microgrid operation
23	Embedded Systems Developer	IT Service Provider	20	Peer-to-peer electricity trading - retail
24	Electrical Engineer	Research Institute	19	Microgrid operation
25	CTO	Non Profit Organization	1	E-roaming
26	Lead Technical Solutions and Product Quality	IT Service Provider	21	Labeling of electricity
27	Attorney-at-law	Consumer Protection Association	22	Peer-to-peer electricity trading - retail
28	Head of Communication and Energy Policy	Energy utility	23	Peer-to-peer electricity trading - wholesale, labeling of electricity
29	Energy Expert	Energy Trading House	24	Peer-to-peer electricity trading - wholesale, Decentralized system services, labeling of electricity
30	Head of Market Management Department	Distribution System Operator	25	Decentralized system services
31	Researcher	Research Institute	26	Peer-to-peer electricity trading - wholesale, Decentralized system services, Microgrid operation, Labeling of electricity, Certificate trading
32	Researcher	Research Institute	27	Peer-to-peer electricity trading - retail, Peer-to-peer electricity trading - wholesale, Microgrid operation, E-roaming
33	Researcher	Research Institute	27	Peer-to-peer electricity trading - wholesale, Microgrid operation, E-roaming
34	Head of Venture Creation	IT Service Provider	28	Peer-to-peer electricity trading - retail, Microgrid operation, E-roaming
35	Head of Sales and Business Area Development	Start-Up	29	Peer-to-peer electricity trading - retail, Labeling of electricity, Certificate trading
36	Researcher	Research Institute	30	Labeling of electricity, Certificate trading
37	Researcher	Research Institute	30	Peer-to-peer electricity trading - wholesale, Decentralized system services, Microgrid operation, Labeling of electricity, Certificate trading
38	Partnership Development and Regulatory Affairs	Non Profit Organization	31	Peer-to-peer electricity trading - wholesale, Decentralized system services, Microgrid operation
39	Lead IoT Architect and Software Developer	Energy Utility	32	Peer-to-peer electricity trading - retail, Decentralized system services, Microgrid operation, Labeling of electricity, Certificate trading
40	Blockchain Product Owner	Energy Utility	32	Peer-to-peer electricity trading - wholesale, Microgrid operation, Labeling of electricity
41	Founder and CEO	Start-Up	33	Machine identities, Labeling of electricity; Peer-to-peer electricity trading - retail

(*continued on next page*)

(*continued*)

Interview No.	Job Title	Organization Type	Organization No.	Discussed Use Cases
42	Founder and CEO	Start-Up	34	Machine identities
43	Researcher	Research Institute	35	Machine identities, Peer-to-peer electricity trading - retail, E-roaming
44	Blockchain Architect and Head of SSI	Start-Up	36	Machine identities
45	Co-Founder and CEO	Start-Up	37	Machine identities, Labeling of electricity, Certificate trading, Peer-to-peer electricity trading - retail, Decentralized system services, Microgrid operation

Use case analysis

Appendix A5 Analyzed sources per use case

Here we list the sources on which we based our analysis of the identified use cases.

Use Case	Sources
Peer-to-peer electricity trading – retail	**Literature**
	Ableitner et al. (2020), Ahl et al. (2019), Ahl et al. (2020), Akter et al. (2020), Al-Obaidi et al. (2021), AlAshery et al. (2021), An et al. (2020), Andoni et al. (2019), Antal et al. (2021), Ante et al. (2021), Bischi et al. (2021), Choobineh et al. (2022), Christidis et al. (2021), Di Silvestre et al. (2019), Diestelmeier et a. (2019), Doan et al. (2021), Dong et al. (2018), Esfahani (2022), Esmat et al. (2021), Foti & Vavalis (2019), Guerrero et al. (2020), Guerrero et al. (2021), Hahnel et al. (2019), Han et al. (2020), Hasankhani et al. (2021), Hayes et al. (2020), Hirsch et al. (2018), Hua et al. (2020), Jiang et al. (2020), Johnson & Mayfield (2020), Kanakadhurga et al. (2022), Khorasany et al. (2021), Kobashi et al. (2020), Lei et al. (2021), Li et al. (2018), Li et al. (2019), Lin et al. (2019), Long et al. (2018), Lowitzsch et al. (2020), Luo et al. (2018), Lüth et al. (2018), Maneesha & Swarup (2021), Mehdinejad et al. (2022), Mengelkamp et al. (2018), Mengelkamp et al. (2019), Mika et al. (2021), Milchram et al. (2020), Neves et al. (2020), Noor et al. (2018), Nour et al. (2022), Paiho et al. (2021), Perrons et al. (2020), Prinsloo et al. (2018), Roberts et al. (2019), Saha et al. (2021), Soto et al. (2021), Sousa et al. (2019), Thukral (2021), Tsao & Thanh (2021), Tushar et al. (2021), van Cutsem et al. (2020), van Leeuwen et al. (2020), Vieira & Zhang (2021), Wang et al. (2020), Wang et al. (2021), Warneryd et al. (2020), Wu &, Zhang (2021), Wu et al. (2019), Wu et al. (2021), Yun et al. (2021), Zhao et al. (2022)
	Reports
	Accenture (2018), Atlantic Council (2019), BNetzA (2019), Bundesblock (2019), Capgemini (2019), CDC Canada (2019), CLI (2019), Congressional Research Service (2019), Council on Foreign Relations (2018), Deloitte (2019), Detecon (2018), Energy Futures Initiative (2018), EU Blockchain Observatory and Forum (2019), FFE (2018), FSR (2019), Germanwatch (2018), IFC (2018), IRENA (2019), NERA (2019), NREL (2020), Renew Nexus (2019), SAP (2018), Smart Service Welt (2020), Solarplaza (2019), Stanford (2019), Vise (2019), World Energy Council (2019)
	Interviews
	1, 2, 4, 6, 8, 9, 10, 11, 12, 14, 15, 17, 18, 19, 20, 21, 23, 27, 32, 34, 35, 39, 40, 41, 43, 45
Peer-to-peer electricity trading - wholesale	**Literature**
	Ableitner et al. (2020), Ahl et al. (2019), Ahl et al. (2020), An et al. (2020), Andoni et al. (2019), Antal et al. (2021), Ante et al. (2021), Bhushan et al. (2020), Choobineh et al. (2022), Choobineh et al. (2022), Di Silvestre et al. (2019), Diestelmeier et al. (2019), Dong et al. (2018), Esmat et al. (2021), Foti & Vavalis (2019), Han et al. (2020), Han et al. (2020), Hasankhani et al. (2021), Hayes et al. (2020), Johnson & Mayfield (2020), Li et al. (2018), Li et al. (2021), Lin et al. (2019), Maneesha & Swarup (2021), Maneesha et al. (2021), Mengelkamp et al. (2019), Mika et al. (2021), Noor et al. (2018), Nour et al. (2022), Paiho et al. (2021), Perrons et al. (2020), Soto et al. (2021), Sousa et al. (2019), Thukral (2021), Tushar et al. (2021), Wang et al. (2020), Wang et al. (2021), Wu et al. (2019), Wu et al. (2021), Yan et al. (2022)
	Reports
	Accenture (2018), Council on Foreign Relations (2018), DENA (2019), Detecon (2018), Energy Futures Initiative (2018), EY (2019), FFE (2018), FSR (2019), Germanwatch (2018), GIZ Mexico (2019), NERA (2019), Renew Nexus (2019), Solarplaza (2019)
	Interviews
	2, 22, 28, 29, 31, 32, 33, 37, 38, 40
Decentralized system services	**Literature**
	Ahl et al. (2019), Christidis et al. (2021), Lin et al. (2019), Ableitner et al. (2020), Ahl et al. (2020), Al-Obaidi et al. (2021), An et al. (2020), Andoni et al. (2019), Ante et al. (2021), Choobineh et al. (2022), Di Silvestre et al. (2019), Diestelmeier et a. (2019), Dong et al. (2018), Esmat et al. (2021), Foti & Vavalis (2019), Guerrero et al. (2020), Han et al. (2020), Hasankhani et al. (2021), Hayes et al. (2020), Kanakadhurga et al. (2022), Lei et al. (2021), Li et al. (2018), Li et al. (2021), Mengelkamp et al. (2019), Mika et al. (2021), Noor et al. (2018), Paiho et al. (2021), Roberts et al. (2019), Soto et al. (2021), Sousa et al. (2019), Thukral (2021), Tsao et al. (2021), Tushar et al. (2021), Wang et al. (2020), Wang et al. (2021), Yan et al. (2022)
	Reports
	BNetzA (2019), DENA (2019), EnergyWeb (2019), FFE (2018), FSR (2019), Germanwatch (2018), IRENA (2019), NERA (2019), NREL (2020), Renew Nexus (2019), SAP (2018), Smart Service Welt (2020)
	Interviews
	3, 9, 10, 11, 29, 30, 31, 37, 38, 39, 45
Microgrid operation	**Literature**
	Ahl et al. (2019), Ahl et al. (2020), Andoni et al. (2019), Antal et al. (2021), Ante et al. (2021), Bandeiras et al. (2020), Bhushan et al. (2020), Bian et al. (2022), Choobineh et al. (2022), Christidis et al. (2021), Das et al. (2020), Di Silvestre et al. (2019), Diestelmeier et a. (2019), Dong et al. (2018), Esfahani (2022), Esmat et al. (2021), Hasankhani et al. (2021), Hayes et al. (2020), Kanakadhurga et al. (2022), Khan et al. (2019), Khorasany et al. (2021), Kobashi et al. (2020), Li et al. (2018), Li et al. (2019), Long et al. (2018), Luo et al. (2018), Maneesha & Swarup (2021), Mengelkamp et al. (2018), Mengelkamp et al. (2019), Noor et al. (2018), Nour et al. (2022), Paiho et al. (2021), Perrons et al. (2020), Prinsloo et al. (2018), Roberts et al. (2019), Soto et al. (2021), Tsao & Thanh (2021), Tsao et al. (2021), Tsao, Thanh & Wu (2021), Tushar et al. (2021), van Cutsem et al. (2020), van Leeuwen et al. (2020), Vieira & Zhang (2021), Wang et al. (2019), Wang et al. (2020), Wu et al. (2021), Zhang et al. (2018), Zhang et al. (2020), Zhao et al. (2022)
	Reports
	Atlantic Council (2019), Capgemini (2019), CLI (2019), Council on Foreign Relations (2018), CSIS (2019), Deloitte (2019), Energy Futures

(*continued on next page*)

(*continued*)

Use Case	Sources
	Initiative (2018), EnergyWeb (2019), FFE (2018), FSR (2019), IFC (2018), IRENA (2019), NERA (2019), Netherlands Innovation Network (2019), NITI Aayog (2019), Renew Nexus (2019), Smart Service Welt (2020), Solarplaza (2019) **Interviews** 16, 22, 24, 31, 32, 33, 34, 37, 38, 39, 40, 45
E-roaming	**Literature** Al-Obaidi et al. (2021), Andoni et al. (2019), Bhushan et al. (2020), Christidis et al. (2021), Christidis et al. (2021), Fu et al. (2020), Hasankhani et al. (2021), Khorasany et al. (2021), Lei et al. (2021), Nour et al. (2022), Soto et al. (2021), Thukral (2021), Tushar et al. (2021), Zhang et al. (2018), Zhang et al. (2022) **Reports** Accenture (2018), BNetzA (2019), Council on Foreign Relations (2018), DENA (2019), Detecon (2018), Energy Futures Initiative (2018), FFE (2018), Germanwatch (2018), IRENA (2019), NERA (2019), SAP (2018) **Interviews** 1, 9, 12, 13, 25, 32, 33, 34, 43
Labeling of electricity	**Literature** Ahl et al. (2019), Ahl et al. (2020), Andoni et al. (2019), Di Silvestre et al. (2019), Fu et al. (2020), Howson (2019), Hua et al. (2020), Lei et al. (2021), Mika et al. (2021), Nour et al. (2022), Wang et al. (2020) **Reports** Bundesblock (2019), CLI (2019), Council on Foreign Relations (2018), European Commission (2019), FFE (2018), FSR (2019), GIZ Mexico (2019), NERA (2019), SAP (2018), Smart Service Welt (2020), Stanford (2019) **Interviews** 3, 4, 7, 26, 28, 29, 31, 34, 35, 36, 37, 39, 40, 41, 45
Certificate trading	**Literature** Ahl et al. (2019), Ahl et al. (2020), Andoni et al. (2019), Di Silvestre et al. (2019), Fu et al. (2020), Howson (2019), Hua et al. (2020), Lei et al. (2021), Mika et al. (2021), Nour et al. (2022), Wang et al. (2020) **Reports** Accenture (2018), BNetzA (2019), Capgemini (2019), CLI (2019), Cognizant (2018), Congressional Research Service (2019), DENA (2019), Energy Futures Initiative (2018), EnergyWeb (2019): EU Blockchain Observatory and Forum (2019), EY (2019), FFE (2018), FSR (2019), GIZ Mexico (2019), IRENA (2019), NERA (2019), Netherlands Innovation Network (2019), Smart Service Welt (2020), Stanford (2019) **Interviews** 1, 3, 5, 7, 10, 15, 31, 35, 36, 37, 39, 45
Machine identities	**Literature** Hirsch et al. (2018), Li et al. (2019), Ante et al. (2021) **Reports** enisa (2022), Fraunhofer FIT (2021), UTCID Report (2021), Bitkom (2020), EU Blockchain Observatory and Forum (2019) **Interviews** 41, 42, 43, 44, 45

References

[1] Jensen T, Hedman J, Henningsson S. How TradeLens delivers business value with blockchain technology. MIS Q Exec 2019;18:221–43. https://doi.org/10.17705/2msqe.00018.

[2] Jović M, Tijan E, Žgaljić D, Aksentijević S. Improving maritime transport sustainability using blockchain-based information exchange. Sustainability 2020;12:1–19. https://doi.org/10.3390/su12218866.

[3] Mengelkamp E, Gärttner J, Rock K, Kessler S, Orsini L, Weinhardt C. Designing microgrid energy markets: A case study: The Brooklyn Microgrid. Appl Energy 2018;210:870–80. https://doi.org/10.1016/j.apenergy.2017.06.054.

[4] Lüth A, Zepter JM, Crespo del Granado P, Egging R. Local electricity market designs for peer-to-peer trading: The role of battery flexibility. Appl Energy 2018;229:1233–43. https://doi.org/10.1016/j.apenergy.2018.08.004.

[5] Andoni M, Robu V, Flynn D, Abram S, Geach D, Jenkins D, et al. Blockchain technology in the energy sector: A systematic review of challenges and opportunities. Renew Sustain Energy Rev 2019;100:143–74. https://doi.org/10.1016/j.rser.2018.10.014.

[6] Di Silvestre ML, Gallo P, Guerrero JM, Musca R, Riva Sanseverino E, Sciumè G, et al. Blockchain for power systems: Current trends and future applications. Renew Sustain Energy Rev 2020;119:109585. https://doi.org/10.1016/j.rser.2019.109585.

[7] Baumgarte F, Glenk G, Rieger A. Business models and profitability of energy storage. IScience 2020;23:101554. https://doi.org/10.1016/j.isci.2020.101554.

[8] Lin J, Pipattanasomporn M, Rahman S. Comparative analysis of auction mechanisms and bidding strategies for P2P solar transactive energy markets. Appl Energy 2019;255:113687. https://doi.org/10.1016/j.apenergy.2019.113687.

[9] Accenture. Blockchain for utilities: Beyond the Buzz. 2018.

[10] de Vries A. Bitcoin's energy consumption is underestimated: A market dynamics approach. Energy Res Soc Sci 2020;70:101721.

[11] Stoll C, Klaaßen L, Gallersdörfer U. The carbon footprint of bitcoin. Joule 2019;3(7):1647–61. https://doi.org/10.1016/j.joule.2019.05.012.

[12] Rieger A, Roth T, Sedlmeir J, Fridgen G. We need a broader debate on the sustainability of blockchain. Joule 2022;6(6):1137–41. https://doi.org/10.1016/j.joule.2022.04.013.

[13] Mengelkamp E, Gärttner J, Rock K, Kessler S, Orsini L, Weinhardt C. Designing microgrid energy markets: A case study: The Brooklyn Microgrid. Appl Energy 2018;210:870–80. https://doi.org/10.1016/j.apenergy.2017.06.054.

[14] Choobineh M, Arab A, Khodaei A, Paaso A. Energy innovations through blockchain: Challenges, opportunities, and the road ahead. Electr J 2022;35:107059. https://doi.org/10.1016/j.tej.2021.107059.

[15] Akter MN, Mahmud MA, Haque ME, Oo AM. An optimal distributed energy management scheme for solving transactive energy sharing problems in residential microgrids. Appl Energy 2020;270:115133. https://doi.org/10.1016/j.apenergy.2020.115133.

[16] Zhang W, Wei C-P, Jiang Q, Peng C-H, Zhao JL. Beyond the block: A novel blockchain-based technical model for long-term care insurance. J Manag Inf Syst 2021;38(2):374–400. https://doi.org/10.1080/07421222.2021.1912926.

[17] Bian Z, Zhang Q. Combined compromise solution and blockchain-based structure for optimal scheduling of renewable-based microgrids: Stochastic information approach. Sustain Cities Soc 2022;76:103441. https://doi.org/10.1016/j.scs.2021.103441.

[18] Lei N, Masanet E, Koomey J. Best practices for analyzing the direct energy use of blockchain technology systems: Review and policy recommendations. Energy Policy 2021;156:112422. https://doi.org/10.1016/j.enpol.2021.112422.

[19] Ahl A, Yarime M, Goto M, Chopra SS, Kumar NM, Tanaka K, et al. Exploring blockchain for the energy transition: Opportunities and challenges based on a case study in Japan. Renew Sustain Energy Rev 2020;117:109488. https://doi.org/10.1016/j.rser.2019.109488.

[20] Mika B, Goudz A. Blockchain-technology in the energy industry: blockchain as a driver of the energy revolution? With focus on the situation in Germany. Energy Syst 2021;12(2):285–355. https://doi.org/10.1007/s12667-020-00391-y.

[21] Wang L, Liu J, Yuan R, Wu J, Zhang D, Zhang Y, et al. Adaptive bidding strategy for real-time energy management in multi-energy market enhanced by blockchain. Appl Energy 2020;279:115866. https://doi.org/10.1016/j.apenergy.2020.115866.

[22] Ante L, Steinmetz F, Fiedler I. Blockchain and energy: A bibliometric analysis and review. Renew Sustain Energy Rev 2021;137:110597. https://doi.org/10.1016/j.rser.2020.110597.

[23] Hirsch A, Parag Y, Guerrero J. Microgrids: A review of technologies, key drivers, and outstanding issues. Renew Sustain Energy Rev 2018;90:402–11. https://doi.org/10.1016/j.rser.2018.03.040.

[24] Bischi A, Basile M, Poli D, Vallati C, Miliani F, Caposciutti G, et al. Enabling low-voltage, peer-to-peer, quasi-real-time electricity markets through consortium blockchains. Appl Energy 2021;288:116365. https://doi.org/10.1016/j.apenergy.2020.116365.

[25] Tushar W, Yuen C, Saha TK, Morstyn T, Chapman AC, Alam MJE, et al. Peer-to-peer energy systems for connected communities: A review of recent advances and emerging challenges. Appl Energy 2021;282:116131. https://doi.org/10.1016/j.apenergy.2020.116131.

[26] Sedlmeir J, Buhl HU, Fridgen G, Keller R. The Energy Consumption of Blockchain Technology: Beyond Myth. Bus Inf Syst Eng 2020;62:599–608. https://doi.org/10.1007/s12599-020-00656-x.

[27] Li Y, Yang W, He P, Chen C, Wang X. Design and management of a distributed hybrid energy system through smart contract and blockchain. Appl Energy 2019;248:390–405. https://doi.org/10.1016/j.apenergy.2019.04.132.

[28] Roth T, Stohr A, Amend J, Fridgen G, Rieger A. Blockchain as a driving force for federalism: A theory of cross-organizational task-technology fit. Int J Inf Manage 2022:102476. https://doi.org/10.1016/j.ijinfomgt.2022.102476.

[29] Zhang H, Wang J, Ding Y. Blockchain-based decentralized and secure keyless signature scheme for smart grid. Energy 2019;180:955–67. https://doi.org/10.1016/j.energy.2019.05.127.

[30] Mahmoudian EM. A hierarchical blockchain-based electricity market framework for energy transactions in a security-constrained cluster of microgrids. Int J Electr Power Energy Syst 2022;139:108011. https://doi.org/10.1016/j.ijepes.2022.108011.

[31] Crosby M, Pattanayak P, Verma S, Kalyanaraman V. Blockchain technology: Beyond bitcoin Appl Innov 2016;2:71.

[32] Wüst K, Gervais A. Do you need a blockchain? 2018 Crypto Val. Conf. Blockchain Technol., IEEE; 2018, p. 45–54.

[33] Bhushan B, Khamparia A, Sagayam KM, Sharma SK, Ahad MA, Debnath NC. Blockchain for smart cities: A review of architectures, integration trends and future research directions. Sustain Cities Soc 2020;61:102360. https://doi.org/10.1016/j.scs.2020.102360.

[34] Christidis K, Sikeridis D, Wang Y, Devetsikiotis M. A framework for designing and evaluating realistic blockchain-based local energy markets. Appl Energy 2021;281:115963. https://doi.org/10.1016/j.apenergy.2020.115963.

[35] Esmat A, de Vos M, Ghiassi-Farrokhfal Y, Palensky P, Epema D. A novel decentralized platform for peer-to-peer energy trading market with blockchain technology. Appl Energy 2021;282:116123. https://doi.org/10.1016/j.apenergy.2020.116123.

[36] Watanabe, H., Fujimura, S., Nakadaira, A., Miyazaki, Y., Akutsu, A., Kishigami, J., Blockchain contract: Securing a blockchain applied to smart contracts. 2016 IEEE Int Conf Consum Electron ICCE 2016 2016:467–8. 10.1109/ICCE.2016.7430693.

[37] Chen S, Shen Z, Zhang L, Yan Z, Li C, Zhang N, et al. A trusted energy trading framework by marrying blockchain and optimization. Adv Appl Energy 2021;2:100029. https://doi.org/10.1016/j.adapen.2021.100029.

[38] Butijn B-J, Tamburri DA, Heuvel W-J. Blockchains: A Systematic Multivocal Literature Review. ACM Comput Surv 2021;53(3):1–37.

[39] Körner M-F, Sedlmeir J, Weibelzahl M, Fridgen G, Heine M, Neumann C. Systemic risks in electricity systems: A perspective on the potential of digital technologies. Energy Policy 2022;164:112901. https://doi.org/10.1016/j.enpol.2022.112901.

[40] Thomas L, Zhou Y, Long C, Wu J, Jenkins N. A general form of smart contract for decentralized energy systems management. Nat Energy 2019;4:140–9. https://doi.org/10.1038/s41560-018-0317-7.

[41] Zhang T, Pota H, Chu CC, Gadh R. Real-time renewable energy incentive system for electric vehicles using prioritization and cryptocurrency. Appl Energy 2018;226:582–94. https://doi.org/10.1016/j.apenergy.2018.06.025.

[42] Wu Y, Wu Y, Guerrero JM, Vasquez JC. Digitalization and decentralization driving transactive energy Internet: Key technologies and infrastructures. Int J Electr Power Energy Syst 2021;126:106593. https://doi.org/10.1016/j.ijepes.2020.106593.

[43] Kitchenham B. Procedures for performing systematic reviews. Keele, UK, Keele Univ 2004;33:1–26.

[44] Moher D. Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. Ann Intern Med 2009;151(4):264.

[45] Orlikowski WJ, Baroudi JJ. Studying Information Technology in Organizations: Research Approaches and Assumptions. Inf Syst Res 1991;2:1–28. https://doi.org/10.1287/isre.2.1.1.

[46] Corbin JM, Strauss A. Grounded theory research: Procedures, canons, and evaluative criteria. Qual Sociol 1990;13:3–21. https://doi.org/10.1007/BF00988593.

[47] Starr MA. Qualitative and mixed-methods research in economics: surprising growth, promising future. J Econ Surv 2014;28(2):238–64. https://doi.org/10.1111/joes.12004.

[48] Hesse-Biber SN, Johnson RB, editors. The Oxford Handbook of Multimethod and Mixed Methods Research Inquiry. Oxford University Press; 2015.

[49] Cohen J. Weighted kappa: Nominal scale agreement provision for scaled disagreement or partial credit. Psychol Bull 1968;70:213–20. https://doi.org/10.1037/h0026256.

[50] Wolf R. Rating scales. J Keeves (Ed), Educ Res Methodol Meas an Int Handb 1997: 958–965.

[51] Schneiders A, Shipworth D. Community energy groups: Can they shield consumers from the risks of using blockchain for peer-to-peer energy trading? Energies 2021;14(12):3569. https://doi.org/10.3390/en14123569.

[52] Noor S, Yang W, Guo M, van Dam KH, Wang X. Energy Demand Side Management within micro-grid networks enhanced by blockchain. Appl Energy 2018;228:1385–98. https://doi.org/10.1016/j.apenergy.2018.07.012.

[53] Jiang Y, Zhou K, Lu X, Yang S. Electricity trading pricing among prosumers with game theory-based model in energy blockchain environment. Appl Energy 2020;271:115239. https://doi.org/10.1016/j.apenergy.2020.115239.

[54] Mengelkamp E, Schlund D, Weinhardt C. Development and real-world application of a taxonomy for business models in local energy markets. Appl Energy 2019;256:113913. https://doi.org/10.1016/j.apenergy.2019.113913.

[55] Ableitner L, Tiefenbeck V, Meeuw A, Wörner A, Fleisch E, Wortmann F. User behavior in a real-world peer-to-peer electricity market. Appl Energy 2020;270:115061. https://doi.org/10.1016/j.apenergy.2020.115061.

[56] Guerrero J, Gebbran D, Mhanna S, Chapman AC, Verbič G. Towards a transactive energy system for integration of distributed energy resources: Home energy management, distributed optimal power flow, and peer-to-peer energy trading. Renew Sustain Energy Rev 2020;132:110000. https://doi.org/10.1016/j.rser.2020.110000.

[57] Hoess A, Roth T, Sedlmeir J, Fridgen G, Rieger A. With or without blockchain?: Towards a decentralized, SSI-based eRoaming architecture. Proc Hawaii Int Conf Syst Sci 2022, 2022.:4621–30. https://doi.org/10.24251/hicss.2022.562.

[58] Kirli D, Couraud B, Robu V, Salgado-Bravo M, Norbu S, Andoni M, et al. Smart contracts in energy systems: A systematic review of fundamental approaches and implementations. Renew Sustain Energy Rev 2022;158:112013. https://doi.org/10.1016/j.rser.2021.112013.

[59] Morstyn T, Farrell N, Darby SJ, McCulloch MD. Using peer-to-peer energy-trading platforms to incentivize prosumers to form federated power plants. Nat Energy 2018;3:94–101. https://doi.org/10.1038/s41560-017-0075-y.

[60] Sousa T, Soares T, Pinson P, Moret F, Baroche T, Sorin E. Peer-to-peer and community-based markets: A comprehensive review. Renew Sustain Energy Rev 2019;104:367–78. https://doi.org/10.1016/j.rser.2019.01.036.

[61] Alt R, Wende E. Blockchain technology in energy markets – An interview with the European energy exchange. Electron Mark 2020;30(2):325–30. https://doi.org/10.1007/s12525-020-00423-6.

[62] German Energy Agency. DENA: Blockchain in the integrated energy transition. Dena Multi-stakeholder Study 2018:84.

[63] Chanson M, Bogner A, Bilgeri D, Fleisch E, Wortmann F. Blockchain for the IoT: privacy-preserving protection of sensor data. J Assoc Inf Syst 2019:1272–307. https://doi.org/10.17705/1jais.00567.

[64] Mehdinejad M, Shayanfar H, Mohammadi-Ivatloo B. Peer-to-peer decentralized energy trading framework for retailers and prosumers. Appl Energy 2022;308:118310. https://doi.org/10.1016/j.apenergy.2021.118310.

[65] An J, Lee M, Yeom S, Hong T. Determining the Peer-to-Peer electricity trading price and strategy for energy prosumers and consumers within a microgrid. Appl Energy 2020;261:114335. https://doi.org/10.1016/j.apenergy.2019.114335.

[66] Neves D, Scott I, Silva CA. Peer-to-peer energy trading potential: An assessment for the residential sector under different technology and tariff availabilities. Energy 2020;205:118023. https://doi.org/10.1016/j.energy.2020.118023.

[67] Imani MH, Ghadi MJ, Ghavidel S, Li L. Demand response modeling in microgrid operation: a review and application for incentive-based and time-based programs. Renew Sustain Energy Rev 2018;94:486–99. https://doi.org/10.1016/j.rser.2018.06.017.

[68] Gao H, Xu S, Liu Y, Wang L, Xiang Y, Liu J. Decentralized optimal operation model for cooperative microgrids considering renewable energy uncertainties. Appl Energy 2020;262:114579. https://doi.org/10.1016/j.apenergy.2020.114579.

[69] Yang J, Dai J, Gooi HB, Nguyen HD, Wang P. Hierarchical Blockchain Design for Distributed Control and Energy Trading Within Microgrids. IEEE Trans Smart Grid 2022;13:3133–44. https://doi.org/10.1109/TSG.2022.3153693.

[70] Yang J, Dai J, Gooi HB, Nguyen H, Paudel A. A Proof-of-Authority Blockchain Based Distributed Control System for Islanded Microgrids. IEEE Trans Ind Informatics 2022;1. https://doi.org/10.1109/TII.2022.3142755.

[71] Hasankhani A, Mehdi Hakimi S, Bisheh-Niasar M, Shafie-khah M, Asadolahi H. Blockchain technology in the future smart grids: A comprehensive review and frameworks. Int J Electr Power Energy Syst 2021;129:106811. https://doi.org/10.1016/j.ijepes.2021.106811.

[72] Perrons RK, Cosby T. Applying blockchain in the geoenergy domain: The road to interoperability and standards. Appl Energy 2020;262:114545. https://doi.org/10.1016/j.apenergy.2020.114545.

[73] Utz M, Johanning S, Roth T, Bruckner T, Strüker J. From ambivalence to trust: Using blockchain in customer loyalty programs. Int J Inf Manage 2022:102496. https://doi.org/10.1016/j.ijinfomgt.2022.102496.

[74] Luke MN, Anstey G, Taylor W, Sirak A. Blockchains in Power Markets. Decentralized Disruption or Incremental Innovation? 2019.

[75] Amend J, Fridgen G, Rieger A, Roth T, Stohr A. The evolution of an architectural paradigm-using blockchain to build a cross-organizational enterprise service bus. 54th Hawaii Int Conf Syst Sci (HICSS), Maui, Hawaii 2021.

[76] Beck R, Müller-Bloch C, King JL. Governance in the blockchain economy: A framework and research agenda. J Assoc Inf Syst 2018:1020–34.

[77] Hawlitschek F, Notheisen B, Teubner T. The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy. Electron Commer Res Appl 2018;29:50–63. https://doi.org/10.1016/j.elerap.2018.03.005.

[78] Ahl A, Yarime M, Tanaka K, Sagawa D. Review of blockchain-based distributed energy: Implications for institutional development. Renew Sustain Energy Rev 2019;107:200–11. https://doi.org/10.1016/j.rser.2019.03.002.

[79] Diniz EH, Yamaguchi JA, dos Santos TR, de Carvalho AP, Alego AS, Carvalho M. Greening inventories: Blockchain to improve the GHG Protocol Program in scope 2. J Clean Prod 2021;291:125900. https://doi.org/10.1016/j.jclepro.2021.125900.

[80] Fernando Y, Rozuar NHM, Mergeresa F. The blockchain-enabled technology and carbon performance: Insights from early adopters. Technol Soc 2021;64:101507. https://doi.org/10.1016/j.techsoc.2020.101507.

[81] Khorasany M, Dorri A, Razzaghi R, Jurdak R. Lightweight blockchain framework for location-aware peer-to-peer energy trading. Int J Electr Power Energy Syst 2021;127:106610. https://doi.org/10.1016/j.ijepes.2020.106610.
[82] Abad AV, Dodds PE. Green hydrogen characterisation initiatives: Definitions, standards, guarantees of origin, and challenges. Energy Policy 2020;138:111300. https://doi.org/10.1016/j.enpol.2020.111300.
[83] Li W, Wang L, Li Ye, Liu Bo. A blockchain-based emissions trading system for the road transport sector: policy design and evaluation. Clim Policy 2021;21(3): 337–52. https://doi.org/10.1080/14693062.2020.1851641.
[84] Houtan B, Hafid AS, Makrakis D. A survey on blockchain-based self-sovereign patient identity in healthcare. IEEE Access 2020;8:90478–94. https://doi.org/10.1109/ACCESS.2020.2994090.
[85] Bandara E, Liang X, Foytik P, Shetty S, Hall C, Bowden D, et al. A blockchain empowered and privacy preserving digital contact tracing platform. Inf Process Manag 2021;58:102572. https://doi.org/10.1016/j.ipm.2021.102572.
[86] Ehrlich T, Richter D, Meisel M, Anke J. Self-sovereign identity as the basis for universally applicable digital identities. HMD Prax Der Wirtschaftsinformatik 2021;58:247–70. https://doi.org/10.1365/s40702-021-00711-5.
[87] Anania L, Le GG, van Kranenburg R. Disposable identities? Why digital identity matters to blockchain disintermediation and for society. Disintermediation Econ., Springer 2021:297–327. https://doi.org/10.1007/978-3-030-65781-9_14.
[88] Alam SM, Al MMA, Hossain MS, Samiruzzaman M. A novel approach to manage ownership and VAT using blockchain-based digital identity. Int Symp Ubiquitous Netw., Springer 2021:255–68. https://doi.org/10.1007/978-3-030-86356-2_21.
[89] Sedlmeir J, Smethurst R, Rieger A, Fridgen G. Digital identities and verifiable credentials. Bus Inf Syst Eng 2021;63(5):603–13. https://doi.org/10.1007/s12599-021-00722-y.
[90] Lacity M, Carmel E. Implementing Self-Sovereign Identity (SSI) for a Digital Staff Passport at UK National Health Service (NHS) 2022.
[91] Sikorski JJ, Haughton J, Kraft M. Blockchain technology in the chemical industry: Machine-to-machine electricity market. Appl Energy 2017;195:234–46. https://doi.org/10.1016/j.apenergy.2017.03.039.
[92] Foti M, Vavalis M. Blockchain based uniform price double auctions for energy markets. Appl Energy 2019;254:113604. https://doi.org/10.1016/j.apenergy.2019.113604.
[93] Luo F, Dong ZY, Liang G, Murata J, Xu Z. A Distributed Electricity Trading System in Active Distribution Networks Based on Multi-Agent Coalition and Blockchain. IEEE Trans Power Syst 2019;34:4097–108. https://doi.org/10.1109/TPWRS.2018.2876612.
[94] Zimmermann H, Hoppe J. Blockchain-Opportunities and threats for the energy transition. Germanwatch 2018.
[95] Diestelmeier L. Changing power: Shifting the role of electricity consumers with blockchain technology – Policy implications for EU electricity law. Energy Policy 2019;128:189–96. https://doi.org/10.1016/j.enpol.2018.12.065.
[96] Lowitzsch J, Hoicka CE, van Tulder FJ. Renewable energy communities under the 2019 European Clean Energy Package – Governance model for the energy clusters of the future? Renew Sustain Energy Rev 2020;122:109489. https://doi.org/10.1016/j.rser.2019.109489.
[97] Sedlmeir J, Ross P, Luckow A, Lockl J, Miehle D, Fridgen G. The DLPS: A new framework for benchmarking blockchains. Proc 54th Hawaii Int Conf Syst Sci 2021:6855–64. https://doi.org/10.24251/hicss.2021.822.
[98] de Vries A. Renewable Energy Will Not Solve Bitcoin's Sustainability Problem. Joule 2019;3:893–8. https://doi.org/10.1016/j.joule.2019.02.007.
[99] Rieger A, Roth T, Sedlmeir J, Weigl L, Fridgen G. Not yet another digital identity. Nat Hum Behav 2022;6:3. 10.1038/s41562-021-01243-0.
[100] Rieger A, Lockl J, Urbach N, Guggenmos F, Fridgen G. Building a blockchain application that complies with the EU general data protection regulation. MIS Q Exec 2019;18:263–79. https://doi.org/10.17705/2msqe.00020.
[101] Sedlmeir J, Lautenschlager J, Fridgen G, Urbach N. The transparency challenge of blockchain in organizations. Electron Mark 2022. https://doi.org/10.1007/s12525-022-00536-0.
[102] Toufaily E, Zalan T, Dhaou SB. A framework of blockchain technology adoption: An investigation of challenges and expected value. Inf Manag 2021;58(3):103444. https://doi.org/10.1016/j.im.2021.103444.
[103] van Leeuwen G, AlSkaif T, Gibescu M, van Sark W. An integrated blockchain-based energy management platform with bilateral trading for microgrid communities. Appl Energy 2020;263:114613. https://doi.org/10.1016/j.apenergy.2020.114613.
[104] Zia MF, Elbouchikhi E, Benbouzid M. Microgrids energy management systems: A critical review on methods, solutions, and prospects. Appl Energy 2018;222: 1033–55. https://doi.org/10.1016/j.apenergy.2018.04.103.
[105] García Vera YE, Dufo-López R, Bernal-Agustín JL. Energy management in Microgrids with Renewable Energy Sources: A Literature Review. Appl Sci 2019;9(18):3854. https://doi.org/10.3390/app9183854.
[106] Rieger A, Thummert R, Fridgen G, Kahlen M, Ketter W. Estimating the benefits of cooperation in a residential microgrid: A data-driven approach. Appl Energy 2016;180:130–41. https://doi.org/10.1016/j.apenergy.2016.07.105.
[107] Sedlmeir J, Völter F, Strüker J. The next stage of green electricity labeling: using zero-knowledge proofs for blockchain-based certificates of origin and use. ACM SIGENERGY Energy Informatics Rev 2021;1(1):20–31. https://doi.org/10.1145/3508467.3508470.
[108] Equigy. A multi-TSO initiative to catalyse the cost-effective use of balancing potential provided by flexible distributed energy resources. 2020.
[109] Fu Z, Dong P, Ju Y. An intelligent electric vehicle charging system for new energy companies based on consortium blockchain. J Clean Prod 2020;261:121219. https://doi.org/10.1016/j.jclepro.2020.121219.
[110] Acharya S, Mieth R, Karri R, Dvorkin Y. False data injection attacks on data markets for electric vehicle charging stations. Adv Appl Energy 2022;7:100098. 10.1016/j.adapen.2022.100098.
[111] Politou E, Alepis E, Patsakis C. Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. J Cybersecur 2018;4. https://doi.org/10.1093/cybsec/tyy001.
[112] Strüker J, Schellinger B, Völter F, Wohlleben J. InDEED Forschungsprojekt untersucht den Einsatz von Blockchain im Energiesektor 2022.
[113] Fraunhofer Institute for Industrial Engineering IAO. Smart Energy Communities Smart Services für die dezentrale Energiewirtschaft der Zukunft 2022.
[114] Carbonfuture. Carbon Removal you can trust. 2022.
[115] Richard P, Mamel S. Blockchain machine identity ledger. Future Energy Lab 2022.
[116] Energy Web Foundation. EWF and Elia Group Self-Sovereign-Identity (SSI) Wallet Components 2022.
[117] MiCA. Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 2020;593 final:1–167.
[118] European Commission. Regulation of the European Parliament and of the council - amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity 2021.
[119] Gourisetti SNG, Sebastian-Cardenas DJ, Bhattarai B, Wang P, Widergren S, Borkum M, et al. Blockchain smart contract reference framework and program logic architecture for transactive energy systems. Appl Energy 2021;304:117860. https://doi.org/10.1016/j.apenergy.2021.117860.
[120] Garrido GM, Sedlmeir J, Uludağ Ö, Alaoui IS, Luckow A, Matthes F. Revealing the landscape of privacy-enhancing technologies in the context of data markets for the IoT: A systematic literature review. J. Netw. Comput. Appl. 2022:103465. https://doi.org/10.1016/j.jnca.2022.103465.
[121] Sedlmeir J, Wagner T, Djerekarov E, Green R, Klepsch J, Rao S. A serverless distributed ledger for enterprises. Proc 55th Hawaii Int Conf Syst Sci 2021: 7382–91. https://doi.org/10.24251/hicss.2022.886.

RP3: Lacity, M., Carmel, E., Young, A. G., & Roth, T. (2023). **The Quiet Corner of Web3 That Means Business.** *MIT Sloan Management Review*, *64(3).* URL: https://sloanreview.mit.edu/article/the-quiet-corner-of-web3-that-means-business/

Journal Rating: 4.9 (CiteScore); 1.100 (SNIP)

MITSloan
Management Review

SPRING 2023
ISSUE

Mary Lacity
Erran Carmel
Amber Grace Young
Tamara Roth

The Quiet Corner of Web3 That Means Business

While the metaverse still lacks legs and crypto stumbles, managers who are keeping an eye on Web3 can learn from promising implementations of decentralized credentials.

Vol. 64, No. 3 • Reprint #64317 • sloanreview.mit.edu

The Quiet Corner of Web3 That Means Business

While the metaverse still lacks legs and crypto stumbles, managers who are keeping an eye on Web3 can learn from promising implementations of decentralized credentials.

By Mary Lacity, Erran Carmel, Amber Grace Young, and Tamara Roth

EXECUTIVES ARE HEARING A LOT about Web3, a blockchain-based road map for the future internet whose building blocks include cryptocurrencies, non-fungible tokens, decentralized autonomous organizations, and, perhaps most famously, the persistent virtual worlds that the so-called metaverse comprises. It's early days for most of these developments — but leaders who want to be out in front on emerging technologies should take note of decentralized credentials, one of the quieter but more promising applications under the Web3 umbrella.

While not every organization will need to build a brand in a metaverse or transact with cryptocurrencies, all organizations manage credentials as issuers, holders, and verifiers. Every organization *issues* credentials to employees, customers, suppliers, and partners; an account for identity management is the most ubiquitous credential issued. Every organization *holds* multiple credentials, such as a license to operate, taxpayer identification, and securities registration. Every organization *verifies* proof of credentials from employees, customers, suppliers, and partners. These three roles, along with a governing authority, form a credentials ecosystem. Today, organizations manage their credentialing needs with centralized databases or by paying trusted third parties. Solutions are often expensive, slow, frustrating to use, and wrought with cybersecurity risks. Let's not forget that the 2020 SolarWinds breach that affected hundreds of U.S. government organizations and businesses was enabled by stolen log-in credentials.

Decentralization empowers holders to control their own credentials via a digital wallet. It's up to the holder to accept a digital credential offered to them by an issuer or to provide proof of a credential to a verifier. Privacy is enhanced because holders often need to present only a part of a credential to a verifying organization. For example, customers ordering a beer at a pub can prove they are of legal drinking age without revealing other information that may be found on a driver's license, such as their name, exact birth date, disability status, or home address.

For verifiers, decentralized credentials are efficient because digital verification happens in seconds, without

Andy Potts

the need to contact the issuer directly. One of the most promising use cases is onboarding new employees. Hiring companies spend significant resources to verify a job candidate's background. On average, it costs $4,129 per hire, but the price tag can be as high as $40,000 per position for highly skilled workers.[1] Issuers can generate credentials once, with no need to recertify unless the credential has expired or changed.

Decentralized credentials also offer enhanced privacy because they're stored in digital wallets rather than in centralized databases, which are attractive targets for cyberthieves.

How Decentralized Credentials Work

Digital wallets are used to orchestrate interactions among issuers, holders, and verifiers of decentralized credentials. The wallets manage peer-to-peer relationships between two parties, such as an issuer and a holder, or a holder and a verifier. Both sides must agree that they want to be connected, and either side can terminate the connection at any time.

Once a peer-to-peer relationship has been established, transactions can take place. Issuers can send digitally signed credentials to holders, and holders can send proof of credentials to verifiers. The verifier's wallet pings a distributed trust registry (normally a blockchain) to ensure that the issuer, and only the issuer, could have digitally signed the credential.

Under the hood, the digital wallets and distributed trust registries can make use of decentralized identifiers. A wallet can create as many decentralized identifiers as needed. Each identifier is controlled by a private-public key pair. The private key resides in the wallet. Issuers, holders, and verifiers use one of their public keys to establish a peer-to-peer connection; issuers create digital credentials for one of the holder's public keys, and issuers sign credentials with one of the issuer's private keys.[2]

While decentralized credentials are still early in their maturity curve, with only a few implementations, leaders should learn about them now while keeping one eye on other Web3 technologies. (See "Envisioning the Next Web," p. 23.) The main challenge — beyond concerns about the technology's immaturity — is convincing the ecosystem participants to adopt decentralized credentials; training issuers, holders, and verifiers in new processes and technologies; and scaling the solution. Two recent standards from the World Wide Web Consortium (W3C) provide a framework for credential privacy, security, and interoperability.[3] While it's still too soon to make definitive prescriptions, our research shows that live production pilots have had encouraging results.

Below, we share stories and insights from three live but small implementations of decentralized credentials by the National Health Service (NHS) England, the Canadian province of British Columbia, and a U.S.-based consortium of financial credit unions. Each implementation addresses specific pain points in its credentialing ecosystem as part of a larger strategic initiative.

NHS England's Digital Staff Passport for Enabling Staff Movement

Credential issuers: NHS England's employing organizations

The reason for adoption: NHS England needed to move staff members among work sites quickly and safely during the COVID-19 pandemic. The solution, called the COVID-19 Digital Staff Passport, is part of its strategic people plan. NHS England comprises over 200 organizations (such as hospitals) operating as independent units, each with its own human resources systems. Staff members (doctors, nurses, and others) move around frequently, making more than 1 million transfers per year. In the past, each time an employee moved within the system, HR spent days verifying a slew of credentials: diplomas, training certificates, professional registration licenses, specific medical certifications, results of criminal background checks, and prior employment credentials. The paperwork involved was nightmarish. For just the doctors in training — a small segment of all transfers — the working time lost while they waited for credentials to be verified added up to a significant sum that was estimated to be in the millions of pounds sterling per month.[4]

The adoption journey: In 2019, NHS England convened ecosystem partners to work on the pilot solution, including NHSX (a joint unit between the U.K.'s Department of Health and Social Care, NHS England, and NHS Improvement), the U.K.'s General Medical Council, several NHS hospitals, and technology providers. The team adopted the W3C's verifiable credential standard and used a commercial product from Avast (formerly Evernym) as the digital wallet. For the pilot, NHS England chose the Sovrin Network for verifying that the issuer had signed the credential.[5] The Digital Staff Passport was launched in the summer of 2020 to help with staff movements during the pandemic.

Only existing NHS staff members are eligible to participate in the pilot, and adoption is voluntary. HR serves as the primary recruitment and training channel, since every transfer begins and ends with a visit to HR. The department is also best positioned to ensure that the hospital generates digital credentials for the correct employee, a process called identity binding.

At the exiting hospital, HR explains the benefits of the Digital Staff Passport: faster onboarding, carrying all required credentials in one convenient place on their phones, providing backup and recovery of their credentials in case their phone is lost or damaged, and controlling who sees their credentials. The NHS employee downloads the wallet onto their phone, and HR sends the employee's wallet a request for a peer-to-peer connection. After the employee accepts the request, HR invites them to load their credentials into their wallet. Each credential essentially certifies, "This is an employee of the originating hospital, and we have already vetted their credentials for X, Y, and Z." At this point, the employee possesses a loaded wallet and controls with whom they will share their credentials. Now the employee can easily transfer from hospital to hospital as needed. At each new hospital, the employee sends HR proof of credentials that is machine-verified to ensure that an authorized issuer digitally signed the employee's credentials. The staff member is now ready to care for patients.

Results so far and next steps: As of November 2022, 105 NHS organizations had registered to use the system.[6] NHS England has reported promising results, though it has not published any statistics. We estimate that over 1,000 employees were onboarded with the Digital Staff Passport. NHS England has achieved cost savings from reduced administrative burden, increased staffing flexibility through easier transfers, and better health care services because employees are able to spend more time with patients. The employees have reported benefits from possessing all of their credentials in one place and having the ability to control the application at every step. Philip Graham, digital program director at Blackpool Teaching Hospitals, a leading NHS organization, said, "The solution enabled the rapid movement of staff during the pandemic and is still being used as part of COVID recovery activities. One of the next steps is to implement a strategic Digital Staff Passport with the interoperability of digital wallets, based on standards, to avoid vendor lock-in and put the staff member in control."

THE RESEARCH

- The authors have been studying decentralized credentials for nearly three years and have conducted over 100 interviews with thought leaders, early adopters, standards-making bodies, technology providers, and government agencies in North America and Europe.
- Their research also relies heavily on participant observation methods during the authors' involvement in the Trust Over IP Foundation, the COVID-19 Credentials Initiative, the Good Health Pass Collaborative, and the European Blockchain Services Infrastructure.

British Columbia's Verifiable Credentials for Businesses and Citizens

Credential issuers: The province of British Columbia (BC)

The reason for adoption: Digital credentials are part of the province's strategy to improve its ability to deliver services in the digital economy. John Jordan, executive director of the BC Digital Trust Service, explained that "online services" for many agencies often means emailing copies of credentials like registrations, licenses, passports, and permits, resulting in higher risks for fraud and identity theft. In such a scenario, government is not fulfilling its role to provide the digital foundation for businesses and citizens to help them easily lease property, open a bank account, apply for loans, seek insurance, and conduct other transactions that require onerous proof of registrations, licenses, or permits, Jordan said.

BC aims to create more open, trusted, and easy-to-use credentials for its businesses and citizens. It sees the move to digital credentials as the next evolution of credentials from handwritten documents decades ago and from more recent hard-to-counterfeit documents with seals and watermarks. It chose decentralized digital credentials based on the model created by the Linux Foundation's Trust Over IP Foundation.[7]

The adoption journey: BC started adopting digital credentials in 2018 with business registrations. As the issuer of these credentials, the province could easily create digital versions. Importantly, business registrations are in the public domain, so there was no unease about working with personally identifiable information in the pilot project.

The team comprised a manager and several developers. They first built the BC wallet with a web-based user interface for holders and verifiers, but they ran into a snag: With millions of business registrations in the province's wallet, searching for a particular business was slow. BC needed an enterprise-grade digital wallet, so it launched a successful 50,000 Canadian dollar ($37,000) public competition to build it as open-source software. (The province is holding the credentials on behalf of businesses for this first step. Ideally, in the future, authorized representatives of businesses will have their own wallets.) Like the NHS, the team chose the Sovrin Network to verify digital signatures. The solution, called OrgBook, was launched in 2019.[8] Now anyone can search the website to find verifiable business registrations.

In addition to the province's business registration credentialing initiative, in which it is an issuer, BC piloted a

Envisioning the Next Web

WHAT'S THE DIFFERENCE BETWEEN Web3 and Web 3.0? To understand what's shaping the competing visions for where the internet is going, we need to quickly review how it has evolved to date.

The internet as most of us experience it was born in 1989, when Tim Berners-Lee invented the World Wide Web, including the first web server and web browser, and HTML. These breakthroughs created commercial and consumer potential for what had been largely a network infrastructure used by governments and research institutions. With the introduction of commercial browsers and search engines in the early 1990s, individuals were able to find information hosted on servers and download static webpages.

What we call Web 2.0 came about around 2003-2004 as webpages became dynamic and interactive, enabling users to contribute content. Developers built web apps with rich functionality to create new social media networks and e-commerce platforms; the most successful have become tech giants with near-monopoly power thanks to commercial network effects. Users "pay" for nominally free online services by allowing their personal data to be collected and their online activity to be tracked so that advertisers can target them. Harvard Business School professor Shoshana Zuboff has famously dubbed this practice "surveillance capitalism."

Proponents of the third significant evolution of the web aim to disperse power and control to individuals. Different communities have different ideas for how to achieve this. The Web3 Foundation, led by Ethereum cofounder Gavin Wood, believes the goal can be met with a decentralized web that is based on cryptography and blockchain.[i] Key components of what this group calls Web 3.0 include digital wallets, asset tokenization, self-executing agreements, the persistent virtual worlds of the so-called metaverse, and the subject of this article — decentralized credentials.

W3C Consortium director Berners-Lee also uses the term Web 3.0 to describe a decentralized web based on the Solid protocol, which grew out of a research project at MIT. This approach aims to give users control of their data and information via decentralized data stores called pods. The Solid website describes these as secure personal web servers for data; users control which people and applications can access their pods. (Two decades ago, Berners-Lee was more focused on developing a future "semantic web" of machine-readable data.) He has publicly rejected the Web3 idea of a new system for internet applications built on blockchain, calling it "not the web at all."[ii]

Decentralized credentials encompass the cryptography of Web3 but also conform to the W3C standards of the current web.

— *Elizabeth Heichler*

solution where the government acts as a verifier. For this credentialing ecosystem, the Law Society is the issuer of membership credentials; 100 lawyers were selected as the holders for the pilot, and the Justice Services Branch of the Ministry of Attorney General is the verifier. This initiative facilitates the credentialing process that allows lawyers to access recorded court sessions and obtain other classified documents from the government. In September 2022, BC deployed its own digital wallet as a soft launch; anyone can download the wallet app on their phone and follow instructions to practice receiving and sharing fictitious credentials in preparation for a future rollout with real credentials.[9]

Results so far and next steps: Jordan described the province's decentralized credentials adoption journey as a "responsible and respectful rollout" overall. Incremental value is delivered with each step, such as providing a free public service for anyone to search, find, and validate business credentials. BC — in cooperation with other jurisdictions — plans to develop its own distributed trust registry. "When verifiable credentials take off, it becomes critical infrastructure that the government should provide for its citizens so that they can confidentially conduct their digital lives," Jordan said.

Bonifii's MemberPass for Credit Union Members

Credential issuers: Credit unions

The reason for adoption: Bonifii is a service organization that supports 70 U.S.-based credit unions. The credit unions sought more secure and trusted digital services. Their centralized identity systems, based on accounts and passwords, kept getting more onerous as members needed to use two- or three-step authentication. Scammers increasingly sent members fraudulent texts or email messages, increasing the risks of identity theft and fraud. Decentralized credentials offered a better way for the credit unions to verify members and for members to verify that they were in fact interacting with their credit unions.

The adoption journey: Bonifii, three credit unions, and a technology provider first tackled proof of membership and started to develop MemberPass in 2019. As in the previous two cases, the Sovrin Network serves as the public registry to verify digital signatures. Sovrin is based on the Trust Over IP Foundation's and FIDO (Fast ID Online) Alliance's principles.[10] MemberPass claims to be "the first [Know Your Customer]-compliant member-controlled digital identity issued by credit union cooperatives."[11]

The digital credential was kept simple: It provided machine-verifiable proofs of member ID number, credit union name, and membership activation date. The credit unions first recruited current members to adopt the credential when they visited a branch. Soon after launch, they enabled phone enrollment. MemberPass can now be used in person, at a branch, at ATMs, on phone calls to call centers, and online.[12]

Results so far and next steps: By the second quarter of 2021, seven credit unions were participating and over 22,000 members had downloaded the MemberPass wallet. By the first quarter of 2022, 10 credit unions had joined the effort and the number of adopters had increased fivefold. For members, the key benefits are convenience and confidence that they are dealing with their credit unions and not with fraudsters. The benefits for the credit unions are more efficient transactions, reduced risk of fraud, and more trusted relationships with members.

A new version of MemberPass with additional features was released in August 2022. Credit unions and Bonifii continue to work on scaling MemberPass to a target population of 6.5 million members. Overall, scaling the technology has been slow. John Ainsworth, CEO of Bonifii, said to us in 2022 that "decentralized credentials are still early days but will be a crucial part of Web3."

Insights From the Pioneer Cases and Beyond

As the three cases demonstrate, implementations show promising results for all roles in the credentials ecosystem: Holders possess and control who sees their credentials; issuers can generate credentials once, with no need to recertify unless the credential changes or is revoked; and verifiers can validate credentials in seconds. (See "Key Roles in Credentials.") In these cases, transaction costs are low for issuers and free for holders and verifiers.[13] At the ecosystem level, cybersecurity benefits arise from managing relationships with peer-to-peer connections instead of with centralized accounts and passwords, and from storing credentials on edge devices in digital wallets rather than in centralized databases.

While these results are promising, we wondered whether a centralized solution could have delivered similar outcomes, so we asked the pioneers. For the NHS, integrating and centralizing HR records from 1,200 hospitals would be technically and politically prohibitive. Furthermore, decentralization means that hospitals do not relinquish control. Bonifii is in a similar situation, since credit unions are independent. In Canada, a centralized solution would not be appropriate, as the provinces are the authoritative issuers of credentials such as birth certificates, driver's licenses, and business registrations.

Despite the promised value, there are significant adoption challenges to overcome, such as recruiting ecosystem partners, managing change, and scaling the solution to support increased participation and additional types of credentials. Interoperability and technical immaturity also raise concerns. Here's our take on adoption at this point:

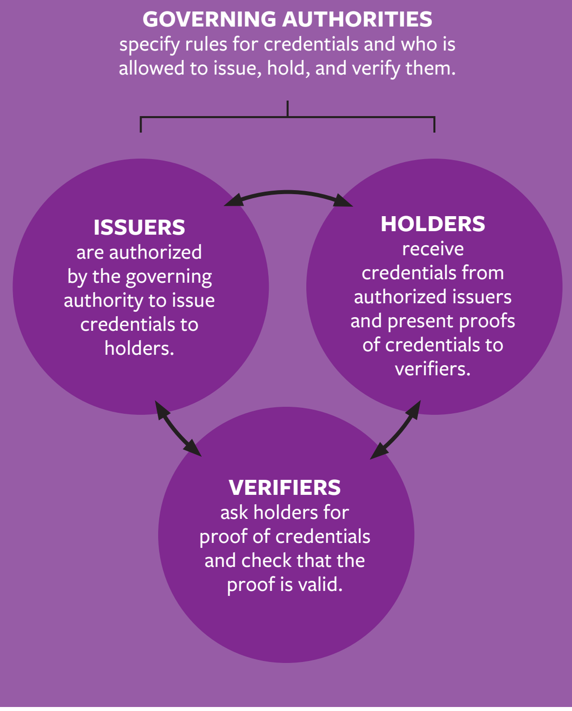
1. Get started with issuers, which are best positioned to lead adoption. Unlike most software applications that are adopted within organizational boundaries, decentralized credentials work only if an entire ecosystem adopts it. To jump-start a solution, there must be authorized credentials available, so it makes sense that issuers led the pilots in all three of the cases above, with support from the governing authorities. In both the NHS and Bonifii cases, the hospitals and credit unions (respectively) are simultaneously issuers and verifiers, thus reducing the recruitment effort.

2. Don't boil the ocean: Start with a subset of issuers, holders, and verifiers. Starting with a subset of adopters allows the development team to deliver a solution fast. If successful, the team proves the value to the larger ecosystem. NHS England started with just a fraction of its 1,200 hospitals and staff members. Bonifii started with three credit unions and a small percentage of members. As the issuer, the province of British Columbia

Many experts argue that governments must invest in decentralized credentials as part of an international digital infrastructure.

KEY ROLES IN CREDENTIALS

Every credentialing system involves four roles: governing authorities, issuers, verifiers, and holders.



GOVERNING AUTHORITIES specify rules for credentials and who is allowed to issue, hold, and verify them.

ISSUERS are authorized by the governing authority to issue credentials to holders.

HOLDERS receive credentials from authorized issuers and present proofs of credentials to verifiers.

VERIFIERS ask holders for proof of credentials and check that the proof is valid.

started with business registrations for its first service. For another service, it included one issuer (the Law Society), one verifier (the Justice Services Branch of the Ministry of Attorney General), and 100 lawyers.

3. Make holder adoption voluntary and onboarding easy. Holders need to understand how they would benefit from adopting a digital wallet. Once they agree to try the solution, they must download the correct digital wallet and learn how to accept connection requests, load credentials from issuers, and share proof of credentials with verifiers. Issuers in two cases recruited, trained, and performed the important first step of identity binding at the point of service. For NHS England, identity binding took place when a staff member was about to be transferred; for MemberPass, it occurred when a member visited a credit union branch. Initially, each organization recruited and trained holders one at a time. Eventually, additional communication and onboarding channels were added, such as websites, promotional videos, and email invitations.

4. Consider interoperability: Will standards save us? While all three cases used the Sovrin Network to verify digital signatures because, as multiple research participants told us, “it was the only decentralized credentials network that existed at the time,” over 100 competing networks are underway.[14] Interoperability will be a problem if networks operate as islands. Also, only a few digital wallets are commercially available, with many more anticipated. Research participants fear that organizations may replace a plethora of accounts and passwords with a plethora of digital wallets. This may evolve to look like the many apps we all have on our smartphones today.

Many standards organizations are working directly or tangentially on decentralized credentials, such as for the use of biometrics for identity binding. The standards landscape includes the W3C for decentralized identifiers and verifiable credentials; the Trust Over IP Foundation for white papers, specifications, and recommendations for wallets to be interoperable with any distributed trust registry; the Decentralized Identity Foundation for an interoperable and open ecosystem; FIDO for authentication on edge devices such as smartphones; and the International Standards Organization for several related standards, including one around mobile driver’s licenses. Standards may complement or compete with one another, depending on how they develop.

5. Consider scalability: Should governments take the lead? So far, there are no scaled solutions. Because so many of society’s bedrock credentials come from governments, many experts we spoke with argued that governments must step up and invest in decentralized credentials as part of an international digital infrastructure. After all, the U.S. government assumed a similar role in the past by funding and supporting the development of the internet in its nascent stages.

Perhaps the most interesting government-led initiative is the European Digital Identity Wallet project. Cross-border identity authentication has long been a challenge in Europe, where each country issues unique credentials and privacy concerns are paramount. The European Union has taken a top-down approach in leading the charge for interoperable digital identity wallets. Early national proof-of-concept and pilot projects include the NESSI project for digital tax IDs in the German state of Bavaria, and Validated ID with CaixaBank and Aigües de Barcelona for customer identification in Spain. A currently piloted cross-border use case is European Blockchain Services Infrastructure’s digital diploma multi-university project. Revision of the EU’s Electronic Identification and Trust Services Regulation, rolling out this year, will provide identity verification and credential authentication for ID cards and driver’s licenses.

Other experts believe that even if governments catalyze some key credentials, some issuers may still resist switching to a business model where credentials are verified with public trust registries instead of with their internal databases. Some issuers, like credit reporting companies, make their money by charging for verifications, and the decentralized credentials model we described in the three cases would disrupt that model. David Huseby, who formerly worked on security at Hyperledger, believes the scaling of decentralized credentials models that rely on digital wallets and external validation has been slow because they require a "rip and replace" business model. Huseby and Rick Cranston, a cofounder of Bonifii, have cofounded Cryptid, where their new decentralized solution does not use digital wallets but instead relies on APIs to existing infrastructure. In their solution, holders still digitally control requests from verifiers, but the holders can also route requests to issuers. Issuers respond at the time of the requests to retrieve the most up-to-date proof of credentials from their internal databases. Issuers can continue to charge fees for verification, but there is a downside that should be acknowledged: Issuers can track user activity.

THE MODEST STARTS WE STUDIED SIGNAL A promising future for decentralized credentials in business and society. Decentralized credentials offer a very different model for online trust. If we can solidify the technological foundations, value-added use cases abound. Entrepreneurs will be able to open a bank account and get competing offers for a business loan with the click of a button. Companies won't need to issue W-2 forms in order for workers to file tax returns in the U.S. Running background checks and onboarding employees and suppliers will be virtually instantaneous. Employees won't fall for phishing attacks, because it will be easy to verify the origin of a message. Increased transparency around suppliers' credentials will inhibit money laundering and promote ethical supply chains. Streaming services will be able to quickly verify that the user renting a PG-13 movie is age 13 or older. Stores will be able to sell alcohol online, or as part of a grocery pickup order, without the risk of the buyer being under the legal drinking age. Patients will be able to share medical records with doctors in different hospital systems and order prescription medicines online.

In addition to providing credentials for humans, decentralized credentials can be used for anything that needs one, including animals, plants, pharmaceuticals, raw materials, machines, and finished products. Company or product attributes such as "woman-owned" or "certified fair trade" will be more meaningful for being verifiable.

Such possibilities are not inevitable; they will happen only if governments, businesses, and individuals learn about decentralized credentials and actively participate in the development and standardization of supportive ecosystems that can interoperate across a multitude of domains. Broad-scale cooperation and regulation will be pivotal to timely adoption and the ability to realize value from this critical Web3 component. ■

Mary Lacity *is the David D. Glass Chair and Distinguished Professor of Information Systems at the Sam M. Walton College of Business at the University of Arkansas.* **Erran Carmel** *is a professor of information technology at the Kogod School of Business at American University.* **Amber Grace Young** *is director of the information systems doctoral degree program and assistant professor of information systems at the Sam M. Walton College of Business.* **Tamara Roth** *is a postdoctoral researcher at the Interdisciplinary Centre for Security, Reliability and Trust at the University of Luxembourg.*

REFERENCES

1. B. Turczynski, "2020 HR Statistics: Job Search, Hiring, Recruiting, & Interviews," Zety, updated Jan. 9, 2020, https://zety.com; and "Your Organization's Reputation on the Line: The Real Cost of Academic Fraud," PDF file (Herndon, Virginia: National Student Clearinghouse, 2016), https://nscverifications.org.
2. A. Preukschat and D. Reed, "Self-Sovereign Identity: Decentralized Digital Identity and Verifiable Credentials" (Shelter Island, New York: Manning Publications, 2021).
3. The W3C is an international community that develops open standards to ensure the long-term growth of the web. The W3C's Verifiable Credential standard was published in 2019; its Decentralized Identifiers standard was published in July 2022.
4. M. Lacity and E. Carmel, "Self-Sovereign Identity and Verifiable Credentials in Your Digital Wallet," MIS Quarterly Executive 21, no. 3 (2022): article 6.
5. The Sovrin Network is managed by the nonprofit Sovrin Foundation. The foundation has authorized over 80 independent volunteers on six continents to operate the network's nodes.
6. The NHS lists the organizations that have registered to use the Digital Staff Passport on its website.
7. The Trust Over IP Foundation was launched in 2020 with the mission to develop a complete architecture for internet digital trust.
8. The OrgBook for the province of British Columbia is available and can be searched online.
9. "BC Wallet," Government ID, Government of British Columbia, accessed Jan. 11, 2023, https://www2.gov.bc.ca.
10. The FIDO Alliance is an open industry association with a mission to reduce the world's overreliance on passwords.
11. "Bonifii and Entersekt Announce New Context-Aware Authentication Solution for Credit Unions," Bonifii, April 21, 2022, https://bonifii.com.
12. P. Windley, "Building an SSI Ecosystem: MemberPass and Credit Unions," Phil Windley's Technometria, June 7, 2021, www.windley.com.
13. The three cases all use the Sovrin Network. In this network, transaction costs are low; only issuers are charged a modest fee (about $10) to post their public keys to the registry, and the issuer can use the key to sign an unlimited number of credentials. At this point, verifiers are not charged for reading the registry.
14. The W3C lists 136 methods for decentralized credentials. See "DID Specification Registries: The Interoperability Registry for Decentralized Identifiers," W3C, updated Jan. 7, 2023, www.w3.org.
i. "About," Web3 Foundation, accessed Jan. 11, 2023, https://web3.foundation.
ii. R. Browne, "Web Inventor Tim Berners-Lee Wants Us to 'Ignore' Web3: 'Web3 Is Not the Web at All,'" CNBC, Nov. 4, 2022, www.cnbc.com.

Reprint 64317. For ordering information, see page 4.

RP4: Rieger, A., Roth, T., Sedlmeir, J., Fridgen, G., & Young, A. G. (2024). **Organizational Identity Management Policies.** *Journal of the Association for Information Systems*, 25(3), 522–527.
Journal Rating: 9.0 (CiteScore); 2.244 (SNIP)

Journal of the Association for Information Systems

Volume 25 | Issue 3 Article 10

2024

Organizational Identity Management Policies

Alexander Rieger
University of Arkansas / University of Luxembourg, arieger@walton.uark.edu

Tamara Roth
University of Arkansas / University of Luxembourg, troth@walton.uark.edu

Johannes Sedlmeir
University of Luxembourg, johannes.sedlmeir@uni.lu

Gilbert Fridgen
University of Luxembourg, gilbert.fridgen@uni.lu

Amber Young
University of Arkansas, ayoung@walton.uark.edu

Recommended Citation

Rieger, Alexander; Roth, Tamara; Sedlmeir, Johannes; Fridgen, Gilbert; and Young, Amber (2024) "Organizational Identity Management Policies," *Journal of the Association for Information Systems*, 25(3), 522-527.
DOI: 10.17705/1jais.00887
Available at: https://aisel.aisnet.org/jais/vol25/iss3/10

Journal of the Association for Information Systems (2024) **25**(3), 522-527
doi: 10.17705/1jais.00887

POLICY EDITORIAL

ISSN 1536-9323

Organizational Identity Management Policies

Alexander Rieger,[1] Tamara Roth,[2] Johannes Sedlmeir,[3] Gilbert Fridgen,[4] Amber Young[5]
[1]Sam M. Walton College of Business, University of Arkansas, USA /
Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg, Luxembourg, arieger@walton.uark.edu
[2]Sam M. Walton College of Business, University of Arkansas, USA /
Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg, Luxembourg, troth@walton.uark.edu
[3]Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg, Luxembourg, johannes.sedlmeir@uni.lu
[4]Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg, Luxembourg, gilbert.fridgen@uni.lu
[5]Sam M. Walton College of Business, University of Arkansas, USA, ayoung@walton.uark.edu

Abstract

Effective identity management is essential for secure organizational processes, but organizations often do not approach it strategically. To break this trajectory, organizational policymakers need to define a clear and sustainable identity management strategy. This paper presents an overview and guidelines to help shape such strategy. It analyzes the key characteristics and trade-offs of today's identity management models. Moreover, it offers practical recommendations for organizational policymakers when choosing among these models.

Keywords: Authentication, Digital Wallets, Identity and Access Management (IAM), Identity Models, Trade-Offs

John L. King was the accepting senior editor. This editorial was submitted in January 2023 and underwent four revisions.

1 Introduction

Identity management challenges are as old as humankind. In the Book of Genesis, Jacob disguises himself with goat fur to confuse his father and steal his brother Esau's birthright. During the early days of Rome, Carthaginian general Hannibal used a signet ring taken from slain Roman consul Marcellus to deceive Rome's allies (Livius, 1943; Sheldon, 2015). These challenges continue in a digital world where secure but efficient identity management is essential for various organizational processes (Smith & McKeen, 2011; Windley, 2023).

Yet many organizations do not approach identity management strategically. Rather, organizations often purchase pre-packaged software solutions and assign the IT department responsibility for identity management. IT departments may be tempted to focus on security over usability, leading to inconvenient policies, such as rules for long and complex passwords or extensive multifactor authentication. As a result, users may spend more time authenticating / proving their identity than receiving the service.

To break this trajectory, we advocate for a strategic approach to identity management. Specifically, we propose that organizational policymakers define a strategy for managing their users' identity data. In what follows, we outline key policy questions that organizational policymakers should ask as they engage in developing an identity management strategy. We begin with a high-level description of today's dominant models for identity management and their strategic trade-offs in terms of control vs. responsibility and convenience vs. security. We then present recommendations for developing a fitting organizational policy.

2 Today's Identity Models and Their Trade-Offs

Organizational identity management is typically concerned with user authentication, source verification, and the storage of identity data. *User authentication* describes how users (persons, organizations, or IoT devices) can prove their identity as previously registered. These proofs are typically generated with so-called credentials or authentication factors. These factors can be "something the user knows" (e.g., a password), "something the user is" (e.g., face or fingerprint), or "something the user has" (e.g., an ID card, a temporary code, or a hardware token) (Benantar, 2005; Lacity et al., 2023; Windley, 2023). *Source verification* allows organizations to validate the correctness of identity claims made by a user, such as being a certain age or possessing a valid driver's license.

There are three identity management models available today to realize user authentication, source verification, and the storage of identity data: fragmented, federated, and wallet-based. While the fragmented and federated models are in use worldwide, the wallet-based model is being pushed in Europe, Canada, and a few US states. We describe each model in turn and contrast them in Table 1.

Table 1. Description and Organizational Trade-Offs Associated with the Three Identity Models

	Fragmented model	Federated model	Wallet-based model
Description	***Enrollment and source verification:*** Users create an account with the organization and fill in a form with required identity attributes. When source verification of identity attributes is required, the organization must employ costly digital or in-person verification processes. ***Identification and authentication:*** Users log in to their account with a username-password combination or passkey as well as additional authentication factors if required.	***Enrollment and source verification:*** Users create an account with the organization and authorize their SSO provider to forward required identity attributes. When SSO providers do not offer source verification, the organization must employ the same processes as in the fragmented model. ***Identification and authentication:*** Users are redirected to their SSO provider, where they log in with a username-password combination or passkey as well as additional authentication factors if required.	***Enrollment and source verification:*** Users create an account with the organization and forward the required identity attributes from a digital wallet. The organization can easily verify the provided attributes using cryptographic checks that are sent together with the identity attributes. ***Identification and authentication:*** Users log in to their account with their digital wallet. Additional authentication factors are limited to those required to log in to the digital wallet app.
Control vs. responsibility	***Control:*** The organization collects and stores users' identity attributes. ***Responsibility:*** The organization is responsible for complying with regulatory requirements for the processing of user identity attributes.	***Control:*** The organization can outsource the collection and storage of identity attributes to SSO providers. ***Responsibility:*** The organization can delegate to the SSO provider some of the responsibility for complying with regulatory requirements for the processing of user identity attributes.	***Control:*** The organization can outsource the collection and storage of identity attributes to users. ***Responsibility:*** Users are responsible for managing their identity attributes and consenting to requests for presentation.
Convenience vs. security	***Convenience:*** Password management is tedious for users. Passkeys are more convenient but require users and the organization to abide by the rules of the passkey ecosystem. In both cases, source verification is slow, costly, and error-prone for the organization. ***Security:*** Security is limited without complex password rules, multifactor authentication, and user compliance with security policies.	***Convenience:*** SSO services are convenient for users and some SSO providers deliver source-verified identity data in a standardized format to the organization. ***Security:*** The likelihood of security incidents is low due to substantial security measures on the SSO provider side, but their impact can be severe.	***Convenience:*** Digital wallet apps are convenient for users and deliver source-verified identity data in a standardized format to the organization. ***Security:*** The likelihood and impact of security incidents are low as individual wallets are relatively unattractive targets for hacks.

The *fragmented model* describes the familiar experience of having separate accounts with username-password logins for each digital service. This model is easy to set up and gives organizations direct access to a trove of personal data that can be used, e.g., for marketing purposes. However, enrolling new users can be costly—especially when know-your-customer laws require organizations to verify physical identity documents. Moreover, when an organization stores sensitive identity data, securing the data against loss, unauthorized use, and hacks requires significant investment (Windley, 2023). The fragmented model also presents an undesirable trade-off between convenience and security when users need to choose unique and ever stronger passwords to keep up with mounting security threats. Password managers offer some help, but they are honeypots for hackers (Winder, 2023). Furthermore, user experience suffers when additional authentication factors are required and when they differ substantially across organizations. Some of these challenges can be addressed with so-called passkeys that replace username-password logins with cryptographic keys stored on mobile devices. Passkeys are highly secure by design and can be protected, for instance, with biometrics (FIDO Alliance, 2023). However, passkeys do not address costly enrollment and source verification problems (Yeoh et al., 2023).

The *federated model* mitigates these challenges. It limits the use of username-password logins, passkeys, and additional authentication factors to a small number of single sign-on (SSO) services by the likes of companies such as Alphabet, Apple, Meta, and Microsoft. The consistent authentication offered by the federated model makes it convenient for users. The federated model is also convenient for organizations, as they can outsource their responsibility for identity data management to SSO providers. However, ceding control over authentication to SSO providers can be problematic from a compliance and strategy perspective (Smith & McKeen, 2011). Source verification by SSO providers is also often limited, e.g., to phone numbers and driver's licenses. Moreover, cases abound in which SSO providers falsely blocked users and were slow to correct their mistakes (Hill, 2022). Lastly, SSO services are known for tracking user behavior on the web (Zuboff, 2015).

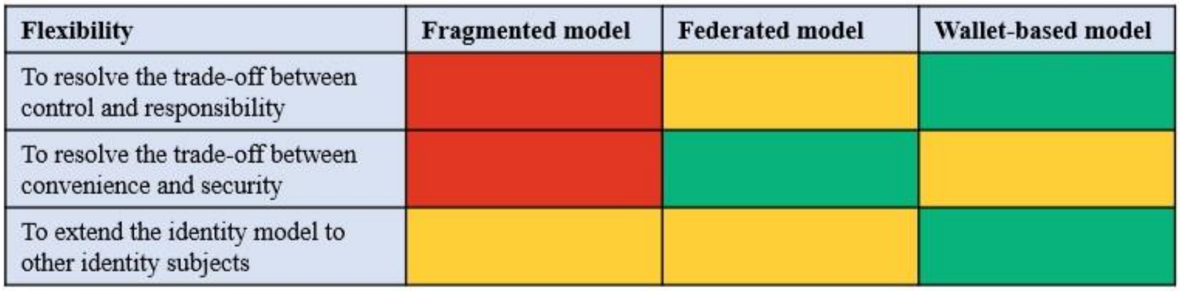
The *wallet-based model* is different in that it puts more control and responsibility for identity management on users. The European Union, along with several Canadian provinces and a few US states, is touting it as the future of identity management (Rieger et al., 2022; Sedlmeir et al., 2021). Under this model, users collect cryptographically verifiable identity attributes from trustworthy issuing organizations. The wallet-based model is convenient for users because digital wallets make passwords and multifactor authentication redundant (Lacity et al., 2023). It can also drastically reduce enrollment, source verification, and authentication costs. The downsides of the wallet-based model are that it is still immature and requires compatibility with identity wallets and solutions for device loss or theft. Moreover, organizations need to define policies for the trustworthiness and acceptance of identity attributes from different issuing organizations.

3 Three Recommendations for Organizational Policymakers

Identity management seems to be a rather mundane topic to some organizations, but it is a Rosetta Stone for solving many of the challenges organizations face in their processes today. We thus encourage organizational policymakers to take a strategic approach to identity management and carefully choose between the three different models. We next present three recommendations for making this choice.

Organizational policymakers should first consider the trade-off between control and responsibility. User and usage data can be highly relevant for some organizations, be it for the personalization of services, market segmentation, or the identification of opportunities for cross- and upselling. For these organizations, the costs associated with collecting and storing identity data may be well spent. If the organization is not using this data productively, outsourcing its protection to SSO providers may be wise. Yet, outsourcing identity management to SSO providers introduces strategic dependencies. Alternatively, they can ask their users to assume more responsibility. This can be helpful to reduce the organization's costs for secure storage of identity data and to support users across jurisdictions. However, controlling one's own identity data can be demanding for users. Increased user agency requires educated users (e.g., in terms of how to detect phishing attacks, how to create backups for recovery, etc.), and many users may not be skilled enough to manage their data or willing to tolerate high levels of responsibility.

Second, organizational policymakers should strike a balance between convenience and security. External SSO services may be convenient and more secure than most organizational services but do not always offer the required levels of source verification. For some organizations, the balance will need to be on the side of security. Compromised medical or financial processes, for instance, are not only embarrassing but can have serious consequences for affected users. For these processes, federated or wallet-based models may be the better choice. Where instances of incorrect identity data are inconsequential, policymakers should also consider whether identity data requires costly source verification.



Flexibility	Fragmented model	Federated model	Wallet-based model
To resolve the trade-off between control and responsibility	🟥	🟨	🟩
To resolve the trade-off between convenience and security	🟥	🟩	🟨
To extend the identity model to other identity subjects	🟨	🟨	🟩

Figure 1. Flexibility Associated with the Three Identity Models.

Finally, organizational policymakers should think beyond customer identities before selecting a model. Using the same model to manage identities and access for customers and employees, suppliers, partner organizations, and even IoT devices may substantially reduce complexity and costs (Glöckler et al., 2023; Guggenberger et al., 2023; Sedlmeir et al., 2023). In this regard, the wallet-based model may trump the other two models. Policymakers should also consider the political landscapes in which they operate. In certain industries and certain countries, regulators may mandate certain identity models. The European Union, for instance, will mandate the wallet-based model for customer identity management in various industries (Council of the European Union, 2024). Organizational policymakers should be aware of these mandates and consider adopting the same model for other users to streamline IT processes across the organization.

Figure 1 summarizes these recommendations and offers an indication of the ability of the three identity models to align with them. While the federated and wallet-based models may often provide more flexibility than the fragmented model, it is important to carefully consider their strategic implications. Ultimately, there is no "fire and forget" solution for identity management. Instead, identity management is a challenge that requires organizational policymakers to take stock of their organizations' needs and resources, carefully consider the available models, and adapt to changes in the identity market (Smith & McKeen, 2011). Organizations should regularly revisit their identity management policies to keep up with developments in the digital landscape, including security trends, regulatory changes, and technological advancements.

Acknowledgments

We are grateful to John L. King for his insightful feedback and guidance throughout the process and to the members of the policy posse for their helpful comments that strengthened the paper. This research was funded in part by the Luxembourg National Research Fund (FNR), grant reference 16326754, and PayPal, PEARL grant reference 13342933/Gilbert Fridgen. For the purpose of open access and in fulfillment of the obligations arising from the grant agreements, the authors have applied a Creative Commons Attribution 4.0 International (CC BY 4.0) license to any author-accepted manuscript version arising from this submission.

References

Benantar, M. (2005). *Access control systems: security, identity management and trust models* (2006 edition). Springer.

Council of the European Union. (2024). *European digital identity (eID)*. https://www.consilium.europa.eu/en/press/press-releases/2024/03/26/european-digital-identity-eid-council-adopts-legal-framework-on-a-secure-and-trustworthy-digital-wallet-for-all-europeans/

FIDO Alliance. (2023). *Passkeys (Passkey authentication).* https://fidoalliance.org/passkeys/

Glöckler, G., Sedlmeir, J., Frank, M., & Fridgen, G. (2023). A systematic review of identity and access management requirements in enterprises and potential contributions of self-sovereign identity. *Business & Information Systems Engineering*. https://doi.org/10.1007/s12599-023-00830-x

Guggenberger, T., Kühne, D., Schlatt, V., & Urbach, N. (2023). Designing a Cross-organizational Identity Management System: Utilizing SSI for the Certification of Retailer Attributes. *Electronic Markets*, *33*(1). https://doi.org/10.1007/s12525-023-00620-z

Hill, K. (2022). A dad took photos of his naked toddler for the doctor. Google flagged him as a criminal. *The New York Times.* https://www.nytimes.com/2022/08/21/technology/google-surveillance-toddler-photo.html

Lacity, M., Carmel, E., Young, A. G., & Roth, T. (2023). The quiet corner of Web3 that means business. *MIT Sloan Management Review*, *64*(3). https://sloanreview.mit.edu/article/the-quiet-corner-of-web3-that-means-business/

Livius, T. (1943). *Livy: History of Rome, VII, Books 26-27* (F. G. Moore, Trans., Reprint Edition). Harvard University Press.

Rieger, A., Roth, T., Sedlmeir, J., Weigl, L., & Fridgen, G. (2022). Not yet another digital identity. *Nature Human Behaviour*, *6*, Article 3.

Sedlmeir, J., Rieger, A., Roth, T., & Fridgen, G. (2023). Battling disinformation with cryptography. *Nature Machine Intelligence*, *5,* 1056-1057

Sedlmeir, J., Smethurst, R., Rieger, A., & Fridgen, G. (2021). Digital identities and verifiable credentials. *Business & Information Systems Engineering*, *63*(5), 603-613.

Sheldon, R. M. (2015). Hannibal as spy chief. Een Geschiedenis van Spionage En Inlichtingendiensten, *Leidschrift: Kennis Is Macht, 30*, 25–46.

Smith, H. A., & McKeen, J. (2011). The identity management challenge. *Communications of the Association for Information Systems*, *28*, 169-180.

Winder, D. (2023). Why you should stop using Lastpass after new hack method update. *Forbes.* https://www.forbes.com/sites/daveywinder/2023/03/03/why-you-should-stop-using-lastpass-after-new-hack-method-update/?sh=5b6d7db28fc9

Windley, P. J. (2023). *Learning digital identity: design, deploy, and manage identity architectures*. O'Reilly Media.

Yeoh, W.-Z., Kepkowski, M., Heide, G., Kaafar, D., & Hanzlik, L. (2023). Fast IDentity Online with Anonymous Credentials (FIDO-AC). *Proceedings of the 32nd USENIX Security Symposium*.

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, *30*(1), 75–89.

About the Authors

Alexander Rieger is an assistant professor of information systems at the Sam M. Walton College of Business at the University of Arkansas. His research focuses on innovation with emerging technologies in highly structured environments. His work has appeared in *Nature Human Behavior, Nature Machine Intelligence, Information & Organization, International Journal of Information Management*, and *MIS Quarterly Executive*. He has several years of experience working in industry and consulting for the European Commission as well as various public and private sector organizations in Germany and Luxembourg. He holds a master's degree and a PhD in information systems.

Tamara Roth is an assistant professor of information systems at the Sam M. Walton College of Business at the University of Arkansas. Her research explores how emerging technologies can be leveraged to promote social good and achieve positive organizational change. She combines theories and methods from neurobiology, psychology, social sciences, and management. Tamara's work has appeared in *MIT Sloan Management Review, International Journal of Information Management, Nature Human Behavior,* and *Nature Machine Intelligence.* She has an interdisciplinary education with master's degrees in biology and education, a PhD in educational psychology, and is currently finalizing her PhD in information systems.

Johannes Sedlmeir is a postdoctoral researcher at the Interdisciplinary Centre for Security, Reliability, and Trust (SnT), University of Luxembourg. In his research, he focuses on the effective use of emerging digital technologies in organizations by designing and evaluating innovative IT artifacts based on, e.g., distributed ledgers, digital identity attestations, and zero-knowledge proofs. His research has appeared in *Business & Information Systems Engineering, Electronic Markets, Information & Management,* and the *Journal of Network and Computer Applications*. He holds a master's degree in theoretical and mathematical physics and a PhD in information systems.

Gilbert Fridgen is a full professor and PayPal-FNR PEARL Chair in Digital Financial Services at the Interdisciplinary Centre for Security, Reliability, and Trust (SnT), University of Luxembourg, and coordinator of the National Centre of Excellence in Research on Financial Technologies. In his research, he analyses the transformative effects of digital technologies on individual organizations and on the relationship between organizations. He addresses especially emerging technologies like distributed ledgers, digital identities, machine learning, and the internet-of-things.

Amber Young is an associate professor of information systems at the Sam M. Walton College of Business at the University of Arkansas. Her research focuses on how information systems can promote social good and positive organizational outcomes. Amber serves as an associate editor for *MIS Quarterly*. Her research has appeared in *MIS Quarterly*, *Journal of Management Information Systems*, *Journal of the AIS*, *Information Systems Journal*, *Information & Organization*, *MIT Sloan Management Review, International Journal of Information Management, AIS Transactions on Replication Research*, and *Communications of the Association for Information Systems*.

RP5: Rieger, A., Roth, T., Sedlmeir, J., & Fridgen, G. (2022). **We Need a Broader Debate on the Sustainability of Blockchain.** *Joule*, *6(6),* 1137–1141. https://doi.org/10.1016/j.joule.2022.04.013
Journal Rating: 60.6 (CiteScore); 4.950 (SNIP)

CellPress

Commentary

We need a broader debate on the sustainability of blockchain

Alexander Rieger,[1,*] Tamara Roth,[1,2] Johannes Sedlmeir,[3,4] and Gilbert Fridgen[1]

Alexander Rieger is a postdoctoral researcher at the Interdisciplinary Centre for Security, Reliability and Trust (SnT) at the University of Luxembourg. His research interests include innovative digital technologies such as blockchain, decentralized digital identities, and artificial intelligence. Alex leads the scientific advisory team for the FLORA blockchain project of Germany's Federal Office for Migration and Refugees and acts as advisor to the European Blockchain Partnership and various public and private sector partners in Germany and Luxembourg.

Tamara Roth is a postdoctoral researcher at the Interdisciplinary Centre for Security, Reliability and Trust (SnT) at the University of Luxembourg. Her research interests include the interplay of innovative technologies such as blockchain and decentralized digital identities with sociocultural and socioethical constructs in public administration and healthcare. Moreover, she investigates technology adoption and implications of technologies for sustainable development from a psychological and neurobiological perspective.

Johannes Sedlmeir is a researcher on information systems at the FIM Research Center, University of Bayreuth. In his research, he focuses on the energy consumption and performance benchmarking of different blockchains, the application of cryptographic methods such as zero-knowledge proofs for scalable and privacy-oriented blockchain solutions in different sectors, and decentralized digital identities. He received his M.Sc. in theoretical and mathematical physics.

Gilbert Fridgen is professor and PayPal-FNR PEARL chair in digital financial services at the Interdisciplinary Centre for Security, Reliability and Trust (SnT) at the University of Luxembourg. In his research, he analyzes the transformative effects of digital technologies on individual organizations and on the relationship between organizations. He addresses potentially disruptive technologies like blockchain, decentralized digital identities, artificial intelligence, or the Internet of Things. His research involves information systems engineering and IT strategy and (risk) management, as well as regulatory compliance. In his projects and partnerships, he collaborates with partners in financial services, energy, mobility, manufacturing, and consulting, as well as with public bodies and governments.

Cryptocurrencies are often criticized not only for their enormous energy consumption and e-waste but also for their carbon emissions, impact on local air quality, and detrimental health effects for humans and animals.[1,2] Criticism ignites especially around the proof of work (PoW) consensus mechanism that, for instance, Bitcoin and Ethereum—the two largest cryptocurrencies by market capitalization—use to synchronize and secure their underlying blockchains. This criticism is empirically substantiated and justified, but it is often generalized to all blockchains.

As a result, blockchains have gained a negative reputation as environmental polluters even though non-PoW blockchains have comparatively low energy needs and carbon footprints. These blockchains warrant not only a more differentiated analysis but also a discussion about the environmental benefits of blockchain. In fact, there is reason to believe that non-PoW blockchains may enable applications that contribute to sustainability, for instance, by reducing wasteful practices in food supply chains,[3] container shipment,[4] and public services[5] or by facilitating more efficient carbon markets.[6]

In this commentary, we consequently argue for a broader debate on the sustainability of blockchain. We begin our argument with a discussion of the significant energy savings that can be realized for public blockchains by using proof of stake (PoS) instead of PoW. In the second part, we provide measurements for the energy consumption of prominent private blockchains to complement those for major PoW[1,2] and PoS[7] blockchains. We conclude with a discussion of blockchain applications that may well add to sustainability. Overall, we aim to provide a clearer picture of the energy needs of different blockchains and help to identify areas of application where blockchains can be a source of sustainability.

Energy-efficient public blockchains

The high energy demand of PoW blockchains is rooted in the basic challenge of blockchain networks: ensuring that the blockchain's distributed copies are updated truthfully and reliably. In public settings, the challenge is typically resolved by consensus mechanisms that financially reward network participants for the addition of a truthful new block. The reward can be a certain cryptocurrency balance or/and fees for the transactions included in this block. To guide the election of the network participant who can add the next block, these consensus mechanisms use scarce resources—that is, resources that are costly to replicate. Connecting the probability of being elected to a scarce resource helps public blockchain networks prevent Sybil attacks. With such attacks, adversaries could take control over the network's consensus process. For instance, when all participants in a blockchain network contributed to the consensus mechanism by submitting votes, an attacker could mount a Sybil attack by creating countless dummy participants that outvote honest participants.[8]

PoW blockchains are a special—and historically the first—type of public blockchains. As the scarce resource, they use computational power spent on solving cryptographic puzzles and, by extension, "mining" hardware and electric power. Submitting solutions to these puzzles, which are connected to batches of transactions, convinces the other nodes in the blockchain network that a participant has invested the corresponding scarce resource. To keep the number of transactions that a PoW blockchain can process stable, the difficulty of the puzzle automatically adjusts to the amount of computational power in the network. Rising prices of the cryptocurrency, in turn, encourage investments in more computational power, which drives up the puzzle's difficulty and leads to higher energy demand and carbon emissions.[1,2,8] This interdependence means that, for instance, in March 2022, Bitcoin has consumed as much electricity as countries like Poland or South Africa.[9] It also means that more energy-efficient hardware will not reduce the energy consumption of PoW blockchains in the long run.[8]

To avoid this effect, other cryptocurrency networks, like Polkadot and Solana—two of the largest PoS cryptocurrencies by market capitalization—use their cryptocurrency as the scarce resource. These PoS networks require that a certain amount of the cryptocurrency is "put at stake" to be elected to add the next block. In other words, they tie voting power to the amount of cryptocurrency a voter possesses instead of computational power and energy. For some PoS networks, ownership of the cryptocurrency is sufficient for a higher chance at being selected. For others, only locked cryptocurrency balances increase the odds. Locking ensures that the balance cannot be used for a certain time and turns it into a collateral that disincentivizes malicious behavior.

Consequently, the energy needs associated with consensus finding in PoS blockchains are many orders of magnitude smaller than in PoW blockchains. Recent measurements suggest that even the most energy-intensive PoS blockchains require less than 0.002% of the energy needs of Bitcoin, the most energy-intensive PoW blockchain.[7] In fact, the energy needs of PoS blockchains are comparable to conventional enterprise IT systems: that is, a payment with a PoS cryptocurrency has similar energy requirements as a payment with PayPal[10] or Visa.[11] It is true that these payment systems process significantly more transactions than common PoS blockchains, but their total energy consumption is significantly higher as well. So, when broken down to the transaction level, both types of systems are in fact comparable.

Besides significantly lower energy needs, research suggests that PoS can also provide a comparably high level of security as PoW blockchains,[12] at least after a phase of fair distribution. Consequently, Ethereum—the cryptocurrency with the currently second largest market capitalization—has decided to switch from PoW to PoS[13] and will likely complete this transition in summer 2022.

Low energy needs of private blockchains

In corporate and government blockchain networks, the number of nodes can be controlled. Moreover, the involved participants know the identities of other participants; that is, they can associate the public keys of the blockchain nodes with an organization or individual. In such "private" networks, identity can act as the scarce resource and enable consensus mechanisms that build on "one participant, one vote" or reputation-weighted voting. Like PoS, these "identity-based" consensus mechanisms do not require the competitive solving of cryptographic puzzles to resist Sybil attacks. Accordingly, they also have low electricity needs.

In Figure 1, we present measurement of these needs for a selection of popular private blockchains. Specifically, we selected blockchains that are both used extensively in industry and government projects and that have been subjected to performance analyses in the academic literature. For our measurements, we deployed these blockchains on Amazon Web Services, where each node ran on a separate virtual machine. We then measured the virtual machines' resource utilization for different throughput levels between 1 tx/s and the respective networks' maximum capacity. From these resource utilizations, we derived power consumption levels. Specifically, we first checked that there was a strong linear relation between transaction throughput and marginal power consumption levels; that is, we verified that energy consumption increased

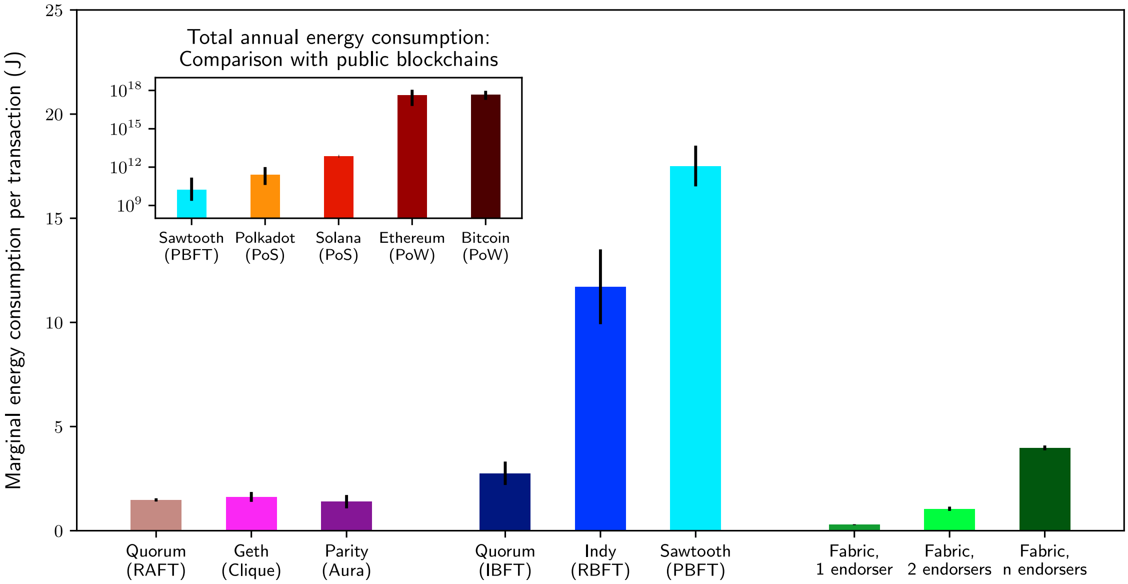


Figure 1. Marginal energy consumption per transaction for selected private blockchains (network size of 32 nodes)
The ''marginal energy per transaction'' values in the main panel exclude idle consumption; the corresponding error bars represent standard deviations across several measurements and throughput levels. We chose a network size of 32 nodes for the panel as this size is representative of many larger private networks, such as the European Blockchain Services Infrastructure.[5] See the supplemental information for details on the underlying calculations of the main panel. The small panel in the top-left corner offers a comparison against selected public blockchains on a ''total annual energy consumption'' basis. It applies a logarithmic scale. For the public PoS blockchains, we used measurements by the Crypto Carbon Ratings Institute for Polkadot and Solana.[7] Polkadot and Solana are the public PoS blockchains with the smallest and largest ''total annual energy consumption'' among the six public PoS blockchains with the highest market capitalization.[7] For the public PoW blockchains, we used Digiconomist values to calculate lower bounds and best guesses for Ethereum and Bitcoin,[9] as well as current cryptocurrency prices, transaction fees, and a lower bound of 0.05 USD per kWh of electricity for their upper bounds.[1,2] We illustrate these lower and upper bounds with the error bars in the small panel. Ethereum and Bitcoin are the public PoW blockchains with the highest market capitalization and energy consumption.

with the number of processed transactions. We then calculated the values presented in Figure 1 as the average over the different throughput levels. The error bars in the main panel represent the standard deviation over these averaged levels.

Figure 1 highlights that private blockchains, like public PoS blockchains, have low energy needs. These needs naturally increase with network size and tend to grow with the required level of resilience to failure and attack (Figure 2). Yet, total energy consumption remains low even for high transaction throughput because most private blockchain networks are comparatively small due to performance, data privacy, and data separation considerations. In essence, private blockchain networks are just a small collection of servers that host a shared database.

The interpretation of Figures 1 and 2 requires some caveats. The marginal energy consumption per transaction metric is useful for non-PoW blockchains in which transaction processing can represent a major share of the overall energy needs. However, it is not perfect, as ''idle'' consumption can also present a sizable share for these blockchains.[5] Moreover, it should not be used for PoW blockchains in which overall energy consumption is largely independent of the number and complexity of processed transactions; that is, a higher number and complexity of transactions, such as for the creation of non-fungible tokens (NFTs), would not increase the total power consumption of PoW blockchains in a meaningful way.[8] Slightly elevated energy needs are nevertheless possible due to increased cumulative transaction fees and a higher cryptocurrency price as a result of popularity gains.

Sustainability with blockchain

While the debate on energy consumption, e-waste, and other environmental and health impacts of blockchain is extensive,[1,2,7,8] potential benefits are often marginalized. This is surprising because companies and governments increasingly use blockchain applications that could contribute to sustainability. For instance, blockchain has gained traction for sustainable supply chain management, where its use can ensure increased efficiency and prevent unnecessary waste and surplus production. IBM FoodTrust is a prominent example.[3] IBM created FoodTrust in collaboration with major retailers such as Walmart and Unilever to enable extensive product monitoring across supply chains and to prevent fresh produce from being disposed of due to insufficient monitoring. This, in turn, can boost the sustainability of food supply chains. Other blockchain applications enable the digitalization of previously

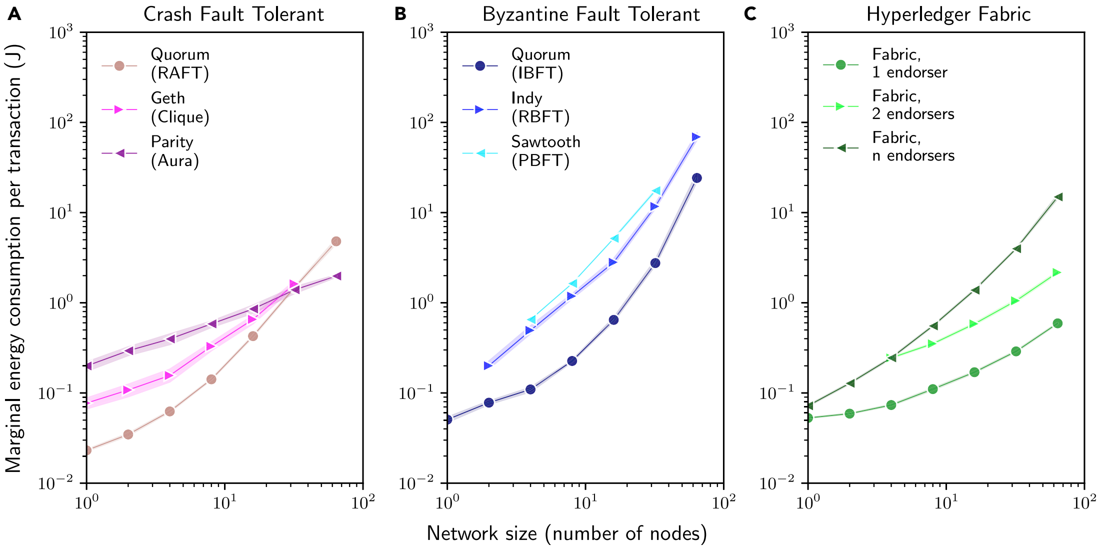


Figure 2. Scaling behavior of the marginal energy consumption per transaction for selected private blockchains

(A–C) Private blockchains have low energy needs—irrespective of their tolerance to faults and manipulations.

The consensus mechanisms in (A; crash fault tolerant) are resistant to a certain number of faulty nodes. The mechanisms in (B; Byzantine fault tolerant) can additionally cope with a certain number of malicious nodes. Hyperledger Fabric networks (C) are resistant to failure and certain attacks. The error regions represent standard deviations across three series of measurements.

See the supplemental information for more details on the consensus mechanisms and underlying calculations.

paper-based processes, such as TradeLens.[4] TradeLens was developed by IBM and Maersk, the world's largest container shipping company, to reduce paper- and often airmail-based data exchange in container shipment.

Even if we assume that these private blockchain applications were completely powered by coal (average 2020 US emission factor for coal: 1.01 kg or 2.23 pounds CO_2 eq per kWh[14]), this translates into a carbon footprint of 2.81×10^{-7} kg CO_2 eq for each joule. In comparison to the possible carbon savings, this value is marginal. For instance, it would be enough if one FoodTrust transaction helped to avoid the disposal of 1 gram of field vegetables (estimated carbon footprint of 3.30×10^{-4} kg CO_2 eq[15]) or if one TradeLens transaction shortens the voyage time of a container ship by 0.001 s (estimated 2018 carbon footprint of international shipping: 1.33 kg CO_2 eq per s[16]). Of course, these estimates are subject to some degree of uncertainty, and the total CO_2 footprint of private blockchains may be higher—for instance, due to the additional footprint of the underlying hardware. However, it is unlikely that more precise estimates will add the several orders of magnitude required to offset possible savings. In effect, there is growing indication that companies and governments can contribute to the sustainability of supply chains with blockchain, not despite blockchain.

Naturally, using blockchain for increased sustainability is not limited to supply chain management. Similar efforts to reduce inefficiencies in public administration are under way with the European Union's European Blockchain Services Infrastructure.[5] Blockchain technology is also frequently discussed as a key to more efficient carbon markets.[6] Overall, the use of blockchain technology could contribute to sustainability in areas where it can (1) make processes more efficient, (2) replace the paper-based exchange of sensitive information, or (3) reduce the use of fossil fuels or loss of produce and where the environmental costs of using blockchain do not exceed sustainability benefits.[3–5]

Conclusion

Given the broad range of blockchains beyond PoW, we argue for a more differentiated debate about the sustainability of blockchain technology. We particularly caution against blindly extending the critique of PoW to PoS and private blockchains, which both have low energy needs. Since some of them may even add to sustainability, we also see a need for a more balanced debate that goes beyond environmental costs and reflects on environmental benefits. This debate can build on ongoing efforts to identify areas of application in which blockchain could contribute to sustainability.[8] Moreover, it can add to a comprehensive overview of reference projects, their benefits and costs, and the consensus mechanisms used.

Standardization bodies could also make an important contribution to differentiation and balance with a carbon accounting framework for blockchain applications. With such a framework, companies could evaluate different blockchain designs and hosting options and establish the corresponding net carbon emissions. Moreover, such a framework would allow auditors to certify the sustainability of blockchain applications. A promising starting point can be established frameworks for corporate carbon accounting.

SUPPLEMENTAL INFORMATION

Supplemental information can be found online at https://doi.org/10.1016/j.joule.2022.04.013.

ACKNOWLEDGMENTS

A.R., T.R., and G.F. are supported by PayPal and the Luxembourg National Research Fund FNR (P17/IS/13342933/PayPal-FNR/Chair in DFS/Gilbert Fridgen). PayPal's financial support is administered via the FNR, and by contractual agreement, PayPal has no involvement in A.R., T.R., and G.F.'s research.

DECLARATION OF INTERESTS

The authors declare no competing interests.

1. Gallersdörfer, U., Klaaßen, L., and Stoll, C. (2020). Energy consumption of cryptocurrencies beyond Bitcoin. Joule *4*, 1843–1846. https://doi.org/10.1016/j.joule.2020.07.013.

2. de Vries, A., Gallersdörfer, U., Klaaßen, L., and Stoll, C. (2022). Revisiting Bitcoin's carbon footprint. Joule *6*, 498–502. https://doi.org/10.1016/j.joule.2022.02.005.

3. IBM Food Trust. https://www.ibm.com//blockchain/solutions/food-trust.

4. TradeLens. https://www.tradelens.com/.

5. European Blockchain Services Infrastructure. https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Home.

6. Sadawi, A.A., Madani, B., Saboor, S., Ndiaye, M., and Abu-Lebdeh, G. (2021). A comprehensive hierarchical blockchain system for carbon emission trading utilizing blockchain of things and smart contract. Technol. Forecast. Soc. Change *173*, 121124. https://doi.org/10.1016/j.techfore.2021.121124.

7. Gallersdörfer, U., Klaaßen, L., and Stoll, C. (2022). Energy efficiency and carbon footprint of proof of stake blockchain Protocols. Crypto Carbon Ratings Institute. https://www.carbon-ratings.com/dl/pos-report-2022.

8. Sedlmeir, J., Buhl, H.U., Fridgen, G., and Keller, R. (2020). The energy consumption of blockchain technology: Beyond myth. Business & Information Systems Engineering *62*, 599–608. https://doi.org/10.1007/s12599-020-00656-x.

9. Digiconomist Bitcoin energy consumption Index and Ethereum energy consumption Index. https://digiconomist.net/.

10. Paypal (2019). Global impact Report. https://www.paypalobjects.com/marketing/web/us/globalimpact/PayPal_2019_Global_Impact_Report_FINAL.pdf.

11. VISA (2019). Corporate Responsibility & Sustainability Report. https://usa.visa.com/dam/VCOM/download/corporate-responsibility/visa-2019-corporate-responsibility-report.pdf.

12. David, B., Gaži, P., Kiayias, A., and Russell, A. (2018). Ouroboros Praos: an adaptively-secure, semi-synchronous proof-of-stake blockchain. In Advances in Cryptology – EUROCRYPT 2018, J. Nielsen and V. Rijmen, eds. (Springer), pp. 66–98. https://doi.org/10.1007/978-3-319-78375-8_3.

13. Ethereum Beacon Chain. https://ethereum.org/en/eth2/beacon-chain/.

14. US Energy Information Administration (2021). How much carbon dioxide is produced per kilowatthour of U.S. electricity generation. https://www.eia.gov/tools/faqs/faq.php?id=74&t=11.

15. Petersson, T., Secondi, L., Magnani, A., Antonelli, M., Dembska, K., Valentini, R., Varotto, A., and Castaldi, S. (2021). A multilevel carbon and water footprint dataset of food commodities. Sci. Data *8*, 127. https://doi.org/10.1038/s41597-021-00909-8.

16. International Maritime Organization (2020). Fourth Greenhouse Gas Study. https://www.imo.org/en/OurWork/Environment/Pages/Fourth-IMO-Greenhouse-Gas-Study-2020.aspx.

[1]Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg, Luxembourg, Luxembourg

[2]University of Bayreuth, Bayreuth, Germany

[3]FIM Research Center, University of Bayreuth, Bayreuth, Germany

[4]Branch Business & Information Systems Engineering of Fraunhofer FIT, Bayreuth, Germany

*Correspondence: alexander.rieger@uni.lu

https://doi.org/10.1016/j.joule.2022.04.013

RP6: Sedlmeir, J., Huber, J., Barbereau, T. J., Weigl, L., & Roth, T. (2022). **Transition Pathways towards Design Principles of Self-Sovereign Identity.** *ICIS 2022 Proceedings*.
https://aisel.aisnet.org/icis2022/is_implement/is_implement/4
Conference Ranking: 2 (GGS Class); A- (GGS Rating)

Transition Pathways towards Design Principles of Self-Sovereign Identity

Completed Research Paper

Johannes Sedlmeir
FIM Research Center
Bayreuth, Germany
johannes.sedlmeir@fim-rc.de

Jasmin Huber
University of Bayreuth
Bayreuth, Germany
jasmin.huber@uni-bayreuth.de

Tom Barbereau
Linda Weigl
Tamara Roth
SnT, University of Luxembourg
Luxembourg, Luxembourg
{tom.barbereau, linda.weigl,
tamara.roth}@uni.lu

Abstract

Society's accelerating digital transformation during the COVID-19 pandemic highlighted clearly that the Internet lacks a secure, efficient, and privacy-oriented model for identity. Self-sovereign identity (SSI) aims to address core weaknesses of siloed and federated approaches to digital identity management from both users' and service providers' perspectives. SSI emerged as a niche concept in libertarian communities, and was initially strongly associated with blockchain technology. Later, when businesses and governments began to invest, it quickly evolved towards a mainstream concept. To investigate this evolution and its effects on SSI, we conduct design science research rooted in the theory of technological transition pathways. Our study identifies nine core design principles of SSI as deployed in relevant applications, and discusses associated competing political and socio-technical forces in this space. Our results shed light on SSI's key characteristics, its development pathway, and tensions in the transition between regimes of digital identity management.

Keywords: Certificate, digital wallet, distributed ledger, innovation, public key infrastructure, verifiable credential

Introduction

According to Kim Cameron, Microsoft's former Chief Architecture of Identity, "the Internet was built without a way to know who and what [people] are connecting to" (Cameron, 2005). It typically only allows the identification of physical endpoints and the associated organizations (Tobin and Reed, 2016). End-users experience this design daily when they interact with the servers of digital service providers using an https connection (Preukschat and Reed, 2021). Servers identify themselves with cryptographic key pairs and SSL certificates, i.e., documents that are electronically signed by one of a few dozen global "certificate authorities" (Soltani et al., 2021). The resulting public key infrastructure (PKI) can thus be considered the Internet's equivalent of a public "address book" or "telephone book" for public entities, maintained by a list of reputed organizations (Adams and Lloyd, 2003). Through its integration into web browsers and mobile applications, it provides the backbone of today's trusted interactions via the Internet (Jøsang, 2014).

Despite the apparent success of digital certificates, they are rarely extended to end-users. One of the few examples include the European Union's Digital COVID certificates (Rieger et al., 2021) and the introduction of staff passports for the United Kingdom's national health service during the pandemic (Lacity and Carmel, 2022). Instead, end-user identities are typically managed through *siloed* and *federated* systems (El Maliki and Seigneur, 2007). In the siloed approach, users need to register a new account for each digital service that they interact with. Oftentimes, these accounts are just a combination of an identifier, such as a username or an e-mail address, and a credential to prove control over the identifier, such as a password or a smart-card (Whitley et al., 2014). Registering or maintaining an account may also involve filling in registration forms and visiting a company branch or government office that verifies claims such as the possession of a valid driver's license (Sedlmeir et al., 2021). Resulting records can be verified by the digital service provider and stored on its servers, so simplifying future verification processes. However, manual registration and the secure management of passwords for sometimes hundreds of digital services presents a substantial challenge and inconvenience to end-users (Bonneau et al., 2012). Related challenges for companies and governments lie in maintaining security, supporting operations, and manually verifying users' attributes (Schlatt et al., 2021; Smith and McKeen, 2011).

To address these downsides, dedicated identity providers (IdPs) entered the market (Maler and Reed, 2008). Examples for IdPs are companies like Google and Microsoft and government agencies like the Unique Identification Authority of India (Sedlmeir et al., 2021). As in the siloed approach, IdPs store (and to some extent verify) their users' identity attributes. Additionally, they enable users to authenticate with other service providers that connect with the IdP using their IdP account. Technically, when logging in to a digital service, users are redirected to their IdP, where they sign in with their corresponding credential. The IdP then forwards an attestation of the required identity attributes to the service provider (Madsen et al., 2005; Maler and Reed, 2008). As the resulting network of IdPs and digital service providers resembles a federation, this identity paradigm is called federated identity management (Maler and Reed, 2008). While the "single sign-on" experience of the federated approach is efficient and convenient for users, it is often criticized for the centralized storage of identity data and corresponding cyber-security risks and surveillance risks. Moreover, IdPs often monetize their users' identity and usage data (van Bokkem et al., 2019; Zuboff, 2015), taking powerful market positions. Federated identity management also has not yet addressed the lack of machine-verifiable digital representations of core identity-related documents such as passports, driver's licenses, or diplomas (Sedlmeir et al., 2021).

The shortcomings of the siloed and federated approaches have led to growing interest in a *user-centric* and *decentralized* digital identity paradigm (El Maliki and Seigneur, 2007; Kubach et al., 2020; OECD, 2011). Attempts to implement this paradigm in the context of e-commerce and enterprise IT systems date back to the early 2000s (Backes et al., 2005; Chadwick et al., 2003). These endeavors have ultimately led to the concept of self-sovereign identity (SSI) – an expression of personal digital sovereignty. It emerged as a "technological niche" (Geels, 2004) among digital identity communities, most notably, the Internet Identity Workshops (IIWs), which previously played a major role in the development of federated identity standards (Preukschat and Reed, 2021). Subsequently, Allen (2016), who was a leading figure in incubating SSI, coined the term as a principle-based framework for a decentralized system of user-centric digital identities. His "10 principles of SSI" provide the first definition of SSI. At that time, there were no relevant reference standards or practical experiences with the large-scale deployment of SSI-based systems and their interaction with the regulatory, technical, and economic environment. Since then, through inter- and intra-organizational proofs of concept and pilot projects in businesses and public services, SSI has evolved considerably (Schellinger et al., 2022). Different technological components of SSI and various identification and authentication scenarios were explored (Sedlmeir et al., 2021; Soltani et al., 2021). However, the development of guidelines and design considerations for SSI system implementation or evaluation has stalled or, at best, evolved in heterogeneous directions based on no or weak scientific evidence. For instance, Allen's principles stem from a blog post and mainly focus on libertarian values like autonomy and privacy; yet, applications of SSI in industry and e-government also require specific authenticity and accountability guarantees (Kubach et al., 2020). Moreover, regulatory aspects like the different "levels of assurance" formulated in the European electronic Identification, Authentication and Trust Services (eIDAS) regulation impact practical SSI implementations (Schellinger et al., 2022; Schwalm et al., 2022). The continuous innovation and evolution process within the SSI community hence cannot be viewed merely from a techno-centric perspective. Indeed, the concepts of "sovereignty" and "decentralization" in the context of digital identity are contested (Sedlmeir et al., 2021) and subject to different interpretations according to actors' social and institutional context (Weigl et al., 2022). Consequently, SSI-solutions should be understood and analyzed as innovations with "political-economic dimensions" (Dijck and Jacobs, 2020).

Related research on SSI is scarce and has not captured this context thus far. As a result, "SSI is still only loosely defined" (Mühle et al., 2018) and there seems to be no updated definition of SSI that includes both practitioners' and researchers' perspectives. The academic debate on SSI is also fuzzy: while initially scholarship emphasized the role of blockchain as an essential technological building block (e.g., Koens and Meijer, 2018; Mühle et al., 2018), more recent research suggests a smaller role for blockchain (Schlatt et al., 2021). In the last years, there has been a noticeable trend towards, among others, a stronger focus on applications in regulated domains, user experience, privacy-oriented implementations, and the bundling of attestations (Feulner et al., 2022; Sartor et al., 2022; Schwalm et al., 2022; Soltani et al., 2021). Harmonized design principles (DPs) are required for research and practice, e.g., to evaluate identity management concepts and solutions consistently and not only from a techno-centric and deductive perspective (e.g., see Koens and Meijer (2018)). Considering the diversity of technical niche innovations, socio-technical developments, and the influence of an exogenous landscape which impacted the adoption of SSI, we believe that a rigorous and timely assessment of the key characteristics of SSI is required. We provide an updated model in the form of DPs for SSI that supplements the libertarian concept as introduced by Allen (2016) with influences of the technical environment as well as regulatory and business requirements in terms of accountability, authenticity, and trust structures.

To derive these principles, we use the multi-level perspective (MLP) by Geels and Schot (2007) as a theoretical lens to retrace the *transition pathway* of SSI from a technological niche towards a mainstream concept. Through this theoretical lens, we derive the DPs following a design science research (DSR) study (Hevner et al., 2004; Peffers et al., 2007). We introduce Geels and Schot's MLP and use it to give a first, informal overview of different SSI-related historical milestones and evolutions in identity management. They illustrate the complexity of technical foundations and paths involved, and highlight the need for multi-faceted research to formally structure and map these developments (Whitley et al., 2014). Next, we present our DSR, which involves a systematic literature review (SLR) to develop the initial version of DPs for SSI and four subsequent iterative refinement and evaluation cycles in which we interview 15 experts from academia and businesses on SSI. We then discuss the implications of the developed DPs for the area of SSI, especially in the context of Allen's principles. We also point to related tensions that we observed in SSI's transition from being principally a libertarian theoretical construct to a practical identity management paradigm. Finally, we summarize our findings and outline the need for further developments and research in the area of SSI.

Background

Digital identity management models can be viewed as socio-technical constructs undergoing a permanent process of innovation (Seltsikas and O'Keefe, 2010; Smith and McKeen, 2011; Whitley et al., 2014). Leaning on Science and Technology Studies (STS), questions pertaining to technology development build on theories of technological entrenchment and strategies to incubate or sustain novel technologies. The concept of entrenchment stems from the idea that "when change is easy, the need for it cannot be foreseen; [though] when the need for change is apparent, change has become expensive, difficult, and time-consuming" (Collingridge, 1980). That is, the convenience of an established solution, called the "entrenched" solution, makes change difficult to achieve as neither social nor economic or political drivers for change exist (Geels, 2002). Over the past 40 years, numerous researchers have analyzed this phenomenon in the context of technological innovations (e.g., Callon, 1986; Hughes, 1983). They assume innovation takes place in protected niches where technologists safely develop and improve their technology, which – over time – "stabilizes as the outcome of successive learning processes" to form new regimes (Geels, 2004).

The multi-level perspective (MLP) was introduced as part of STS and dissects the innovation process in terms of 'technological niches", the established "socio-technical regime", and the larger "exogenous landscape" (Geels, 2004). Respectively, the framework consists of three levels –- the micro, meso, and macro

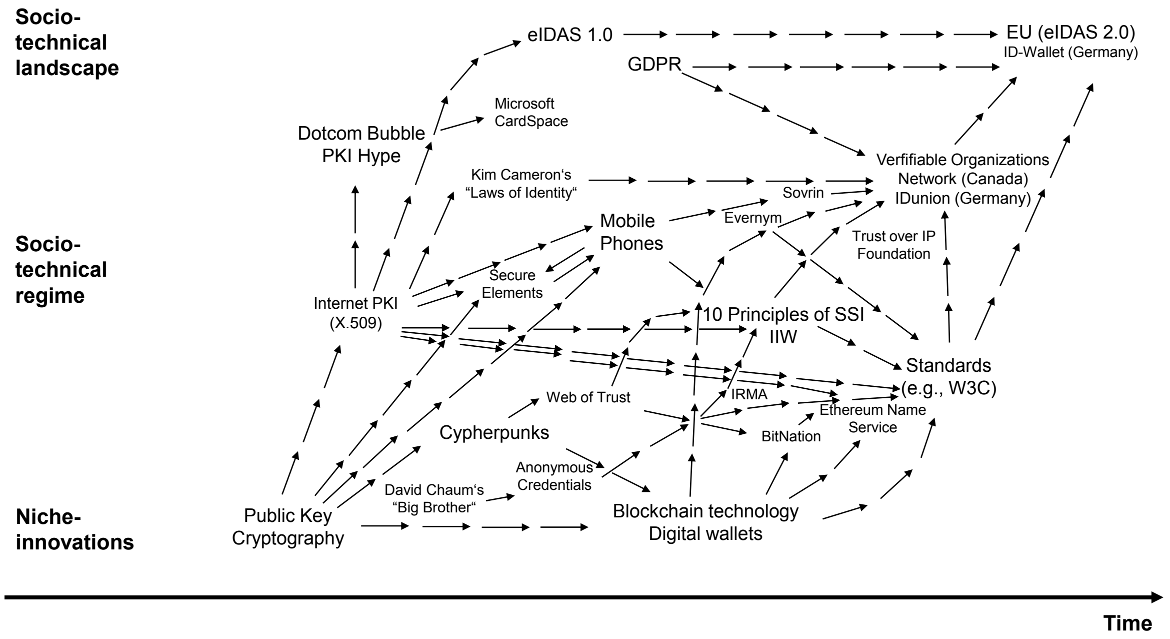


Figure 1. Multilevel perspective on selected key events and their interdependencies in identity management.

level – upon which different selection factors apply to drive innovation and shape technology development. Technological niches construct the framework's micro-level. At this level, radical novelties emerge, that is, innovations deviating considerably from the existing regime. Established regimes reside at the meso level and are often characterized by lock-in and path-dependent mechanisms of economic, social, organizational, or political nature (Geels, 2002). Lastly, the macro level contains the wider exogenous landscape in terms of the socio-political and economic conditions that may change and create "windows of opportunity" through which niche innovations can emerge (Geels, 2004; Geels and Schot, 2007). We aim to use the MLP as a theoretical lens to consolidate and contextualize the phenomenon of SSI-based identity management. Moreover, our work contributes to the stream of Information Systems research that explores technical opportunities and policy recommendations as well as more general managerial and societal questions associated with the development of identification technologies (Sedlmeir et al., 2021; Whitley et al., 2014). Prior to doing so, the development of SSI ought to be contextualized within past regimes. Hence, by adopting the MLP, Figure 1 structures the key events and their influences on the evolution of SSI that we present in the following.

Public key cryptography can be considered the most foundational part of both the existing trust layer on the Internet and implementations of SSI. While originally invented by Ellis and Cocks in 1973/74, the first publication by Rivest et al. (1978) resulted in an instantiation of the eponymous RSA cryptosystem. Public key cryptography uses one-way functions to derive a public key – typically a large number that can be considered a non-human-readable identifier – from a randomly generated secret key. The ownership of the key pair, i.e., knowledge of the secret key, can be proven mathematically without disclosing the secret key itself. The mathematical connection between the secret key as credential and the public key as identifier also opens up new opportunities for digital identity management beyond mere authentication. When it comes to presenting identity attributes for the purpose of identification or authorization, these can be verifiably claimed through digital certificates. That is, an "issuer" – either a reputed person or an organization known by its public key – uses its own secret key to electronically sign a document that lists the subject's public "binding" key along with its other identity attributes. An identity subject can then send this digital certificate and a proof of ownership of the binding key in a *verifiable presentation* directly to a relying ("verifying") party, for instance, to a service provider. The latter can cryptographically check the integrity of this digital certificate based on the issuer's digital signature. Provided that the verifying party trusts the issuer, it can then rely on the attested attributes. In the context of institutions and their digital services, this has evolved into today's system of X.509 certificates for servers and the Internet's PKI (Chadwick et al., 2003). Within the MLP, we understand PKI standards and related infrastructural components as a socio-technical regime that received significant adoption with the Dotcom bubble, became stable, and remained widespread through its crucial role for https-based communication.

"Cypherpunks" is the name given to libertarian and privacy-oriented communities that make use of cryptographic tools to pursue their goals (Narayanan, 2013). Some of these groups made early attempts to create a "Web of Trust" using cryptographic key pairs and digital certificates, issued by end-users for end-users (Zimmermann, 1995). An example of this is the implementation of "Pretty Good Privacy". In the early 2000s, attempts were made to base these efforts on institutional trust instead of social trust. A key goal was to improve digital identity management in areas such as e-commerce or enterprise IT by extending the Internet's PKI for organizations and their servers to use by individuals. They used, for instance, smartcards that securely store key pairs and certificates issued by the users' employers (Chadwick et al., 2003). While the vision to extend this user-centric and cryptography-oriented approach failed to gain large-scale traction, it prevailed for some time in niche communities. This mostly included computer scientists and cypherpunks who took seriously Chaum's warnings of surveillance threats on the Internet and corresponding spillover effects on society (Chaum, 1985, "Big Brother"). They explored cryptographic tools to minimize information exposure during a verifiable presentation. In cryptography research, this led to innovative solutions. In contrast to established digital certificates, anonymous credentials (also called attribute-based credentials) facilitate zero-knowledge proofs to provide data-minimal evidence on the ownership of a digital certificate and required attributes. That is, an anonymous credential allows to derive verifiable presentations without revealing all the attributes that it attests. It also allows to avoid the disclosure of an associated unique identifier, such as the binding public key or the value of the issuer's digital signature (Backes et al., 2005; Camenisch and Lysyanskaya, 2001). IRMA ("I Reveal My Attributes") was one of the first practical implementations of these anonymous credentials (Alpár and Jacobs, 2013). Besides privacy, niche innovations also emerged in communities of cryptographers and cypherpunks who sought to minimize the involvement of trusted third parties like certificate authorities. After Bitcoin and blockchain technologies gained a broader foothold, actors driven by libertarian values saw opportunities to establish a registry for digital identities by mapping individuals to their public keys on a transnational digital infrastructure. This rekindled interest in using public key cryptography for end-users' identity management resulted in projects like BitNation (Kuperberg, 2019). In addition, the popularity of tools to manage cryptocurrencies made citizens and decision-makers in industry and politics aware of the opportunities of identity management via digital wallets applications on smartphones (Jørgensen and Beck, 2022; Sartor et al., 2022).

The term SSI was coined by Allen (2016) in a blog post. His "principles of SSI" encompass users' independent *existence* (1); the *control* (2) they must have over their identities; the *access* (3) users are granted to their own data; the *transparency* (4) of related systems and algorithms' implementation; the *persistence* (5) of identities for as long as users wish; the *portability* (6) of attestations tied to users' identities; *interoperability* (7); *consent*-based (8) sharing of users' identity data; privacy through disclosure *minimalization* (9); and, finally, users' rights *protection* (10). The concept has since become a focal topic far beyond the relatively narrow focus of the half-yearly IIW conferences (Čučko and Turkanović, 2021; Soltani et al., 2021). While gathering "internal momentum" (Geels and Schot, 2007), the principles stipulated within this group soon became reference points for SSI solutions. In parallel, the first blockchain-based implementations of SSI appeared, such as Evernym's solution based on what later became Hyperledger Indy and Aries. Their efforts significantly influenced technical and non-technical standards, which were refined from a governance perspective, for instance, by Sovrin and the Trust over IP foundation and from a technical perspective by the World Wide Web Consortium (W3C) and the Decentralized Identity Foundation. Arguably, the two most important standards in the context of SSI are "decentralized identifiers" – public keys enriched with meta-data – and "verifiable credentials" – digitally signed attestations that offer higher flexibility with regard to semantics and that enable them to incorporate meta-data and features of anonymous credentials (Sedlmeir et al., 2021). Within these smaller regimes, respective socio-technical configurations for SSI were established.

The configurations in individual regimes, however, are not homogeneous. Instead, they can be considered "sequences of multiple component-innovations" (Geels and Schot, 2007) that are continuously reconfigured and converge into a solution. The heterogeneity in configurations manifests itself, for instance, in the contested use of blockchain as a component. The realization that pseudonymous public keys do not provide sufficient privacy (Sedlmeir et al., 2022), and that the immutability of a blockchain is not required for digital attestations signed by an issuer (Schlatt et al., 2021), diminished the role of blockchain in more recent SSI implementations. In many projects, end-users' identifiers, endpoints, and attestations are now exclusively stored in digital wallets on their devices. A blockchain then at most hosts the PKI for public institutions as well as revocation registries (Lacity, 2022; Schlatt et al., 2021). This can be seen, for instance, in Canada's Verifiable Organizations Network, the European cooperative society IDunion, and the European Self-Sovereign Identity Framework's technical approaches. SSI projects are often tied to dynamics in the socio-technical landscape. Ongoing political initiatives, like the revision of the European eIDAS regulation and the desire to establish a German ID Wallet, manifest the attention SSI has obtained from the regulatory domain. The development of SSI for identity management hence reflects the interplay of the MLP's different levels and the corresponding technical, socio-economical, and political selection factors. SSI is often hailed as a revolutionary innovation, yet its implementations are not considerably different from early proposals of using PKI and anonymous credentials stored on end users' portable computing devices (Backes et al., 2005; Chadwick et al., 2003). Arguably, public key cryptography alone contributes significantly to more secure and efficient identity management (Bonneau et al., 2012). Blockchain technology, which is still a component of many instantiations of SSI, only plays a minor role from a technical perspective (Schlatt et al., 2021). Yet, it appears to have contributed to its initial broad-based hype, as previous moderate attempts to lobby for the adoption of public key cryptography and digital certificates by end-users in research (e.g., Rannenberg et al., 2015) and policy (e.g., eIDAS) have not received the anticipated widespread adoption (Kubach et al., 2020). This mirrors Geels (2004)'s proposition that despite technical superiority over the incumbent technical solution, other factors beyond the technological regime influence successful adoption of a new regime. Since SSI connected with blockchain technology, there has been somewhat unprecedented support from political decision makers (Weigl et al., 2022).

Research Approach

For our DSR approach, we first identified the problem space to obtain descriptive knowledge on SSI solutions that researchers currently discuss through an initial SLR (Gregor and Hevner, 2013; vom Brocke et al., 2020). We then gathered qualitative data from the SLR and subsequent 15 expert interviews (Sonnenberg and vom Brocke, 2012). During data collection, we challenged, validated, and refined our tentative results against current practices and discussion in IT development and industry in iterative rephrase-and-evaluate loops (Gregor and Hevner, 2013; Hevner et al., 2004; Peffers et al., 2007). In this process, the MLP allowed us to contextualize our findings from the SLR on the various characteristics of SSI and the trajectories of its technical constituents. To integrate existent design knowledge into our endeavor to create additional, generalizable design knowledge (vom Brocke et al., 2020), we focused on the present solution space of SSI. More specifically, we reviewed and consolidated existing DPs from literature and SSI projects in a DSR study to derive DPs for SSI as a form of decentralized digital identity management. As related developments are driven by both theory and practice (Allen, 2016; Camenisch and Lysyanskaya, 2001; Preukschat and Reed, 2021; Whitley et al., 2014), DSR allowed us to consolidate observations from either perspective. A first set of DPs typically builds on Ω-knowledge or descriptive knowledge, which conveys an understanding of the laws and regularities of an observed phenomenon. Subsequent evaluation and sense-making processes then help derive a finite set of DPs, commonly referred to as Λ-knowledge or prescriptive knowledge (Gregor and Hevner, 2013; vom Brocke et al., 2020). According to the knowledge contribution framework, our DSR approach follows the precept of *exaptation*. Exaptation requires the extension of a known solution to new problems (Gregor and Hevner, 2013). Digital identity management is a well-known research topic (Smith and McKeen, 2011; Whitley et al., 2014) and often makes use of cryptographic components. Yet, the challenges we identified in the Introduction section have necessitated a paradigm shift. Current design knowledge, however, is often too unspecific and applications too versatile to derive generally accepted DPs for SSI (Preukschat and Reed, 2021). To address this problem, we consolidate existing and extend current design knowledge in generalizable and actionable DPs (Gregor and Hevner, 2013).

In line with Webster and Watson (2002) and Fink (2005), we extracted 2,504 publications from 14 databases, including ACM DL, IEEE Xplore, ScienceDirect, Scopus, Springer Link, Web of science, and Google scholar for our SLR. We started with two initial search strings, "self-sovereign identity" and "self-sovereignty", to get an overview of current research on SSI. We used the initial results to extract additional relevant keywords that had not yet been included in our search string. Owing to the close connection between blockchain and SSI communities as discussed in the Background section, our final search string then comprised keywords from the identity and blockchain realm: "self-sovereign identity" OR self-sovereignty OR (identity AND (blockchain OR decentrali*ed)). The term "decentralized", as influenced by Kuperberg (2019), seems an essential characteristic of SSI and inextricably linked to the concept, also through its strong link to blockchain communities (Weigl et al., 2022). In a title screening, we identified 84 publications as potentially being relevant. After a detailed full-text analysis of these contributions and applying inclusion (detailed discussion or use of design or evaluation criteria for SSI systems) and exclusion criteria (no English language, article not accessible, purely cryptographic content), 14 publications remained. A subsequent forward and backward search (Fink, 2005; Webster and Watson, 2002) yielded another 8 publications, seven of which are gray literature, technical standards (e.g., by the W3C), or laws (the EU's General Data Protection Regulation (GDPR)). Yet, two of the most popular contributions on SSI (Allen (2016) and Cameron (2005)) could not be extracted with our SLR, as they represent blog posts that are typically not listed in academic databases. We included these two contributions in our knowledge base since they contain essential definitions of SSI and discussions about key requirements.

Our approach towards DPs for SSI-based digital identity management follows the two modes of "kernel theory to design entity grounding" and "design entity to design theory grounding" to enrich the current knowledge base (vom Brocke et al., 2020). The evaluation of various approaches to implement SSI based on our SLR in combination with information retrieved from the basket of literature and projects on identity management referenced in the Introduction and Background sections helped us to derive design requirements. These served as solution fitness criteria for the challenges of digital identity management from the perspective of end-users, businesses, and regulators. Evaluations of existing approaches additionally delivered design features that we included in the development of a first set of DPs (Gregor and Hevner, 2013; vom Brocke et al., 2020). To increase their projectability, we evaluated and complemented them in four iterative evaluation cycles. The outcome was a nascent design theory in the form of a consolidated set of DPs (Hevner et al., 2004; Peffers et al., 2007; vom Brocke et al., 2020). Throughout this iterative process, we followed the suggested procedure of Hevner et al. (2004) to refine the DPs in 15 evaluation interviews with six researchers and nine industry experts, who are all highly esteemed in the field of SSI design and implementation. The practitioners represent relevant organizations and projects from niche innovations and the socio-technical regime (some have multiple of the following roles): Five interviewees have been regular attendees and presenters at last years' IIWs, and eight of them are actively involved in SSI-related standardization bodies like Sovrin, the Trust over IP foundation, and the W3C. Two interviewees are among the four editors of the W3C decentralized identifiers standard, which is also co-authored by Christopher Allen. Five interviewees are in leading positions for the implementation of the Verifiable Organizations Network or the IDunion project within their company, and four of them represent businesses that develop cloud and edge SSI wallets in Europe and North America. Moreover, we communicated our findings beyond exchanging ideas in the expert interviews as recommended for the DSR (Hevner et al., 2004). This included presentations of our work at the IIW, where it served as a discussion basis for the Principles of SSI, which were later – including adjustments – published by the Sovrin Foundation (2021). This work also considerably influenced a related compilation by the Trust over IP Foundation (2021). The aim of the interviews was to ensure the parsimony of our DPs for the creation of SSI-based solutions. To achieve parsimony, we controlled for the completeness, usefulness, and understandability of our DPs throughout the interviews. Interviewees were each encouraged to review the entire list of DPs and to provide (1) additions to the list, (2) reframing of existing DPs, and (3) changes to the definition of DPs. We also discussed openly the current state of decentralized digital identity management as well as the technical and social foundations, opportunities, and challenges of these approaches as perceived by the interviewees. The semi-structured interviews hence allowed the interviewees to elaborate on their professional perspective of SSI. We conducted each interview remotely. The interviews lasted between 30 and 60 minutes and were audio-recorded and transcribed afterwards. We refrained from scheduling new interviews once we reached a point where the interviewees provided us with almost identical feedback and did not suggest any further additions (Myers and Newman, 2007). For both the coding of selected literature and the interviews, we performed a two-stage process of inductive and deductive coding, as recommended by Miles et al. (2018). That is, two authors first separately analyzed the data, assigning codes to identify factors relevant to the design of SSI applications. They then abstracted these codes into higher-level concepts, i.e., our first tentative DPs from literature (deductive coding) and their refinement during the analysis of the interviews (inductive coding). After the literature coding and every fifth interview, the independent authors compared and discussed their results where diverging (Miles et al., 2018).

We connected the DPs with our kernel theory, the MLP, by discussing them against the backdrop of SSI's trajectory through the socio-political landscape and its interaction with legacy systems. This should ensure the relevance of our DPs (Hevner et al., 2004; Peffers et al., 2018) and, moreover, demonstrate that SSI as a form of decentralized digital identity management has developed from a radical niche to an acknowledged design (Geels, 2004; Geels and Schot, 2007) in private- and public-sector applications (Schlatt et al., 2021; Soltani et al., 2021). That is, our nascent design theory can be categorized as a design relevant explanatory or predictive theory. Our DPs enrich theories that have been relevant to initial design choices (Kuechler and Vaishnavi, 2012) such as those defined by Allen (2016). Our discussion of the resulting DPs through the lens of MLP additionally epitomizes the ascendance of technologies into broad-based adoption and provides an outlook for how SSI could further develop (Geels, 2004; Geels and Schot, 2007).

Findings

In the SLR coding process, we focused on identifying design requirements and design features for SSI management systems. While both design requirements and design features are often broad, they provide the basis for the formulation of DPs (Hevner et al., 2004; vom Brocke et al., 2020). Some requirements within the literature are already formulated as DPs (e.g., Allen (2016) and Tobin and Reed (2016)) but – dependent on their definition and relative position in the history of SSI development – may only cover a fraction of what may be relevant to date. We clustered these design requirements and features into a first set of nine DPs. In the following evaluation rounds, we added and removed one DP and adapted the remaining DPs until we reached a point where three subsequent interviews did not propose any meaningful changes. We first present the tentative DPs compiled on the basis of the SLR, and subsequently describe the changes implemented during the refinement cycles.

From Design Requirements and Features to Tentative Design Principles

DP1: Human Replicate. To account for the target group of SSI-based digital identities, the design requirements "human integration" (Cameron, 2005) and "human requirements [in the form of] privacy [and] empowerment" (Goodell and Aste, 2019) as well as the design feature "biometric interfaces" (Koens and Meijer, 2018) show a clear focus of SSI on natural persons, who seek to play a more active role in the management of their identity-related data. The features "reliable credential management" (Grüner et al., 2019), "data ownership", "data control", "consent to data processing" (Ferdous et al., 2019), and "portability of data" (Tobin and Reed, 2016) further emphasize the purpose of SSI as a collection of attributes related to a natural person. These can be kept for a person's entire life and, upon display, be used to disclose identity attributes. Thus, SSI enables increased agency and independence for natural persons, who wish to manage access to and distribution of their personal data. An identity considered as "self-sovereign" hence needs to be understood as collection of attributes of a real existing human being, but only of the parts they are willing to show – also called partial identities (Clauß and Köhntopp, 2001). Moreover, Abdullah et al. (2019) emphasize the concept of guardianship to give all individuals equal access to using an SSI.

DP2: Control. The design requirement of "deciding on the displayed information" (Ferdous et al., 2019) grants users of SSI "data control" (e.g., Alsayed Kassem et al., 2019; Whitley, 2009; Windley, 2019). How and when their data is being used warrants their explicit "consent to data processing" (Allen, 2016; Alsayed Kassem et al., 2019; Cameron, 2005; Ferdous et al., 2019). Controlling hence limits "what personal data is made available to others" (Whitley, 2009). This also includes the design feature of "updateability" and "revocability of consent" (Moe and Thwe, 2019) and is directly linked to the proposed identity life cycle of Koens and Meijer (2018), which contains the design features "create, attest, show, prove, renew, delete, and revoke". As such, SSI involves not only consent and control when sharing identity-related information but also "availability", i.e., the identity subject's ability to access and share verifiable information anywhere and at any time (Ferdous et al., 2019). Yet, in the context of verifiability, this does not mean that users should be able to modify all their identity information according to their liking.

DP3: Flexibility. To share their data anywhere and at any time, user-centric applications of SSI need to consider the design features "standardization" and "interoperability" (Allen, 2016; Ferdous et al., 2019; Tobin and Reed, 2016) among the different digital identity management solutions. The feature "pluralism of operators and technologies" (Cameron, 2005) should not hamper the feature "integration" (Kuperberg, 2019) of the various approaches to fulfill the design requirement of a "consistent experience across contexts" (Cameron, 2005). This also includes the design feature "portability of data" (Abraham, 2017; Allen, 2016; Ferdous et al., 2019; Tobin and Reed, 2016) in the form of identity attributes and corresponding attestations to other providers. That is, users should be able to decide which implementation to build upon – including a choice of their digital wallet. They should be empowered to consider their needs, independent of providers, and should be guaranteed interoperability with underlying technical and semantic standards.

DP4: Security. Aside from interoperability and standards, SSI-based solutions must also guarantee for the design requirement "confidentiality" which – besides availability and integrity – constitutes security. It not only entails the design features of "protection" from data accumulation, data fraud, and more powerful entities (Allen, 2016; Tobin and Reed, 2016) but also the limitation of storage and use of information for non-specified purposes as demanded by the GDPR. Overall, users should be protected from unwittingly or mistakenly sharing information with third parties, thus providing "end-to-end security" (Cavoukian, 2009). This includes also purely bilateral communication, end-to-end encryption (Goodell and Aste, 2019), and the verification of the involved verifying party's identity in a verifiable presentation to avoid man-in-the-middle attacks (Toth and Anderson-Priddy, 2019).

DP5: Privacy. Closely related to security is user privacy. In the context of SSI, it generally refers to the minimal disclosure of information, which provides users control over the degree of anonymity in interactions based on the support for unique pairwise pseudonyms for each individual private connection. Relevant design requirements and design features either directly demand "privacy by design and by default" (Cavoukian, 2009) and a high level of "pseudonymity" via pairwise unique digital identities and public keys as well as "private agents" with no storage of private data on the underlying ledger (Alsayed Kassem et al., 2019; Moe and Thwe, 2019; Windley, 2019). This allows to ensure the "unobservability" and "unlikability" (Moe and Thwe, 2019) of user information, if required. Moreover, "selective disclosure" serves as a design feature to reveal only the identity attributes relevant for a specific interaction and purpose (Cameron, 2005; Ferdous et al., 2019; Windley, 2019). Anonymous credentials (Soltani et al., 2018) and zero-knowledge proofs (Stokkink and Pouwelse, 2018; van Bokkem et al., 2019) are often mentioned as technical backbone for such enhanced privacy design features.

DP6: Credibility. Despite the goal of privacy protection, information should be authentic and verifiable also regarding timeliness. This includes the opportunity to revoke attestations from the side of the user in the case of loss or theft of the digital wallet, or or from issuers' side to account for changes of attributes and authorizations (Mühle et al., 2018). One way of implementing these design features without the need to interact with the issuer in a verifiable presentation is through the support for expiration dates and the use of revocation registries (Mühle et al., 2018). Credibility also reflects the design requirements of "transparency" (Abraham, 2017; Allen, 2016; Tobin and Reed, 2016) as well as the design features of "disclosure" (Ferdous et al., 2019), "identity assurance" and "identity verification" (Toth and Anderson-Priddy, 2019).

DP7: Authenticity. Only the respective subject should be able to pass on their data to requesting third parties. Pseudonym or credential sharing among different users, or the creation of new credentials by combining ones that do not belong to a single individual, should not be possible. Such systems exhibit "consistency of credentials", which can, for instance, be achieved through biometric interfaces and hardware-bound link secrets or be disincentivized by corresponding PKI-assured economic bonds or all-or-nothing non-transferability (Camenisch and Lysyanskaya, 2001; Hardman, 2019). If transactions break general laws or credentials are used in an unauthorized way, global or local anonymity revocation may be useful (Camenisch and Lysyanskaya, 2001; Koens and Meijer, 2018).

DP8: Usability and Performance. Aside from verification and authentication mechanisms as the very core of SSI-based solutions, general concepts of usability must be considered to fulfil the design requirement of "user empowerment" (Abraham, 2017; Alsayed Kassem et al., 2019; Goodell and Aste, 2019). A related requirement, "positive end-user experience" (Kuperberg et al., 2019), plays a major role in delivering other requirements, such as "user trust" – which is essential for acceptance (Seltsikas and O'Keefe, 2010) – and "self-sovereign digital identity management" (Yan et al., 2017). While the "positive end-user experience" mainly complements the design feature of "user-friendly interfaces", it may also concern features such as "scalability" (Koens and Meijer, 2018), "minimum downtime", and "efficient performance" (Camenisch and Lysyanskaya, 2001; Kuperberg et al., 2019). Thus, SSI-based digital identity management approaches require intuitive and easy access personal data, as well as the streamlined and quick sharing of information.

DP9: Future orientation. In addition, the success of SSI largely depends on how well it fits the surrounding environment (Kuperberg et al., 2019). To enable such a fit, there are a number of economic design requirements, including the "prevention of monopolization" as well as "empowerment of businesses" (Goodell and Aste, 2019) and "manageable costs" (Ferdous et al., 2019). These requirements rely heavily on design requirements such as "efficient protocols" (Camenisch and Lysyanskaya, 2001), "organizational flexibility" and "local storage" (Abraham, 2017) as well as design features such as "decentralized governance" (Ferdous et al., 2019; Windley, 2019). Thus, we conclude that SSI-based digital identity management approaches need an innovative environment that allows structural changes to implement SSI, including adaptations of governance and agile management.

Design Iterations

From the first to the second design iteration, we removed the specification of "Human" before the first tentative principle Human Replicate (TDP1). We did this because according to Expert 2 (Practitioner), smart devices and organizations can also use an SSI. Regarding Control (TDP2; DP2), Experts 1 (Researcher) and 2(P) detected potential tensions between increased control (i.e., user empowerment) and an undesirable amount of responsibility that "people now are not used to having". Open-source licensing agreements and legal compliance may be additional determining factors of Flexibility (TDP3; DP3). This was also closely linked to criticism on Credibility (TDP6) and Authenticity (TDP7), which would currently neglect the "rules of trust and basically Web of Trust, where you have to make sure the data coming from the issuer is credible" (Expert 2(P)). Experts 1(R) and 2(P) generally regarded "performance [to be] a subtopic of usability" (TDP8) and both as non-functional requirements instead of a DP, so we adjusted our TDP8 on Usability and Performance accordingly. Regarding Future orientation (TDP9), Expert 2(P) missed "bridging the gap between self-sovereign identity and the existing world of authentication and authorization" to create functional SSI.

From the second to the third design iteration, Security (TDP4; DP5) and Privacy (TDP5; DP5) were highlighted as particularly relevant (Experts 4(P), 6(R)), while the adjusted Usability (TDP8) still appeared to be deficient, neglecting other "important usability factors", such as "ease of use" and literacy, as well as the simplicity of information access. Expert 4(P) considered Future orientation (TDP9) as important, yet more of a requirement than a principle. It would indirectly already be represented in several other DPs, such as Control (TDP2) and Flexibility (TDP3). For Credibility (TDP6), the focus on revocability of consent was too narrow ("revoke the credential if it is a fake passport or whatever"), which is why we took the more general term "revocability" to also account for revocation due to incorrect data. Moreover, we renamed the previously iterated TDP1 Replicate to Representation (DP1), as the term Replicate may be uncommon and difficult to understand.

From the third to the fourth design iteration, we eliminated Future orientation (TDP9). This is because the experts considered an environment with both innovative and legacy features to be more a basic requirement than a DP specific for the implementation of SSI. As the interviewees considered the term of DP1 to be a subset of the principle alongside authentication – "because it is everything, like identification, authentication, and that you exist" (Expert 6(R)) – we renamed and redefined the DP. Regarding Flexibility

Principle	Description (Key features)
DP1: Representation	SSI can represent any entity digitally – human, legal, or technical. (Attributes, authentication, existence, identification, partial identities, persistence)
DP2: Control	Only the actual controller has decision-making power over their digital identity. (Access, manage, ownership, right to be forgotten, single source of truth, update)
DP3: Flexibility	No vendor lock-in: low switching costs, focus on interoperable standards, and open-source projects. (Documentation, integration, no monopoly, portability, standards, transparency)
DP4: Security	State-of-the-art cryptographic tools and authenticated, end-to-end encrypted interactions. (Identification of relying party, key management, protection, secure communication, tamper-proofness)
DP5: Privacy	In each interaction, only the data that is essential for its purpose is revealed. (Bilateral by default, consent, minimized correlation, need to know, selective disclosure)
DP6: Verifiability	The validity and timeliness of credentials can be checked efficiently. (Certificate chain, credential management, machine readability, provability, revocability)
DP7: Authenticity	Credentials are bonded to their initial bearers. (Binding, consistency of credentials, identity fraud protection, limited transferability, risk-based authentication)
DP8: Reliability	There is guidance that helps verifiers to decide which issuers they can trust in a highly dependable infrastructure. (Decentralization, governance, guidance, no single point of failure, public registration, scalability, Web of Trust)
DP9: Usability	Success and durability factors. (Efficiency, end-user experience, minimum downtime, multiple access points, performance, recovery, simplicity, support)

Table 1. Final design principles and their definitions, including key features for implementation.

(TDP3), Experts 5(P) and 11(P) suggested renaming it "openness". We refrained from doing so as it would neglect other essential properties of the principle such as interoperability and portability. In accordance with interview feedback, which offered criticism that it was "too specific" and did not include "more general points" (Expert 9(R)), we redefined Privacy (TDP5). Experts 2(P), 5(P), and 6(R) also suggested redefining Credibility (DP6), as they considered it to be too focused on technological building blocks that yet have to be established. We refrained from adding "decentralization" as a separate DP as it is a basic "prerequisite of the infrastructure" (Expert 5(P)) but added it to Future orientation (TDP9). Moreover, we renamed Credibility (TDP6) to Verifiability (DP6) and redefined Authenticity (DP7).

During the fourth design iteration – which yielded the final and consolidated set of DPs – we received positive feedback from our Experts 13(P), 14(R), and 15(R). In accordance with their feedback, we summarized the current definitions within the most relevant and generalizable core statement and exchanged the order of Usability (TDP8) and Reliability (TDP9) to Usability (DP9) and Reliability (DP8) in line with their perceived importance. Table 1 features the final DPs, including a subset of terms often used in related work and by the interviewees. The DPs characterize SSI as a user-centric "identification infrastructure" (Whitley et al., 2014) based on cryptographically verifiable attestations not only for organizations and their servers but also for end-users, maintained and controlled in digital wallets on their mobile devices (Sedlmeir et al., 2021; Soltani et al., 2021).

Discussion

The derivation of DPs delivered theoretical insights into how to develop design knowledge from such broad-based technological innovations using DSR. At first glance, our derived DPs are similar to the "Ten Principles of SSI" by Allen (2016). When Allen conceived these, SSI was mainly a theoretical concept and a formulation of key characteristics of an identity management that neither had a foundation for technical implementation, nor a history of real-world use. Yet, our SLR has revealed other seminal papers that propose practical design and evaluation criteria for SSI implementations that may be more actionable. Our interviews with practitioners, who work on the adoption of SSI in the public and private sector, allowed us to incorporate their experiences into our assessment.

Using the lens provided by the MLP, a key insight from our iterative DSR evaluation was that different types of regimes apply selection criteria at different velocities. Instead of continuously stabilizing the outcome of successive learning processes to turn innovation into a new regime, the policy regime forced a breakthrough in the implementation of SSI by taking advantage of a perceived "window of opportunity" (Geels, 2004; Geels and Schot, 2007). In the meantime, both the socio-cultural regime and technological regime are still at the stage of negotiation, not yet having produced a dominant design (Sedlmeir et al., 2021; Weigl et al., 2022). This was reflected in our interviews, where several interviewees emphasized that their recommendation on how to best implement SSI-based digital identity management solutions relies on their learning from ongoing IT-projects. Specifically, this involved integration into legacy identity and access management solutions and regulatory constraints. Knowing that SSI is still in a trial phase, and that its long-term success is dependent on negotiation with selection factors of the incumbent socio-technical regime, the interviewees appreciated the overall structure of our nine DPs. Yet, they also indicated that the definitions may require adaption over time as this space becomes increasingly mature.

Our study thus contributes to various levels of the current research discussions. Theoretically, it presents a novel way of combining a constructivist theoretical lens from STS with the design science paradigm. Thereby, it adds to the epistemological diversity in the Information Systems field. As a result, our study does not only address the gap of a missing theory or framework on identity management, it also introduces a new theoretical perspective of kernel theory development. It does this through critical reflection about the materiality and non-materiality of the observed construct, thus bypassing the positivist and techno-centric presumptions that often form the basis of DSR (McKay and Marshall, 2005; Niehaves, 2007). Practical implications, on the other hand, can be drawn from the iterative refinement of our DPs with the interview partners. They provide a common denominator for research on SSI and the development and evaluation of corresponding identity management systems in practice. The final DPs also allow us to identify several tensions that may be relevant for both researchers and practitioners. These tensions not only pertain to the novelty of SSI but also to the selection environment created by the incumbent regime and the larger exogenous socio-technical landscape of the MLP (Geels, 2004; Geels and Schot, 2007). The tensions also reflect and align with the findings of Weigl et al. (2022), who studied the interpretive flexibility of SSI. Hence, we believe that these tensions represent promising research directions.

Firstly, we observed a tension between selection factors of the policy regime and the socio-cultural regime. The establishment of Data Privacy (DP5) and User Control (DP2) in SSI-based digital identity management solutions may compromise its Applicability (DP6, DP7): For example, aspects such as the theft or sharing of mobile devices were often not sufficiently considered by the originators of this concept. These originators tended to be libertarians and cryptographers whose focus was often on ensuring control and in particular minimal disclosure and anonymity. The result was a lack of unique identifiers for processes that organizations need to consider in practical applications (Allen, 2016; Camenisch and Lysyanskaya, 2001; Cameron, 2005). To mitigate the risk of identity-related fraud with stolen mobile devices or credentials, Tobin (2017) and Koens and Meijer (2018) suggest revocation and escrow mechanisms if credentials are used in an unlawful way or if they contradict the user-specific consistency of credentials (Camenisch and Lysyanskaya, 2001). To retain a high level of privacy, zero-knowledge proofs enable minimum disclosure while compliant with regulation that requires the verification and authentication of a certain amount of user data (Sedlmeir et al., 2021). Yet, the tools currently available for zero-knowledge proofs are difficult to integrate into existing secure elements that facilitate hardware-binding (Schellinger et al., 2022). This currently still leads to a trade-off between privacy and authenticity that – despite the availability of technical solutions (Delignat-Lavaud et al., 2016; Rosenberg et al., 2022) – has not yet been resolved in practical implementations.

A second tension arises from the conflicting selection forces of the policy regime and the socio-cultural regime. The challenge pertains to the requirement to balance Verifiability (DP6) and Reliability (DP8) against end-user expectations like Control (DP2) and Privacy (DP5). This tension has its roots in the libertarian ideals of minimal disclosure, anonymity support, and full control of users over displayed data – ideals that are commonly associated with SSI (Allen, 2016; Preukschat and Reed, 2021; Weigl et al., 2022). While a milder version of these ideals forms the core of SSI, the verifiable credentials stored in the users' wallets require a trustworthy issuer and a proof of this originator. Trust registries and qualified electronic signatures, as, for instance, implemented in the context of eIDAS, may mediate this tension in the practical implementation of SSI (Schwalm et al., 2022). Should an organization issue an incorrect attestation – whether intentionally or not – the option for revocation must be available (Interviewee 10). It should also be possible to remove an unreliable issuer from certain trust registries. As a result, abandoning information silos is only practical in the cross-domain sense: While issuers are no more involved in verifiable presentations, they still need to store some of the attestation-related information to facilitate potential future revocation.

A third tension emerges from selection factors of the socio-cultural and the technological regimes. This tension pertains to the balance between the desire for maximum flexibility and the functional requirements of Interoperability (DP3). With an initially strong focus on libertarian values (Allen, 2016), the conceptual version of SSI emphasized a high degree of freedom and personalization of the technological application for users (Preukschat and Reed, 2021). This, however, makes interoperability between solutions cumbersome and impairs the desired flexibility to choose a solution that fits individual needs. Consequently, one currently "cannot copy credentials from wallet to wallet [...] and if you want to switch your identity to a different network, that requires reissuing the credentials on the other network" (Interviewee 10). A more "mainstream" version of SSI, thus, would have to mediate between flexibility and interoperability by enforcing some degree of standardization, yet without hampering the portability of digital wallets that hold the cryptographic keys and credentials to avoid vendor lock-in (Allen, 2016; Ferdous et al., 2019; Koens and Meijer, 2018; Yan et al., 2017).

Our DSR study contextualizes the current development and discusses factors that helped develop SSI as a new regime of identity management from a broad, transnational perspective. Yet, we cannot guarantee that we incorporated all relevant events and practical implementations of SSI in this study. We aimed to ensure a comprehensive perspective via using broad search strings, many databases, and forward and backwards searches in our SLR. During the interviews that guided the refinement of DPs, we made inquiries about other interviewees or projects that may be of relevance. Nevertheless, it should be noted that, with the exception of one Asian researcher, all our interview partners were European and North American. Moreover, the interviews were distributed only over 6 months. A more longitudinal study that rigorously analyzes discussions from events (such as the latest IIWs) or amendments in regulatory documents) may be required to consolidate the chronology of changes. Our DPs form a snapshot of the current design knowledge on SSI and a perspective on its pathway through regimes of identity management. Yet, they may be subject to change, not least, from advances in knowledge gained from successful or failed applications of SSI. We will seek better retracing of the selection factors of each regime by conducting further interviews with experts in the respective regimes. In addition, to grasp the considerations of the socio-cultural regime and that of end-users, future research may add a survey-based evaluation.

Conclusion

Our study retraces the historical development of SSI using the MLP as a theoretical lens. Our SLR in combination with DSR delivered a set of nine DPs that consolidate existing design knowledge of the SSI concept. We refined and extended this consolidated knowledge in four iterations with 15 experts from industry and academia. We used the MLP as a frame to help us to better understand the development of the concept of SSI. It was originally introduced mainly by a radical niche, but is now widely taken into account by states and industy consortia. Use currently seems focused in North America and Europe, including the eIDAS 2.0 regulation designed for large-scale productive use. Our work may help to better understand SSI in the context of business and regulated domains and to communicate its key characteristics and technical building blocks to decision makers and end-users. We also discovered tensions between the different negotiating regimes and suggested ways to mediate these. In this context, we elaborated on the difficulties that different velocities of regime negotiation could have on the prudent use of windows of opportunity. The relevance of our research comes from the close interaction with stakeholders who take part in projects in the SSI ecosystem. Aside from direct experience, our research also draws on observations from crucial requirements and real-life failures, as illustrated, for instance, by the German government's digital driver's license. While the knowledge gained from this, and changes to the concept may initially seem to considerably impair SSI's key goal of giving users more control, it also contributed to establishing an open ecosystem of verifiable digital interaction. We learned that if SSI aims to embrace digital identity management in practice, updates to its core principles are indispensable. By establishing consensus on an updated model of SSI that is integrated in regulatory and institutional requirements, our findings also suggest that a perception of SSI as a concept driven by anti-democratic forces owing to its name may be a minor issue (Sedlmeir et al., 2021). Consequently, our contribution indicates that research that consolidates historical influences on SSI may help to mediate tensions and contribute to achieving a feasible identity management solution beyond authentication (Bonneau et al., 2012). Our DPs also aim to provide a common basis for future research on design choices and trends within decentralized digital identity systems. Based on such a common understanding, researchers may tackle some of the remaining open questions concerning the design of SSI-based solutions. This involves, among others, further studying user experience requirements and corresponding success factors (Sartor et al., 2022), investigating the necessity of improved anonymous credential implementations with extended privacy capabilities (Rosenberg et al., 2022), and studying the fitness of technical tools like blockchain for decentralized governance, enhanced availability, or social recovery (Benchaya Gans et al., 2022).

References

Abdullah, A., Breeijen, S. d., Cooper, K., Corning, M., Coutts, O., Cranston, R., Dahl, H., Hardman, D., Hickman, N., and Neubauer, N. (2019). *On Guardianship in Self-Sovereign Identity.*

Abraham, A. (2017). *Whitepaper About the Concept of Self-Sovereign Identity Including its Potential.*

Adams, C. and Lloyd, S. (2003). *Understanding PKI: Concepts, Standards, and Deployment Considerations,* Addison-Wesley Professional.

Allen, C. (2016). *The Path to Self-Sovereign Identity.*

Alpár, G. and Jacobs, B. (2013). "Towards Practical Attribute-Based Identity Management: The IRMA Trajectory," in *IFIP Working Conference on Policies and Research in Identity Management,* Springer.

Alsayed Kassem, J., Sayeed, S., Marco-Gisbert, H., Pervez, Z., and Dahal, K. (2019). "DNS-IdM: A Blockchain Identity Management System to Secure Personal Data Sharing in a Network," *Applied Sciences* (9:15).

Backes, M., Camenisch, J., and Sommer, D. (2005). "Anonymous yet Accountable Access Control," in *Proceedings of the ACM Workshop on Privacy in the Electronic Society,* pp. 40–46.

Benchaya Gans, R., Ubacht, J., and Janssen, M. (2022). "Governance and Societal Impact of Blockchain-Based Self-Sovereign Identities," *Policy and Society* (41:3), pp. 402–413.

Bonneau, J., Herley, C., Van Oorschot, P. C., and Stajano, F. (2012). "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes," in *Symposium on Security and Privacy,* IEEE, pp. 553–567.

Callon, M. (1986). "The Sociology of an Actor-Network: The Case of the Electric Vehicle," in *Mapping the Dynamics of Science and Technology,* M. Callon, J. Law, and A. Rip (eds.). Palgrave, pp. 19–34.

Camenisch, J. and Lysyanskaya, A. (2001). "An Efficient System for Non-Transferable Anonymous Credentials with Optional Anonymity Revocation," in *International Conference on the Theory and Applications of Cryptographic Techniques,* Springer, pp. 93–118.

Cameron, K. (2005). *The Laws of Identity.* Microsoft.

Cavoukian, A. (2009). *Privacy by Design... Take the Challenge,* Information and Privacy Commissioner.

Chadwick, D., Otenko, A., and Ball, E. (2003). "Role-Based Access Control with X.509 Attribute Certificates," *IEEE Internet Computing* (7:2), pp. 62–69.

Chaum, D. (1985). "Security without Identification: Transaction Systems to Make Big Brother Obsolete," *Communications of the ACM* (28:10), pp. 1030–1044.

Clauß, S. and Köhntopp, M. (2001). "Identity Management and its Support of Multilateral Security," *Computer Networks* (37:2), pp. 205–219.

Collingridge, D. (1980). *The Social Control of Technology,* Open University Press.

Čučko, Š. and Turkanović, M. (2021). "Decentralized and Self-Sovereign Identity: Systematic Mapping Study," *IEEE Access* (9), pp. 139009–139027.

Delignat-Lavaud, A., Fournet, C., Kohlweiss, M., and Parno, B. (2016). "Cinderella: Turning Shabby X.509 Certificates into Elegant Anonymous Credentials with the Magic of Verifiable Computation," in *Symposium on Security and Privacy,* IEEE, pp. 235–254.

Dijck, J. van and Jacobs, B. (2020). "Electronic Identity Services as Sociotechnical and Political-Economic Constructs," *New Media & Society* (22:5), pp. 896–914.

El Maliki, T. and Seigneur, J.-M. (2007). "A Survey of User-Centric Identity Management Technologies," in *International Conference on Emerging Security Information, Systems, and Technologies,* IEEE, pp. 12–17.

Ferdous, M. S., Chowdhury, F., and Alassafi, M. O. (2019). "In Search of Self-Sovereign Identity Leveraging Blockchain Technology," *IEEE Access* (7), pp. 103059–103079.

Feulner, S., Sedlmeir, J., Schlatt, V., and Urbach, N. (2022). "Exploring the Use of Self-Sovereign Identity for Event Ticketing Systems," *Electronic Markets.*

Fink, A. (2005). *Conducting Research Literature Reviews: From the Internet to Paper,* SAGE.

Geels, F. W. (2002). "Technological Transitions as Evolutionary Reconfiguration Processes: A Multi-Level Perspective and a Case-Study," *Research Policy* (31:8-9), pp. 1257–1274.

Geels, F. W. (2004). "From Sectoral Systems of Innovation to Socio-Technical Systems," *Research Policy* (33:6–7), pp. 897–920.

Geels, F. W. and Schot, J. (2007). "Typology of Sociotechnical Transition Pathways," *Research Policy* (36:3), pp. 399–417.

Goodell, G. and Aste, T. (2019). "A Decentralized Digital Identity Architecture," *Frontiers in Blockchain* (2).

Gregor, S. and Hevner, A. R. (2013). "Positioning and Presenting Design Science Research for Maximum Impact," *MIS Quarterly* (37:2), pp. 337–355.

Grüner, A., Mühle, A., Gayvoronskaya, T., and Meinel, C. (2019). "A Comparative Analysis of Trust Requirements in Decentralized Identity Management," in *International Conference on Advanced Information Networking and Applications,* Springer, pp. 200–213.

Hardman, D. (2019). *What If Someone Steals My Phone?* Available at: https://sovrin.org/wp-content/uploads/2019/03/What-if-someone-steals-my-phone-110319.pdf [Accessed: September 29, 2022].

Hevner, A. R., March, S. T., Park, J., and Ram, S. (2004). "Design Science in Information Systems Research," *MIS Quarterly* (28:1), pp. 75–105.

Hughes, T. P. (1983). *Networks of Power: Electrification in Western Society, 1880-1930,* John Hopkins University Press.

Jørgensen, K. P. and Beck, R. (2022). "Universal Wallets," *Business & Information Systems Engineering* (64), pp. 115–125.

Jøsang, A. (2014). "Identity Management and Trusted Interaction in Internet and Mobile Computing," *IET Information Security* (8:2), pp. 67–79.

Koens, T. and Meijer, S. (2018). *Matching Identity Management Solutions to Self-Sovereign Identity Principles.*

Kubach, M., Schunck, C. H., Sellung, R., and Roßnagel, H. (2020). "Self-Sovereign and Decentralized Identity as the Future of Identity Management?," in *Open Identity Summit 2020,* Gesellschaft für Informatik eV, pp. 35–47.

Kuechler, W. and Vaishnavi, V. (2012). "A Framework for Theory Development in Design Science Research: Multiple Perspectives," *Journal of the Association for Information Systems* (13:6), pp. 395–423.

Kuperberg, M. (2019). "Blockchain-Based Identity Management: A Survey From the Enterprise and Ecosystem Perspective," *IEEE Transactions on Engineering Management* (63:4), pp. 1008–1027.

Kuperberg, M., Kemper, S., and Durak, C. (2019). "Blockchain Usage for Government-Issued Electronic IDs: A Survey," in *International Conference on Advanced Information Systems Engineering,* Springer, pp. 155–167.

Lacity, M. and Carmel, E. (2022). *Implementing Self-Sovereign Identity (SSI) for a Digital Staff Passport at UK NHS.*

Lacity, M. C. (2022). "Blockchain: From Bitcoin to the Internet of Value and Beyond," *Journal of Information Technology*.

Madsen, P., Koga, Y., and Takahashi, K. (2005). "Federated Identity Management for Protecting Users from ID Theft," in *Proceedings of the 2005 Workshop on Digital Identity Management,* pp. 77–83.

Maler, E. and Reed, D. (2008). "The Venn of Identity: Options and Issues in Federated Identity Management," *IEEE Security & Privacy* (6:2), pp. 16–23.

McKay, J. and Marshall, P. (2005). "A Review of Design Science in Information Systems," in *Proceedings of the 16th Australasian Conference on Information Systems,* AIS.

Miles, M. B., Huberman, A. M., and Saldaña, J. (2018). *Qualitative Data Analysis: A Methods Sourcebook,* 4th ed. SAGE.

Moe, K. S. and Thwe, M. (2019). "Investigation of Blockchain Based Identity System for Privacy Preserving University Identity Management System," *International Journal of Trend in Scientific Research and Development* (3:6), pp. 336–341.

Mühle, A., Grüner, A., Gayvoronskaya, T., and Meinel, C. (2018). "A Survey on Essential Components of a Self-Sovereign identity," *Computer Science Review* (30), pp. 80–86.

Myers, M. D. and Newman, M. (2007). "The Qualitative Interview in IS Research: Examining the Craft," *Information and Organization* (17:1), pp. 2–26.

Narayanan, A. (2013). "What Happened to the Crypto Dream?, Part 1," *IEEE Security & Privacy* (11:2), pp. 75–76.

Niehaves, B. (2007). "On Epistemological Diversity in Design Science: New Vistas for a Design-Oriented IS Research?," in *Proceedings of the 28th International Conference on Information Systems,* AIS.

OECD (2011). *Digital Identity Management: Enabling Innovation and Trust in the Internet Economy*.

Peffers, K., Tuunanen, T., and Niehaves, B. (2018). "Design Science Research Genres: Introduction to the Special Issue on Exemplars and Criteria for Applicable Design Science Research," *European Journal of Information Systems* (27:2), pp. 129–139.

Peffers, K., Tuunanen, T., Rothenberger, M. A., and Chatterjee, S. (2007). "A Design Science Research Methodology for Information Systems Research," *Journal of Management Information Systems* (24:3), pp. 45–77.

Preukschat, A. and Reed, D. (2021). *Decentralized Digital Identity and Verifiable Credentials: Self-Sovereign Identity,* Manning.

Rannenberg, K., Camenisch, J., and Sabouri, A. (2015). "Attribute-Based Credentials for Trust," *Identity in the Information Society, Springer*.

Rieger, A., Roth, T., Sedlmeir, J., and Fridgen, G. (2021). "The Privacy Challenge in the Race for Digital Vaccination Certificates," *Med* (2:6), pp. 633–634.

Rivest, R. L., Shamir, A., and Adleman, L. (1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM* (21:2), pp. 120–126.

Rosenberg, M., White, J., Garman, C., and Miers, I. (2022). *zk-creds: Flexible Anonymous Credentials from zkSNARKs and Existing Identity Infrastructure*.

Sartor, S., Sedlmeir, J., Rieger, A., and Roth, T. (2022). "Love at First Sight? A User Experience Study of Self-Sovereign Identity Wallets," in *Proceedings of the 30th European Conference on Information Systems,* AIS.

Schellinger, B., Sedlmeir, J., Willburger, L., Strüker, J., and Urbach, N. (2022). *Mythbusting Self-Sovereign Identity (SSI): Discussion Paper on User-Centric Identities*.

Schlatt, V., Sedlmeir, J., Feulner, S., and Urbach, N. (2021). "Designing a Framework for Digital KYC Processes Built on Blockchain-Based Self-Sovereign Identity," *Information & Management*, p. 103553.

Schwalm, S., Albrecht, D., and Alamillo, I. (2022). "eIDAS 2.0: Challenges, Perspectives and Proposals to Avoid Contradictions between eIDAS 2.0 and SSI," in *Open Identity Summit 2022,* Gesellschaft für Informatik eV, pp. 63–74.

Sedlmeir, J., Lautenschlager, J., Fridgen, G., and Urbach, N. (2022). "The Transparency Challenge of Blockchain in Organizations," *Electronic Markets*.

Sedlmeir, J., Smethurst, R., Rieger, A., and Fridgen, G. (2021). "Digital Identities and Verifiable Credentials," *Business & Information Systems Engineering* (63:5), pp. 603–613.

Seltsikas, P. and O'Keefe, R. M. (2010). "Expectations and Outcomes in Electronic Identity Management: The Role of Trust and Public Value," *European Journal of Information Systems* (19:1), pp. 93–103.

Smith, H. A. and McKeen, J. D. (2011). “The Identity Management Challenge,” *Communications of the Association for Information Systems* (28:1), pp. 169–180.

Soltani, R., Nguyen, U. T., and An, A. (2018). “A New Approach to Client Onboarding Using Self-Sovereign Identity and Distributed Ledger,” in *IEEE International Conference on Internet of Things and IEEE Green Computing and Communications and IEEE Cyber, Physical and Social Computing and IEEE Smart Data,* IEEE, pp. 1129–1136.

Soltani, R., Nguyen, U. T., and An, A. (2021). “A Survey of Self-Sovereign Identity Ecosystem,” *Security and Communication Networks*.

Sonnenberg, C. and vom Brocke, J. (2012). “Evaluations in the Science of the Artificial – Reconsidering the Build-Evaluate Pattern in Design Science Research,” in *International Conference on Design Science Research in Information Systems,* Springer, pp. 381–397.

Sovrin Foundation (2021). *Principles of SSI V2*.

Stokkink, Q. and Pouwelse, J. (2018). “Deployment of a Blockchain-Based Self-Sovereign Identity,” in *International Conference on Internet of Things and Green Computing and Communications and Cyber, Physical and Social Computing and Smart Data,* IEEE, pp. 1336–1342.

Tobin, A. (2017). *Sovrin: What Goes on the Ledger?*

Tobin, A. and Reed, D. (2016). *The Inevitable Rise of Self-Sovereign Identity*. The Sovrin Foundation.

Toth, K. C. and Anderson-Priddy, A. (2019). “Self-Sovereign Digital Identity: A Paradigm Shift for Identity,” *IEEE Security & Privacy* (17:3), pp. 17–27.

Trust over IP Foundation (2021). *Principles of SSI*.

van Bokkem, D., Hageman, R., Koning, G., Nguyen, L., and Zarin, N. (2019). *Self-Sovereign Identity Solutions: The Necessity of Blockchain Technology*.

vom Brocke, J., Winter, R., Hevner, A., and Maedche, A. (2020). “Special Issue Editorial – Accumulation and Evolution of Design Knowledge in Design Science Research: A Journey through Time and Space,” *Journal of the Association for Information Systems* (21:3), pp. 520–544.

Webster, J. and Watson, R. T. (2002). “Analyzing the Past to Prepare for the Future: Writing a Literature Review,” *MIS Quarterly* (26:2), pp. 13–26.

Weigl, L., Barbereau, T. J., Rieger, A., and Fridgen, G. (2022). “The Social Construction of Self-Sovereign Identity: An Extended Model of Interpretive Flexibility,” in *Proceedings of the 55th Hawaii International Conference on System Sciences,* pp. 2543–2552.

Whitley, E. A. (2009). “Informational Privacy, Consent and the “Control” of Personal Data,” *Information Security Technical Report* (14:3), pp. 154–159.

Whitley, E. A., Gal, U., and Kjaergaard, A. (2014). “Who Do You Think You Are? A Review of the Complex Interplay between Information Systems, Identification and Identity,” *European Journal of Information Systems* (23:1), pp. 17–35.

Windley, P. J. (2019). “Multisource Digital Identity,” *IEEE Internet Computing* (23:5), pp. 8–17.

Yan, Z., Gan, G., and Riad, K. (2017). “BC-PDS: Protecting Privacy and Self-Sovereignty through BlockChains for OpenPDS,” in *Symposium on Service-Oriented System Engineering,* IEEE, pp. 138–144.

Zimmermann, P. R. (1995). *The Official PGP User’s Guide,* MIT Press.

Zuboff, S. (2015). “Big Other: Surveillance Capitalism and the Prospects of an Information Civilization,” *Journal of Information Technology* (30:1), pp. 75–89.

Acknowledgements

We thank our interview partners for their time and dedication and their valuable insights. Further, we want to express our gratitude to Alexander Rieger and the anonymous reviewers for their constructive feedback. This work was supported by PayPal and the Luxembourg National Research Fund FNR (P17/IS/13342933/PayPal-FNR/Chair in DFS/Gilbert Fridgen). Moreover, we would like to acknowledge the support of the European Union (EU) within its Horizon 2020 programme, project MDOT (Medical Device Obligations Taskforce), Grant agreement 814654.

RP7: Hoess, A., Rieger, A., Roth, T., Fridgen, G., & Young, A. (2023). **Managing Fashionable Organizing Visions: Evidence from the European Blockchain Services Infrastructure.** *ECIS 2023 Proceedings*. https://aisel.aisnet.org/ecis2023_rp/337

Conference Ranking: 3 (GGS Class); B (GGS Rating)

MANAGING FASHIONABLE ORGANIZING VISIONS: EVIDENCE FROM THE EUROPEAN BLOCKCHAIN SERVICES INFRASTRUCTURE

Research Paper

Alexandra Hoess, SnT, University of Luxembourg, Luxembourg, alexandra.hoess@uni.lu.

Alexander Rieger, SnT, University of Luxembourg, Luxembourg, alexander.rieger@uni.lu.

Tamara Roth, SnT, University of Luxembourg, Luxembourg, tamara.roth@uni.lu.

Gilbert Fridgen, SnT, University of Luxembourg, Luxembourg, gilbert.fridgen@uni.lu.

Amber Grace Young, Sam M. Walton College of Business, University of Arkansas, United States, ayoung@walton.uark.edu

Abstract

Grand visions for organizational transformation increasingly build on fashionable information technologies. Organizational leaders may be tempted to adopt these visions due the high degree of legitimacy and mobilization they afford. However, their fashionable nature makes adoption risky. In this paper, we explore how organizations can manage this risk and successfully navigate the adoption of fashionable organizing visions. Specifically, we track how over the last five years the European Blockchain Partnership adopted a self-sovereign identity organizing vision based on blockchain. We find that successful adoption requires dynamic coupling and decoupling between vision and IT – both on a discursive and the material levels. Moreover, it requires effective management of 'sensegiving' and 'sensebreaking' by the innovation community.

Keywords: Blockchain, Fashionable IT, Organizing vision, Self-sovereign identity, Sensemaking.

1 Introduction

Many IT innovations are accompanied by grand organizing visions (Miranda et al., 2015; Ramiller and Swanson, 2003; Swanson and Ramiller, 1997). These visions are the rhetorical product of an ongoing and cross-organizational discourse (Currie, 2004; Miranda et al., 2015) and manifest "a focal community idea for the application of information technology in organizations" (Swanson and Ramiller, 1997, p. 460). The discourse around organizing visions is often diverse and full of flexibility and ambiguity, which makes it impossible to adopt organizing visions 'off-the-shelf' (Swanson and Ramiller, 1997). Instead, they demand adopting organizations to engage in a discursive sensemaking process and craft their own interpretations of the vision – so-called visions-in-use (Miranda et al., 2015) – that fit the organization's technical, cultural, and political structure (Ansari, 2010; Canato et al., 2013). This sensemaking typically happens through a recursive process of interpretation and implementation (Berente et al., 2011; Roth et al., 2022). Many of these emerging visions-in-use are then looped back into the larger discourse, reciprocally shaping the larger organizing vision and their specific visions-in-use (Miranda et al., 2015; Ramiller and Swanson, 2003). As a result, organizing vision discourses may become cluttered over time with multiple competing views and visions-in-use (Currie, 2004; Swanson and Ramiller, 1997). This ultimately complicates the adoption and use of organizing visions.

Organizing visions tend to be especially complex when they are constructed around fashionable ITs (Swanson and Ramiller, 2004). A fashionable core technology can impose a bell-shape on the discourse with a single sharp up- and downswing. Moreover, fashionable ITs are often loaded with cultural and political values that may influence the organizing vision (Lichti and Tumasjan, 2022; Roth et al., 2022). Many organizations nevertheless readily adopt organizing visions that involve fashionable IT to benefit from high degrees of legitimacy and mobilization during their up-swing phase as well as purportedly beneficial cultural and political loadings (Swanson and Ramiller, 2004; Wang, 2010). However, it is not clear how organizations can successfully navigate the adoption of such 'fashionable' organizing visions. This research thus aims to investigate the process of their organizational sensemaking and materialization. It asks the following research question:

How can adopting organizations successfully make sense of and materialize fashionable organizing visions?

To answer this research question, we conduct an inductive longitudinal case study (Yin, 2009). Our case of analysis is the development of the European Blockchain Services Infrastructure (EBSI) by the European Blockchain Partnership (EBP) and the European Commission. In their development of EBSI, the EBP and the European Commission adopted a self-sovereign identity (SSI) organizing vision that was centered around blockchain technology. Three members of our research team were closely involved with the EBP in different functions for close to five years, which offers rich insights into how the EBP made sense of and materialized blockchain-based SSI.

Our analysis provides a more nuanced understanding of the organizational sensemaking of fashionable organizing visions and the complexities that may arise along these processes. Specifically, we find that adopting organizations may experience pronounced discursive and material dissonance between their organizing vision-in-use and the vision's fashionable core technology. To mitigate this dissonance, they can employ discursive and material processes of 'coupling' and 'decoupling. Furthermore, we find that the evolution of the larger organizing vision discourse plays a pivotal role in the development of organizing visions-in-use. It can support both sensegiving and sensebreaking, especially when it questions the role of the fashionable technology for the organizing vision. We translate these findings into a tentative recursive process theory for the sensemaking of fashionable organizing visions.

Our paper is structured as follows: The subsequent sections outline the theoretical background of our work and present our case study design. We then present how the EBP made sense of and materialized its organizing vision-in use of blockchain-based SSI. Thereafter, we translate our findings into a tentative recursive process theory and discuss our contributions. Our paper concludes with a summary of our findings, an outline of limitations, and avenues for future work.

2 Theoretical Background

2.1 Fashionable Organizing Visions

Organizing vision theory emerged as a complementary lens to study the diffusion of IT innovation (Currie, 2004; Miranda et al., 2015; Swanson and Ramiller, 1997). In contrast to more traditional theories of economic rationality, it focuses on the role of inter-organizational discourses (Miranda et al., 2015). Organizing visions describe the opportunities for embedding one or multiple core technologies in an organization. That is, they provide a "vision for organizing" around a focal IT (Swanson and Ramiller, 1997). Organizing visions give rise to a shared "social account" that provides a common ground for *interpreting* and *legitimizing* IT innovations and *mobilizing* actions for their realization and application (Currie, 2004; Gorgeon and Swanson, 2011). Some organizing visions target existing business problems, others are "solution[s] in search of a problem" (Miranda et al., 2015).

Organizing visions are often replete with ambiguity and buzzwords. These buzzwords act as a center of gravity for the discourse and allow organizing visions to attract and coordinate a variety of heterogeneous parties, such as prospective adopters, consulting firms, technology vendors, journalists, or academics (Swanson and Ramiller, 1997; Wang and Swanson, 2007). These parties reciprocally interact, shape, and enrich the organizing vision (Miranda et al., 2015; Wang and Swanson, 2007). In some cases, these interactions make an organizing vision more coherent, in others, they drive diversity and even contradiction (Ramiller and Swanson, 2003; Wang and Swanson, 2007). Organizing visions are thus fluid by nature. Moreover, they have 'careers' that are marked by alternating up- and downswings of visibility, prominence, influence, and tenor until they finally fade away – either as a result of institutionalization or abandonment (Currie, 2004; Ramiller and Swanson, 2003).

Coherence and diversity within the organizing vision discourse as well as the tenor of discourse are valuable indicators for how an organizing vision's career will play out (Miranda et al., 2015; Wang and Swanson, 2007). While diversity allows an organizing vision to attract a larger innovation community, "a lack of coherence will not be tolerated indefinitely" (Swanson and Ramiller, 1997, p. 463). Adopting organizations are a pivotal driver for an organizing vision's diversity and coherence. They materially engage with the core technology, which often sets boundaries for the organizing vision (Miranda et al., 2022), especially if core technologies are unavailable or poorly defined (Currie, 2004; Swanson and Ramiller, 1997). Moreover, they develop tailored organizing visions-in-use that fit their organizational contexts (Miranda et al., 2015). These visions-in-use support other organizations in their sensemaking efforts and can be decisive for an organizing vision's ultimate success. While successful visions-in-use additionally legitimize an organizing vision, stories of failure can drive abandonment (Wang and Swanson, 2007). In some cases, however, an organizing vision's fate is determined not by those who embrace it but by those who do not. If powerful actors refrain from engaging with an organizing vision, an organizing vision's legitimacy and mobilizing effects can be undermined (Currie, 2004).

Building an organizing vision around a fashionable technology can increase the legitimacy and mobilizing effects of organizing visions (Swanson and Ramiller, 2004). An IT is said to be fashionable when it is surrounded by a "transitory collective belief that an information technology is new, efficient, and at the forefront of practice" (Wang, 2010, p. 66). Like organizing visions, this collective belief is the rhetoric product of a community discourse. Unlike organizing visions, however, it typically follows a well-defined, bell-shaped trajectory, with a sharp up- and downswing (Baskerville and Myers, 2009; Swanson and Ramiller, 2004). Organizing visions with fashionable core technologies tend to inherit this trajectory. They have a very rich and enthusiastic upswing discourse full of unbalanced and at-times unsubstantiated claims and down-swing discourses marked by negative and critical statements (Swanson and Ramiller, 2004; Wang, 2010). Furthermore, the discourse around fashionable IT is often loaded with cultural and political values. These values typically entail specific views of organizing that introduce an additional degree of complexity into fashionable organizing visions (Lichti and Tumasjan, 2022; Roth et al., 2022; Swanson and Ramiller, 2004).

The higher the degree of complexity of an organizing vision, the more important it is for adopting organizations to engage in a process of organizational sensemaking that iterates between interpretation of the organizing vision and implementation of the underlying fashionable IT (Berente et al., 2011; Roth et al., 2022). The exact process, however, remains poorly understood.

2.2 Self-Sovereign Identity and the Role of Blockchain

00/00/0000 00:00:00Since the invention of the internet, organizations have been trying to develop effective identity management on the web (Sedlmeir et al., 2022). Over time, two dominant models emerged: fragmented and federated identity management (Schlatt et al., 2021). However, limited interoperability and convenience of fragmented and high risks of security and privacy breaches of federated identity management have sparked and legitimized a rethinking of current ways of organizing (Sedlmeir et al., 2022). Thus, a new vision of decentralized or self-sovereign identity (SSI) management emerged (Allen, 2016). The SSI vision is increasingly gaining support by various stakeholders, such as technology vendors, consultancies, prospective adopters from the public and private sector, and even policy makers (Lacity et al., 2023). SSI seeks to enable users to conveniently manage and share their identity data without being dependent on an identity provider (Lacity and Carmel, 2022; Weigl et al., 2022). In this sense, SSI is commonly interpreted as a digital way of organizing that is comparable to today's physical identity management (Hoess et al., 2022).

The SSI organizing vision builds on three core technologies: digital credentials, digital wallets, and trust infrastructures (Sedlmeir et al., 2021). Digital credentials are cryptographically signed, machine-verifiable, and tamper-resistant digital certificates that attest certain identity claims (Feulner et al., 2022). One of the most popular standards for these certificates is the W3C's verifiable credentials standard (W3C, 2022). The exchange of digital credentials is organized in a bilateral fashion (Lacity et al., 2023). Issuers attest specific identity claims in the form of digital credentials and transfer these credentials to their subjects, who can manage them in a digital wallet (Rieger et al., 2022). When requested, subjects can use their digital wallet to selectively present their credentials or certain attributes in these credentials to a verifier, such as an online service provider (Mühle et al., 2018; Sedlmeir et al., 2022). To verify the presented credentials, verifiers typically make use of (cryptographic) trust infrastructures that provide them with the required information to establish the authenticity and validity of the presented identity information (Lacity et al., 2023; Sedlmeir et al., 2021). While the general SSI idea has been very coherent, it provides a certain degree of rhetorical flexibility concerning the interpretation of self-sovereignty. Furthermore, there is diverse discourse regarding the use of blockchain as trust infrastructures (Hoess et al., 2022; Sedlmeir et al., 2022).

Characterized by stark upswing and downswing phases, blockchain is a fashionable IT that has kept organizations across different sectors on their toes (Beck et al., 2018; Miranda et al., 2022). From a technological point of view, blockchains are distributed transactional databases that are jointly operated by the nodes of a peer-to-peer network (Beck et al., 2018; Rossi et al., 2019). Data entries, so-called transactions, are grouped into blocks, which are cryptographically linked in chronological order. These features provide a high degree of resilience to unauthorized changes and enable a "trusted" state of information without requiring a central trusted third-party (Chanson et al., 2019; Rieger et al., 2019).

Blockchain began its career modestly as a technical backbone for the processing of cryptocurrency transactions (Nakamoto, 2008). However, things changed quickly when it was extended with advanced features, such as flexible programming logic, that enabled various applications beyond the processing of financial transactions (Casino et al., 2019; Lacity, 2022). This broader applicability enabled a veritable blockchain hype from 2016 onwards, with vivid discourses around blockchain's promises to establish a new era of decentralization (Beck et al., 2018; Miranda et al., 2022). The blockchain hype also influenced the discourse around SSI and led to an SSI variant that positioned blockchain as the only sensible core technology for SSI's trust infrastructures (Lacity, 2022; Sedlmeir et al., 2021). However, criticism soon emerged around this positioning of blockchain, which was amplified by the European Commission's development of a competing vision and framework that was independent of blockchain (European Commission, 2023). These developments and the competing variants in the SSI discourse make SSI a particularly interesting candidate for studying the adoption of fashionable organizing visions.

3 Research Method

To explore how adopting organizations can successfully make sense of fashionable organizing visions, we opted for an inductive research design that would allow us to generate new process insights (Eisenhardt, 1989; Sarker et al., 2018). Specifically, we chose to conduct a longitudinal single case study. Case study research is a very fruitful approach for investigating sensemaking processes given their socially embeddedness and contingency on contextual factors, such as the organizational domain and the larger organizing vision discourse (Benbasat et al., 1987; Yin, 2009). A longitudinal design, in turn, allows to examine these processes in-depth and facilitates rich theorizing on how they unfold over time (Yin, 2009).

3.1 Case description

In our case study, we investigate the adoption of blockchain-based SSI by the European Blockchain Partnership (EBP). The EBP was founded in April 2018 as a joint initiative of the European Commission and the EU's member states (plus Liechtenstein and Norway) with the goal of developing a blockchain-based infrastructure – the European Blockchain Services Infrastructure (EBSI) – for delivering cross-border public services.

The EBP is structured and managed through a loose organizational framework. The European Commission assumes responsibility for the coordination of the partnership and the technical development of EBSI. The operation of EBSI, in turn, is distributed across node operators in the participating countries. The 'EBP technical group' – a group of technical experts from all participating countries – supports the development of EBSI by providing technical advice. Decisions, in turn, are made by the 'EBP policy group', which consists of one delegate from each participating country. These decisions include, among others, the definition of formal governance structures or the endorsement of public services that should inform the development of EBSI. Each of these services has a dedicated working group that develops specifications and defines required interfaces and business applications.

Soon after its inception, the EBP created a working group that developed a blockchain-based SSI vision-in-use and materialized it as the so-called European Self-Sovereign Identity Framework (ESSIF). ESSIF became the dominant vision for EBSI when the EBP decided to focus its piloting efforts on public services related to digital identity management. These services include digital (university) diplomas and a digital European Social Security Pass. EBSI's digital diploma service received particular traction when the EBP and the European Commission launched a multi-university pilot for digital diplomas in early 2021. This pilot provided funding for prospective adopters, such as universities and public authorities, and technology vendors, such as digital wallet providers, to engage in national piloting.

3.2 Data collection

To enable data triangulation and increase the validity of our theorizing, we collected data from three different sources: interviews, participant observations, and documentation. Interviews were our primary source of evidence (Yin, 2009). We conducted a first set of 7 interviews in the fall of 2020 to study the adoption of SSI. These interviews suggested mounting (discursive) tensions from the coupling of blockchain and SSI. Over time and with increasing material dissonances, these tensions dominated EBSI's adoption of blockchain-based SSI. A later set of interviews revealed how the EBP navigated the sensemaking and materialization of blockchain-based SSI. Specifically, we interviewed 21 partners in the summer and autumn of 2022 to reflect on the EBPS' management of interdependencies and dissonances between SSI and blockchain.

Our informants included representatives from the European Commission and other organizations involved in EBSI like national and local governments, technology providers, and universities (Table 1). We selected informants from those organizations that were either actively involved in EBSI on a strategic and discursive level; engaged in the implementation of EBSI, ESSIF, and the digital diploma service; or both. We also considered the backgrounds and areas of expertise of interviewees to better understand the evolving vision-in-use as well as its materialization. The selected informants helped us gain a comprehensive view and rich insights into how the EBP made sense of and materialized blockchain-based SSI.

	Number of interviewed experts from organizations involved in the EBP			
	European Commission	**National and local government**	**EBP technology partner**	**Universities**
Wave 1	1	3	3	-
Wave 2	5	8	5	3

Table 1. Overview of interviewees.

For our interviews, we employed a semi-structured design (Schultze and Avital, 2011). Each of our interviews followed a logical sequence. We first asked our informants about their reasons to engage with the EBP and its blockchain-based SSI organizing vision. This also included a short discussion about their initial expectations of blockchain-based SSI. Interviewees then gave their opinion on the EBP's emerging vision-in-use. Moreover, we asked interviewees how they perceived the effects of implementation. Our last (set of) questions encouraged interviewees to reflect on how their understanding of the relationship between blockchain and SSI evolved over time. We audio-recorded each of the interviews and additionally transcribed them to support our data analysis. The interviews had an average duration of 56 minutes.

We complemented these interviews with participant observations. Three authors of this work were actively involved with EBSI in different roles and regularly attended the different working groups involved in EBP's sensemaking of blockchain-based SSI. More specifically, the second and fourth author of this work started to engage with the EBP in October 2018. Both served as national representatives for EBP's technical working group and occasionally attended meetings of the ESSIF and policy working groups. From March 2021 to March 2023, both the second and fourth author engaged in one of the national projects for piloting digital diplomas based on EBSI and ESSIF. The first author of this work joined this national project in November 2021. When joining this project, the first author also started to regularly participate in the technical, policy, and ESSIF working group and the negotiation of the national strategy regarding EBSI and SSI. To make these observations available for later analysis, the observing authors took notes and collected presentations and protocols. In addition, we gathered internal and publicly available documents (Table 2) (Eisenhardt et al., 2016; Yin, 2009). Overall, our active involvement gave us rich first-hand insights into how the EBP, and its members made sense of and implemented blockchain-based SSI. To ensure a balanced analysis and objectivity, we added two co-authors to the team who have not been involved with the EBP (Gioia and Chittipeddi, 1991).

	Types of documents	**Total number of pages**
Internal documents	Internal presentations, Legal assessments, Internal project reports, Technical documentation	210+ pages
Public documents	Blog posts & other marketing material, Press releases, Public presentations, Public reports	160+ pages

Table 2. Overview of Secondary Evidence.

3.3 Data analysis

Following our data collection, we retraced the evolution of the EBP's engagement with blockchain-based SSI and its materialization. Specifically, we performed a two-stage coding process to analyse the collected data. For open coding, we assigned initial codes to all statements we considered relevant for our research (Corbin and Strauss, 1990; Saldaña, 2013). Our early theme discovery focused on topics such as the evolution of ESSIF, the emergence of initially supportive and later discouraging discourses around blockchain-based SSI, discussions on the meaning of SSI for EBSI, and approaches to the technical integration of SSI with EBSI. Based on the identified themes, we performed a second, iterative process of axial coding. This helped us to refine our codes and aggregate synonymous codes into overarching categories. Moreover, we specified the dimensions and properties of each category, and analysed our codes and categories regarding interdependencies (Corbin and Strauss, 1990; Saldaña, 2013). The emerging constructs focused on the derivation of a specific vision-in-use, the interplay between discursive and material engagement, how material coupling and decoupling led to the de- and reframing of the vision-in-use, and how the larger innovation community affected these sensemaking processes through sensegiving and sensebreaking. The process yielded first theoretical explanations which we refined by iterating between data and theory (Eisenhardt et al., 2016; Gibbert et al., 2008; Yin, 2009). Overall, our coding process produced more than 1900 codes, which we managed using the MAXQDA software.

The coding was performed by the first author of this work, who iterated the identified codes and theoretical insights in close collaboration with the second author. These two authors regularly discussed emerging themes with the third author to enhance objectivity (Dubé and Paré, 2003; Gibbert et al., 2008). Throughout the axial coding process, we triangulated our different sources of evidence to enhance the construct validity and generalizability of our research (Dubé and Paré, 2003; Eisenhardt et al., 2016).

4 Emerging Theoretical Framework

The EBP's sensemaking and materialization of blockchain-based SSI can be bracketed into three phases, each with a different emphasis. While sensegiving by the innovation community served as a catalyst for *adopting and materializing blockchain-based SSI* in a first phase, challenges with further materialization resulted in a recursive process of material coupling and decoupling of SSI and blockchain in a second phase. These efforts helped the EBP to better understand and frame the interplay between SSI and blockchain. In a third phase, the revision of the European Union's regulation on electronic identification, authentication and trust services (eIDAS) led to sensebreaking and inevitably demanded *navigating a competing organizing vision*.

4.1 Adopting and materializing a fashionable organizing vision

In April 2018, the EU's member states, Liechtenstein, and Norway formed the EBP to facilitate the delivery of cross-border public services with a shared blockchain infrastructure. The EBP's first activities centered around the joint identification of relevant public services that should inform the development of a European Blockchain Services Infrastructure.

For the selection of these services, political fit, a sound legal basis, and the prospect that blockchain can improve current practice were important guiding criteria. While investigating potential services, the EBP became aware of the organizing vision of blockchain-based SSI, which had become fashionable in the internet identity community. This organizing vision resonated well with some of the EBP members, who still struggled with the largely unsuccessful implementation of the first version of the eIDAS regulation. To them, the organizing vision of SSI was a promising way forward "*to overcome limitations"* and *"initiate a change in the eIDAS system."* It provided a common interpretation for rethinking current approaches of digital identity management. They also saw the potential of blockchain-based SSI for a privacy-preserving, self-determined identity management for European citizens. Moreover, the fashionable character of blockchain-based SSI granted the EBP a legitimate organizing vision for EBSI and acted as a *"catalyst"* for mobilizing required stakeholders. In the words of one of the EBP's technology providers and one EBP member state representative:

"I think this really goes also back to this [internet identity] community that wants to solve identity in the most user-centric way. And now, with blockchain [...], they found a way of giving people actual ownership, whatever that means, over their identities."

"We really believe[d] that the ledgers and the network supported by a blockchain can play a very important role to protect the privacy of citizens and to enable the self-sovereign identity of the user."

Eventually, the EBP decided to adopt the fashionable organizing vision of blockchain-based SSI and established a working group for the development and materialization of a more specific vision-in-use – the European Self-Sovereign Identity Framework in April 2019. This ESSIF working group should inform EBSI services focused on the exchange of identity-related information and the use of digital credentials. Soon, the ESSIF working group began to explore the interplay of blockchain and SSI. The group collected requirements and developed guidelines for implementing SSI features. Moreover, it investigated opportunities to align ESSIF with the requirements outlined by the eIDAS regulation. The ESSIF working group was "*enthusiastic about blockchain as a technology*". It perceived blockchain and SSI to be highly resonant and foresaw a brilliant future for blockchain-based SSI. One year later, the working group materialized a first version of ESSIF in the form of a conceptual architecture. This materialization specified EBSI as a trusted infrastructure for the exchange of digital credentials. From a more technical perspective, it defined EBSI as a storage layer for digital credentials and related information. One representative from the European Commission and one national government representative explain this initial materialization:

"We thought that aside of using blockchain for storing information about accreditation organizations, which accredits the issuers to issue specific credentials, we can also store some additional information such as decentralized digital identifiers of natural persons.

In the ESSIF solution, there are decentralized digital identifiers [...] and verifiable credentials anchored [on the blockchain]. That's currently the ESSIF model.

4.2 Addressing materialization challenges through coupling and decoupling

In early 2021, the EBP started to pilot ESSIF and engage more materially with blockchain-based SSI by piloting the digital diploma service. The pilot aimed to assess EBSI's technical viability and the added value of the digital diploma service. The EBP also used the pilot to determine ESSIF's effects on citizens' privacy and its compliance with the EU's General Data Protection Regulation (GDPR). As piloting proceeded, ESSIF increasingly became a bone of contention as it dawned on the EBP that the idea of a privacy-preserving SSI framework and the intended use of blockchain as a core technology were difficult to reconcile. This dissonance occurred in two stages, to which the EBP responded with material decoupling.

The first dissonance emerged when the ESSIF working group developed specifications for the information that should be stored on EBSI. They informed their specifications by examining other initiatives and their visions-in-use. The ensuing sensemaking of the various visions-in-use led the ESSIF working group to realize that blockchain is not relevant for all information. They understood that credentials do not need to be stored on a blockchain to ensure their integrity and make them verifiable. On the contrary, the planned storage of credentials – albeit in encrypted form or as a hash of the credential – may contradict with one of SSI's key principles, namely the protection of users' privacy. One EBP member state representative reflects:

"We did consider saving a hash of the [credential] on the blockchain. But we soon discarded this idea for many reasons. One of them is that well [...] who knows if in 20 years someone could obtain the original information from a hash. [...] So, we decided to remove that information from the blockchain"

To mitigate this dissonance, the EBP revised its conceptual architecture so that digital credentials would only be stored in the holder's digital wallet, but not on EBSI. In other words, the EBP approached dissonance reduction by materially decoupling the storage of digital credentials, a pivotal SSI component, from EBSI. At the same time, the ESSIF working group promoted material coupling of SSI and blockchain where they perceived high resonance between both. This led to the implementation of services that help store decentralized digital identifiers of credential issuers and holders on EBSI. However, the storage of holder identifiers was highly controversial due to the resulting privacy implications. Although some members of the EBP, including representatives from our research team, emphasized these concerns, the ESSIF working group, nonetheless, decided to implement both services. They thought storing identifiers of issuers and holders on EBSI is essential to facilitate the cryptographic verifiability of credentials and assure a binding between digital credentials and their holders. In the words of one of the EBP's technology providers:

So, the idea of [the EBP] is to store DIDs that identify natural persons on a blockchain. But there's still the question, if that is even a good idea or if that is already too much. There's a really large group of people who believe that even that is already too much to be stored on a public ledger."

As piloting progressed, the EBP could successfully demonstrate EBSI's technical feasibility and the added value of its digital diploma service. However, a few months later, in February 2022, the results of an assessment related to EBSI's compliance with the EU's GDPR introduced a more critical perspective and further dissonances concerning blockchain-based SSI. The GDPR assessment concluded that a natural person's decentralized identifiers constitute personally identifiable information and must not be stored on a blockchain. To comply with GDPR requirements, the EBP had to remodel ESSIF and removed the storage of natural persons' decentralized identifiers from EBSI. In effect, the

EBP had to decouple SSI and blockchain even further to mitigate dissonance between blockchain and SSI, so that "*the blockchain layer was becoming thinner and thinner. Much more things are [now] happening outside the blockchain network because of privacy issues.*" The new ESSIF featured EBSI only as a registry for trusted issuer information. One representative from the European Commission and one technology provider recount:

"We went through a long, long, long battle with the data protection officers and lawyers and policymakers. And we've understood if we would allow to store the decentralized identifiers of natural persons on the ledger, on EBSI, the EBSI service wouldn't be GDPR-compliant. So, our brave architects and masterminds found out that, we don't really need to store it on the ledger. We can keep it on the wallet side, and that's the new version of conformance."

"Over time, the vision that you can use blockchain for digital identity has certainly diminished. It still has its legitimacy, but it is significantly smaller than at the beginning."

These material changes inevitably raised discursive dissonances with the vision-in-use originally propagated by the EBP. The European Commission thus launched a marketing campaign to disseminate a reframed vision-in-use that would support the EBP members' sensemaking. This marketing campaign focused on giving sense of the use and benefits of EBSI – as a trusted issuer registry – for the exchange verification of digital (diploma) credentials.

4.3 Navigating a competing vision

In parallel to the EBP's efforts to make sense of and materialize blockchain-based SSI, the European Commission announced the revision of its eIDAS regulation in October 2020. Eight months later, in June 2021, the European Commission disclosed more details on their vision for eIDAS v2. Although not officially coined "SSI", this vision for eIDAS v2 employed various ideas and concepts of SSI. Most notably, the European Commission emphasized a citizen-centric digital identity management based on digital identity wallets, which enables citizens to store and control their digital credentials.

Yet, the released details lacked information regarding a core technology for eIDAS v2's trust infrastructure. This raised hopes but also caused uncertainties regarding EBSI's and ESSIF's future role in digital identity management in Europe. Some members of the EBP clearly viewed EBSI and ESSIF as core elements of eIDAS v2, as one EBP representative from the European Commission points out:

"If anybody that is interested in blockchain would read this, one would see blockchain written everywhere. It's not said blockchain. It's not. They don't say decentralized ID the way we do, but the way it's phrased seems to be hinting at that. This is a possible answer to what they want to do."

Other EBP members, however, sensed resentment around blockchain-based SSI among members of the eIDAS expert groups. Specifically, these groups considered blockchain as less mature, secure, and privacy-preserving than the centralized trust infrastructures already in place for eIDAS v1. These concerns were fueled by the failed launch of a blockchain-based SSI application for Germany's mobile driving license in September 2021. A national EBP representative and an EBSI adopter highlight:

"I would say that especially the people that created eIDAS are not all positive about blockchain [...] The IT people who really developed it, they can show that there is a system that is working. They are not necessarily convinced why we would need something new."

"The recognition has pretty much backfired with the failed launch of Germany's mobile driving licence, which was massively criticized."

As the eIDAS revision moved through the EU's legislative process, uncertainties regarding EBSI and ESSIF further increased. In February 2022, the European Commission published the first outline of the eIDAS v2 reference architecture framework to materialize its vision. However, details regarding the core technology for the underlying trust infrastructure were still missing. Instead, the European Commission emphasized that the regulation will be technology neutral, leaving the EBP with hopes but also uncertainties. These uncertainties and divided opinions about EBSI's and ESSIF's fit with the new regulation provoked a sensebreaking and destruction of the EBP's understanding of blockchain-based SSI. The EBP also perceived that its vision of blockchain-based SSI had lost its legitimacy with the emergence of a competing vision that will be legally mandated. One national EBP representative and one representative from the European Commission explain:

"Do I need a blockchain for a digital identity? [...] The eIDAS revision has given a lot of space to this discussion. Because there is a clear will to break away from [blockchain] and the revision is also supposed to be technology-neutral, [...], there is no further talk about blockchain."

"The situation was much more comfortable for EBSI to develop ESSIF before the proposal for the new eIDAS regulation. [...] Because we were investigating the solution of the future, whereas now we are in a situation where it seems that we are competing with a solution which is much more legitimate."

The EBP's broken sense is currently triggering feverish attempts to find new sense. At this stage, the EBP is questioning blockchain-based SSI altogether and SSI. Some even perceive SSI as a "*child that has outgrown its parent [blockchain]'s home.*" To account for these concerns, the EBP has begun to actively reframe ESSIF and drop all mentioning of SSI in favor of a less fashionable framework centered around digital credentials. This reframing better reflects EBSI's role as a registry for meta-information that is required for verifying digital credentials. Furthermore, the EBP attempts to reduce uncertainties by strengthening EBSI's portfolio of services that require verifiability of non-personal identity-related data. This not only includes the further development of a Social Security Pass service, but also experimentation with a new, much broader organizing vision. In particular, the EBP now positions EBSI as a trusted registry for metadata required to verify information, such as verifiable credentials. Two representatives from the European Commission explain:

"It's no more appropriate to claim that we are developing a new framework for self-sovereign identity. So, for me at least, the message is that we continue to work on our concept of the exchange of verifiable credentials."

"At the end, EBSI is ultimately used as a source of trust. That's the main purpose of blockchain: to build resilient lists that allow everyone from everywhere to get the required data to verify some other information."

5 Discussion

Organizations interested in IT innovation are often tempted to adopt organizing visions built on a fashionable IT to profit from the IT fashion's legitimation and mobilization benefits (Currie, 2004; Swanson and Ramiller, 2004). Yet, these decisions are not without risk. Fashionable organizing visions can be full of unbalanced claims and poorly align with the underlying fashionable IT, which complicates the adoption of both the organizing vision and the IT (Roth et al., 2022; Swanson and Ramiller, 1997). Our inductive single case study sheds light on the resulting complexities and how adopting organizations can nevertheless successfully navigate the sensemaking and materialization of the fashionable organizing vision.

5.1 Tentative Process Model

Our core contribution is a tentative recursive process model (Cloutier and Langley, 2020) of the sensemaking of fashionable organizing visions (Figure 1). The model builds on theories about the adoption of organizing visions (Miranda et al., 2015; Swanson and Ramiller, 1997) and fashionable ITs (Baskerville and Myers, 2009; Roth et al., 2022; Wang, 2010).

The coupling of organizing visions with fashionable ITs serves as a starting point for our theoretical model. Adopting organizations often buy into coupling narratives that emphasize the fit of organizing visions and IT fashions and establish their own fashionable visions-in use. Through recursive attempts to make sense of these organizing visions-in-use, adopting organizations may discover resonant and dissonant elements between the organizing vision and the underlying fashionable ITs (Currie, 2004; Roth et al., 2022; Swanson and Ramiller, 1997). Further materialization efforts help adopting organizations to substantiate these resonances and dissonances and better understand the fit between the organizing vision and fashionable IT as well as the vision-in-use's fit with the organizational context.

To reinforce resonance and to mitigate dissonance, adopting organizations can undergo cyclical processes of *material coupling* and *material decoupling*. More specifically, adopting organizations can enhance resonance by selectively implementing resonant elements with the fashionable IT. We refer to this practice as *material coupling*. They can also reduce dissonance by not implementing certain elements emphasized in the vision-in-use or by implementing those elements with non-fashionable ITs. We term this practice *material decoupling*. These implementation efforts can guide the de- and reframing of fashionable visions-in-use. Specifically, adopting organizations can apply *discursive coupling* and *decoupling* to emphasize fit between the vision-in-use (discourse) and the material implementation (Roth et al., 2022). These revised visions-in-use may serve as a basis for subsequent sensemaking cycles.

Along this cyclical and re-cursive sensemaking and materialization process, the larger organizing vision discourse also evolves (Wang and Ramiller, 2009). This can happen when the discourse community's knowledge on the role of the underlying fashionable ITs increases (Miranda et al., 2022), or when powerful actors step into the discourse and promote specific views. The evolution of the larger organizing vision discourse continuously influences organizational sensemaking and materialization. Once the underlying IT goes out of fashion, the discourse may become laden with decoupling narratives and ultimately dominated by a variant of the organizing vision that does no longer include the fashionable IT. This evolution can destruct the adopting organization's understanding of the interplay between the organizing vision and its fashionable core technology. The risk of such a turn of events is especially high when decoupling narratives are promoted by powerful actors (Nielsen et al., 2014). Their sensebreaking can eventually create a sense void that is hard to fill (Maitlis and Christianson, 2014; Pratt, 2000).

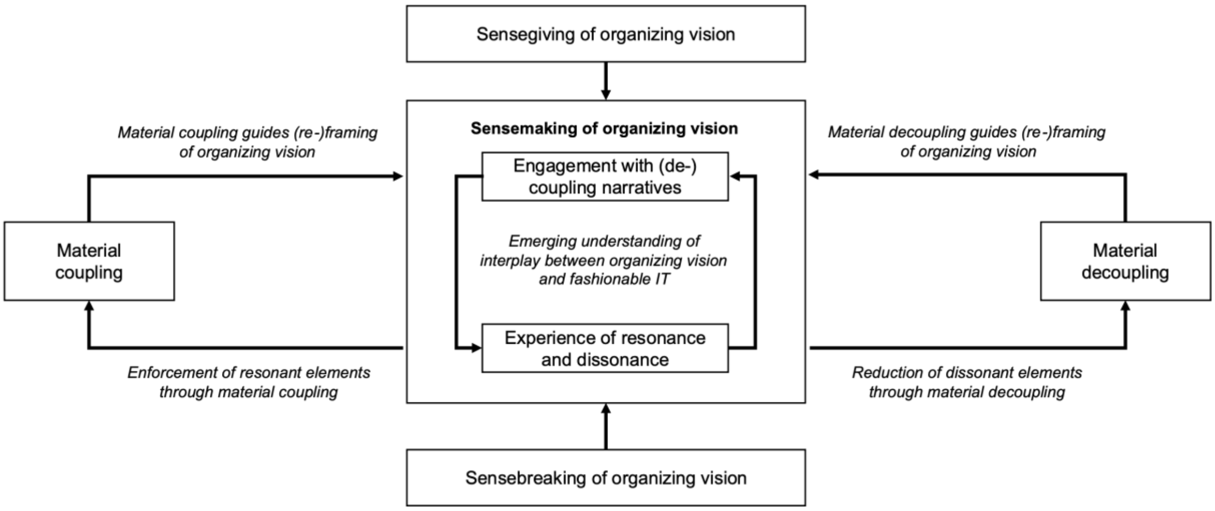

Sensegiving of organizing vision
Material coupling guides (re-)framing of organizing vision
Sensemaking of organizing vision
Material decoupling guides (re-)framing of organizing vision
Engagement with (de-) coupling narratives
Material coupling
Emerging understanding of interplay between organizing vision and fashionable IT
Material decoupling
Experience of resonance and dissonance
Enforcement of resonant elements through material coupling
Reduction of dissonant elements through material decoupling
Sensebreaking of organizing vision

Figure 1. Process model for the sensemaking and materialization of fashionable organizing visions.

5.2 Contribution to Theory

Our theoretical process model contributes to the literature on organizing visions by providing a more nuanced understanding of how adopting organizations make sense of and materialize fashionable organizing visions. We find that the adoption of fashionable organizing visions engenders complex sensemaking and materialization processes – especially when adopting organizations experience dissonance between the organizing vision and the fashionable IT. Adopting organizations can mitigate this dissonance through discursive and material decoupling. In turn, they can amplify resonant elements through discursive and material coupling.

Moreover, our research offers empirical support that material engagement plays a pivotal role in how adopting organizations frame (fashionable) visions-in-use0/0/0000 0:00:00 AM. In line with Miranda et al. (2022) and Swanson and Ramiller (1997), our findings suggest that materialization forces a critical reflection on the organizing visions and the capabilities of fashionable ITs. More specifically, our research provides corroborative evidence that materialization efforts may uncover material constraints of the fashionable core technology. They may even require adopting organizations to de- or reframe their visions-in-use and, thereby, set boundaries that constrain the larger organizing vision discourses (Currie, 2004; Miranda et al., 2022; Swanson and Ramiller, 1997).

What is more, our research provides an improved understanding on the interplay between organizing visions and derived visions-in-use. In line with Miranda et al. (2015), our findings illustrate that adopting organizations establish more specific visions-in-use through recursive efforts of interpretation and materialization. What we unpack in this work is that these recursive processes may not only support sensemaking but can also have a sensebreaking effect. Specifically, we find that when the larger discourse shifts and drops a particular core technology, adopting organizations that built their visions-in-use around the dropped core technology will be unmoored.

Lastly, our research contributes to the literature on blockchain and SSI by providing a more nuanced understanding of how the discourse of blockchain-based SSI evolved over time. Our research offers empirical support that the fashion around blockchain served as an enabler for the diffusion of the SSI organizing vision (Mühle et al., 2018; Sedlmeir et al., 2022). Moreover and in line with the more technical research on SSI, our findings illustrate that a strong material coupling of both technologies is not necessarily required (Feulner et al., 2022; Hoess et al., 2022). On the contrary, we find that a strong association with blockchain may even have become undesirable now that the blockchain hype has died down and risks encumbering the adoption of SSI.

5.3 Practical Implications

Our findings are also relevant beyond research. They provide practitioners with a more nuanced understanding of the interplay between organizing visions and fashionable ITs and the management of such fashionable organizing visions. Our findings suggest that fashionable organizing visions can be a tough nut to crack. Even when they appear to fit an adopting organization's legitimization and business needs perfectly in the beginning, they may turn out to be dangerous affairs. Sticking with fashionable organizing visions can lead to serious technical debt down the road.

In particular, practitioners should be aware that the understanding of fashionable organizing visions is typically limited at the beginning, and dissonances are very likely to emerge only at a later stage through materialization efforts. Undeterred practitioners should thus undertake first, small-scale materialization efforts early. These efforts may reveal resonance and dissonances between the organizing vision and the fashionable IT and provide essential guidance for the way forward, be it a modified organizing vision-in use or abandonment.

Furthermore, practitioners should keep in mind that fashionable organizing visions will enter a downswing at a later point. During this downswing, competing visions that are independent of the fashionable IT may start to dominate the discourse. If powerful actors promote one of these competing visions, fashionable visions-in-use might lose their legitimization and mobilization properties.

Consulting not only with experts within the innovation community but also with those from outside may help practitioners to gain a more balanced perspective and to avoid costly failures. This is where IS researchers may play a pivotal role since they can provide more neutral reflections and informed knowledge on the interplay of organizing visions and fashionable ITs (Baskerville and Myers, 2009).

5.4 Boundary Conditions

Boundary conditions help to understand a theoretical model's descriptive power. Our process model is subject to three such conditions. The first boundary condition for our theoretical model is the effect of an adopting organization's vision-in-use on the overall (fashionable) organizing vision. While our model describes that materialization efforts trigger de- and reframing of visions-in-use, it cannot predict how these adaptations will impact the overarching (fashionable) organizing vision discourse.

A second boundary condition relates to the entry and ending conditions of our recursive process model. Our theorizing builds on a project that adopted the fashionable IT first and later complemented it with a fashionable organizing vision. Thus, our model cannot predict whether adopting organizations that buy into a fashionable organizing vision will necessarily move beyond informational engagement and really implement the underlying fashionable IT. Moreover, as we investigated the sensemaking and materialization of a fashionable organizing vision during its inception, our research cannot predict the ending conditions for the sensemaking of fashionable organizing visions. In that sense, it cannot predict whether organizations would favor the institutionalization of visions-in-use over the institutionalization of fashionable ITs when changes in the larger discourse force a decoupling.

The third boundary condition concerns the transferability of our results to different combinations of organizing visions and fashionable ITs. We develop our process theory from a case study on the adoption of blockchain-based SSI. Our model may thus not be able to predict how the adoption of other fashionable organizing visions will unfold. However, looking at recent fashionable organizing visions, such as generative artificial intelligence (AI) and the underlying large language models (core technologies), we see many parallels with our case. As with blockchain-based SSI and prior AI organizing visions, engagement with generative AI and implementation of large language models soon uncovered their technical constraints (Dwivedi et al., 2023). Organizations will have to navigate the resulting dissonance between the grand and unbalanced vision of a generative AI and the technical capabilities of large language models. Moreover, the generative AI hype will likely fade away at some point in the future and be supplanted by a new one. As with prior AI hypes, organizations may then need to refine their organizing visions-in-use of generative AI by specifying what type of work generative AI may take over (Berente et al., 2021). This refinement, in turn, may also open a window for incorporating new core technologies. In effect, we see substantial ground to surmise that our findings are also generalizable to other fashionable organizing visions.

6 Conclusion and Limitations

Fashionable ITs can give organizing visions for IT innovations more legitimacy, which is why adopting organizations increasingly adopt organizing visions with a fashionable core technology. However, the bell-curved shape of IT fashions and their cultural and political loadings may result in significant complexities and costs for adopting organizations. This paper sheds light on how these complexities can play out and how organizations can successfully navigate the adoption of such fashionable organizing visions. Using an inductive single case study on the development of EBSI, we develop a recursive process model that unpacks how organizational sensemaking and materialization can support the adoption process. Moreover, our process model explains how organizations can amplify fit between their visions-in-use and the underlying fashionable ITs. We find that adopting organizations may do so through opposing cycles of material and discursive coupling and decoupling.

As the research design of a single case study naturally comes with questions of generalizability, we see room for further exploration in future research. Further studies on blockchain-based SSI in may help to account for potential effects of our case context. Besides, studying other fashionable organizing visions could provide further insights into the transferability of our findings to different combinations of organizing visions and fashionable ITs.

Acknowledgments

This research was funded in part by: Luxembourg's Ministry for Digitalisation; the Luxembourg National Research Fund (FNR) grant reference 14783405; FNR and PayPal, PEARL grant reference 13342933/Gilbert Fridgen; and the European Union (EU) within its Horizon 2020 programme, project MDOT (Medical Device Obligations Taskforce) grant agreement 814654. For the purpose of open access, the author has applied a Creative Commons Attribution 4.0 International (CC BY 4.0) license to any Author Accepted Manuscript version arising from this submission.

References

Allen, C. (2016). *The Path to Self-Sovereign Identity*. URL: http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html

Ansari, S. M. (2010). "Made to Fit: How Practices Vary as They Diffuse," *Academy of Management Review*, 35(1), 67–92. https://doi.org/10.5465/amr.35.1.zok67

Baskerville and Myers. (2009). "Fashion Waves in Information Systems Research and Practice," *MIS Quarterly*, *33*(4), 647–662. https://doi.org/10.2307/20650319

Beck, R., Müller-Bloch, C., and King, J. L. (2018). "Governance in the Blockchain Economy: A Framework and Research Agenda," *Journal of the Association for Information Systems*, 19(10), 1020–1034. https://doi.org/10.17705/1jais.00518

Benbasat, I., Goldstein, D. K., and Mead, M. (1987). "The Case Research Strategy in Studies of Information Systems," *MIS Quarterly*, 11(3), 69–386. https://doi.org/10.2307/248684

Berente, N., Gu, B., Recker, J., and Santhanam, R. (2021). "Managing Artificial Intelligence," *MIS Quarterly*, *45*(3), 1433–1450.

Berente, N., Hansen, S., Pike, J. C., and Bateman, P. J. (2011). "Arguing the Value of Virtual Worlds: Patterns of Discursive Sensemaking of an Innovative Technology," *MIS Quarterly*, *35*(3), 685–709. https://doi.org/10.2307/23042804

Canato, A., Ravasi, D., and Phillips, N. (2013). "Coerced Practice Implementation in Cases of Low Cultural Fit: Cultural Change and Practice Adaptation During the Implementation of Six Sigma at 3M," *Academy of Management Journal*, *56*(6), 1724–1753. https://doi.org/10.5465/amj.2011.0093

Casino, F., Dasaklis, T. K., and Patsakis, C. (2019). "A systematic literature review of blockchain-based applications: Current status, classification and open issues," *Telematics and Informatics*, *36*, 55–81. https://doi.org/10.1016/j.tele.2018.11.006

Chanson, M., Bogner, A., Bilgeri, D., Fleisch, E., and Wortmann, F. (2019). "Blockchain for the IoT: Privacy-Preserving Protection of Sensor Data," *Journal of the Association for Information Systems*, 20(9), 1272–1307. https://doi.org/10.17705/1jais.00567

Cloutier, C., and Langley, A. (2020). "What Makes a Process Theoretical Contribution?" *Organization Theory*, *1*(1). https://doi.org/10.1177/2631787720902473

Corbin, J. M., and Strauss, A. (1990). "Grounded theory research: Procedures, canons, and evaluative criteria," *Qualitative Sociology*, *13*(1), 3–21.

Currie, W. L. (2004). "The organizing vision of application service provision: A process-oriented analysis," *Information and Organization*, *14*(4), 237–267. https://doi.org/10.1016/j.infoandorg.2004.07.001

Dubé, L., and Paré, G. (2003). "Rigor in information systems positivist case research: Current practices, trends, and recommendations," *MIS Quarterly*, *27*(4), 597–636. https://doi.org/10.2307/30036550

Dwivedi, Y. K., Kshetri, N., Hughes, L., Slade, E. L., Jeyaraj, A., Kar, A. K., Baabdullah, A. M., Koohang, A., Raghavan, V., Ahuja, M., Albanna, H., Albashrawi, M. A., Al-Busaidi, A. S., Balakrishnan, J., Barlette, Y., Basu, S., Bose, I., Brooks, L., Buhalis, D., … Wright, R. (2023). "So what if ChatGPT wrote it? Multidisciplinary perspectives on opportunities, challenges and implications of generative conversational AI for research, practice and policy," *International Journal of Information Management*, *71*. https://doi.org/10.1016/j.ijinfomgt.2023.102642

Eisenhardt, K. M. (1989). "Building theories from case study research," *Academy of Management Review*, *14*(4), 532–550. https://doi.org/10.5465/amr.1989.4308385

Eisenhardt, K. M., Graebner, M. E., and Sonenshein, S. (2016). "Grand Challenges and Inductive Methods: Rigor without Rigor Mortis," *Academy of Management Journal*, *59*(4), 1113–1123. https://doi.org/10.5465/amj.2016.4004

European Commission. (2023). *The Common Union Toolbox for a Coordinated Approach Towards a European Digital Identity Framework*. URL: https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture-and-reference-framework

Feulner, S., Sedlmeir, J., Schlatt, V., and Urbach, N. (2022). “Exploring the use of self-sovereign identity for event ticketing systems,” *Electronic Markets*, *32*(3). https://doi.org/10.1007/s12525-022-00573-9

Gibbert, M., Ruigrok, W., and Wicki, B. (2008). “What passes as a rigorous case study?” *Strategic Management Journal*, *29*(13), 1465–1474. https://doi.org/10.1002/smj.722

Gioia, D. A., and Chittipeddi, K. (1991). “Sensemaking and Sensegiving in Strategic Change Initiation,” *Strategic Management Journal*, *12*(6), 433–448. https://doi.org/10.1002/smj.4250120604

Gorgeon, A., and Swanson, E. B. (2011). “Web 2.0 according to Wikipedia: Capturing an organizing vision,” *Journal of the American Society for Information Science and Technology*, *62*(10), 1916–1932. https://doi.org/10.1002/asi.21612

Hoess, A., Roth, T., Sedlmeir, J., Fridgen, G., and Rieger, A. (2022). “With or Without Blockchain? Towards a Decentralized, SSI-based eRoaming Architecture,” in *Proceedings of the 55th Hawaii International Conference on System Sciences (HICSS)*.

Lacity, M. (2022). “Blockchain: From Bitcoin to the Internet of Value and beyond,” *Journal of Information Technology*, 37(4), 326-340. https://doi.org/10.1177/02683962221086300

Lacity, M., and Carmel, E. (2022). “Self-Sovereign Identity and Verifiable Credentials in Your Digital Wallet,” *MIS Quarterly Executive*, *21*(3), 6.

Lacity, M., Carmel, E., Young, A., and Roth, T. (2023). “The Quiet Corner of Web3 That Means Business,” *MIT Sloan Management Review*, *64*(3).

Lichti, C. W., and Tumasjan, A. (2022). “My Precious!: A Values-Affordances Perspective on the Adoption of Bitcoin,” *Journal of the Association for Information Systems*, *69*.

Maitlis, S., and Christianson, M. (2014). “Sensemaking in Organizations: Taking Stock and Moving Forward,” *Academy of Management Annals*, *8*, 57–125. https://doi.org/10.5465/19416520.2014.873177

Miranda, S. M., Kim, I., and Summers, J. D. (2015). “Jamming with Social Media: How Cognitive Structuring of Organizing Vision Facets Affects IT Innovation Diffusion,” *MIS Quarterly*, *39*(3), 591–614. https://doi.org/10.25300/MISQ/2015/39.3.04

Miranda, S. M., Wang, D., and Tian, C. (2022). “Discursive fields and the diversity-coherence paradox: An ecological perspective on the blockchain community discourse,” *MIS Quarterly*, *46*(3), 1421–1452.

Mühle, A., Grüner, A., Gayvoronskaya, T., and Meinel, C. (2018). “A survey on essential components of a self-sovereign identity,” *Computer Science Review*, *30*, 80–86. https://doi.org/10.1016/j.cosrev.2018.10.002

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. URL: https://assets.pubpub.org/d8wct41f/31611263538139.pdf

Nielsen, J. A., Mathiassen, L., and Newell, S. (2014). “Theorization and Translation in Information Technology Institutionalization: Evidence from Danish Home Care,” *MIS Quarterly*, *38*(1), 165–186. https://doi.org/10.25300/MISQ/2014/38.1.08

Pratt, M. G. (2000). “The Good, the Bad, and the Ambivalent: Managing Identification among Amway Distributors,” *Administrative Science Quarterly*, *45*(3), 456–493. https://doi.org/10.2307/2667106

Ramiller, N. C., and Swanson, E. B. (2003). “Organizing Visions for Information Technology and the Information Systems Executive Response,” *Journal of Management Information Systems*, *20*(1), 13–50. https://doi.org/10.1080/07421222.2003.11045760

Rieger, A., Guggenmos, F., Lockl, J., Fridgen, G., and Urbach, N. (2019). “Building a Blockchain Application that Complies with the EU General Data Protection Regulation,” *MIS Quarterly Executive*, *18*(4), 263–279. https://doi.org/10.17705/2msqe.00020

Rieger, A., Roth, T., Sedlmeir, J., Weigl, L., and Fridgen, G. (2022). “Not yet another digital identity,” *Nature Human Behaviour*, *6*(1), 3–3. https://doi.org/10.1038/s41562-021-01243-0

Rossi, M., Mueller-Bloch, C., Thatcher, J. B., and Beck, R. (2019). “Blockchain Research in Information Systems: Current Trends and an Inclusive Future Research Agenda,” *Journal of the Association for Information Systems*, *20*(9), 1388–1403. https://doi.org/10.17705/1jais.00571

Roth, T., Rieger, A., Utz, M., and Young, A. G. (2022). "The Role of Cultural Fit in the Adoption of Fashionable IT: A Blockchain Case Study," *Forty-Third International Conference on Information Systems, Copenhagen 2022*.

Saldaña, J. (2013). *The coding manual for qualitative researchers*, 2nd Edition. Thousand Oaks: SAGE.

Sarker, S., Xiao, X., Beaulieu, T., and Lee, A. S. (2018). "Learning from First-Generation Qualitative Approaches in the IS Discipline: An Evolutionary View and Some Implications for Authors and Evaluators (PART 1/2)," *Journal of the Association for Information Systems*, *19*, 752–774. https://doi.org/10.17705/1jais.00508

Schlatt, V., Sedlmeir, J., Feulner, S., and Urbach, N. (2021). "Designing a Framework for Digital KYC Processes Built on Blockchain-Based Self-Sovereign Identity," *Information & Management*, 59(7). https://doi.org/10.1016/j.im.2021.103553

Schultze, U., and Avital, M. (2011). "Designing interviews to generate rich data for information systems research," *Information and Organization*, *21*(1), 1–16. https://doi.org/10.1016/j.infoandorg.2010.11.001

Sedlmeir, J., Huber, J., Barbereau, T. J., Weigl, L., and Roth, T. (2022). "Transition Pathways towards Design Principles of Self-Sovereign Identity," *Forty-Third International Conference on Information Systems*.

Sedlmeir, J., Smethurst, R., Rieger, A., and Fridgen, G. (2021). "Digital Identities and Verifiable Credentials," *Business & Information Systems Engineering*, *63*(5), 603–613. https://doi.org/10.1007/s12599-021-00722-y

Swanson, E. B., and Ramiller, N. C. (1997). "The Organizing Vision in Information Systems Innovation," *Organization Science*, *8*(5), 458–474. https://doi.org/10.1287/orsc.8.5.458

Swanson and Ramiller. (2004). "Innovating Mindfully with Information Technology," *MIS Quarterly*, *28*(4), 553–584. https://doi.org/10.2307/25148655

W3C. (2022). *Verifiable Credentials Data Model v1.1*. URL: https://www.w3.org/TR/vc-data-model/

Wang, P. (2010). "Chasing the Hottest IT: Effects of Information Technology Fashion on Organizations," *MIS Quarterly*, 24. https://doi.org/10.2307/20721415

Wang, P., and Swanson, E. B. (2007). "Launching professional services automation: Institutional entrepreneurship for information technology innovations," *Information and Organization*, *17*(2), 59–88. https://doi.org/10.1016/j.infoandorg.2007.02.001

Wang and Ramiller. (2009). "Community Learning in Information Technology Innovation," *MIS Quarterly*, *33*(4), 709–734. https://doi.org/10.2307/20650324

Weigl, L., Barbereau, T. J., Rieger, A., and Fridgen, G. (2022). "The Social Construction of Self-Sovereign Identity: An Extended Model of Interpretive Flexibility," in *Proceedings of the 55th Hawaii International Conference on System Sciences (HICSS)*.

Yin, R. K. (2009). *Case study research: Design and methods*. 4th Edition. Thousand Oaks: SAGE.

RP8: Roth, T., Rieger, A., & Hoess, A. (2024). **From Mutualism to Amensalism: A Case Study of Blockchain and Digital Identity Wallets.** In B. Shishkov (Ed.), *Business Modeling and Software Design (Forthcoming)*. Springer Nature Switzerland.

From Mutualism to Amensalism: A Case Study of Blockchain and Digital Identity Wallets

Tamara Roth✉1,2[0000-0002-9062-1489], Alexander Rieger1,2[0000-0001-7996-4678], and Alexandra Hoess2[0000-0002-8106-9661]

[1] Sam M. Walton College of Business, University of Arkansas, 220 N McIlroy Ave #301, Fayetteville, AR 72701, USA; Troth@walton.uark.edu; ARieger@walton.uark.edu
[2] Interdisciplinary Centre for Security, Reliability, and Trust, University of Luxembourg, 29 Av. John F. Kennedy, 1855 Kirchberg, Luxembourg; alexandra.hoess@uni.lu

Abstract. Innovation with emerging technologies is often challenging. They are still evolving and are often surrounded by unbalanced claims and hyperbole, which give rise to ambiguity and complicate adoption. These difficulties become even more pronounced when organizations attempt to introduce two loosely coupled emerging technologies. Building on a six-year case-study of the European Blockchain Partnership that attempted to simultaneously introduce blockchain and digital identity wallets, we flesh out the evolution their relationship. Our analysis surfaces a complex material-discursive process that first only discursively and later also materially de-coupled the two technologies along three population ecology principles for species interaction: technological mutualism, technological commensalism, and technological amensalism. Our study contributes an information systems perspective on the enactment and evolution of loosely coupled emerging technologies. Moreover, we use insights from population ecology to better explain and understand the underlying mechanisms.

Keywords: Organizing Vision Theory, Emerging IT, Loose Coupling, Mutualism, Commensalism, Amensalism.

1 Introduction

Organizations are in constant need for innovation to keep up with the dynamic changes in their environments [1]. This need turns some into voracious consumers of emerging information technologies (IT). These technologies come to the marketplace with high promises but in an "[often] immature state, puzzling as to [their] benefits, future prospects, and long-term form" [2]. This ambiguity makes emerging IT malleable and leaves room for interpretation regarding their application in an organizational context [3], [4]. Organizations typically use this room to envision how the technology could address pertinent business problematics [5], [6]. Over time, the ensuing sense-making processes may surface important organizational needs and spotlight specific expectations in a so-called organizing vision (OV), i.e., "a focal community idea for the application of information technology in organizations"[2].

Earlier OVs are often incoherent and replete with variegated discursive frames and value-laden buzzwords. This makes it difficult for organizations to assess their true potential [4], [7]. At the same time, the resulting frame diversity allows organization across multiple industries to engage with the IT [3], [4] and can also facilitate a discursive connection to other (emerging) technologies . Parameswaran et al. (2023), for instance, explore complementary frames for emerging technologies that are tightly coupled, i.e., codependent, using the example of RFID tags and RFID readers [8]. Such co-dependent have typically not been developed as a "single-whole" innovation, such as enterprise resource planning systems with their various modularized components [8]. Instead, they are each adopted in two different adopter communities where their joint adoption boosts value creation but where on their own, each IT would have little value [9], [10]. The early stages of this co-dependence are influenced by internal-external influencers who introduce resonant discursive elements into the enacting organization and inform the respective innovation communities about the material outcomes in the organization [8].

Little is known, however, about how these processes play out when the emerging ITs are 'loosely coupled' and each can create substantial value on their own. While singular studies exist that elaborate on the transition pathways of innovations with a similar trajectory, the examples of comparable innovation have a higher degree of materiality than the innovations at hand [11], [12]. We thus engage in a theory-building effort and ask the following research question:

How can organizations in enactment fields discursively and materially navigate loose coupling between emerging ITs?

To build our theory, we conduct an inductive longitudinal case study of the European Blockchain Services Infrastructure (EBSI) [13], [14], which brought together two loosely coupled emerging ITs: blockchain technology and digital identity wallets. Since all three authors of this work were involved with EBSI in different functions over the last six years, we could gain particularly rich insights into how the EBSI project made sense of initially overlapping frames between the organizing visions for the two technologies and materialized these frames. We could also observe the further development of this joint materialization once it became clear that blockchain was not required for the success of digital identity wallets and certain members of the wallet innovation community began to advocate for separation.

Our findings from the project are twofold. First, we find that loosely coupled, emerging ITs require continuous sense-making and materialization processes to maintain discursive resonance and preserve material complementarity. Second, we find that these technologies will retain "evidence of separateness and identity" [9] and their individual development, which can affect their co-development. Especially when resonance is difficult to achieve or the community discourses change drastically, the initial mutually beneficial relationship (mutualism) can evolve to benefit only one technology (commensalism) and even actively harm one technology to ensure the survival of the other (amensalism). We translate these findings into a conceptual model for the material-discursive co-enactment of loosely coupled ITs, adding an information systems perspective to innovation with complementary technologies that have a higher degree of material malleability.

The rest of the paper is structured as follows. The theoretical background section provides an overview of the key concepts. The research method section then presents details on our case study, data collection and analysis. In the next section, we present the insights from our case study before we synthesize our insights into a conceptual model in the discussion section. After discussing theoretical contributions and practical implications, we present boundary conditions and conclude with a summary of key insights.

2 Theoretical Background

2.1 Sense-making of IT Organizing Visions

Organizing visions are typically created by innovation communities and aim to provide an explanation for the use and function of emerging information technologies beyond rational-economic considerations [15], [16]. They provide a joint account of "the innovation's existence and purpose relative to its broader social, technical, and economic context" [2]. Their goal is to reduce uncertainty concerning an emerging IT through extensive innovation community sense-making. This sense-making gauges the emerging IT's potential to address specific business problematics and envisions various other uses based on the IT's alleged technical capabilities [3], [4]. The resulting interpretations often imbue the organizing vision with wishful and unbalanced claims that manifest in variegated discursive frames, i.e., linguistic constructs that produce specific meaning, and value-laden buzzwords [4]. While these frames and buzzwords can help the IT achieve contagion, they limit the organizing vision's coherence and can be a source of confusion [3], [5], [17].

Organizations interested in enacting emerging technologies thus need to engage in their own sense-making processes to cut through the thicket of discursive frames and buzzwords [4]. The goals of this organization-level sense-making are typically the same as those of community-level sense-making: (1) interpretation, i.e., gauging the usefulness of specific discursive frames; (2) legitimation, i.e., demonstrating the capability of the emerging IT to address pertinent business problematics; and (3) mobilization, i.e., gaining support and momentum for further diffusion of the IT organizing vision [2], [7], [8]. Organization-level sense-making often benefits from early material enactment of the organizing vision, which helps organizations determine if specific discursive frames should be retained or discarded [3], [18]. This materialization of the discourse can transpire in different forms, ranging from text, media, and intonations to artifacts and implementations. In whichever form, it is relevant to better understand the practical implications of the produced meaning [19].

Organizational sense-making processes are often accompanied by sense-giving, sense-taking, and sense-breaking processes [20]. Sense-giving pushes specific discursive frames that align with interpretations of trusted sense-givers [3], [21], [22]. Sense-taking imports discursive frames relevant to achieving desired organizational outcomes

[20], [22], [23]. Sense-breaking, in turn, allows to remove dissonant elements when the selected frames do not resonate with the wider organizational context [4].

2.2 Loose Coupling and Population Ecology Principles of Species Interaction

Organizing visions are typically created for single-whole innovations. However, they can also be constructed for two ITs when they have a high degree of (perceived) complementarity [8]. A good example are co-dependent technologies, such as RFID chips and readers that are tightly coupled and depend on co-enactment in different user communities [8], [9], [10]. However, joint organizing visions may also emerge for independent and loosely coupled technologies that can be enacted separately [24], [25], [26].

Loose coupling is often defined as "elements [of a system] that are responsive but retain evidence of separateness and identity [where they] affect each other […] suddenly (rather than continuously), occasionally (rather than constantly), negligibly (rather than significantly), indirectly (rather than directly), and eventually (rather than immediately)" [9]. It can also be defined according to the responsiveness and distinctiveness of the elements. Where elements are responsive but not distinct, the system is tightly coupled. Where they are distinct but not responsive, the system is considered decoupled. Only where systems are both responsive and distinct, they are loosely coupled [9], [25]. Loose coupling is possible on a material level, which is typically not influenced by community discourse, but also on a discursive level, which often derives inspiration from the innovation community [9], [10].

Loosely coupled technologies often behave in a way that mirrors basic population ecology principles for species interaction, that is, how certain factors influence their interaction [27], [28] and [29]. For instance, when two technologies benefit from being combined, the relationship can be described as technological mutualism [27], [28], [30]. When only one technology benefits but the other is unaffected, the relationship can be described as technological commensalism. This often happens when a host technology functions as a springboard for the commensal technology [27], [28], [31] . Technology amensalism emerges when one technology is actively inhibited, for instance due to bad reputation, but the other technology is not [32], [33].

2.3 The Co-evolution of Blockchain Technology and Digital Identity Wallets

Two technologies that are particularly suited for the study of co-enactment of two loosely coupled emerging technologies are blockchain and digital identity wallets. Blockchains are distributed databases that allow a network of so-called blockchain nodes to keep a synchronized state of the database [34], [35]. The basic ordering element of the database are blocks that are connected via cryptographic hash functions, which allows for the transparent tracing of transactions [36], [37], [38]. Digital identity wallets, in turn, allow users to collect secure digital credentials, and selectively present the identity attributes in these credentials [39], [40], [41], [42].

Originally, the two technologies emerged from a similar technological 'niche' shaped by libertarian ideals [11], [43]. This niche positioned blockchain as the only technology that could deliver the 'trust' infrastructures and revocation registries required to verify the authenticity and validity of digital identity attributes [11], [42], [43], [44]. Over time, however, it became clear that blockchain may have been a good starting point but is no essential component [11], [42]. Digital credentials, for instance, do not need to be stored on a blockchain to be verifiable and to ensure their integrity [42], [45], [46]. These shared beginnings combined with later parting make blockchain and digital identity wallets appealing candidates to address our research question.

3 Research Method

3.1 Case Selection

To investigate how organizations discursively and materially navigate loose coupling in the co-enactment of emerging ITs – including changes in their relationship – we conduct a case-study of the European Blockchain Partnership (EBP). The EBP was established in 2018 between the European Commission and the EU's member states (plus Liechtenstein and Norway) with the objective of establishing a blockchain-based infrastructure – the European Blockchain Services Infrastructure (EBSI) – for delivering cross-border public services.

Soon after its creation, the EBP created a working group focused on using EBSI to support the issuance and verification of digital credentials. This group developed an identity framework that other groups could use to issue various credentials, such as digital (university) diplomas and social security passes. EBSI's digital diploma use case received particular attention when the EBP launched an early-adopter program in the beginning of 2021. Since the project involves both blockchain and digital identity wallets, it offered particularly rich insights into the enactment of loosely coupled emerging ITs.

3.2 Data Collection

For our case study, we collected data from three different sources [13]: interviews, documentation, and participant observations. Interviews were our primary source of evidence and we conducted them in three waves to "minimize the elapsed time between the events of interest and the collection of data" [47]. Specifically, we conducted a first set of 7 interviews with EBP members, member state governments, and technology partners (incl. infrastructure operators) in the fall of 2020 to explore the EBP's view on blockchain and digital identity wallets. These interviews suggested mounting (discursive) tensions from the loose coupling of the two technologies. Over time, these tensions intensified and dominated EBSI's development. To surface the EBP's sense-making and response to these tensions, we interviewed another 21 EBP members and partners in the summer and fall of 2022 (wave 2), a third set of six interviews in the spring of 2023 (wave 3)(Table 1).

Our informants included European Commission representatives, delegates from national and local governments, technology providers, and universities (Table 1). We sampled our informants based on their involvement with EBSI in general and the diploma use case in particular [47]. We focused on interviewees who were highly "knowledgeable about" the case [47] and

All our interviews were semi-structured and followed a logical sequence [47]. We first asked our informants why and how they became involved with the EBP. We then segued to questions about their initial expectations of the interplay between blockchain and digital identity wallets and how they perceived the EBP's implementation process. Our last (set of) questions prodded our informants to critically reflect on how their perception of the mutual relevance of blockchain and digital identity wallets evolved over time. We audio-recorded and transcribed all interviews. They took 56 minutes on average.

Table 1. Overview of the conducted interviews.

	Number of interviewed experts			
	European Commission	National & local governments	Technology partners	Piloting Organizations
Wave 1 Fall 2020	1	3	3	-
Wave 2 Fall & Summer 2022	5	8	5	3
Wave 3 Spring 2023	-	2	3	1

We complemented these interviews with internal and publicly available project documents [13]. The internal documents ranged from meeting presentations over legal assessments and internal project reports to technical documentation. The publicly available documentation included blog posts & other marketing material, press releases, public presentations, and public reports (Table 2).

Table 2. Overview of the collected project documents.

	Types of documents	**Total number of pages**
Internal documents	Internal presentations, legal assessments, internal project reports, technical documentation	210+ pages
Public documents	Blog posts & other marketing material, press releases, public presentations, public reports	160+ pages

Our third source of evidence were participant observations. All authors of this study were actively involved with the EBP in different roles and regularly attended EBP meetings dedicated to different aspects of EBSI. More specifically, the second author of this work became involved with the EBP in October 2018 as a national representative for EBP's technical advisory group and occasionally attended meetings dedicated to the identity framework and the digital diploma use case. From March 2021 to March 2024, both the first and second author were involved with one of the national early-adopter projects for the digital diplomas use case. The third author of this work joined the project in November 2021 and then regularly attended meetings of the EBP's technical, policy and use case group. Moreover, they participated in strategic negotiation meetings regarding the future of blockchain and digital identity wallets.

Throughout these meetings, the observing authors took notes and collected presentations and protocols for later analysis. Overall, our participant observations provided us with rich insights into how the EBP made sense of a joint organizing vision for blockchain and digital identity wallets and materialized a loose coupling between these technologies.

3.3 Data Analysis

Following our data collection, we retraced how the EBP made sense of the joint organizing vision for blockchain and digital identity wallets and materialized selected complementary frames. We also analyzed how this discursive-material complementarity developed over the course of the project. For this purpose, we performed a three-stage coding process [48], [49].

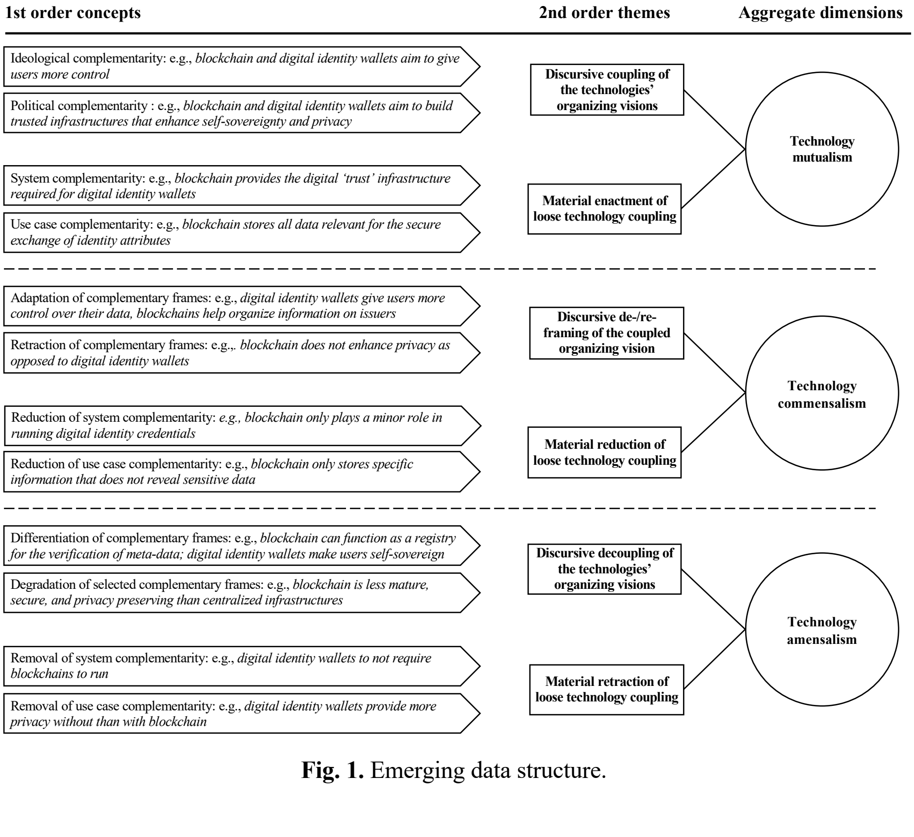

1st order concepts
2nd order themes
Aggregate dimensions
Ideological complementarity: e.g., *blockchain and digital identity wallets aim to give users more control*
Political complementarity : e.g., *blockchain and digital identity wallets aim to build trusted infrastructures that enhance self-sovereignty and privacy*
System complementarity: e.g., *blockchain provides the digital 'trust' infrastructure required for digital identity wallets*
Use case complementarity: e.g., *blockchain stores all data relevant for the secure exchange of identity attributes*
Discursive coupling of the technologies' organizing visions
Material enactment of loose technology coupling
Technology mutualism
Adaptation of complementary frames: e.g., *digital identity wallets give users more control over their data, blockchains help organize information on issuers*
Retraction of complementary frames: e.g.,. *blockchain does not enhance privacy as opposed to digital identity wallets*
Reduction of system complementarity: *e.g., blockchain only plays a minor role in running digital identity credentials*
Reduction of use case complementarity: e.g., *blockchain only stores specific information that does not reveal sensitive data*
Discursive de-/re-framing of the coupled organizing vision
Material reduction of loose technology coupling
Technology commensalism
Differentiation of complementary frames: e.g., *blockchain can function as a registry for the verification of meta-data; digital identity wallets make users self-sovereign*
Degradation of selected complementary frames: e.g., *blockchain is less mature, secure, and privacy preserving than centralized infrastructures*
Removal of system complementarity: e.g., *digital identity wallets to not require blockchains to run*
Removal of use case complementarity: e.g., *digital identity wallets provide more privacy without than with blockchain*
Discursive decoupling of the technologies' organizing visions
Material retraction of loose technology coupling
Technology amensalism

Fig. 1. Emerging data structure.

In a first, open coding round, we focused on theme discovery in the interviews and project documents and assigned initial codes to statements we considered relevant. We were especially interested in themes related to discursive sense-making of complementary frames and their materialization but maintained an open mind. Based on the identified themes, we then performed a second, axial coding round. This second round helped us to refine our codes and aggregate them into overarching constructs and identify interdependencies between these constructs [48], [49]. The constructs that emerged over the second coding round showed differences in both the discursive sense-making and material enactment over time and surfaced marked differences in the relationship between the two focal technologies.

We then refined these constructs and their interdependencies by iterating between our codes and the pertinent theories on loose coupling [9], [24], [25] and population ecology principles of species interaction [22], [23], [24]. As a last step, we conducted selective coding to fill-in the gaps of our theoretical insights. Throughout the axial and selective coding process, we triangulated our interview transcripts and project documents with our participant observations to enhance construct validity and generalizability of our research [14], [50]. Overall, our coding process produced more than 2300 codes, which we managed using the MAXQDA software kit. Figure 1 summarizes our findings of the qualitative coding in a data structure.

4 Emerging Theoretical Framework

The EBP's engagement with blockchain and digital identity wallets can be bracketed into three phases. While the first phase was dominated by attempts to frame and materialize a coupled organizing vision (mutualism phase), challenges along the development process soon required discursive and material de-coupling to maintain legitimacy (commensalism phase). In a third phase, digital identity wallets were introduced into a revision of the European Union's regulation on electronic identification, authentication and trust services (eIDAS), which afforded a high degree of legitimization and mobilization. But the revised regulation cut the connection to blockchain, inevitably demanding that the EBP respond to a competing, de-coupled organizing vision for digital identity wallets (amensalism phase).

4.1 Establishing Mutualism between the Two Emerging ITs

When the EBP was founded in April 2018, its first activities were focused on identifying cross-border public services that could be supported by a blockchain-based infrastructure. Throughout this process of finding resonant discursive frames, several member states began to promote a coupled organizing vision between blockchain and digital identity wallets that had been developed by the so-called Internet Identity Workshop community. This coupled organizing vision painted blockchain and digital identity wallets as uniquely complementary technologies that would allow users to regain control over their digital identities and establish 'self-sovereign identities'. Resonance was especially high with those member states that felt that the EU's current eIDAS framework was difficult to implement. Blockchain and digital identity wallets provided a welcome departure from this framework – not least because they aligned well with political priorities of the van-der-Leyen presidency, such as data privacy and digital sovereignty. One EBP member state representative explains this perceived technological mutualism:

> *"We really believe[d] that the ledgers and the network supported by a blockchain can play a very important role to protect the privacy of citizens and to enable the self-sovereign identity of the user."*

In April 2019, the early sense-making efforts resulted in the creation of a EBP working group for the development of a new digital identity framework based on blockchain and digital identity wallets. Drawing on the organizing vision promoted by the Internet Identity Workshop community, the new framework was nicknamed the European Self-Sovereign Identity Framework (ESSIF). The plan was for ESSIF to inform and support various EBSI services focused on the issuance and verification of identity documents. During its early days, the ESSIF working group was *"enthusiastic about blockchain as a technology"* and perceived a high degree of complementarity between the two technologies. Over the course of the next year, the ESSIF working group set out to materialize this perceived complementarily in a conceptual architecture. This architecture anchored blockchain as a core 'trust' infrastructure that would store various data required for the secure issuance and verification of identity attributes. For instance, this data included cryptographic identifiers for issuers, issuer accreditation organizations, and credential holders, as well as data in or about the credentials. A European Commission representative explains:

> *"We thought that aside of using blockchain for storing information about accreditation organizations, which accredits the issuers to issue specific credentials, we can also store some additional information such as decentralized digital identifiers of natural persons."*

4.2 Handling Commensalism between the Two Emerging ITs

By early 2021, the EBP had decided to implement ESSIF in EBSI and pilot it for the exchange of digital university diplomas. However, the piloting phase soon surfaced problems with the coupled organizing vision that led to a phase of technological commensalism, in which increased functionality and budget were directed towards digital identity wallets. Increased functionality resulted especially from difficulties reconciling the storage of personal information such as digital credentials and identifiers on the blockchain with the requirements of the EU's General Data Protection Regulation (GDPR). This dissonance first dawned on the ESSIF working group when they began to develop specifications for the information that should be stored on EBSI. This specification exercise included a survey of how other projects approached the implementation of 'self-sovereign identities', which revealed that digital credentials did not need to be stored on a blockchain. On the contrary, such storage would contradict one of the core principles of self-sovereign identities, namely the protection of the user's privacy. One EBP member state representative reflects:

> *"We did consider saving a hash of the [credential] on the blockchain. But we soon discarded this idea for many reasons. One of*

> *them is that well [...] who knows if in 20 years someone could obtain the original information from a hash. [...] So, we decided to remove that information from the blockchain"*

To reduce the resulting dissonance, the EBP revised EBSI's architecture so that digital credentials would only be stored in digital identity wallets, but not on EBSI. To salvage the rest of the vision, the ESSIF working group doubled down on those data for which they perceived continued complementarity, including identifiers for credential issuers and holders. But the storage of holder identifiers was again problematic from a privacy perspective, which became evident during a formal GDPR assessment. The assessment unequivocally concluded that a natural person's identifiers should also not be stored on a blockchain. The ESSIF working group was now again forced to engage in a material dissonance reduction process that *made "the blockchain layer become thinner and thinner. Much more things are [now] happening outside the blockchain network because of privacy issues".* The resulting ESSIF architecture only used EBSI as a registry for trusted issuer information and put digital identity wallets center-stage. One European Commission representative recounts:

> *"We went through a long, long, long battle with the data protection officers and lawyers and policymakers. And we've understood if we would allow to store the decentralized identifiers of natural persons on the ledger, on EBSI, the EBSI service wouldn't be GDPR-compliant. [But] we don't really need to store it on the ledger. We can keep it on the wallet side, and that's the new version of conformance."*

These material compromises inevitably led to problems with how EBSI had been marketed to the member states. The European Commission responded with a marketing campaign that promoted an adapted organizing vision that better reflected the material reality. EBSI officially became a trusted issuer registry.

4.3 Navigating Amensalism between the Two Emerging ITs

In parallel to the EBP's efforts, the European Commission had announced plans to rework the eIDAS identity framework and regulation in October 2020. Eight months later, in June 2021, the European Commission revealed a proposal for a new framework and regulation. The proposal had a substantial part dedicated to the use of digital identity wallets but did not mention blockchain as a preferred technology for implementing trust infrastructures. The proposal hit the EBP hard. Some chose to maintain a positive attitude and promoted the interpretation that blockchain was not explicitly excluded. Other EBP members were more skeptical as they sensed open resentment against blockchain by the eIDAS expert groups. These groups saw blockchain as an inferior alternative to the eIDAS trust registries already in place. A national EBP representative explains:

> *"I would say that especially the people that created eIDAS are not all positive about blockchain [...] The IT people who really developed it, they can show that there is a system that is working. They are not necessarily convinced why we would need something new."*

As the eIDAS revision moved through the EU's legislative process, the uncertainty around blockchain's future role for digital identity wallets intensified, plunging the EBP into a phase of technological amensalism, where digital identity wallets benefitted from having a 'host' technology that helped demonstrate their viability but blockchain suffered from the relationship. In February 2022, the European Commission then published a first outline for the reference architecture framework under eIDAS 2.0. However, blockchain was again not mentioned. Instead, the European Commission argued that the regulation should be technology neutral, which provoked a sense-breaking process and the destruction of the EBP's coupled organizing vision. One national EBP representative explains:

> *"Do I need a blockchain for a digital identity? [...] The eIDAS revision has given a lot of space to this discussion. Because there is a clear will to break away from [blockchain] and the revision is also supposed to be technology-neutral, [...], there is no further talk about blockchain."*

To cope with the looming break-down of the coupled organizing vision, the EBP engaged into a soul-searching process and feverish attempted to find a new organizing vision for blockchain and EBSI. At this stage, the EBP questioned digital identity wallets altogether. Some even perceived them as a "*child that has outgrown its parent [blockchain]'s home."* As a first measure, the EBP again reframed EBSI's presentation, dropping all mentioning of 'self-sovereign identity' in favor of a framing EBSI as a multi-purpose registry for trustworthy information. Furthermore, the EBP doubled down on other use cases that did not require digital identity wallets, such as product traceability. A European Commission explains:

> *"At the end, EBSI is ultimately used as a source of trust. That's the main purpose of blockchain: to build resilient lists that allow everyone from everywhere to get the required data to verify some other information."*

5 Discussion

We now elaborate on the insights we gained from our analysis and describe the observed discursive and material processes in the co-enactment of blockchain and digital identity wallets from an initially mutualistic to a commensalistic and later amensalistic relationship. We also explain how these relationship changes influenced the loose coupling of the two technologies.

5.1 Tentative Model

Our core contribution is a conceptual model of the discursive-material processes underlying the co-enactment of loosely coupled emerging ITs (Figure 2). The model builds on theories about the creation and diffusion of (co-dependent) organizing visions [2], [3], [4], [8], loose coupling of organizational systems [9], [24], and population ecology principles of species interaction transferred to technology-technology and technology-system interaction [27], [28], [32], [33].

The co-enactment will usually start with a sense-giving process by the innovation communities responsible for the creation of organizing visions for two single-whole emerging technologies. Sometimes, these innovation communities are grounded in the same technological 'niche', which can increase the degree of complementary discursive frames [8]. Blockchain technology and digital identity wallets, for instance came from the same libertarian niche that imbued their organizing visions with various complementary frames, such as self-sovereignty and privacy [11], [44].

Once organizations in enactment fields detect complementarities between selected discursive frames in both organizing visions, they can engage in a process of discursive sense-taking that more systematically extracts and discursively couples complementary frames [8], creating a relationship of technology mutualism [28]. In a next step, they can then materially enact these coupled frames [7]. Where this enactment does not resonate well with the wider organizational context, the frames either need to be adapted (where possible) or retracted. Otherwise, unsuccessful coupling frames may raise questions about the technologies' complementarity [4]. The enactment process may also be complicated by the continued development of the organizing visions for each of the individual technologies, especially when other enacting organizations chose different adaptation or retraction strategies.

Since it may often be difficult to enact all (purported) complementarities, the technologies may naturally become more loosely coupled over time. For instance, blockchain became a 'host' technology for digital identity wallets during the second phase of the EBSI project, turning their relationship from technology mutualism to technology commensalism. The commensal technology, in this case digital identity wallets, profited from the 'host' technology blockchain, while the host remained unaffected [28], [31]. Condensed into a conjecture, we can state:

Conjecture 1: Loosely coupled emerging technologies will become commensalistic if complementary frames are difficult to enact in the wider organizational environment.

Should the re-framed joint organizing vision still prove difficult to reconcile with the wider organizational context despite looser coupling and a clear host-commensal distinction, organizations can enter a discursive sense-breaking process. Such sense-breaking can be exacerbated when, for instance, one innovation community actively opposes the loose coupling and counteracts complementarities with the commensal technology. This happened during the EBSI project when the eIDAS working groups actively opposed coupling digital identity wallets with blockchain. In response, the EBP reduced the technologies' loose coupling to a minimum and blockchain once again became a single-whole technology in search of a use case. On a discursive level, the relationship between the technologies changed to technology amensalism, where one technology is negatively affected while the other remains neutral [32], [33]. Materially, the relationship remained commensalistic. Condensed into a conjecture, we can state:

Conjecture 2: Organizations in enactment fields cannot resolve an amensalistic relationship between loosely coupled emerging technologies as long as one of the innovation communities works against the coupling.

5.2 Theoretical Contributions

This research contributes to the literature on the enactment of emerging ITs by unpacking the discursive-material processes that initiate (loose) coupling between such technologies in a joint organizing vision and influence the evolution of their relationship during their co-enactment. While organizing visions are a widely studied topic in information systems [2], [3], [4], [16], studies on the co-enactment of two complementary, emerging ITs are scarce [8]. Moreover, loose coupling has been primarily researched between organizational processes and technologies but not between organizing visions. Our analysis of the EBSI project thus not only demonstrates the challenges involved in enacting a coupled organizing vision for two emerging ITs, but also elaborates on the difficulties navigating loose coupling between two immature technologies prone to change.

More specifically, we add to literature on organizing visions [2], [3], [4] by demonstrating how organizational sense-making [21], [22] and population ecology [27], [28], [30] lenses can be integrated to describe and navigate the implementation of loosely coupled emerging ITs. In particular, we surface three coupling types - technology mutualism, technology commensalism, and technology amensalism - that highly depend on the degree of discursive and material complementarity between the emerging ITs. We also describe how the coupling type may change for the worse in response to enactment challenges and discursive opposition to the coupling in the organizing visions of the individual technologies. Where such changes occur, enacting organizations can respond with discursive and material changes to salvage the remaining complementarities or to emphasize the distinctiveness of one of the technologies as a single-whole innovations to guarantee its survival. But our research also indicates that once the process of decoupling is initiated, it may be difficult to stop and reverse.

5.3 Practical Implications

Our findings suggest that managers interested in emerging information technologies should be careful when it comes to investing into bundles of such technologies - especially when they are only loosely coupled. While such a shotgun marriage can be beneficial in legitimizing the bundled technologies and increasing their mobilization potential, it can quickly degenerate once the honeymoon phase is over, and it becomes apparent that initially perceived complementarities are hard to realize. In these instances, organizations need to engage in discursive and material 'marriage counseling' to set aside differences and ensure a shared bedrock of resonance.

However, these counseling activities may not always be successful. Emerging ITs are often still evolving, and sometimes, they may be appropriated by new conversants in the innovation community that are not interested in maintaining the originally envisioned coupling. In these cases, organizations need to act decisively and question if

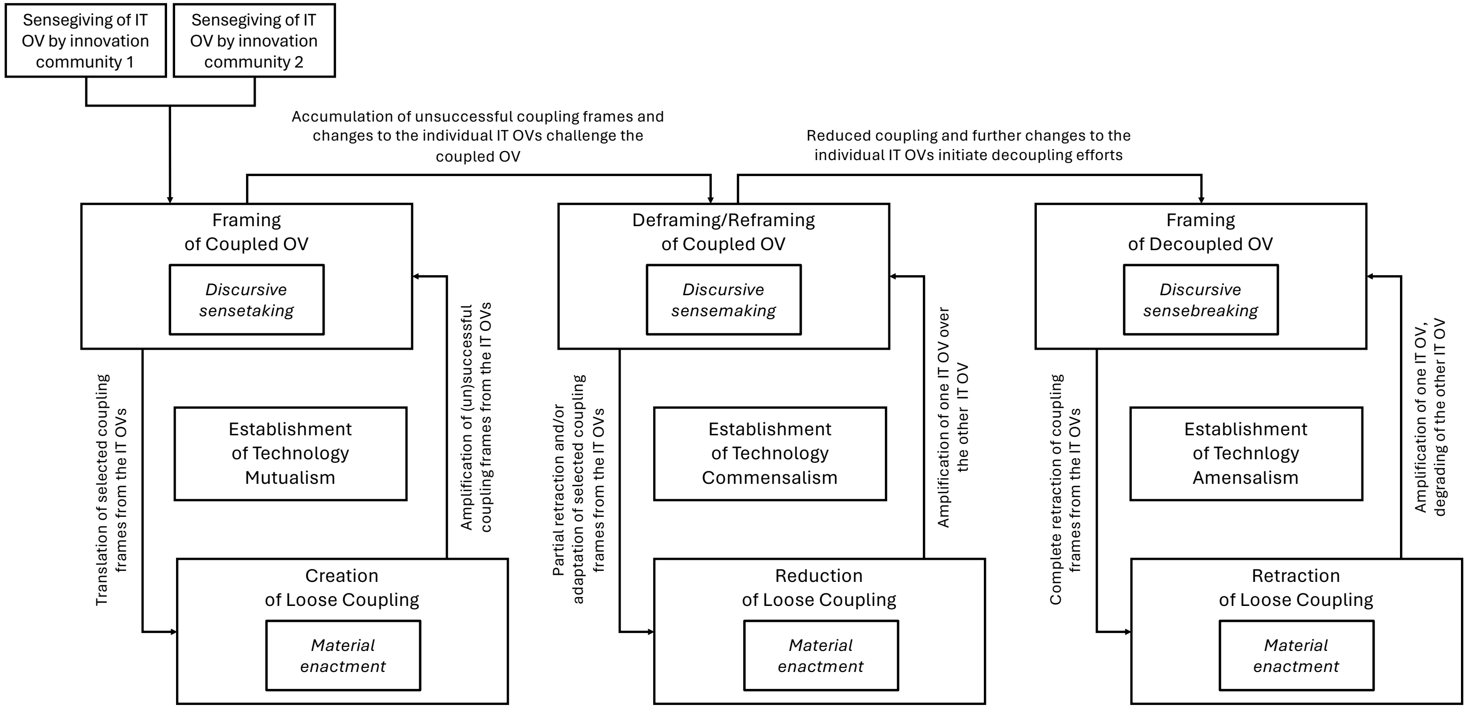

Sensegiving of IT OV by innovation community 1
Sensegiving of IT OV by innovation community 2
Accumulation of unsuccessful coupling frames and changes to the individual IT OVs challenge the coupled OV
Reduced coupling and further changes to the individual IT OVs initiate decoupling efforts
Framing of Coupled OV
Discursive sensetaking
Deframing/Reframing of Coupled OV
Discursive sensemaking
Framing of Decoupled OV
Discursive sensebreaking
Translation of selected coupling frames from the IT OVs
Amplification of (un)successful coupling frames from the IT OVs
Partial retraction and/or adaptation of selected coupling frames from the IT OVs
Amplification of one IT OV over the other IT OV
Complete retraction of coupling frames from the IT OVs
Amplification of one IT OV, degrading of the other IT OV
Establishment of Technology Mutualism
Establishment of Technology Commensalism
Establishment of Technlogy Amensalism
Creation of Loose Coupling
Material enactment
Reduction of Loose Coupling
Material enactment
Retraction of Loose Coupling
Material enactment

Fig. 2. Conceptual Model for the Co-enactment of Loosely Coupled Emerging ITs.

they want and need to keep both technologies. These decisions can be difficult, but they are essential for giving the technology that remains a more promising way forward.

6 Conclusion

Based on insights from the European Blockchain Partnership, our study derives a model for the co-enactment of loosely coupled emerging ITs that possess a lower level of materiality than typical technical innovations. Our model illustrates the challenges involved in co-enacting such ITs and demonstrates how insights from population ecology can help better explain and understand the underlying material-discursive processes that initiate the loose coupling and drive the evolution of their relationship in an organizational context.

Acknowledgements. This research was funded in part by the Luxembourg National Research Fund (FNR) and PayPal, PEARL grant reference 13342933/Gilbert Fridgen, grant reference NCER22/IS/16570468/NCER-FT, and grant reference 14783405, as well as Luxembourg's Ministry for Digitalisation. For the purpose of open access, and in fulfillment of the obligations arising from the grant agreement, the authors have applied a Creative Commons Attribution 4.0 International (CC BY 4.0) license to any Author Accepted Manuscript version arising from this submission.

Disclosure of Interests. The authors have no competing interests to declare.

References

[1] E. Gaspary, G. L. D. Moura, and D. Wegner, "How does the organisational structure influence a work environment for innovation?," *International Journal of Entrepreneurship and Innovation Management*, vol. 24, no. 2–3, pp. 132–153, Jan. 2020, doi: 10.1504/IJEIM.2020.105770.

[2] E. Swanson and N. Ramiller, "The Organizing Vision in Information Systems Innovation," *Organization Science*, vol. 8, no. 5, pp. 458–474, Oct. 1997, doi: 10.1287/orsc.8.5.458.

[3] S. M. Miranda, I. Kim, and J. D. Summers, "Jamming with Social Media: How Cognitive Structuring of Organizing Vision Facets Affects IT Innovation Diffusion," *MIS Quarterly*, vol. 39, no. 3, pp. 591–614, 2015, doi: 10.25300/MISQ/2016/40.2.02.

[4] S. M. Miranda, D. D. Wang, and C. A. Tian, "Discursive Fields and the Diversity-Coherence Paradox: An Ecological Perspective on the Blockchain Community Discourse," *MIS Quarterly*, vol. 46, no. 3, pp. 1421–1452, 2022, doi: 10.25300/MISQ/2022/15736.

[5] W. L. Currie, "The organizing vision of application service provision: a process-oriented analysis," *Information and Organization*, vol. 14, no. 4, pp. 237–267, Oct. 2004, doi: 10.1016/j.infoandorg.2004.07.001.

[6] N. C. Ramiller and E. B. Swanson, "Organizing Visions for Information Technology and the Information Systems Executive Response," *Journal of Management Information Systems*, vol. 20, no. 1, pp. 13–50, 2003.

[7] E. J. Davidson, C. S. Østerlund, and M. G. Flaherty, "Drift and shift in the organizing vision career for personal health records: An investigation of innovation discourse dynamics,"

Information and Organization, vol. 25, no. 4, pp. 191–221, Oct. 2015, doi: 10.1016/j.infoandorg.2015.08.001.

[8] S. Parameswaran, R. Kishore, X. Yang, and Z. Liu, "Theorizing about the Early-Stage Diffusion of Codependent IT Innovations," *Journal of the Association for Information Systems*, vol. 24, no. 2, pp. 379–429, Jan. 2023, doi: 10.17705/1jais.00789.

[9] J. D. Orton and K. E. Weick, "Loosely coupled systems: A reconceptualization," *The Academy of Management Review*, vol. 15, no. 2, pp. 203–223, 1990, doi: 10.2307/258154.

[10] E. Øvrelid and B. Bygstad, "Exploring loose coupling in system interaction," *Selected Papers of the IRIS, Issue Nr 7 (2016)*, Jan. 2016, [Online]. Available: https://aisel.aisnet.org/iris2016/5

[11] J. Sedlmeir, T. J. Barbereau, J. Huber, L. Weigl, and T. Roth, "Transition Pathways towards Design Principles of Self-Sovereign Identity," in *ICIS 2022 Proceedings*, 2022. Accessed: Mar. 29, 2024. [Online]. Available: https://aisel.aisnet.org/icis2022/is_implement/is_implement/4

[12] F. W. Geels and J. Schot, "Typology of sociotechnical transition pathways," *Research Policy*, vol. 36, no. 3, pp. 399–417, Apr. 2007, doi: 10.1016/j.respol.2007.01.003.

[13] R. K. Yin, *Case study research: Design and methods*, 6th ed. SAGE Publications, Inc, 2017. [Online]. Available: https://us.sagepub.com/en-us/nam/case-study-research-and-applications/book250150

[14] K. M. Eisenhardt, "What is the Eisenhardt Method, really?," *Strategic Organization*, vol. 19, no. 1, pp. 147–160, 2021, doi: https://doi.org/10.1177/1476127020982866.

[15] R. Agarwal and J. Prasad, "The Role of Innovation Characteristics and Perceived Voluntariness in the Acceptance of Information Technologies," *Decision Sciences*, vol. 28, no. 3, pp. 557–582, 1997, doi: 10.1111/j.1540-5915.1997.tb01322.x.

[16] I. Kim and S. Miranda, "20 Years Old but Still a Teenager? A Review of Organizing Vision Theory and Suggested Directions," *PACIS 2018 Proceedings*, Jun. 2018, [Online]. Available: https://aisel.aisnet.org/pacis2018/23

[17] P. Wang and N. C. Ramiller, "Community learning in information technology innovation," *MIS Quarterly*, pp. 709–734, 2009, doi: 10.2307/20650324.

[18] C. Hardy and S. Maguire, "Organizing Risk: Discourse, Power, and 'Riskification,'" *AMR*, vol. 41, no. 1, pp. 80–108, Jan. 2016, doi: 10.5465/amr.2013.0106.

[19] W. J. Orlikowski and S. V. Scott, "What Happens When Evaluation Goes Online? Exploring Apparatuses of Valuation in the Travel Sector," *Organization Science*, vol. 25, no. 3, pp. 868–891, 2014, doi: https://doi.org/10.1287/orsc.2013.0877.

[20] S. Maitlis and M. Christianson, "Sensemaking in Organizations: Taking Stock and Moving Forward," *ANNALS*, vol. 8, no. 1, pp. 57–125, Jan. 2014, doi: 10.5465/19416520.2014.873177.

[21] D. A. Gioia and K. Chittipeddi, "Sensemaking and sensegiving in strategic change initiation," *Strategic Management Journal*, vol. 12, no. 6, pp. 433–448, 1991, doi: 10.1002/smj.4250120604.

[22] K. E. Weick, K. M. Sutcliffe, and D. Obstfeld, "Organizing and the Process of Sensemaking," *Organization Science*, vol. 16, no. 4, pp. 409–421, 2005, doi: 10.1287/orsc.1050.0133.

[23] K. E. Weick, "Sensemaking as an organizational dimension of global change," in *Organizational Dimensions of Global Change: No Limits to Cooperation*, D. L. Cooperrider and

J. E. Dutton, Eds., SAGE Publications, Inc, 1999, pp. 39–56. [Online]. Available: https://sk.sagepub.com/books/organizational-dimensions-of-global-change

[24] N. Berente and Y. Yoo, "Institutional Contradictions and Loose Coupling: Postimplementation of NASA's Enterprise Information System," *Information Systems Research*, vol. 23, no. 2, pp. 376–396, Jun. 2012, doi: 10.1287/isre.1110.0373.

[25] V. L. Mitchell and R. W. Zmud, "The Effects of Coupling IT and Work Process Strategies in Redesign Projects," *Organization Science*, vol. 10, no. 4, pp. 424–438, 1999.

[26] S. Nambisan and Y. Luo, "Toward a loose coupling view of digital globalization," *J Int Bus Stud*, vol. 52, no. 8, pp. 1646–1663, Oct. 2021, doi: 10.1057/s41267-021-00446-x.

[27] M. Coccia and J. Watts, "A theory of the evolution of technology: Technological parasitism and the implications for innovation magement," *Journal of Engineering and Technology Management*, vol. 55, p. 101552, Jan. 2020, doi: 10.1016/j.jengtecman.2019.11.003.

[28] M. Coccia, "Classification of Innovation Considering Technological Interaction." Rochester, NY, Jul. 24, 2018. Accessed: Apr. 20, 2024. [Online]. Available: https://papers.ssrn.com/abstract=3218945

[29] L. Gastaldi, F. P. Appio, D. Trabucchi, T. Buganza, and M. Corso, "From mutualism to commensalism: Assessing the evolving relationship between complementors and digital platforms," *Information Systems Journal*, vol. n/a, no. n/a, pp. 1–47, 2023, doi: 10.1111/isj.12491.

[30] W. P. Barnett, "The Organizational Ecology of a Technological System," *Administrative Science Quarterly*, vol. 35, no. 1, pp. 31–60, 1990, doi: 10.2307/2393550.

[31] C. W. I. Pistorius and J. M. Utterback, "Multi-mode interaction among technologies," *Research Policy*, vol. 26, no. 1, pp. 67–84, Mar. 1997, doi: 10.1016/S0048-7333(96)00916-X.

[32] B. A. Sandén and K. M. Hillman, "A framework for analysis of multi-mode interaction among technologies with examples from the history of alternative transport fuels in Sweden," *Research Policy*, vol. 40, no. 3, pp. 403–414, Apr. 2011, doi: 10.1016/j.respol.2010.12.005.

[33] G. Zhang, D. A. McAdams, V. Shankar, and M. M. Darani, "Modeling the evolution of system technology performance when component and system technology performances interact: Commensalism and amensalism," *Technological Forecasting and Social Change*, vol. 125, pp. 116–124, Dec. 2017, doi: 10.1016/j.techfore.2017.08.004.

[34] E. W. Ellinger, R. W. Gregory, T. Mini, T. Widjaja, and O. Henfridsson, "Skin the the Game: The Transformational Potential of Decentralized Autonomous Organizations," *MIS Quarterly (Forthcoming)*, 2023, doi: 10.25300/MISQ/2023/17690.

[35] H. Halaburda, N. Levina, and M. Semi, "Digitization of transaction terms as a shift parameter within TCE: strong smart contract as a new mode of transaction governance," *MIS Quarterly (Forthcoming)*, 2023, doi: https://doi.org/10.25300/MISQ/2023/17818.

[36] R. Beck, C. Müller-Bloch, and J. L. King, "Governance in the blockchain economy: A framework and research agenda," *Journal of the Association for Information Systems*, vol. 19, no. 10, pp. 1020–1034, 2018, doi: 10.17705/1jais.00518.

[37] A. Chong, E. Lim, X. Hua, S. Zheng, and C.-W. Tan, "Business on Chain: A Comparative Case Study of Five Blockchain-Inspired Business Models," *Journal of the Association for Information Systems*, vol. 20, no. 9, Sep. 2019, doi: 10.17705/1jais.00568.

[38] R. Ziolkowski, G. Miscione, and G. Schwabe, “Decision problems in blockchain governance: Old wine in new bottles or walking in someone else’s shoes?,” *Journal of Management Information Systems*, vol. 37, no. 2, pp. 316–348, 2020, doi: https://doi.org/10.1080/07421222.2020.1759974.

[39] J. Glöckler, J. Sedlmeir, M. Frank, and G. Fridgen, “A Systematic Review of Identity and Access Management Requirements in Enterprises and Potential Contributions of Self-Sovereign Identity,” *Bus Inf Syst Eng*, Sep. 2023, doi: 10.1007/s12599-023-00830-x.

[40] M. Lacity and E. Carmel, “Self-Sovereign Identity and Verifiable Credentials in Your Digital Wallet,” *MIS Quarterly Executive*, vol. 21, no. 3, Sep. 2022, [Online]. Available: https://aisel.aisnet.org/misqe/vol21/iss3/6

[41] A. Rieger, T. Roth, J. Sedlmeir, G. Fridgen, and A. G. Young, “Organizational Identity Management Policies,” *Journal of the Association for Information Systems (Forthcoming)*, 2024.

[42] J. Sedlmeir, R. Smethurst, A. Rieger, and G. Fridgen, “Digital Identities and Verifiable Credentials,” *Business & Information Systems Engineering*, vol. 63, no. 5, pp. 603–613, 2021, doi: 10.1007/s12599-021-00722-y.

[43] A. Hoess, A. Rieger, T. Roth, G. Fridgen, and A. Young, “Managing Fashionable Organizing Visions: Evidence from the European Blockchain Services Infrastructure,” in *ECIS 2023 Proceedings*, 2023. [Online]. Available: https://aisel.aisnet.org/ecis2023_rp/337

[44] M. C. Lacity, “Blockchain: From Bitcoin to the Internet of Value and beyond,” *Journal of Information Technology*, vol. 37, no. 4, pp. 326–340, 2022, doi: 10.1177/02683962221086300.

[45] A. Kudra, A. Rieger, T. Roth, J. Sedlmeir, G. Fridgen, and A. G. Young, “Digital Identity Wallets,” *University of Arkansas Working Paper*, 2024.

[46] A. Rieger, T. Roth, J. Sedlmeir, L. Weigl, and G. Fridgen, “Not Yet Another Digital Identity,” *Nature Human Behaviour*, vol. 6, no. 1, pp. 3–3, 2022, doi: 10.1038/s41562-021-01243-0.

[47] G. P. Huber and D. J. Power, “Retrospective Reports of Strategic-Level Managers: Guidelines for Increasing Their Accuracy,” *Strategic Management Journal*, vol. 6, no. 2, Art. no. 2, 1985, doi: https://doi.org/10.1002/smj.4250060206.

[48] J. M. Corbin and A. Strauss, “Grounded theory research: Procedures, canons, and evaluative criteria,” *Qual Sociol*, vol. 13, no. 1, pp. 3–21, Mar. 1990, doi: 10.1007/BF00988593.

[49] J. Saldaña, *The Coding Manual for Qualitative Researchers*, Fourth. SAGE Publications Ltd, 2021. Accessed: Apr. 20, 2024. [Online]. Available: https://uk.sagepub.com/en-gb/eur/the-coding-manual-for-qualitative-researchers/book273583

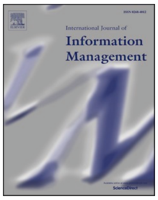
[50] K. M. Eisenhardt, M. E. Graebner, and S. Sonenshein, “Grand Challenges and Inductive Methods: Rigor without Rigor Mortis,” *AMJ*, vol. 59, no. 4, pp. 1113–1123, Aug. 2016, doi: 10.5465/amj.2016.4004.

RP09: Utz, M., Johanning, S., Roth, T., Bruckner, T., & Strüker, J. (2023). **From ambivalence to trust: Using blockchain in customer loyalty programs.** *International Journal of Information Management*, *68*, 102496. https://doi.org/10.1016/j.ijinfomgt.2022.102496
Journal Rating: 41.9 (CiteScore); 5.266 (SNIP)

Contents lists available at ScienceDirect

International Journal of Information Management

journal homepage: www.elsevier.com/locate/ijinfomgt



From ambivalence to trust: Using blockchain in customer loyalty programs

Manuel Utz [a,*], Simon Johanning [b], Tamara Roth [c], Thomas Bruckner [b], Jens Strüker [d]

[a] University of Bayreuth, Faculty of Law, Business & Economics, Universitätsstr. 30, Bayreuth, Germany
[b] Leipzig University, Institute for Infrastructure and Resources Management, Grimmaische Str. 12, Leipzig, Germany
[c] University of Luxembourg, Center for Security, Reliability and Trust, 29 Ave. John F. Kennedy, Luxembourg, Luxembourg
[d] University of Bayreuth, FIM Research Center, Project Group Business & Information Systems Engineering of the Fraunhofer FIT, Universitätsstr. 30, Bayreuth, Germany

ARTICLE INFO

Keywords:
Ambivalence
Blockchain
Customer loyalty
Design Science ResearchDistrust
Trust

ABSTRACT

Global initiatives on climate protection and national sustainability policies are accelerating the replacement of fossil fuels with renewable energy sources. Many electricity suppliers are engaged in efforts to monetize this transition with 'green' services and products, such as Green Electricity Tariffs. These promise customers that their supply includes a specific share of green electricity, yet since electricity suppliers often fail to deliver on those promises, many customers have lost trust in their suppliers. Further information asymmetries may not only exacerbate this loss of trust, but also spark distrust and lead to an overall feeling of ambivalence. Eventually, ambivalent customers may feel inclined to switch suppliers. To prevent this domino effect, electricity suppliers must eliminate ambivalence by increasing customer trust and reducing customer distrust. Here, we discuss how these challenges can be met with a customer loyalty program built on blockchain technology. We developed the program following a Design Science Research approach that facilitated refinement in four iteration and evaluation cycles. Our results indicate that the developed customer loyalty program restores trust, reduces distrust, and resolves customer ambivalence by providing four features: improved customer agency, sufficient and verifiable information, appropriate levels of usability, and unobstructed data access.

1. Introduction

Heightened environmental awareness and a growing need for sustainability have led to various 'green' transformations across multiple sectors, and perhaps nowhere more so than in in the energy industry (Dwivedi et al., 2022; Ågerfalk et al., 2022). These transformations have started to shift power generation from fossil fuels like coal and gas toward Renewable Energy Sources (RES) (Dong, Luo, & Liang, 2018; Hua, Jiang, Sun, & Wu, 2020). Moreover, they change the dynamic of energy consumption by balancing it against the intermittency of many RES (Andoni et al., 2019; Dorfleitner, Muck, & Scheckenbach, 2021). Meanwhile, green electricity has achieved the status of a lifestyle product for many customers; a trend that many electricity suppliers are trying to commercialize with various 'green' services and products (Bogensperger, Zeiselmair, Hinterstocker, & Dufter, 2018; Kley, Lerch, & Dallinger, 2011). Green Electricity Tariffs (GETs) are a case in point (Diaz-Rainey & Ashton, 2011; MacPherson & Lange, 2013; Ozaki, 2011). GETs promise that "some or all of the units of electricity [a] customer buys are 'matched' by units of energy that have been generated from a verified renewable energy source" (Energy, 2013). Although the overall share of RES in the electricity market is steadily increasing (Andoni et al., 2019; Hua et al., 2020), electricity suppliers are not always able to meet these green supply commitments with their own RES. In such cases, they typically purchase 'guarantee of origin' certificates from other RES suppliers (Abad & Dodds, 2020).

The problem with these certificates is that many customers understand neither their nature nor their purpose, which can lead to distrust and fears of 'greenwashing' (Ambrose, 2021; Guo et al., 2014; Mezger, Cabanelas, López-Miguens, Cabiddu, & Rüdiger, 2020). These fears can easily grow into a general feeling of ambivalence (Moody, Galletta, & Lowry, 2014; Moody, Lowry, & Galletta, 2017) that leads customers to question their formerly trusted relationship with their electricity supplier (Arkesteijn & Oerlemans, 2005; Bang, Ellinger, Hadjimarcou, & Traichal, 2000; Hansla, Gamble, Juliusson, & Gärling, 2008). In some cases, customers may even consider switching to a competitor. Many suppliers try to mitigate this risk with preemptive measures that rebuild institution-based trust and safeguard against the development of distrust (Cheng, Fu, & de Vreede, 2021; Moody et al., 2017). Often, customer

[*] Corresponding author.
E-mail addresses: manuel.utz@uni-bayreuth.de (M. Utz), johanning@wifa.uni-leipzig.de (S. Johanning), tamara.roth@uni.lu (T. Roth), bruckner@wifa.uni-leipzig.de (T. Bruckner), jens.strueker@fim-rc.de (J. Strüker).

https://doi.org/10.1016/j.ijinfomgt.2022.102496
Received 29 December 2020; Received in revised form 11 February 2022; Accepted 14 February 2022
Available online 7 March 2022

loyalty programs (Dolšak, Hrovatin, & Zorić, 2019; Peng & Wang, 2006) are conceived to foster a trusting relationship in which information is shared between supplier and customer (Bansal, Taylor, & James, 2005). When successful, these programs strengthen the three dimensions of institution-based trust (Bélanger & Carter, 2008; Cheng et al., 2021; McKnight, Cummings, & Chervany, 1998; McKnight, Lankton, Nicolaou, & Price, 2017) at the same time as they reduce the three dimensions of institution-based distrust (Moody et al., 2014, 2017).

Digital technologies that facilitate such trustful sharing of information are an essential prerequisite for most of these programs. Blockchain technology, in particular, appears to be a suitable technological option (Andoni et al., 2019; Ante, Steinmetz, & Fiedler, 2021). Although a 'trustless' technology by design, given that it does not require trust in a central operator (Werbach, 2018), blockchain's properties, such as secure and distributed data storage, can generate trust (Amend & Kaiser, 2021; Roth, Stohr, Amend, Fridgen, & Rieger, 2022). By virtue of these properties, blockchain can mediate trust concerns in many environments where trust is either nonexistent or severely compromised (Amend & Kaiser, 2021). To assess its further usefulness in resolving trust issues concerning energy supply and consumption, we have set out to answer the following two research questions:

RQ1: How can blockchain technology enhance institution-based trust and reduce distrust in electricity suppliers?

RQ2: How can a trust-based customer loyalty program be designed with blockchain technology?

To answer these questions, we followed a Design Science Research (DSR) approach (Gregor & Hevner, 2013). The use of DSR helped us identify design requirements for the enhancement of institution-based trust and the reduction of institution-based distrust. It also benefitted our investigations into how a customer loyalty program can be designed with blockchain technology. We began with a comprehensive literature review (Webster & Watson, 2002), followed by a workshop with an electricity supplier as well ex-ante interviews with experts to derive design objectives and requirements. Based on these, we then designed Nexo Energy, a conceptual architecture for a customer loyalty program based on blockchain. Using an iterative approach, we continuously refined our artifact through a series of workshops with employees of the electricity supplier, a comprehensive test with customers, and interviews with both groups (see Table A1). Upon completing the refinement and evaluation process, we deduced a nascent design theory that is based on four design principles (Gregor & Hevner, 2013). This design theory makes an important contribution to blockchain research as it illustrates a specific way in which blockchain can help manage ambivalence by facilitating institution-based trust and reducing institution-based distrust. In a broader context, it advances the current investigation into how innovative technologies can be used to build consumer trust (Abbas, Martinetti, Moerman, Hamberg, & van Dongen, 2020; Cheng et al., 2021; Jeon, Kim, Lee, & Lee, 2021).

2. Theoretical background

2.1. Green electricity tariffs and customer satisfaction

At present, global initiatives for climate protection and various national sustainability policies are driving the replacement of finite resources with RES (Ante et al., 2021; Dorfleitner et al., 2021). While RES play a significant role in reaching sustainability goals, their intermittency and volatility introduce not just multiple organizational and technical challenges but also a long list of regulatory issues (Andoni et al., 2019; Baumgarte, Glenk, & Rieger, 2020). What is more, the prominence of RES poses a specific challenge to the traditional business models of electricity suppliers (Ahl et al., 2020; Hua et al., 2020) as they are now expected to meet their customers' surging demand for green electricity (Bogensperger et al., 2018; Luke, Lee, Pekarek, & Dimitrova, 2018).

To this end, electricity suppliers typically employ Green Electricity Tariffs (MacPherson & Lange, 2013). The use of such GETs, however, poses two further challenges. One, GETs are subject to complex electricity market regulation (Andoni et al., 2019; MacDonald & Eyre, 2018), and their implementation is both cumbersome and costly (Bergaentzlé et al., 2019), which is why GETs are often more expensive than conventional electricity tariffs (Fang, Cui, Du, Li, & Kang, 2021; MacDonald & Eyre, 2018). Two, GETs typically involve the use of so-called 'guarantee of origin' certificates (Abad & Dodds, 2020) because many electricity suppliers do not have direct access to the full amount of RES required to satisfy their customers' contractually agreed units of green electricity. To reach the quota, they buy these certificates from other RES suppliers (Hamburger, 2019; Raadal, Dotzauer, Hanssen, & Kildal, 2012). Although guarantee of origin certificates are a legitimate measure to support the distribution of RES, customers often feel deceived by them – be it because they suspect disproportionate charges for green energy or because they do not receive the expected 'kind' of green electricity (Ambrose, 2021; Guo et al., 2014; Mezger et al., 2020). The resentment this causes is often reinforced by negative publicity resulting from double-spending affairs (Castellanos, Coll-Mayor, & Notholt, 2017; Hamburger, 2019).

Such resentment can lower customer satisfaction and ultimately lead to a drop in customer loyalty. Customer satisfaction is typically defined as an important antecedent of customer loyalty, and it is rooted in certain (perceived) service qualities (Berry, Parasuraman, & Zeithaml, 1988; Culiberg, 2010). One important such quality is reliability, which is to say the "ability to perform the promised service dependably and accurately" (Muzahid & Noorjahan, 2009, p.26). This definition of reliability is rather close to the standard definition of customer satisfaction, which can be described as "a feeling [resulting] from a process of evaluation of what has been received against what was expected […]" (Muzahid & Noorjahan, 2009, p.27). It is worth noting that some expectations concerning GETs may have been unrealistic from the get-go and may be attributed to the general public's limited understanding of the complex workings of electricity generation, transmission, and distribution work. It is a separate issue, however, that electricity suppliers have not always been able to provide the desired and promised services (Bang et al., 2000; MacPherson & Lange, 2013; Wüstenhagen, Wolsink, & Bürer, 2007). This incompetence (Moody et al., 2017) to deliver green electricity has led to widespread skepticism (Kramer, 1999) concerning the electricity supplier's ability to improve its services in the future, and this in turn has had two unfortunate consequences. One, customer satisfaction has dropped (Martínez & Rodríguez del Bosque, 2013). Two, customer trust has been reduced and customer distrust has become a considerable problem (Kramer, 1999; McKnight et al., 2017; Moody et al., 2017).

2.2. The loyalty trilemma: Institution-based trust, institution-based distrust, and ambivalence

An important second antecedent of customer loyalty is customer trust (Chu, Lee, & Chao, 2012; Stathopoulou & Balabanis, 2016). Such trust is generally based on the belief that a service provider acts in the long-term interest of its customers (Martínez & Rodríguez del Bosque, 2013). Accordingly, trust is contingent on "the willingness of a party to be vulnerable to another party's actions based on the expectation that the other party will perform a particular action important to the trusting party, irrespective of the ability to monitor or control that other party" (Cheng et al., 2021, p. 3). While this definition of trust (Lewicki & Brinsfield, 2011; Mayer, Davis, & Schoorman, 1995; Tams, Thatcher, & Craig, 2018; van der Werff, Legood, Buckley, Weibel, & de Cremer, 2019) implies a lack of control and monitoring capabilities, it is important to note that the willingness to be vulnerable is not the result of naivety but rather a consequence of the trusting party's rational judgment (Dietz & Gillespie, 2011; van der Werff et al., 2019).

In the energy sector, customers and their electricity suppliers have typically developed a long-standing relationship of trust (Ambrose, 2021). When customers make the switch to GETs, they expect their suppliers to deliver green units of electricity at reasonable prices and with the same reliability with which they previously delivered the 'gray' units (Hartmann & Apaolaza Ibáñez, 2007; Rosell & Ibáñez, 2006). In most cases, electricity suppliers have managed to meet these expectations to such an extent that customers developed a feeling of security concerning the surrounding structure and the inherent legal guarantees (McKnight et al., 1998). This so-called *institution-based trust* (Cheng et al., 2021; McKnight et al., 2017) has three dimensions: *calculation-based*, *cognition-based*, and *knowledge-based trust* (Cheng et al., 2021).

Calculation-based trust is the most basic dimension of trust and builds on the *integrity* of a trusted party (Bilgic, Hoogensen Gjørv, & Wilcock, 2019; Moody et al., 2017). *Calculation-based trust* can be described as taking a "calculated risk" and building a positive affection (Bilgic et al., 2019 p.4). Both elements depend on information about the *integrity* of the trusted party. This information may range from observations of the trusted party's *competence* (Moody et al., 2017) to the keeping of contractual agreements and general demonstrations of openness and reliability (Ibrahim & Ribbers, 2009; Muzahid & Noorjahan, 2009). When such information affirms the trustworthiness of the trusted party, the trusting party may become willing to be vulnerable. This so-called trust motivation can initiate trust development processes (van der Werff et al., 2019) which are just as relevant when it comes to the promotion of the second dimension of trust, *cognition-based trust*. This type of trust depends on a favorable assessment of the trusted party's know-how, goodwill, and reliability. The more information the trusted party provides (*competence*) in a transparent and verifiable manner (*integrity*), the easier it will be for the trusting party to establish trust (Ibrahim & Ribbers, 2009). As for the third dimension of trust, *knowledge-based trust*, this depends on a positive evaluation of experiences in dealing with the trusted party. Of particular concern here is its *benevolence,* and evidence of this can only emerge when there is an interaction history in the course of which the information required to develop such trust could be accumulated (Moody et al., 2017). For this third type of trust to develop, then, trust at the *calculation-* and *cognition-based* level has to be sufficiently advanced to allow for the requisite interaction (McKnight et al., 1998).

It is a matter of some concern, therefore, that guarantee of origin certificates introduce ambiguity into the generation processes of these three trust dimensions. While electricity suppliers interpret both the direct provision of RES and the indirect procurement of guarantee of origin certificates as 'delivering green electricity' (Ambrose, 2021; Guo et al., 2014; Mezger et al., 2020), many customers would disagree with this wider definition. Instead they would contend that only electricity drawn directly from RES deserves to be called 'green' (Andoni et al., 2019; Bogensperger et al., 2018; Perrons & Cosby, 2020). When the supplied electricity diverges notably from the customers' interpretation of green electricity, this constitutes a violation of *cognition-based trust*. Customers are then likely to doubt or even dismiss the supplier's reliability and *competence* to provide the expected service. At this point, the supplier's *integrity* as measured in terms of costs and benefits (*calculation-based trust*) is no longer evident (Bilgic et al., 2019). On the contrary, customers may suspect that they have become victims of 'greenwashing' by paying premiums for green electricity even though they have been receiving gray electricity misleadingly labelled with guarantee of origin certificates to make it appear like green electricity (Ambrose, 2021; Mezger et al., 2020). Where such suspicions lead to resentment, they extend customers' doubts about the *benevolence* of their supplier, at which point some may feel cheated or even taunted (*knowledge-based trust*).

At a more general level, such drastic setbacks in all three trust dimensions undermine *institution-based trust* in electricity suppliers. Furthermore, they also leave room for the growth of *institution-based distrust* (Kramer, 1999; McKnight & Chervany Norman, 2001; McKnight & Choudhury, 2006). Distrust has many definitions, depending on its context (McKnight & Chervany Norman, 2001), but generally speaking it can be described as a "strong negative feeling regarding the conduct of another [party]" (Lee, Lee, & Tan, 2015, p. 162), or a "lack of confidence in the other, a concern that the other may act as to harm one, […] not [caring] about one's welfare […]" (Govier, 1994, p. 240). Distrust is often accompanied by feelings of fear, frustration, and rejection (Govier, 1994; McKnight & Choudhury, 2006). Analogous with the three-part structure of *institution-based trust*, distrust may also have three dimensions, which we describe as *vigilance-based distrust*, *skepticism-based distrust*, and *control-based distrust*. Their respective root causes are perceived *deceit*, *incompetence*, and *malevolence* (McKnight & Choudhury, 2006; McKnight et al., 2017; Moody, Galletta, & Lowry, 2010). While distrust is often overlooked as the 'little brother of trust', it warrants explicit attention for being a key element of risk assessment and risk avoidance (McKnight & Chervany Norman, 2001).

In our GET context, customers are keen to mitigate the risk of falling victim to 'greenwashing' when their suppliers use guarantee of origin certificates (Ambrose, 2021; Andoni et al., 2019; Mezger et al., 2020). They suspect "that the [trusted party] is dishonest and potentially provides false information" (McKnight et al., 2017, p. 4). In due course, such *deceit* will lead to greater *vigilance-based distrust* (Kramer, 1999; McKnight & Chervany Norman, 2001). Customers will pay more attention to the consumed units of electricity and their source, while also taking note of the respective green electricity prices (Bogensperger et al., 2018). However, many electricity suppliers are simply unable to provide green electricity to the required extent because they do not have direct access to RES, and even if they did, it would not change the fact that all electricity in the grid is gray (Luke, Anstey, Taylor, & Sirak, 2019; Peter, Paredes, Rivial, Sepúlveda, & Astorga, 2019). While electricity suppliers believe this to be common sense, customers often have different expectations and conclude that "the [trusted party] lacks the ability to accomplish [this] task" (McKnight et al., 2017 201, p. 4). In short, they perceive the supplier to be incompetent. When customers extend such *incompetence* beliefs to future tasks, they may develop far-reaching *skepticism-based distrust* (Kramer, 1999; McKnight & Chervany Norman, 2001). In some cases, where customers are convinced that GETs help their electricity supplier to 'greenwash' gray electricity (Ambrose, 2021; Guo et al., 2014), this conviction can lead to the feeling "that the [trusted party] has the intention to harm the [trusting party]" (McKnight et al., 2017, p. 4) or to act in a *malevolent* way. This suspected *malevolence* can make a customer seek out more information and exercise greater caution when it comes to their own future actions, eliciting *control-based distrust* (Kramer, 1999; McKnight & Chervany Norman, 2001).

When previously trusting relationships between electricity suppliers and their customers suffer a decrease in trust along with an increase in distrust, the result is a conflict that can best be described as *ambivalence* (Jarvenpaa & Majchrzak, 2010; Moody et al., 2014). *Ambivalence* is commonly defined as "holding simultaneously at least two contradictory attitudes toward the same attitude object" (Moody et al., 2014, p. 267). These attitudes have three dimensions: behaviors, feelings, and beliefs, and each can have different valences (Moody et al., 2017). In the case of GETs, the long-standing relationship with an electricity supplier can, for instance, have a higher valence than their customers' distrust-beliefs and trust-reducing behaviors or feelings. It will not, however, automatically nullify the customers' negative attitudes. Instead, it creates *ambivalence* (Moody et al., 2014; Ning, Feng, Feng, & Liu, 2019). Such *ambivalence* may influence a wide variety of buying decisions and, in the particular case of deciding whether to stay with one's electricity supplier, it can notably affect the customer's loyalty (Moody et al., 2017; Olsen, Wilcox, & Olsson, 2005). After all, ambivalent customers may feel inclined to compare offers and even switch to another supplier.

To safeguard against losing their customers, electricity suppliers must not only rebuild *institution-based trust* (Cheng et al., 2021; McKnight et al., 2017) but also reduce *institution-based distrust* (Moody et al., 2014; Olsen et al., 2005). Typically, their strategy for doing so

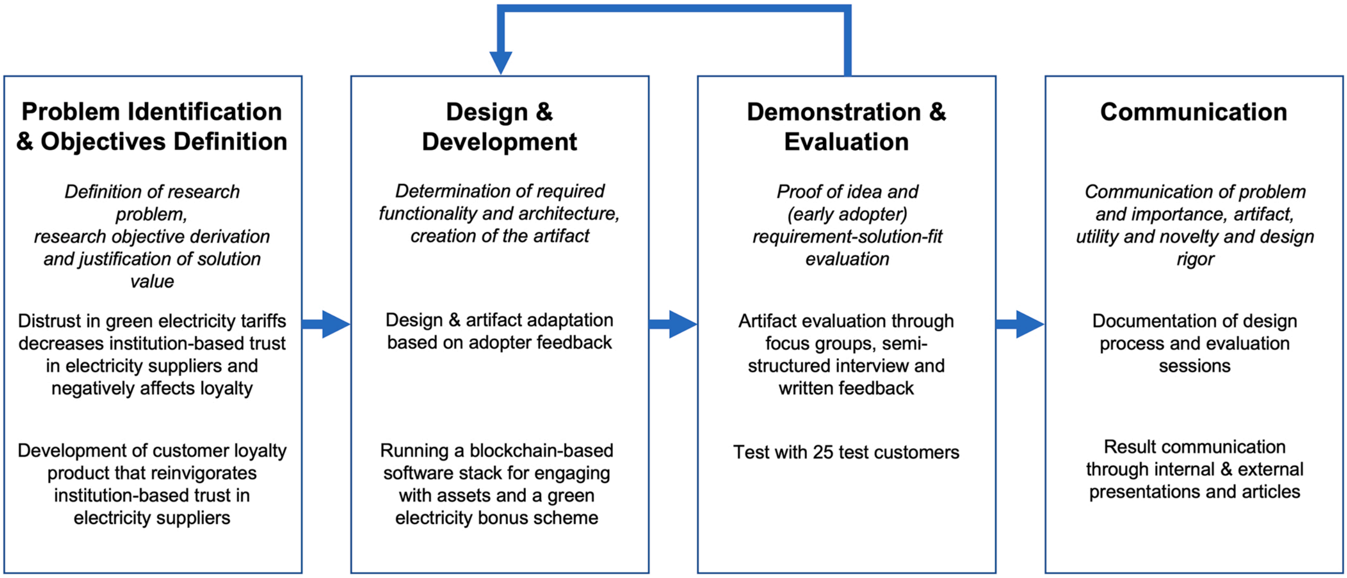

Problem Identification & Objectives Definition
Definition of research problem, research objective derivation and justification of solution value
Distrust in green electricity tariffs decreases institution-based trust in electricity suppliers and negatively affects loyalty
Development of customer loyalty product that reinvigorates institution-based trust in electricity suppliers
Design & Development
Determination of required functionality and architecture, creation of the artifact
Design & artifact adaptation based on adopter feedback
Running a blockchain-based software stack for engaging with assets and a green electricity bonus scheme
Demonstration & Evaluation
Proof of idea and (early adopter) requirement-solution-fit evaluation
Artifact evaluation through focus groups, semi-structured interview and written feedback
Test with 25 test customers
Communication
Communication of problem and importance, artifact, utility and novelty and design rigor
Documentation of design process and evaluation sessions
Result communication through internal & external presentations and articles

Fig. 1. Adapted Design Process Model based on Peffers et al. (2007).

involves the use of customer loyalty programs (Dowling & Uncles, 1997; Uncles, Dowling, & Hammond, 2003). These are often based on innovative technologies, such as blockchain, and aim to both strengthen *institution-based trust* dimensions and weaken *institution-based distrust* dimensions (Abbas et al., 2020; Warkentin & Orgeron, 2020). The expectation is that such customer loyalty programs will replace the feeling of *ambivalence* with trust attitudes, which may ultimately increase customer loyalty (Moody et al., 2017; Olsen et al., 2005).

2.3. Trustless blockchain technology as trust mediator

In recent years, blockchain has received wide attention across many industries for being a ‘trustless’ technology. Various projects have since been initiated to test the prospects and limitations of blockchain applications (Ante et al., 2021; Sedlmeir, Smethurst, Rieger, & Fridgen, 2021; Upadhyay, 2020). Success stories in logistics (Jensen, Hedman, & Henningsson, 2019; Sarker, Henningsson, Jensen, & Hedman, 2021), retail (Bumblauskas, Mann, Dugan, & Rittmer, 2020; Cho, Lee, Cheong, No, & Vasarhelyi, 2021), insurance (Zhang, Wei, Jiang, Peng, & Zhao, 2021) and even public administration (Rieger, Lockl, Urbach, Guggenmos, & Fridgen, 2019) have raised hopes that blockchain may offer similar benefits when used in electric power systems. The aim is to create decentralized electric power systems with the help of a decentralized technology that obviates intermediaries (Diestelmeier, 2019; Mengelkamp, Schlund, & Weinhardt, 2019).

Technically speaking, blockchains are a particular type of distributed ledgers that build on a peer-to-peer network. All data can be replicated, shared, and distributed across multiple servers – so-called nodes (Beck, Müller-Bloch, & King, 2018; Butijn, Tamburri, & Heuvel, 2020; Chanson, Bogner, Bilgeri, Fleisch, & Wortmann, 2019). Such physical decentralization makes secure and distributed data storage possible (Amend, Fridgen et al., 2021; Chanson et al., 2019; Cho et al., 2021). Selected nodes within the network will group transactions into blocks that reference the previous block through a hash-value (Zhang, Wang, & Ding, 2019). These hashes typically make retrospective changes to the blockchain easy to detect. Private blockchains further allow for the distribution of the right to write and the right to access data in accordance with the role and attributed competencies of each involved party (Sedlmeir, Buhl, Fridgen, & Keller, 2020; Ziolkowski, Miscione, & Schwabe, 2020). This reduces complexity by maintaining the commonly shared truth as well as the necessary transparency, without disclosing information that either should not or must not be accessed (Hawlitschek, Notheisen, & Teubner, 2018; Mattke, Hund, Maier, & Weitzel, 2019; Rieger et al., 2019). Beyond storing data, blockchains can process payments and may even execute programming logic with the help of so-called smart contracts (Andersen & Bogusz, 2019; Chong, Lim, Hua, Zheng, & Tan, 2019; Lacity, 2018). These are redundantly executed scripts that enable participants to control the validity of transactions, which can significantly reduce dependencies on third parties as well as the trust that these dependencies require (Chong et al., 2019; Gorkhali, Li, & Shrestha, 2020; Rossi, Mueller-Bloch, Thatcher, & Beck, 2019). This, in turn, mitigates lock-in effects and goes a long way towards preventing the aggregation of market power (Hoess, Roth, Sedlmeir, Fridgen, & Rieger, 2022; Thomas, Zhou, Long, Wu, & Jenkins, 2019). Moreover, distributed data storage and execution of transactions obviate a single point of failure while also enabling reliable information sharing and process automation (Du, Pan, Leidner, & Ying, 2019; Watanabe et al., 2016). This makes blockchain particularly attractive for building and running critical infrastructures (Amend & Kaiser, 2021; Rieger et al., 2019).

On account of its technical characteristics, blockchain is commonly described as an inherently trustless technology (Da Xu & Viriyasitavat, 2019; Gorkhali et al., 2020). Instead of requiring users to trust one another or engaging a trusted third party, blockchain “shift[s] from trusting people to trusting math” (De Filippi, Mannan, & Reijers, 2020 p.6). Specifically, blockchain can be used as a means to collaborate even when the parties do not know or trust each other, which is why many believe blockchain technology to be a direct substitute of trust or a technical manifestation of so-called trustless trust (De Filippi et al., 2020; Risius & Spohrer, 2017; Werbach, 2018). Hawlitschek et al. (2018) have examined this notion of blockchain’s trustlessness in an extensive literature review and found that the key to successful collaboration is not the algorithm-based trust of blockchain technology (Al Khalil, Butler, O’Brien, & Ceci, 2017; Maurer, Nelms, & Swartz, 2013). Rather, it is *institution-based trust* (Abbas et al., 2020; Lustig & Nardi, 2015). Blockchain only mediates this trust by virtue of its underlying technical properties, such as immutability and selective transparency (Amend & Kaiser, 2021; Rieger et al., 2019; Roth et al., 2022). With this in mind, we aimed to design a customer loyalty program for electricity suppliers that is based on blockchain. Such loyalty programs may already be known from the works of Bulbul and İnce (2018) and Choi (2018), who focus on the development and analysis of technical components of blockchain-based customer loyalty programs. Moreover, Agrawal et al. (2018) address related implementation and stakeholder challenges. Extending these works, this paper focuses on ethical design, incorporating the latent dimensions of *institution-based trust* and *institution-based distrust*, which is ideally suited to inspire customer trust and to reduce distrust as essential albeit often neglected factors to customer loyalty.

3. Research method

3.1. Design Science Research approach

We followed a DSR approach to analyze the role that blockchain technology can play in the creation of a customer loyalty program which reinvigorates *institution-based trust*, reduces *institution-based distrust*, and resolves customer *ambivalence*. DSR is a well-established research method, widely used in the design and development of various IT-based artifacts, such as constructs, frameworks, architectures, models, methods, and instantiations or algorithms (Hevner, March, Park & Ram, 2004; Peffers et al., 2012). DSR also covers more abstract artifacts like social innovations and design propositions (van Aken, 2004), technical and social properties (Järvinen, 2007) or related design principles and theories (Costa, Soares, & de Sousa, 2020; Vaishnavi & Uechler, 2008).

Our artifact, Nexo Energy, constitutes a conceptual architecture for a blockchain-based customer loyalty program. Throughout the iterative process of its design and construction (Hevner & Chatterjee, 2012; Hevner et al., 2004), we followed the DSR steps proposed by (Peffers, Tuunanen, Rothenberger, & Chatterjee, 2007) (Fig. 1). We began with a comprehensive literature review to identify the problems and define a preliminary set of design requirements (DR) and objectives (DO) (Webster & Watson, 2002). We then refined these DRs and DOs as represented in our architecture, first in a workshop with an electricity supplier, then in ex-ante interviews with domain experts (DSR process steps 1–3) (Table A1).

To demonstrate and evaluate our conceptual architecture, we conducted a series of workshops with employees of the electricity supplier. We also implemented it in a prototype and tested it with the electricity supplier's customers. Lastly, we addressed its various features in a series of interviews (Table A1) with both groups (DSR process steps 4–6) (Hevner et al., 2004; Peffers et al., 2007).

When working on our final architecture, we developed four design principles (DP) that not only offer contributions to the theories of *institution-based trust* (Cheng et al., 2021; McKnight et al., 2017), *institution-based distrust* (Kramer, 1999; McKnight & Chervany Norman, 2001), and *ambivalence* (Moody et al., 2014, 2017). Our four design principles also form a nascent design theory (Gregor & Hevner, 2013). This theory can be framed as a Design Relevant Explanatory or Predictive Theory (DREPT) that examines why the artifact can have the proposed effects (Kuechler & Vaishnavi, 2012). In contrast to an Information Systems Design Theory (ISDT), a DREPT better explains the relations between the kernel theory and the artifact (Walls, Widmeyer, & Sawy, 2004), thus bridging the gap between abstract theories and "achievable effects" (Kuechler & Vaishnavi, 2012, p. 399). In doing so, our theorizing is in line with demands for relevance of both the theoretical contributions and practical implications of the developed artifact (Gregor & Hevner, 2013; Hevner & Chatterjee, 2012; Hevner, 2007).

Our proposed DREPT makes a knowledge contribution of the exaptation type. Exaptation requires the extension of a known solution to new problems (Gregor & Hevner, 2013). Customer loyalty programs have a long tradition in business literature (Dowling & Uncles, 1997; Nunes & Drze, 2006; Uncles et al., 2003; Yi, Youjae & Hoseong, 2003), ever since American Airlines debuted their 'Frequent Flyer Program' three decades ago. In the intervening years, such programs have gained traction in multiple other areas, such as hospitality, retail, financial services (Hofman-Kohlmeyer, 2016), and the energy industry (Dolšak et al., 2019; Gamma, 2016), where the introduction of RES and GETs is currently a matter of notable contention (Ambrose, 2021; Andoni et al., 2019; Mezger et al., 2020). To mediate these contentions, technological innovations like blockchains are examined. They aim to extend and evolve current customer loyalty programs, while at the same time, their development may be instrumental in delivering generalizable design knowledge for future artifacts (Gregor & Hevner, 2013).

3.2. Identifying the problem and defining the objectives

In line with Webster and Watson (2002), we conducted a preliminary literature search on various databases, including Google Scholar, Scopus, Web of Science, etc. For each search, we used using multiple keywords and combinations, such as "trust distrust", "customer loyalty trust", or "blockchain trust". When reading the literature on blockchain technology in electric power systems and beyond, we focused on publications dating back nor further than 2018, at which time applications reached a level of maturity beyond conceptualization. After our initial keyword search, we eliminated lower-quality publications by considering the journal impact factors and scientific merit criteria applied by Scopus. Upon reviewing the titles and abstracts of this high-quality subset, we identified 95 publications of immediate relevance to our analysis. Having analyzed each of these publications, we extrapolated a preliminary problem statement and derived an initial set of design requirements and design objectives.

In the next step, we refined these requirements and objectives by organizing a workshop with an electricity supplier in Leipzig, Germany. In addition, we also conducted 18 ex-ante interviews with domain experts. Three of the workshop participants were managers of the electricity supplier, two of them employers of its IT service provider. We asked each of our 18 interviewees how their customers had reacted to green electricity, to GETs, and to any associated challenges. As recommended by Myers and Newman (2007), we used a semi-structured interview format. The interviews lasted between 45 and 60 min. They were audio-recorded as well as transcribed for further examination. When moving on to our data analysis, we followed the recommendations of Miles et al. (2018) by performing a two-step coding process based on inductive and deductive coding.

3.3. Demonstration and evaluation

We demonstrated and evaluated our blockchain-based customer loyalty program by means of a series of workshops with employees of the electricity supplier, extensive testing with 25 customers, and a total of 12 semi-structured interviews with members of both groups. This allowed us to continuously review and refine our conceptual architecture in iterative build-and-evaluate loops (Hevner et al., 2004; Peffers et al., 2007). We visited the test customers at regular intervals and noted their experiences and requests for adaption. In our interviews with the electricity supplier and its customers, we initially discussed the status quo, the challenges related to current GETs, and the possible applications of blockchain technology that might validate the identified design requirements and objectives. Subsequently, we presented a draft of our conceptual architecture for a blockchain-based customer loyalty program and gathered feedback. Like the ex-ante interviews, our evaluation interviews were between 45 and 60 min in length, audio-recorded, transcribed, and analyzed in a two-step coding process.

4. A blockchain-based customer loyalty program

4.1. Objectives of the artifact

By way of our literature analysis, ex-ante workshop, and ex-ante expert interviews, we arrived at 14 design requirements and 6 design objectives (Table A2) which together provide the framework for the architecture of our blockchain-based customer loyalty program.

4.1.1. DO1 – Accountability

Typically, customers have to rely on their electricity supplier when it

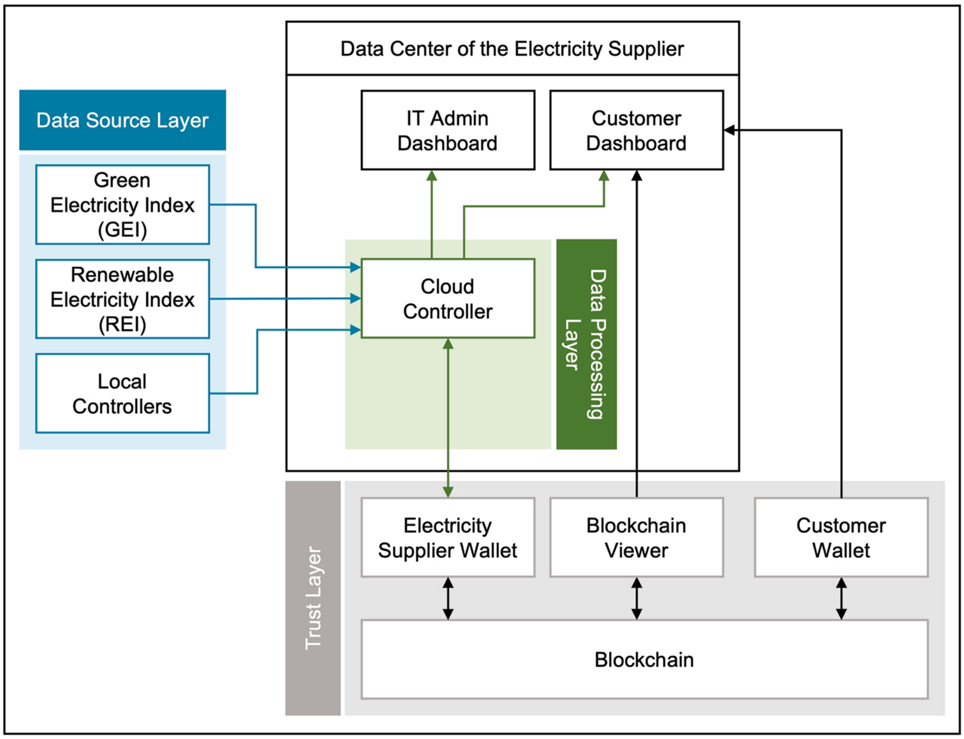


Fig. 2. Nexo Energy's architecture.

comes to their consumption data, the origin of consumed electricity, and electricity pricing (Ahl et al., 2020; Perrons & Cosby, 2020). To give customers more control over their data, and to prevent any subsequent manipulation by the electricity supplier (Andoni et al., 2019; Risius & Spohrer, 2017), one has to provide *tamper-proof and easily accessible storage of data in the blockchain network (DR1)*. Ease of access is of critical importance because many customers are not digitally literate enough to interpret data that is directly extracted from the blockchain (Jang, Han, & Kim, 2020). Instead, data has to be displayed in a readily accessible and verifiable way (Lockl, Schlatt, Schweizer, Urbach, & Harth, 2020; Paymans, Lindenberg, & Neerincx, 2004). This is also true of consumption and generation data which has been transferred to the blockchain. To avoid the storage of erroneous data or its manipulation during the information transfer (Rieger et al., 2019), *tamper-proof and automated data processing (DR2)* is required, for instance via smart contracts.

4.1.2. DO2 – Customizability

In the context of GETs, data on the generation of electricity has for quite some time now been the largest bone of contention between customers and suppliers (Ambrose, 2021; Andoni et al., 2019; Mezger et al., 2020). Collecting and storing such data in the back-end systems of energy suppliers is no longer deemed sufficient by many customers. This has led to requests for additional, secure *storage of generation and consumption data (DR3 and DR4)* in the blockchain network. Access to such securely and immutably stored data (Perrons & Cosby, 2020) enables customers not only to automatically adjust their electricity consumption but also to do so flexibly, depending on the share of renewable or green electricity in the grid. This *intuitive and comprehensive adjustment of electricity consumption (DR5)* is particularly relevant to GET customers who are concerned about the sustainability of their electricity consumption. With this growing demographic in mind, the architecture should also help customers monitor their consumption data. While the direct storage of consumption data in the blockchain network violates privacy regulations, such as the General Data Protection Regulation (GDPR), it is worth noting that pseudonymized transaction values are less critical. Albeit verifiable, they would prevent the inadvertent attribution to customers (Rieger, Roth, Sedlmeir, & Fridgen, 2021).

4.1.3. DO3 – Simplicity

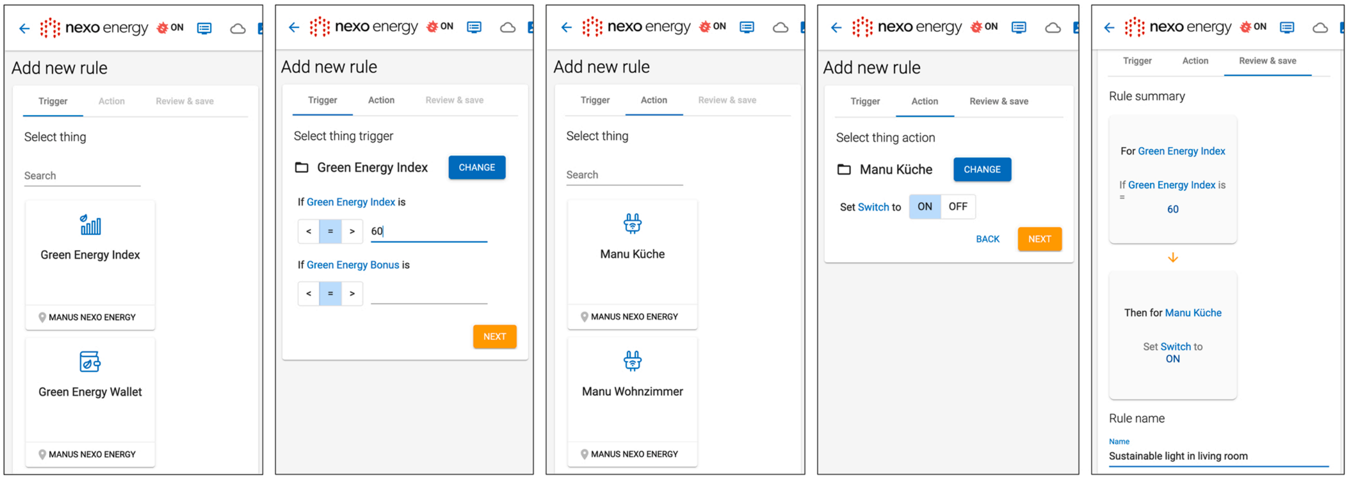
Customers vary in their degree of digital literacy (Paymans et al., 2004; Portes, Cases, & N'Goala, 2020), which is why the architecture requires an *intuitive user interface (DR8)*. Users should not have to deal with the technical details of blockchain technology (Lockl et al., 2020), be it when monitoring generation and consumption data, or when managing their GET and sustainability bonuses. This requirement also applies to system setup and access. Should it be deemed necessary or desirable that the setup can be done without the support of a technician, the electricity supplier is advised to *deliver all information for the setup process (DR6)*. Moreover, the architecture should enable *automatic smart device detection (DR7)* to ease the setup process for customers.

4.1.4. DO4 – Efficiency

A key component of a reliable customer loyalty program is the seamless information exchange between electricity supplier and customer (Andoni et al., 2019; Gorski, Bednarski, & Chaczko, 2019). The specific requirement for this exchange is *fast data synchronization between software components (DR9)*. Since blockchain does not scale as easily as other technologies (Di Silvestre et al., 2020; Khorasany, Dorri, Razzaghi, & Jurdak, 2021; Saha et al., 2021; Sousa et al., 2019) data processing via blockchain should be reduced to a minimum to retain *high software uptime and availability (DR10)*.

4.1.5. DO5 – Maintainability

If the architecture is to work well for all customers, it is important that it can connect to different legacy systems (Ahl et al., 2020; Hasankhani, Mehdi Hakimi, Shafie-khah, & Asadolahi, 2021). Specifically, this means that the uptime of the connection should be *easy to monitor by IT administrator staff (DR11)* to ensure that they can make helpful interventions, should any be required. While customers do not have monitoring and maintenance responsibilities, they should be given responsibility for the design of their service agreement. What this means



Add new rule

Select thing

Search

Green Energy Index

Green Energy Wallet

Add new rule

Select thing trigger

Green Energy Index

If Green Energy Index is

< = > 60

If Green Energy Bonus is

< = >

Add new rule

Select thing

Search

Manu Küche

Manu Wohnzimmer

Add new rule

Select thing action

Manu Küche

Set Switch to ON OFF

Rule summary

For Green Energy Index

If Green Energy Index is
=
60

↓

Then for Manu Küche

Set Switch to
ON

Rule name

Name
Sustainable light in living room

Fig. 3. Connecting smart devices with services via rules (app view).

in practical terms is that Nexo Energy should integrate existing GETs and make it *easy to order for customers (DR12)* who wish to use it in addition to existing or new GETs.

4.1.6. DO6 – Affordability

Participation in a blockchain-based customer loyalty program should remain *affordable for customers (DR13)*. While the architecture should accommodate GETs that are tailored to the needs of individual customers, electricity suppliers should keep the costs for this additional service at bay (Gomes, Melicio, & Mendes, 2021; MacDonald & Eyre, 2018). Customers are already charged a higher price for GETs and would probably become skeptical to the point of cancelling the tariff were they to receive the same electricity mix as before but at an even higher price and with only a slightly improved service offering (Ambrose, 2021; Guo et al., 2014; Mezger et al., 2020). It is, therefore, important for electricity suppliers to ensure *reasonable costs for operation (DR14)* before they implement a blockchain-based customer loyalty program. Related considerations include the choice of consensus mechanism and energy consumption as well as affordable hardware options, such as a Raspberry Pi (Raspberry Pi Foundation, 2016).

4.2. Description of the artifact

The overarching goals of our artifact, Nexo Energy, are the restoration of *institution-based trust*, the reduction of *institution-based distrust*, and the resolution of *ambivalence*. Offering customers transparency and affording them the opportunity to actively participate in their electricity supplier's sustainability efforts can improve the trust between supplier and customer. More specifically, our blockchain-based artifact enables customers to trace electricity generation data and monitor their own electricity consumption. What is more, Nexo Energy allows customers to optimize their consumption patterns according to their sustainability and cost reduction preferences. Customers can set their own rules for their smart appliances, for instance, "consume electricity primarily at times when the share of regional green electricity is particularly high or when electricity prices are exceptionally low". By setting such sustainable rules and consumption patterns, customers qualify for additional loyalty tokens. These tokens are awarded for an increased consumption of green electricity and can be used in a variety of ways: to reduce the price of a customer's GET, to make donations to charity, to use services of other utility companies like electric scooters or car sharing, or to reinvest in shares of RES, which contributes directly to the greater adoption and availability of green electricity. Overall, Nexo Energy comprises three layers: the data source layer, the operation layer, and the trust layer (Fig. 2).

The **data source layer** provides consumption and generation data from authentic sources (DO1). The sustainability of generation can be assessed with the Green Electricity Index (GEI) or another Renewable Energy Index (REI) (Zoerner, 2020). Meanwhile, 'local controllers' provide authentic consumption data for all connected appliances (DO1, DO2). Local controllers are IoT devices that are installed in the households of customers and automatically connect to their smart appliances (Figure A1), whereupon they collect consumption data (DO2, DO4). To process data and to execute the underlying software, they require a reliable and scalable operating system (DO4), but the hardware for local controllers must not exceed a certain price limit. It must also not unduly increase the prices of existing GETs (DO6) and should remain affordable for customers. Based on an analysis of costs, network capabilities, and operating systems, we selected Raspberry Pis (DO6).

The **data processing layer** is at home in the data center of the electricity supplier, where it ensures a high degree of uptime and reliability (DO4). As the main element of data storage and display, it uses a cloud controller (DO5). To safeguard GDPR-compliance, such as the right to erasure (Rieger et al., 2019), the generation and consumption data collected by local controllers is not stored on the blockchain, but rather in the cloud controller's database (DO1, DO2). Individual web applications (see Figure A2) allow customers to display, monitor, and manage their current GET along with their electricity consumption levels (DO1, DO3). Moreover, customers can display their connected smart appliances alongside trustworthy data sources, such as the GEI or another REI (DO3). When using these data sources, customers can set rules for their smart appliances to ensure that their electricity consumption are in line with their sustainability preferences (DO5). For instance, a customer can set the rule that a WIFI-connected lamp shall be switched on or off depending on the availability of green electricity at the time of consumption (Fig. 3). Customers can freely determine the number and nature of such rules (DO3, DO5), while the local controllers synchronize with the cloud controller in short interval loops to transfer and store data (DO4).

The **trust layer** with its underlying blockchain network facilitates the issuance, storage, and verification of loyalty tokens (DO1). Supplier and customer have separate blockchain wallets and both can use their respective wallets to exchange loyalty tokens. These tokens are issued from the supplier's blockchain wallet, based on generation and consumption values transmitted by the cloud controller (DO1, DO2). Technically speaking, these values are the input for two smart contract functions that automatically (DO1, DO5) publish the bonus – a certain amount of loyalty tokens for the use of GETs – and transfer the determined amount of loyalty tokens from the supplier's blockchain address to that of the respective customer. The loyalty tokens can, for instance, be reinvested in RES, used to reduce the costs of current GETs, or transferred into fiat money. To prevent the electricity supplier from making retrospective changes without customers noticing that the original data has been tampered with, hashes of generation and consumption values are stored on the blockchain (DO1). To keep transaction costs at bay (DO6), we decided on the Ethereum blockchain and tested it in the Ethereum test network Ropsten (Github, 2020).

4.3. Evaluation of the artifact

4.3.1. First design iteration

The **first evaluation phase** of Nexo Energy consisted of two testing phases: an extensive technical testing phase and a customer testing phase. For the technical testing phase, we simulated more than 1000 transactions to ensure that data storage on the blockchain and data exchange via smart contracts was secure and resistant to abuse (DO1). Furthermore, we assessed the seamless transmission of data to the cloud component, i.e., the transmission of generation data from the GEI and that of consumption data from local controllers (DO2). This technical testing phase indicated no major flaws in the design and setup of Nexo Energy. Moving on to the user testing phase, we prepared starter kits containing the Raspberry Pi, two WIFI-lamps, and one WIFI-power-socket (Figure A1), as well as relevant installation and setup instructions for 25 test customers. Some of those customers, however, immediately requested more detailed information, especially concerning the function and value proposition of our architecture (DO3). Once installed, the local controller reliably and automatically connected to the two WIFI-lamps, the WIFI-power-socket, and other smart appliances in the test customer's household. Test customers were also able to set their own rules that adjusted the electricity consumption patterns of their connected devices to the availability of local green electricity generation (DO2, DO3).

However, adapting consumption in line with GEI generation was not intuitive and Nexo Energy failed to identify all smart appliances that could have been connected to the local controller (DO3). Another negative to be noted is that customers were unhappy with the original set-up since this required the use of a separate web application (blockchain viewer) to view their loyalty token transactions (Figure A3) (DO1, DO3). Feedback was positive, however, about the use of blockchain to manage loyalty tokens and publish bonuses for the use of GETs. To improve usability in this regard, customers were only provided with a simplified version of this data on the user dashboard. Feedback was also positive in relation to trust-enhancing elements of blockchain, i.e., its transparency and tamper-resistance (DO1). Meanwhile, the costs of hardware and services were deemed acceptable by electricity suppliers and customers alike (DO6). Since the first evaluation phase was primarily aimed at collecting customer feedback on the basic functions of Nexo Energy, questions about maintainability and efficiency were postponed to the second evaluation phase (DO4, DO5).

4.3.2. Second design iteration

In the **second evaluation phase**, we considered the feedback received during the first evaluation phase and adapted the setup and usability of Nexo Energy accordingly. To make the dashboard more accessible to customers, we integrated the blockchain viewer into the cloud dashboard (DO3, DO2). In addition, we engaged a design thinking coach to create illustrations that would explain the basic functions of Nexo Energy to customers and make the underlying value propositions more tangible and comprehensible. Some of these were retrospectively added to the starter kit (DO3). To make the connection of smart appliances less cumbersome, we added a green flower icon in the customer dashboard to all compatible appliances. One click on a smart appliance marked with this green flower icon would open a submenu in which customers could set a threshold for the minimum availability of green electricity in the grid, and this minimum measure could easily be brought in line with GEI. Accordingly, all appliances would turn off when the availability of green energy was below the selected threshold; above it, they would turn on (DO3).

Even though these improvements appealed to customers, we saw fewer interactions and received less feedback. When we asked the test customers about this change in behavior, they indicated that they had been engaging in fewer interactions due to the many down-times and long loading times of their customer dashboards (DO4). Those loading times had gone up from the acceptable maximum of 5–30 s, and customers dealing with more than one local controller were most affected by this negative development (DO2, DO4). We assumed the reason for these prolonged waiting times to be the data synchronization cycles between the local controllers and the cloud controller, but in order to be sure we scheduled a cause investigation for the third evaluation phase.

4.3.3. Third design iteration

In the **third evaluation phase,** we made improvements to downtimes and data synchronization rates (DO4), and added monitoring capabilities for IT administrators (DO5). As suspected, the interoperability and interconnectivity problems were caused by inefficient data synchronization between the cloud controller and local controllers (DO2, DO4). To resolve this issue, we introduced asynchronous queries that keep loading times within acceptable limits. We also managed to reduce downtimes after moving Nexo Energy to a stable development and production environment in which technical tests were simpler. Throughout these tests, we determined that certain flaws in the code were the cause of system instabilities which had led to the initial downtimes (DO4).

In the third evaluation phase, the loading times of local controllers were tracked by both customers and developers. Due to the limited monitoring capabilities of local controllers, however, we had to rely primarily on user feedback to determine exact loading latencies (DO4, DO5). This illustrated the need for an additional, automated monitoring capability (DO5). Customers also had achieved a deeper understanding of the underlying blockchain technology and criticized the management of their blockchain addresses (DO1). In the first and second design iteration, we had bundled the management of the supplier and customer addresses in one blockchain wallet, since doing so took account of usability and digital literacy (DO3), but now customers explicitly requested their own blockchain wallets and more control (DO1). Meanwhile, the general interest that customers showed in Nexo Energy had increased considerably, which is why a separate, simple ordering tool (DO5) was set up for the supplier's entire customer base.

4.3.4. Final design

When working on the **final design** in the fourth evaluation phase of Nexo Energy, we focused on making the monitoring capabilities of IT administrators more efficient, so we introduced an IT admin dashboard (Figure A4). This dashboard allowed IT administrators not just to view the on- or offline status of local controllers but also to assess the latency of loading times as it showed the electricity consumption of all smart appliances connected to local controllers (DO4, DO5). Should a connected appliance not respond, IT administrators were able to initiate a problem diagnosis (DO5). The decision to use only a single blockchain wallet was reversed, and customers were given their own wallets (DO1, DO3). They were further given the opportunity to connect any valid Ethereum blockchain address to their local controllers (DO1). Moreover, it was now possible to order Nexo Energy via the electricity supplier's website (DO5).

Feedback from IT administrators indicated that the IT admin dashboard was as user-friendly as it was functional in performing such essential tasks as monitoring local controllers (DO5). Customers appreciated the possibility to access their blockchain addresses directly, which increased the general feeling of technical emancipation and trust (DO1). Furthermore, the convenient method of ordering Nexo Energy via the electricity supplier's website had a positive impact on its perceived usability (DO3, DO5). The outcome of the four evaluation phases showed that all DRs and DOs had been considered and refined in the various design iterations (Table A3), which allows us to conclude

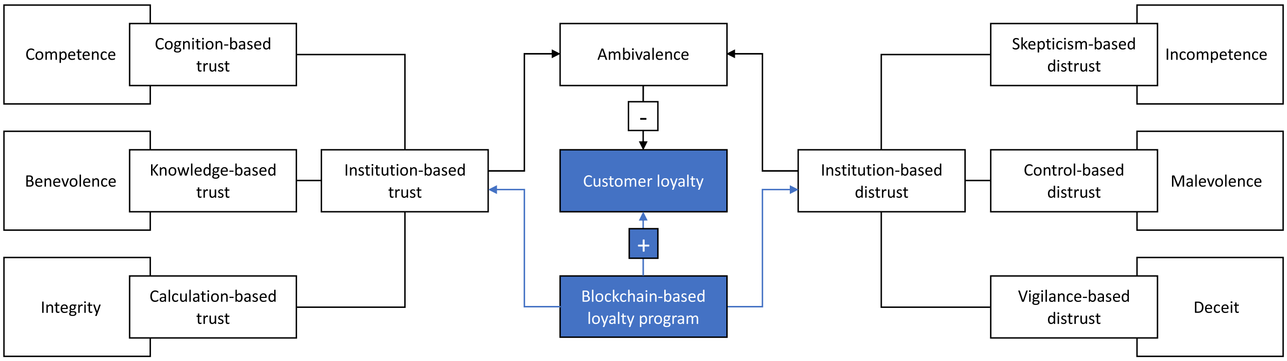


Fig. 4. Overview of the positive effects of our blockchain-based loyalty program on institution-based trust, institution-based distrust, and ambivalence.

that the presented architecture fulfills the required intention-design fit (Gregor & Hevner, 2013; Hevner et al., 2004).

5. Discussion

The evaluation of our conceptual architecture produced a number of insights of general validity concerning the design of blockchain-based customer loyalty programs. Following in the footsteps of Gregor and Hevner (2013) and Baskerville, Baiyere, Gregor, Hevner, and Rossi (2018), we have identified four design principles that promise to be of use to practitioners who wish to design and successfully implement such programs.

In using blockchain technology for our artifact and its multiple design iterations, we also contribute to theory. Specifically, we indicate how blockchain can help to restore *institution-based trust*, restrict *institution-based distrust*, and resolve *ambivalence* for customers dealing with electricity suppliers. In doing so, we connect theories about *institution-based trust* (McKnight et al., 2017; Moody et al., 2017), *ambivalence* (Moody et al., 2017), and *institution-based distrust* (Kramer, 1999; McKnight & Chervany Norman, 2001; McKnight & Choudhury, 2006). In conjunction, these theories account for many of the intricacies of customer loyalty (Chu et al., 2012; Stathopoulou & Balabanis, 2016). Moreover, their successful integration into a DSR approach underlines the importance of bringing together theory and practice when it comes to the development of innovative solutions for complex problems (Gregor & Hevner, 2013; Kuechler & Vaishnavi, 2012).

5.1. Practical implications

The loss of customer loyalty is not a unique problem for electricity suppliers. Across multiple industries, such as hospitality (Kandampully, Zhang, Christina & Bilgihan, 2015; McCall & McMahon, 2016) and retail (Vesel & Zabkar, 2009; Yi, Youjae & Hoseong, 2003), service providers are struggling to retain their customers. One way to reverse this trend and increase customer loyalty is to implement loyalty programs that can help develop long-lasting relationships between service providers and their customers (Hofman-Kohlmeyer, 2016). Basing these programs on blockchain technology, rather than on regular databases, promises to be an important mediator on the customer's journey from *ambivalence* to *institution-based trust*; as we have shown, blockchain does this by virtue of its inherent properties (Amend & Kaiser, 2021; Rieger et al., 2019; Roth et al., 2022; Sedlmeir et al., 2020). Since the four design principles that emerged in the development and evaluation of our conceptual architecture can be abstracted and generalized, they may support a broad variety of practitioners.

5.1.1. DP1 – Give customers agency

When evaluating customer feedback in our design iteration phases, we learned that customers value choices (Interviews 1,3,5,6,7,8,9,12). Although they initially found it somewhat challenging to set their own rules for smart appliances and determine thresholds for electricity in line with GETs, they became increasingly appreciative of the level of personalization afforded to them by Nexo Energy (Interviews 2,3,4,5,10,11,12). Another positive impression shared by several test subjects was that, unlike many other customer loyalty programs (Bulbul & İnce, 2018; Uncles et al., 2003), Nexo Energy allowed customers to use their obtained loyalty tokens for a purpose of their own choosing (Interviews 1,2,3,6,7,8,9,10). Our test customers appreciated that they could exchange their tokens for fiat money or use them at participating public utility companies to pay for such services as the rental of electric scooters or cars. Other options were also welcomed, such as the opportunity to reinvest one's tokens into shares of RES. This general appreciation extended to the fact that the value of these tokens is high because they are not exclusive to the electricity supplier. Indeed, they have value beyond the loyalty program (Interviews 2,3,5,6,7,9,11) since there are multiple other reinvestment opportunities, which give the tokens a much broader appeal. One positive side-effect of this broadened loyalty token scheme is that customers feel their choices are taken seriously, so much so that these choices can have an impact beyond consumption (Interviews 1,2,3,4,6,7,8,10,11). Customers are most likely to enjoy this sense of choice and real agency when customer loyalty programs do not anticipate all services but instead leave room for customers to shape their own portfolio of desired services and functions.

5.1.2. DP2 – Provide customers with sufficient and verifiable information

In the first evaluation phase, customers criticized the customer kit that presented Nexo Energy's value propositions. According to this initial feedback, there was too much information and too little clarity (Interviews 2,3,5,6,8,9,10,11,12). Such poor communication and insufficient verifiability were the root cause of customer skepticism (Interviews 2,3,5,6,7,9,11). With this in mind, we consulted a design thinking coach in the second design iteration to help us provide accessible explanations and tangible value propositions for Nexo Energy. After all, customers require more information than superficial knowledge about the purpose of a service if they are to assess the trustworthiness of their electricity supplier (Interviews 3,5,7,8,9). Of particular interest in this context is the sustainability of electricity. Since all of the information on this key factor is transparently and immutably stored on the blockchain, customers can easily check whether their electricity is as sustainable as promised by their GETs (Interviews 2,3,5,7). Likewise, all other data posted on the user dashboard is verifiable by customers. If need be, customers can control the compliance with individually determined rules and set GET thresholds for every smart appliance and every single transaction. Since such simple consumption management and reliability control of GETs are enormously attractive, customer loyalty programs should proactively ensure that customers can access all required information in an easily verifiable manner.

5.1.3. DP3 – Consider appropriate levels of usability for customers

Customers have varying levels of digital literacy (Interviews

2,4,5,6,7,8,9). What they all have in common, however, is the desire for equal access to offered services (Interviews 1,4,5,6,8,12). Making everything equally accessible is particularly challenging, however, when it involves the use of innovative technologies like blockchain. As evaluations of Nexo Energy have indicated, the user interface should be as simple and intuitive as possible (Interviews 1,2,4,6,7,11,12). Irrespective of how complex the underlying processes turn out to be, the user interface ought to contain nothing more than the didactically minimum of information required to make use of the technology's functions. This also applies to the execution of services. It should be automized as far as possible, which is to say that customers should only have to take individual steps themselves in relevant situations, where either their choice or their consent is required. To improve usability accordingly, Nexo Energy bundled the blockchain addresses of all its customers in the energy provider's wallet. This decision, however, was met with significant backlash from digitally rather emancipated customers, so we reversed it in the fourth design iteration and gave customers their own blockchain wallets (Interviews 4,6,7,8,9). What this process showed us is that, although data stored directly on the blockchain is difficult to read and would exceed the digital literacy of most users, service providers should not decide on behalf of all customers which functions each of them is allowed to use. Instead, service providers would do well to offer a spectrum. As long as the key message is retained also at the didactically most simplified level, users are not disadvantaged, not even if they cannot understand the information at the most granular level (Interviews 1,2,4,5,8,11). In short, customer loyalty programs should not proactively reduce access to more granular information but instead provide different levels of didactical reduction while retaining the basic message.

5.1.4. DP4 – Give data access to customers

Information asymmetry between an electricity supplier and its customers puts the latter in the uncomfortable position of having to take the supplier's assurances on faith, without knowing whether this faith will be repaid (Ambrose, 2021; Guo et al., 2014; Mezger et al., 2020). With the introduction of blockchain technology, however, loyalty programs can provide customers with a tamper-resistant transaction record stored in a distributed fashion (Amend & Kaiser, 2021; Rieger et al., 2019; Sedlmeir et al., 2020). This record includes hashes of all consumption and generation values as well as the respective token transactions. To increase usability, an early version of Nexo Energy only provided customers with a simplified version of this data on the user dashboard. Customers had no way of verifying the displayed data. With advancing digital literacy, however, customers demanded access to their blockchain addresses in order to directly monitor electricity consumption and generation data as well as loyalty token transactions on the blockchain (Interviews 1,4,5,6,7,9). After this considerable reduction of 'data asymmetry', customers came to appreciate that blockchain technology enables the desired checks and balances required to create an equal footing for customers and suppliers (Interviews 1,4,5,7,8,11,12). While many service providers fear the effects of giving customers unlimited and transparent access to their data (Merlo, Eisingerich, Auh, & Levstek, 2018), our analysis of Nexo Energy indicates that such customer emancipation does not alienate customers from their supplier (Interviews 2,3,4,7,8,9). Far from it, the result was a feeling of empowerment that strengthens the bond between customer and service provider (Interviews 1,2,4,5,6,7,10,11). Consequently, customer loyalty programs promise the greatest success if they include an option for customers to be granted access to all relevant and verifiable data.

5.2. Theoretical implications

The four identified design principles provide more than actionable guidelines for the development of specific blockchain-based customer loyalty programs. They also offer insights into *trust*-restoring, *distrust*-reducing, and *ambivalence*-resolving processes, as described in the relevant literature (Kramer, 1999; McKnight & Chervany Norman, 2001; McKnight & Choudhury, 2006; McKnight et al., 2017; Moody et al., 2017). While the relationship between trust and loyalty has been researched and discussed at length (Chu et al., 2012; Martínez & Rodríguez del Bosque, 2013; Nguyen, Leclerc, & LeBlanc, 2013; Stathopoulou & Balabanis, 2016), actionable trust factors have yet to be clearly defined (Chaudhuri & Holbrook, 2001; Stathopoulou & Balabanis, 2016). Some have hypothesized that *institution-based distrust* and *ambivalence* have a negative impact on customer loyalty, but this supposed impact has yet to be observed in practice (Lee et al., 2015; Yen, 2010). In the following, we do exactly that by demonstrating how our blockchain-based architecture and its underlying design principles function as mediating factors (Fig. 4) to rebuild *institution-based trust* (McKnight et al., 2017; Moody et al., 2017), reduce *institution-based distrust* (Kramer, 1999; McKnight & Chervany Norman, 2001; McKnight & Choudhury, 2006; Moody et al., 2017), and resolve *ambivalence* (Moody et al., 2014, 2017).

As illustrated in Fig. 4, our blockchain-based architecture counters *ambivalence* and mediates between the two latent constructs of *trust* and *distrust* as well as their respective latent factors (Kramer, 1999; McKnight & Chervany Norman, 2001; McKnight & Choudhury, 2006; McKnight et al., 1998, 2017).

5.2.1. Impact on institution-based trust

Although some prior studies have made attempts to base customer loyalty programs on blockchain technology (Agrawal et al., 2018; Bulbul & İnce, 2018; Choi, 2018), they have not elaborated on the intricate relationship between *institution-based trust* factors and blockchain properties, nor have they analyzed how their interplay fosters customer loyalty. To do so, we focused on increased customer agency when we defined our **first design principle (DP1)**. Customers are given the opportunity to tailor the services and functions of Nexo Energy in a self-responsible fashion, which is to say they can choose to adjust any and all of them to their needs and priorities. No longer are they passive consumers of electricity at the mercy of predefined GETs (Ambrose, 2021; Guo et al., 2014; Mezger et al., 2020). Instead, customers become actively involved in a bilateral process; directly setting goals for their electricity consumption and indirectly setting goals for their electricity supplier's sustainability agenda. As a result, the supplier and its customers have a common goal, which is an essential dimension in the creation of *cognition-based trust* (Cheng et al., 2021; McKnight et al., 1998). Furthermore, the possibility to reinvest blockchain loyalty tokens into shares of RES proves to customers that the supplier is *competently* supporting the distribution of green electricity, rather than attempting to deceive its customers (Ambrose, 2021; Mezger et al., 2020). Having an immutable and transparent transaction record of loyalty tokens on the blockchain further emancipates customers in the sense that the supplier invests them with verification capabilities (Ziolkowski et al., 2020). Moreover, since the use of Nexo Energy requires continuous interaction between the supplier and its customers, the latter gain the reassuring feeling that their choices are being taken seriously, so much so that they can have a real impact on the supplier's development of its business model. This is a contributing factor to *knowledge-based trust* (Cheng et al., 2021; Li, Pieńkowski, Van Moorsel, & Smith, 2012; McKnight et al., 1998) as it indicates the *benevolence* of electricity suppliers (Moody et al., 2017).

In defining our **second design principle (DP2)**, we took account of the high value that customers place on the possession of sufficient and verifiable information, especially the kind that they can personally access and verify. At present, the poor state of information provision and the insufficient verifiability of said information are the root causes of skepticism concerning GETs and related 'greenwashing' allegations

(Ambrose, 2021; Andoni et al., 2019; Mezger et al., 2020). During the multiple design iterations of Nexo Energy, we tried to eliminate the perceived information asymmetry by giving customers access to the blockchain component. The ensuing verifiability of information about hashes of consumption and generation data (Ahl et al., 2020; Perrons & Cosby, 2020) enabled customers to check whether the system complied with their individually determined rules as well as with the GEI thresholds of smart appliances. As we saw, this lets customers appreciate the supplier's *competency* to uphold contractually agreed services, which is seen as 'evidence of trustworthiness' or 'good reasons' to develop *cognition-based trust* (Cheng et al., 2021; McAllister, 1995). Furthermore, when given access to hashes of values concerning both consumption data and generation data as well as token transactions, customers are better able to assess the benefits of participating in Nexo Energy. Allowing customers to see and calculate all of the costs and benefits proved to be the foundation for *calculation-based trust* (Cheng et al., 2021; McKnight et al., 1998). It also provided obvious evidence of the electricity supplier's *integrity* (Moody et al., 2014, 2017).

In defining our **third design principle (DP3)**, we placed the emphasis on appropriate levels of usability for customers. While innovative technologies like blockchain entail many highly technical functions that would confuse average customers, we found that electricity suppliers do well not to preclude access to more detailed information. This was an important lesson learned during the design iterations of Nexo Energy, where the customers' blockchain wallets and control over their blockchain addresses were initially eliminated yet later reinstated due to notable customer disapproval. Having not only access to information as well as control over it because it is directly stored on the blockchain (Perrons & Cosby, 2020; Seebacher & Schüritz, 2017), customers can judge the reliability of their supplier along with its *competence* (Ibrahim & Ribbers, 2009) to deliver the agreed services (*cognition-based trust*) (Cheng et al., 2021; McAllister, 1995). Perhaps just as important is the fact that they can judge not only its *integrity* to deliver benefits for the customer (*calculation-based trust*) (Li et al., 2012; McKnight et al., 1998), but also its *benevolence* as this is instantly apparent when looking at the immutable transaction-history (*knowledge-based trust*) (Cheng et al., 2021; McKnight et al., 1998). To make such a comprehensive judgement possible, suppliers can provide this immutable and transparent data record on the blockchain (Hameed, Barika, Garg, Amin, & Kang, 2022; Sedlmeir et al., 2020; Zhang et al., 2019). Suppliers can also simplify auditability (Amend & Kaiser, 2021) on the user dashboard to cater to their less digitally-literate customers. As a result, all customers can rest assured that the supplier is trying to engage them equally in its endeavor to rebuild *institution-based trust*.

When defining our **fourth design principle (DP4)**, we concentrated on the importance of sufficient data access for customers. The current information asymmetry between electricity suppliers and customers makes it difficult for the latter to base their trust on rational decision-making (Bélanger & Carter, 2008; Dietz & Gillespie, 2011; van der Werff et al., 2019). It stands to reason, then, that customers are rather unwilling to be vulnerable to a supplier's policy changes (Ambrose, 2021; Cheng et al., 2021; Mezger et al., 2020; Tams et al., 2018). In the interest of more rational decision-making, we found that blockchain technology can be introduced into loyalty programs to ensure that customers have a tamper-resistant transaction record stored in a distributed leger (Amend & Kaiser, 2021; Rieger et al., 2019; Sedlmeir et al., 2020). However, letting customers assess consumption and generation data (Ahl et al., 2020; Perrons & Cosby, 2020) not only restores *cognition-based trust*. It also provides customers with their desired checks and balances (Abbas et al., 2020), which is to say it creates the necessary foundation on which customers can achieve an equal footing with their supplier. This empowerment of customers through the use of blockchain technology indicates a much-needed openness of the part of the electricity suppliers, which drives both *calculative-based* and *knowledge-based trust* (Ibrahim & Ribbers, 2009).

5.2.2. Impact on institution-based distrust

While there is already an extensive body of literature on the relationship between blockchain technology and trust (Abbas et al., 2020; Hawlitschek et al., 2018; Werbach, 2018), the research does not extend to the far-reaching ways in which the use of blockchain technology can reduce *institution-based distrust*. In developing our **first design principle (DP1)**, we discovered that an increase in customer agency leads to a decrease in their fear of *deceit* and thus a decrease in *vigilance-based distrust*. Customers can assume the responsibility of setting rules for their consumption patterns in line with GEIs, and they can use their blockchain-based loyalty tokens to invest in a purpose of their own choosing. They can even look at the blockchain to assess the system's compliance with their predefined choices (Kramer, 1999; McKnight & Chervany Norman, 2001). So far, countless customers are likely to have suspected that their electricity supplier is *incompetent* to deliver the agreed units of green electricity, as indicated by their GETs to date (Ambrose, 2021; Guo et al., 2014). This has encouraged a notable degree of *skepticism-based distrust* (Kramer, 1999; McKnight & Chervany Norman, 2001). Going forward, however, they have the possibility to reinvest their tokens into shares of RES, which would automatically increase the distribution and availability of green electricity. What is more, when a supplier offers customers such reinvestment opportunities, it indicates that they share a common goal.

Both our **second design principle (DP2)** and our **fourth design principle (DP4)** had a moderating effect on *skepticism-based distrust* and *control-based distrus*t. The ample provision of information and access to data immutably stored on the blockchain (Amend & Kaiser, 2021; Rieger et al., 2019; Sedlmeir et al., 2020) enabled customers to accumulate verifiable information. This prevented suspicions of *incompetence* and *malevolence* on the part of the electricity supplier (Kramer, 1999; McKnight & Choudhury, 2006; Moody et al., 2017). After all, since the information on the sustainability of electricity generated with GEI and hashes of consumption data are transparently stored on the blockchain, customers can easily detect retrospective changes to the data history (Sedlmeir et al., 2020).

Our **third design principle (DP3)** indirectly affects all three *institution-based distrust* dimensions: *skepticism-based distrust*, *control-based distrust*, and *vigilance-based distrust*. Without a tool like a blockchain viewer, customers are unable to monitor their data and accumulate the information required to assess the trustworthiness of their electricity suppliers (Kramer, 1999; McKnight & Choudhury, 2006; Moody et al., 2017). Moreover, they are unable to actively decide which individual services they would like to tailor to their specific needs. As our study has shown, however, usability is key to leveraging the potential of blockchain technology for customers, irrespective of how complex the underlying processes may be. Customers should, therefore, be able to access all essential information – even at the didactically most simplified level – to make their own rational choices and risk assessments (McKnight & Chervany Norman, 2001).

5.2.3. Creation of customer loyalty

As indicated in Fig. 4, an increase in *institution-based trust* and a decrease in *institution-based distrust* should notably reduce *ambivalence* (Moody et al., 2017). As we saw when deriving our design principles (DP1-DP4) from our blockchain-based customer loyalty program, it is possible to resolve the conflict between the competing latent constructs of *trust* and *distrust* (Jarvenpaa & Majchrzak, 2010; Moody et al., 2014). By providing unobstructed access to consumption and generation data (DP2, DP4) along with increased customer agency (DP1) and improved usability of technical monitoring tools (DP3), service providers can support the restoration of *institution-based trust* as well as the reduction of *institution-based distrust*.

As discussed in previous literature, reducing *ambivalence* may also have a positive impact on customer loyalty (Moody et al., 2017; Olsen et al., 2005). This would confirm assumptions that *ambivalence* is at the threshold of distrusting attitudes and that the behavior it motivates could negatively affect loyalty (Jonas, Broemer, & Diehl, 2000; Olsen et al., 2005). On the other hand, customers who felt empowered by Nexo Energy and saw themselves as active partners in this trust relationship indicated that they had little reason to distrust their electricity supplier. Since our proposed conceptual architecture facilitates this, it may indeed foster customer loyalty by virtue of resolving *ambivalence*, restoring *institution-based trust*, and reducing *institution-based distrust.*

5.3. Limitations of this study and potential for further research

Our study provides insights into how energy suppliers can design a customer loyalty program based on blockchain technology. The design principles derived from our artifact further indicate how blockchain technology can restore *institution-based trust* as well as reduce *institution-based distrust* and resolve *ambivalence* concerning electricity suppliers. These principles are predicated on theories about *institution-based trust* (McKnight et al., 2017; Moody et al., 2017) and *institution-based distrust* (Kramer, 1999; McKnight & Chervany Norman, 2001; McKnight & Choudhury, 2006). Their multiple dimensions contribute significantly to whether or not customer loyalty is promoted (Chu et al., 2012; Stathopoulou & Balabanis, 2016). Despite our best efforts at rigorous analysis, however, this study is also subject to certain limitations.

Firstly, we did not quantify the electricity volumes that were affected by changes in consumption patterns due to the customers' predefined rules. Such quantification would have been necessary to evaluate effects beyond the customer-supplier relationship, such as the effects on distribution grid management. However, obtaining the necessary amount of quantitative data would have required a considerably larger test group as well as a far longer test period. Future research could, therefore, build on this study to evaluate such effects several months after broad implementation.

Secondly, our four design principles and our propositions concerning their effects on *institution-based trust* and *institution-based distrust* rely on a purely qualitative analysis supported by interviews and a comprehensive literature review. Additional quantitative analysis could determine the connection and interplay between both factors. Further research could particularly explore SEM-plots or hierarchical linear modeling based on quantitative data from questionnaires.

A final observation worth making here is that we only evaluated only one motivational factor, and we did so without considering its interplay with other motivational factors that may be driving how customers select and engage with their electricity suppliers. For instance, not all of them will be equally interested in sustainability, nor are all of them likely to respond with equal enthusiasm to increased customer agency and customer involvement. For many, cost factors may play a much more prominent role. With this in mind, future researchers may want to consider how customer intentions and preferences affect our proposed design principles and trust/distrust factors.

6. Conclusion

In this study, we discuss how blockchain technology can be used to design a customer loyalty program for electricity suppliers and how this blockchain-based customer loyalty program can restore *institution-based trust*, reduce *institution-based distrust*, and resolve *ambivalence* in order to retain or regain customer loyalty. We draw on various theories about the dimensions of *institution-based trust* (McKnight et al., 2017; Moody et al., 2017) and *institution-based distrust* (Kramer, 1999; McKnight & Chervany Norman, 2001; McKnight & Choudhury, 2006). Treating them as antecedents to customer loyalty (Chu et al., 2012; Stathopoulou & Balabanis, 2016), we argue that customer agency, sufficient and verifiable information, appropriate levels of usability, and unobstructed data access can increase customer loyalty. Particularly noteworthy is our finding that the immutable and transparent storage of data on the blockchain can have a significant positive impact on the three dimensions of *institution-based trust* and *institution-based distrust.* The same applies to specifically created customer dashboards for monitoring and blockchain wallets for token transfers. We have reason to believe, therefore, that our DSR approach to customer loyalty can help researchers and practitioners alike in efforts to understand the complex interplay of trust and distrust factors, especially when trying to generate or improve customer loyalty.

CRediT authorship contribution statement

Manuel Utz: Conceptualization, Data curation, Formal analysis, Writing – original draft. **Simon Johanning:** Conceptualization, Data curation, Formal analysis, Writing – original draft. **Tamara Roth:** Conceptualization, Writing – revised draft. **Thomas Bruckner:** Supervision, Writing – review & editing. **Jens Strüker:** Supervision, Writing – review & editing.

Declaration of Competing Interest

None. The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

We gratefully acknowledge the valuable feedback of Alexander Rieger and our anonymous reviewers. Furthermore, we wish to express our gratitude to the Luxembourg National Research Fund (FNR) and PayPal for their support of the PEARL project “P17/IS/13342933/PayPal-FNR/Chair in DFS/ Gilbert Fridgen”.

Appendix

See appendix Figs A1–A4 and Tables A1–A3.

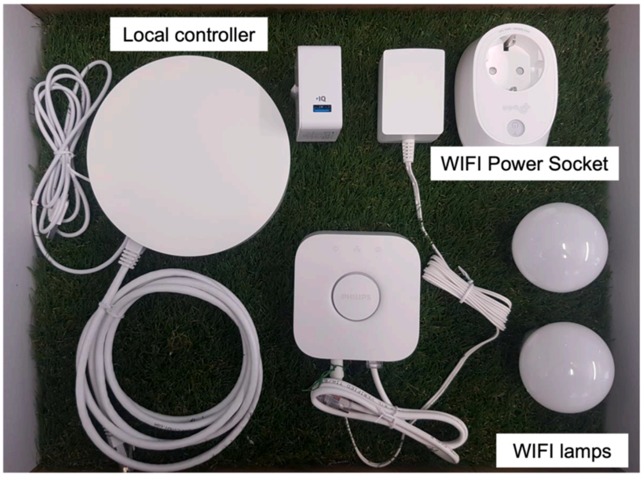
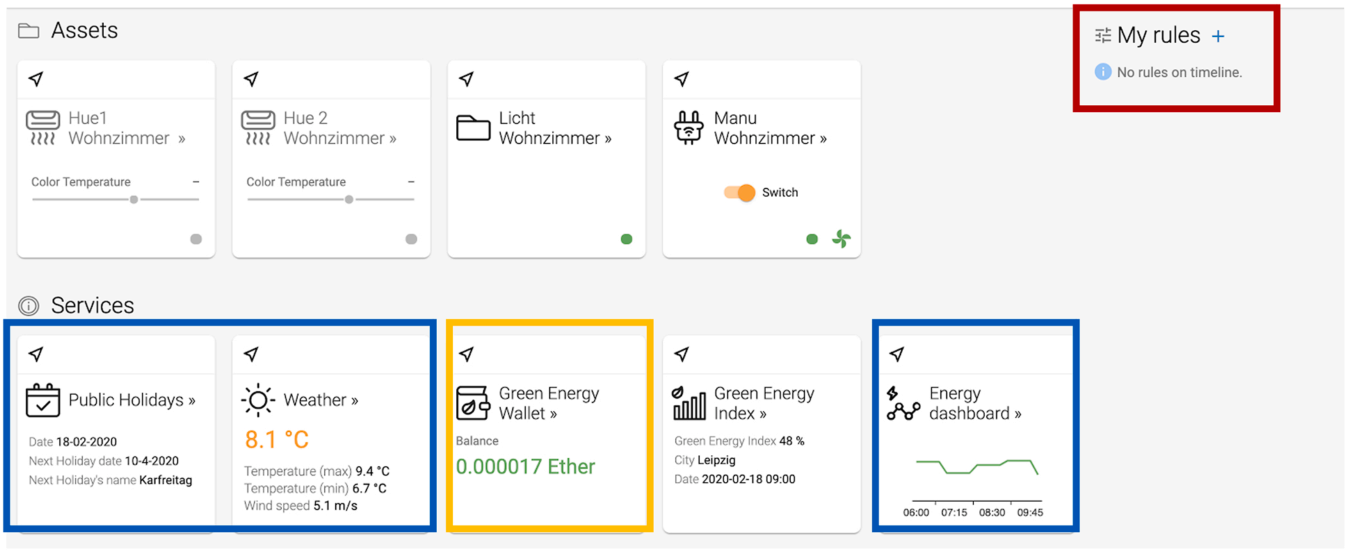


Fig. A1. Nexo Energy Starter Kit.



Assets

Hue1
Wohnzimmer »
Color Temperature

Hue 2
Wohnzimmer »
Color Temperature

Licht
Wohnzimmer »

Manu
Wohnzimmer »
Switch

My rules +
No rules on timeline.

Services

Public Holidays »
Date 18-02-2020
Next Holiday date 10-4-2020
Next Holiday's name Karfreitag

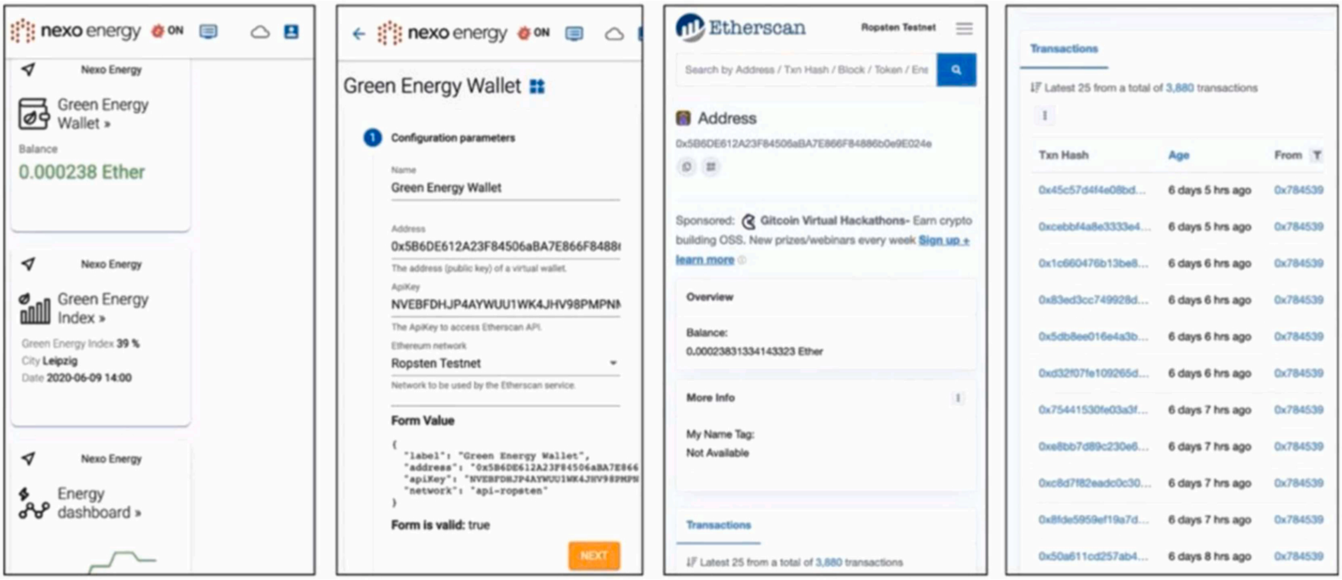
Weather »
8.1 °C
Temperature (max) 9.4 °C
Temperature (min) 6.7 °C
Wind speed 5.1 m/s

Green Energy Wallet »
Balance
0.000017 Ether

Green Energy Index »
Green Energy Index 48 %
City Leipzig
Date 2020-02-18 09:00

Energy dashboard »

Fig. A2. Customer Dashboard.



nexo energy ON

Nexo Energy
Green Energy Wallet »
Balance
0.000238 Ether

Nexo Energy
Green Energy Index »
Green Energy Index 39 %
City Leipzig
Date 2020-06-09 14:00

Nexo Energy
Energy dashboard »

nexo energy ON

Green Energy Wallet

1 Configuration parameters

Name
Green Energy Wallet

Address
0x5B6DE612A23F84506aBA7E866F8488

The address (public key) of a virtual wallet.

ApiKey
NVEBFDHJP4AYWUU1WK4JHV98PMPN

The ApiKey to access Etherscan API.

Ethereum network
Ropsten Testnet

Network to be used by the Etherscan service.

Form Value

```
{
  "label": "Green Energy Wallet",
  "address": "0x5B6DE612A23F84506aBA7E866
  "apiKey": "NVEBFDHJP4AYWUU1WK4JHV98PMPN
  "network": "api-ropsten"
}
```

Form is valid: true

NEXT

Etherscan
Ropsten Testnet

Search by Address / Txn Hash / Block / Token / Ens

Address
0x5B6DE612A23F84506aBA7E866F84886b0e9E024e

Sponsored: Gitcoin Virtual Hackathons- Earn crypto building OSS. New prizes/webinars every week Sign up + learn more

Overview

Balance:
0.00023831334143323 Ether

More Info

My Name Tag:
Not Available

Transactions

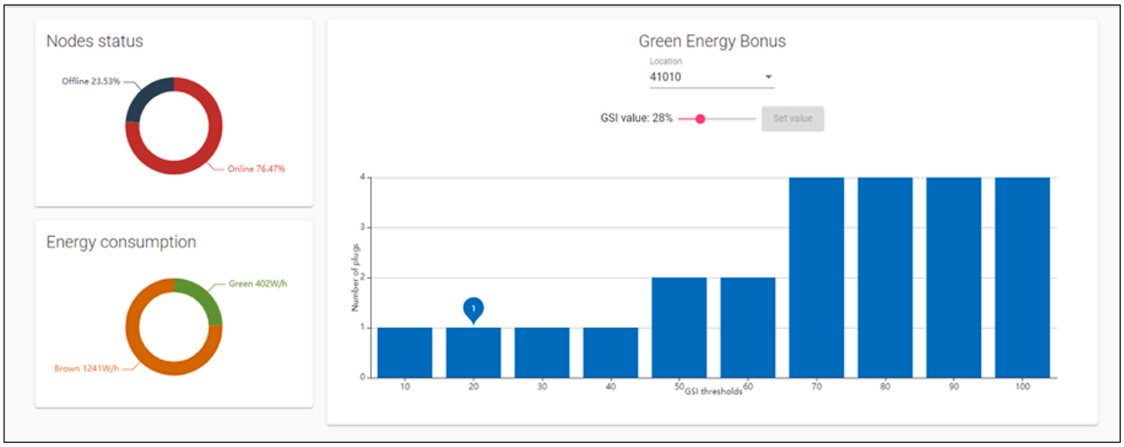
Latest 25 from a total of 3,880 transactions

Transactions

Latest 25 from a total of 3,880 transactions

Txn Hash	Age	From
0x45c57d4f4e08bd...	6 days 5 hrs ago	0x784539
0xcebbf4a8e3333e4...	6 days 5 hrs ago	0x784539
0x1c660476b13be8...	6 days 6 hrs ago	0x784539
0x83ed3cc749928d...	6 days 6 hrs ago	0x784539
0x5db8ee016e4a3b...	6 days 6 hrs ago	0x784539
0xd32f07fe109265d...	6 days 6 hrs ago	0x784539
0x75441530fe03a3f...	6 days 7 hrs ago	0x784539
0xe8bb7d89c230e6...	6 days 7 hrs ago	0x784539
0xc8d7f82eadc0c30...	6 days 7 hrs ago	0x784539
0x8fde5959ef19a7d...	6 days 7 hrs ago	0x784539
0x50a611cd257ab4...	6 days 8 hrs ago	0x784539

Fig. A3. Blockchain Viewer Transaction History.



Nodes status

Energy consumption

Green Energy Bonus

Location
41010

GSI value: 28%

Set value

Fig. A4. IT Admin Dashboard.

Table A1
Ex-Ante and Evaluation Interviews.

No.	Organisation	Role
Evaluation Interviews		
1	Energy utility	Head of Energy Asset Mgmt.
2	Energy utility	Teamlead Energy Products
3	Energy utility	Teamlead Energy Metering
4	Energy utility	IT Architect Digital Energy Solutions
5	Energy utility	Head of Data Security/ Data Center
6	Energy utility	Head of Dev. Ops
7	Energy utility	Head of Virtual Power Plants
8	Energy utility	Head of IT
9	Energy utility	IT Architect Digital Energy Solutions
10	Energy utility	Head of Virtual Power Plants
11	Energy utility	Fullstack Developer
12	Energy utility	Fullstack Developer
Ex-Ante Interviews		
13	Non-Profit Organization	Head of Electric Mobility
14	E-Mobility Start-Up	Product and Partner Manager
15	Energy Start-Up	Energy Sales and Business Development
16	Blockchain Start-Up	Business Development
17	Research Institute	Researcher
18	Software Company	Director Operations
19	Blockchain Start-Up	Chier Operations Officer
20	Consulting	Head of DLT
21	Energy utility	Head of Data Lab
22	Law office	Lawyer
23	Energy Service Provider	Digital Project Lead
24	Software Company	Head of Venture Creation
25	Non-Profit Organization	Head of Electric Mobility
26	E-Mobility Start-Up	Product and Partner Manager
27	Energy Start-Up	Energy Sales and Business Development
28	Blockchain Start-Up	Business Development
29	Research Institute	Researcher
30	Software Company	Director Operations

Table A2
Description of Design Requirements.

DO	DR	Description
DO1 (Accountability)	DR1	Tamper-proof and easily accessible storage of data in the blockchain network
	DR2	Tamper-proof and automated data processing
DO2 (Customizability)	DR3	Secure storage of electricity generation data
	DR4	Secure storage of electricity consumption data
	DR5	Intuitive and comprehensive adjustment of electricity consumption
DO3 (Simplicity)	DR6	Deliver all information for setup process
	DR7	Automatic smart device detection
	DR8	Intuitive user interface
DO4 (Efficiency)	DR9	Fast data synchronization between software components
	DR10	High software uptime and availability
DO5 (Maintainability)	DR11	Easy to monitor by IT administrator staff
	DR12	Easy to order for customers
DO6 (Affordability)	DR13	Affordable for customers
	DR14	Reasonable costs for operation

Table A3
Fulfilment of DOs and DRs during all Design Iterations.

DO	DR	Description	Initial Design	Second Design Iteration	Third Design Iteration	Final Design
DO1	DR1	Tamper-proof and easily accessible storage of data in the blockchain network	🟩	🟩	🟨	🟩
	DR2	Tamper-proof and automated data processing	🟩	🟩	🟩	🟩
DO2	DR3	Secure storage of electricity generation data	🟩	🟩	🟩	🟩
	DR4	Secure storage of electricity consumption data	🟩	🟩	🟩	🟩
	DR5	Intuitive and comprehensive adjustment of electricity consumption	🟨	🟩	🟩	🟩
DO3	DR6	Deliver all information for setup process	🟨	🟩	🟩	🟩
	DR7	Automatic smart device detection	🟩	🟩	🟩	🟩
	DR8	Intuitive user interface	🟨	🟩	🟩	🟩
DO4	DR9	Fast data synchronization between software components	🟧	🟧	🟩	🟩
	DR10	High software uptime and availability	🟧	🟧	🟩	🟩
DO5	DR11	Easy to monitor by IT administrator staff	🟧	🟧	🟧	🟩
	DR12	Easy to order for customers	🟧	🟧	🟧	🟩
DO6	DR13	Affordable for customers	🟩	🟩	🟩	🟩
	DR14	Reasonable costs for operation	🟩	🟩	🟩	🟩

References

Abad, A. V., & Dodds, P. E. (2020). Green hydrogen characterisation initiatives: definitions, standards, guarantees of origin, and challenges. *Energy Policy, 138*, Article 111300. https://doi.org/10.1016/j.enpol.2020.111300

Abbas, Y., Martinetti, A., Moerman, J. J., Hamberg, T., & van Dongen, L. A. M. (2020). Do you have confidence in how your rolling stock has been maintained? A blockchain-led knowledge-sharing platform for building trust between stakeholders. *International Journal of Information Management, 55*, Article 102228. https://doi.org/10.1016/j.ijinfomgt.2020.102228

Agrawal, D., Jureczek, N., Gopalakrishnan, G., Guzman, M., McDonald, M., & Kim, H. (2018). Loyalty Points on the Blockchain. *Business and Management Studies, 4*. https://doi.org/10.11114/bms.v4i3.3523

Ågerfalka, P. J., Axelsson, K., & Bergquist, M. (2022). Addressing climate change through stakeholder-centric information systems research: A Scandinavian approach for the masses. *International Journal of Information Management, 63*, Article 102447. https://doi.org/10.1016/j.ijinfomgt.2021.102447.

Ahl, A., Yarime, M., Goto, M., Chopra, S. S., Kumar, N. M., Tanaka, K., & Sagawa, D. (2020). Exploring blockchain for the energy transition: Opportunities and challenges based on a case study in Japan. *Renewable and Sustainable Energy Reviews, 117*, Article 109488. https://doi.org/10.1016/j.rser.2019.109488

Al Khalil, F., Butler, T., O'Brien, L., & Ceci, M. (2017). Trust in Smart Contracts is a Process. *As Well.* https://doi.org/10.1007/978-3-319-70278-0_32

Ambrose, J. (2021). How green is your 'green' energy tariff? The Guardian. https://www.theguardian.com/business/2021/apr/02/green-energy-tariff-renewable-deals.

Amend, J., Fridgen, G., Rieger, A., Roth, T., & Stohr, A. (2021). The evolution of an architectural paradigm-using blockchain to build a cross-organizational enterprise service bus. 54th Hawaii International Conference on System Sciences (HICSS), Maui, Hawaii (Virtual).

Amend, J., Kaiser, J., Uhlig, L., Urbach, N., & Völter, F. (2021). What do we really need? A systematic literature review of the requirements for blockchain-based e-government services. *Wirtschaftsinformatik 2021 Proceedings. Wirtschaftsinformatik 2021 Proceedings*, 4.

Andersen, J. V., & Bogusz, C. I. (2019). Self-organizing in blockchain infrastructures: generativity through shifting objectives and forking. *Journal of the Association for Information Systems, 20*(9), 1242–1273. https://doi.org/10.17705/1jais.00566

Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., … Peacock, A. (2019). Blockchain technology in the energy sector: a systematic review of challenges and opportunities. *Renewable and Sustainable Energy Reviews, 100*, 143–174. https://doi.org/10.1016/j.rser.2018.10.014

Ante, L., Steinmetz, F., & Fiedler, I. (2021). Blockchain and energy: a bibliometric analysis and review. *Renewable and Sustainable Energy Reviews, 137*, Article 110597. https://doi.org/10.1016/j.rser.2020.110597

Arkesteijn, K., & Oerlemans, L. (2005). The early adoption of green power by Dutch households an empirical exploration of factors influencing the early adoption of green electricity for domestic purposes. *Energy Policy, 33*(2), 183–196. https://doi.org/10.1016/S0301-4215(03)00209-X

Bang, H. K., Ellinger, A. E., Hadjimarcou, J., & Traichal, P. A. (2000). Consumer concern, knowledge, belief, and attitude toward renewable energy: an application of the reasoned action theory. *Psychology and Marketing, 17*(6), 449–468. https://doi.org/10.1002/(SICI)1520-6793(200006)17:6<449::AID-MAR2>3.0.CO;2-8

Bansal, H. S., Taylor, S. F., & James, Y. S. (2005). "Migrating" to new service providers: toward a unifying framework of consumers' switching behaviors. *Journal of the Academy of Marketing Science, 33*(1), 96–115. https://doi.org/10.1177/0092070304267928

Baskerville, R., Baiyere, A., Gregor, S., Hevner, A., & Rossi, M. (2018). Design science research contributions: finding a balance between artifact and theory. *Journal of the Association for Information Systems, 19*, 358–376. https://doi.org/10.17705/1jais.00495

Baumgarte, F., Glenk, G., & Rieger, A. (2020). Business models and profitability of energy storage. *IScience, 23*(10), Article 101554. https://doi.org/10.1016/j.isci.2020.101554

Beck, R., Müller-Bloch, C., & King, J. L. (2018). Governance in the blockchain economy: a framework and research agenda. *Journal of the Association for Information Systems, 19* (10), 1.

Bélanger, F., & Carter, L. (2008). Trust and risk in e-government adoption. *Journal of Strategic Information Systems, 17*(2), 165–176. https://doi.org/10.1016/j.jsis.2007.12.002

Berry, L. L., Parasuraman, A., & Zeithaml, V. A. (1988). SERVQUAL: a multiple-item scale for measuring consumer perceptions of service quality. *Journal of Retailing, 64*(1), 12–40.

Bilgic, A., Hoogensen Gjørv, G., & Wilcock, C. (2019). Trust, distrust, and security: an untrustworthy immigrant in a trusting community. *Political Psychology, 40*(6), 1283–1296. https://doi.org/10.1111/pops.12613

Bogensperger, A., Zeiselmair, A., Hinterstocker, M., & Dufter, C. (2018). Blockchain technology - opportunity to transform the energy industry? Use cases. Forschungsstelle Für Energiewirtschaft e.V.

Bulbul, S., & İnce, G. (2018). Blockchain-based framework for customer loyalty program. *UBMK 2018 - 3rd International Conference on Computer Science and Engineering*, 342–346. https://doi.org/10.1109/UBMK.2018.8566642

Bumblauskas, D., Mann, A., Dugan, B., & Rittmer, J. (2020). A blockchain use case in food distribution: Do you know where your food has been? *International Journal of*

Information Management, 52, Article 102008. https://doi.org/10.1016/j.ijinfomgt.2019.09.004

Butijn, B. J., Tamburri, D. A., & Heuvel, W. J. V. D. (2020). Blockchains: a systematic multivocal literature review. *ACM Computing Surveys, 53*(3). https://doi.org/10.1145/3369052

Castellanos, J. A. F., Coll-Mayor, D., & Notholt, J. A. (2017). Cryptocurrency as guarantees of origin: simulating a green certificate market with the ethereum blockchain. *2017 5th IEEE International Conference on Smart Energy Grid Engineering, SEGE, 2017*, 367–372. https://doi.org/10.1109/SEGE.2017.8052827

Chanson, M., Bogner, A., Bilgeri, D., Fleisch, E., & Wortmann, F. (2019). Blockchain for the IoT: Privacy-preserving protection of sensor data. *Journal of the Association for Information Systems, 20*(9), 1271–1307. https://doi.org/10.17705/1jais.00567

Chaudhuri, A., & Holbrook, M. (2001). The chain of effects from brand trust and brand affect to brand performance: the role of brand loyalty. *Journal of Marketing, 65*, 81–93. https://doi.org/10.1509/jmkg.65.2.81.18255

Cheng, X., Fu, S., & de Vreede, G. J. (2021). Determinants of trust in computer-mediated offshore software-outsourcing collaboration. *International Journal of Information Management, 57*(1), Article 102301. https://doi.org/10.1016/j.ijinfomgt.2020.102301

Cho, S., Lee, K., Cheong, A., No, W. G., & Vasarhelyi, M. A. (2021). Chain of values: examining the economic impacts of blockchain on the value-added tax system. *Journal of Management Information Systems, 38*(2), 288–313.

Choi, J. (2018). Modeling the intergrated customer loyalty program on blockchain technology by using credit card. *International Journal on Future Revolution in Computer Science & Communication Engineering, 4*(2), 388–391. http://www.ijfrcsce.org.

Chong, A. Y. L., Lim, E. T. K., Hua, X., Zheng, S., & Tan, C. W. (2019). Business on chain: A comparative case study of five blockchain-inspired business models. *Journal of the Association for Information Systems, 20*(9), 1308–1337. https://doi.org/10.17705/1jais.00568

Chu, P. Y., Lee, G. Y., & Chao, Y. (2012). Service quality, customer satisfaction, customer trust, and loyalty in an e-banking context. *Social Behavior and Personality, 40*(8), 1271–1284. https://doi.org/10.2224/sbp.2012.40.8.1271

Costa, E., Soares, A. L., & de Sousa, J. P. (2020). Industrial business associations improving the internationalisation of SMEs with digital platforms: a design science research approach. *International Journal of Information Management, 53*, Article 102070. https://doi.org/10.1016/j.ijinfomgt.2020.102070

Culiberg, B. (2010). Identifying service quality dimensions as antecedents to customer satisfaction in retail banking. *Economic and Business Review, 12*(3), 151–166.

Da Xu, L., & Viriyasitavat, W. (2019). Application of blockchain in collaborative internet-of-things services. *IEEE Transactions on Computational Social Systems, 6*(6), 1295–1305.

De Filippi, P., Mannan, M., & Reijers, W. (2020). Blockchain as a confidence machine: the problem of trust & challenges of governance. *Technology in Society, 62*, Article 101284. https://doi.org/10.1016/j.techsoc.2020.101284

Di Silvestre, M. L., Gallo, P., Guerrero, J. M., Musca, R., Riva Sanseverino, E., Sciumè, G., & Zizzo, G. (2020). Blockchain for power systems: current trends and future applications. *Renewable and Sustainable Energy Reviews*, 119. https://doi.org/10.1016/j.rser.2019.109585

Diaz-Rainey, I., & Ashton, J. (2011). Profiling potential green electricity tariff adopters: green consumerism as an environmental policy tool? *Business Strategy and the Environment, 20*, 456–470. https://doi.org/10.1002/bse.699

Diestelmeier, L. (2019). Changing power: shifting the role of electricity consumers with blockchain technology – Policy implications for EU electricity law. *Energy Policy, 128*, 189–196. https://doi.org/10.1016/j.enpol.2018.12.065

Dietz, G., & Gillespie, N. (2011). Building and Restoring Organisational Trust.

Dolšak, J., Hrovatin, N., & Zorić, J. (2019). Can loyalty programs be effective in promoting integrated energy services? Evidence from Slovenian electricity consumers. *Energy Research & Social Science, 48*, 246–256. https://doi.org/10.1016/j.erss.2018.10.011

Dong, Z., Luo, F., & Liang, G. (2018). Blockchain: a secure, decentralized, trusted cyber infrastructure solution for future energy systems. *Journal of Modern Power Systems and Clean Energy, 6*(5), 958–967. https://doi.org/10.1007/s40565-018-0418-0

Dorfleitner, G., Muck, F., & Scheckenbach, I. (2021). Blockchain applications for climate protection: a global empirical investigation. *Renewable and Sustainable Energy Reviews, 149*(June), Article 111378. https://doi.org/10.1016/j.rser.2021.111378

Dowling, G., & Uncles, M. (1997). Do customer loyalty programs really work? *Sloan Management Review, 38*(4), 71–82.

Du, W. D., Pan, S. L., Leidner, D. E., & Ying, W. (2019). Affordances, experimentation and actualization of FinTech: A blockchain implementation study. *Journal of Strategic Information Systems, 28*(1), 50–65.

Dwivedi, Y. K., Hughes, L., Kumar Kar, A., Baabdullah, A. M., Grover, P., Abbas, R., … Wade, M. (2022). Climate change and COP26: Are digital technologies and information management part of the problem or the solution? An editorial reflection and call to action. *International Journal of Information Management, 63*. https://doi.org/10.1016/j.ijinfomgt.2021.102456.

Bergaentzlé, C., GræstedJensen, I., Skytte, K., & JessOlsen, O. (2019). Electricity grid tariffs as a tool for flexible energy systems: A Danish case study. *Energy Policy, 126*, 12–21. https://doi.org/10.1016/j.enpol.2018.11.021.

Energy, C. for S (2013). Green electricity tariffs.

Fang, X., Cui, H., Du, E., Li, F., & Kang, C. (2021). Characteristics of locational uncertainty marginal price for correlated uncertainties of variable renewable generation and demands. *Applied Energy, 282*, Article 116064. https://doi.org/10.1016/j.apenergy.2020.116064

Gamma, K. (2016). Behavioral and attitudinal customer loyalty in the power sector. *Zeitschrift Für Energiewirtschaft, 40*(4), 211–232. https://doi.org/10.1007/s12398-016-0186-3

Ropsten Testnet, retrieved from https://github.com/ethereum/ropsten 2020.

Gomes, I., Melicio, R., & Mendes, V. M. F. (2021). Assessing the value of demand response in microgrids. *Sustainability, 13*(11). https://doi.org/10.3390/su13115848

Gorkhali, A., Li, L., & Shrestha, A. (2020). Blockchain: a literature review. *Journal of Management Analytics, 7*(3), 321–343.

Gorski, T., Bednarski, J., & Chaczko, Z. (2019). Blockchain-based renewable energy exchange management system. *26th International Conference on Systems Engineering, ICSEng 2018 - Proceedings*, 1–6. https://doi.org/10.1109/ICSENG.2018.8638165

Govier, T. (1994). Is it a jungle out there? Trust, distrust and the construction of social reality. *Dialogue, 33*(2), 237–252. https://doi.org/10.1017/S0012217300010519

Gregor, S., & Hevner, A. R. (2013). Positioning and presenting design science - types of knowledge in design science research. *MIS Quarterly, 37*(2), 337–355. https://doi.org/10.2753/MIS0742-1222240302

Guo, X., Liu, H., Mao, X., Jin, J., Chen, D., & Cheng, S. (2014). Willingness to pay for renewable electricity: a contingent valuation study in Beijing, China. *Energy Policy, 68*, 340–347. https://doi.org/10.1016/j.enpol.2013.11.032

Hamburger, Á. (2019). Is guarantee of origin really an effective energy policy tool in Europe? A critical approach. *Society and Economy, 41*(4), 487–507. https://doi.org/10.1556/204.2019.41.4.6

Hameed, K., Barika, M., Garg, S., Amin, M. B., & Kang, B. (2022). A taxonomy study on securing Blockchain-based Industrial applications: an overview, application perspectives, requirements, attacks, countermeasures, and open issues. *Journal of Industrial Information Integration*, Article 100312.

Hansla, A., Gamble, A., Juliusson, A., & Gärling, T. (2008). The relationships between awareness of consequences, environmental concern, and value orientations. *Journal of Environmental Psychology, 28*(1), 1–9. https://doi.org/10.1016/j.jenvp.2007.08.004

Hartmann, P., & Apaolaza Ibáñez, V. (2007). Managing customer loyalty in liberalized residential energy markets: The impact of energy branding. *Energy Policy, 35*(4), 2661–2672. https://doi.org/10.1016/j.enpol.2006.09.016

Hasankhani, A., Mehdi Hakimi, S., Shafie-khah, M., & Asadolahi, H. (2021). Blockchain technology in the future smart grids: a comprehensive review and frameworks. *International Journal of Electrical Power and Energy Systems, 129*, 1–70. https://doi.org/10.1016/j.ijepes.2021.106811

Hawlitschek, F., Notheisen, B., & Teubner, T. (2018). The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy. *Electronic Commerce Research and Applications, 29*, 50–63. https://doi.org/10.1016/j.elerap.2018.03.005

Hevner, A. R. (2007). A three cycle view of design science research. *Scandinavian Journal of Information Systems*, 19.

Hevner, A. R., & Chatterjee, S. (2012). Design research in information systems. *In Springer* (Vol. 28). https://doi.org/10.1007/978-1-4419-6108-2

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly: Management Information Systems, 28*(1), 75–105. https://doi.org/10.2307/25148625

Hoess, A., Roth, T., Sedlmeir, J., Fridgen, G., & Rieger, A. (2022). With or Without Blockchain?: Towards a Decentralized, SSI-based eRoaming Architecture. Proceedings of the Hawaii International Conference on System Sciences 2022.

Hofman-Kohlmeyer, M. (2016). Customer loyalty program as a tool of customer retention: literature review. *CBU International Conference Proceedings, 4*, 199–203. https://doi.org/10.12955/cbup.v4.762

Hua, W., Jiang, J., Sun, H., & Wu, J. (2020). A blockchain based peer-to-peer trading framework integrating energy and carbon markets. *Applied Energy, 279*(July), Article 115539. https://doi.org/10.1016/j.apenergy.2020.115539

Ibrahim, M., & Ribbers, P. M. (2009). The impacts of competence-trust and openness-trust on interorganizational systems. *European Journal of Information Systems, 18*(3), 223–234. https://doi.org/10.1057/ejis.2009.17

Jang, H., Han, S. H., & Kim, J. H. (2020). User perspectives on blockchain technology: user-centered evaluation and design strategies for DApps. *IEEE Access, 8*, 226213–226223. https://doi.org/10.1109/ACCESS.2020.3042822

Jarvenpaa, S. L., & Majchrzak, A. (2010). Vigilant interaction in knowledge collaboration: challenges of online user participation under ambivalence. *Information Systems Research, 21*(4), 773–784. https://doi.org/10.1287/isre.1100.0320

Järvinen, P. (2007). Action research is similar to design science. *Quality and Quantity, 41*, 37–54. https://doi.org/10.1007/s11135-005-5427-1

Jensen, T., Hedman, J., & Henningsson, S. (2019). How TradeLens delivers business value with blockchain technology. *MIS Quarterly Executive, 18*(4), 221–243. https://doi.org/10.17705/2msqe.00018

Jeon, H. G., Kim, C., Lee, J., & Lee, K. C. (2021). Understanding E-commerce consumers' repeat purchase intention: the role of trust transfer and the moderating effect of neuroticism. *Frontiers in Psychology, 12*, 2059. https://doi.org/10.3389/fpsyg.2021.690039

Jonas, K., Broemer, P., & Diehl, M. (2000). Attitudinal ambivalence. *European Review of Social Psychology, 11*(1), 35–74. https://doi.org/10.1080/14792779943000125

Kandampully, J., Zhang, T., (Christina), & Bilgihan, A. (2015). Customer loyalty: a review and future directions with a special focus on the hospitality industry. *International Journal of Contemporary Hospitality Management, 27*(3), 379–414. https://doi.org/10.1108/IJCHM-03-2014-0151

Khorasany, M., Dorri, A., Razzaghi, R., & Jurdak, R. (2021). Lightweight blockchain framework for location-aware peer-to-peer energy trading. *International Journal of Electrical Power and Energy Systems, 127*, Article 106610. https://doi.org/10.1016/j.ijepes.2020.106610

Kley, F., Lerch, C., & Dallinger, D. (2011). New business models for electric cars-a holistic approach. *Energy Policy, 39*(6), 3392–3403. https://doi.org/10.1016/j.enpol.2011.03.036

Kramer, R. M. (1999). Trust and distrust in organizations: emerging perspectives, enduring questions. *Annual Review of Psychology, 50*, 569–598. https://doi.org/10.1146/annurev.psych.50.1.569

Kuechler, W., & Vaishnavi, V. (2012). A framework for theory development in design science research: multiple perspectives. *Journal of the Association for Information Systems, 13*(6), 395–423. http://aisel.aisnet.org/jais/vol13/iss6/3.

Lacity, M. C. (2018). Addressing key challenges to making enterprise blockchain applications a reality. *MIS Quarterly Executive, 17*(3), 201–222.

Lee, J., Lee, J. N., & Tan, B. C. Y. (2015). Antecedents of cognitive trust and affective distrust and their mediating roles in building customer loyalty. *Information Systems Frontiers, 17*(1), 159–175. https://doi.org/10.1007/s10796-012-9392-7

Lewicki, R., & Brinsfield, C. (2011). Measuring trust beliefs and behaviours. *Handbook of Research Methods on Trust*, 29–39. https://doi.org/10.4337/9781781009246.00013

Li, F., Pieńkowski, D., Van Moorsel, A., & Smith, C. (2012). A holistic framework for trust in online transactions. *International Journal of Management Reviews, 14*(1), 85–103. https://doi.org/10.1111/j.1468-2370.2011.00311.x

Lockl, J., Schlatt, V., Schweizer, A., Urbach, N., & Harth, N. (2020). Toward trust in internet of things ecosystems: design principles for blockchain-based IoT applications. *IEEE Transactions on Engineering Management, 67*(4), 1256–1270. https://doi.org/10.1109/TEM.2020.2978014

Luke, M. N., Anstey, G., Taylor, W., & Sirak, A. (2019). *Blockchains in Power Markets: Decentralized Disruption or Incremental Innovation?*

Luke, M. N., Lee, S. J., Pekarek, Z., & Dimitrova, A. (2018). *Blockchain in Electricity: a Critical Review of Progress to Date*.

Lustig, C., & Nardi, B. (2015). Algorithmic authority: the case of bitcoin. *Proceedings of the Annual Hawaii International Conference on System Sciences, 2015*, 743–752. https://doi.org/10.1109/HICSS.2015.95

MacDonald, S., & Eyre, N. (2018). An international review of markets for voluntary green electricity tariffs. *Renewable and Sustainable Energy Reviews, 91*, 180–192. https://doi.org/10.1016/j.rser.2018.03.028

MacPherson, R., & Lange, I. (2013). Determinants of green electricity tariff uptake in the UK. *Energy Policy, 62*, 920–933. https://doi.org/10.1016/j.enpol.2013.07.089

Martínez, P., & Rodríguez del Bosque, I. (2013). CSR and customer loyalty: the roles of trust, customer identification with the company and satisfaction. *International Journal of Hospitality Management, 35*, 89–99. https://doi.org/10.1016/j.ijhm.2013.05.009

Mattke, J., Hund, A., Maier, C., & Weitzel, T. (2019). How an enterprise blockchain application in the U.S. Pharmaceuticals supply chain is saving lives. *MIS Quarterly Executive, 18*(4), 245–261. https://doi.org/10.17705/2msqe.00019

Maurer, B., Nelms, T., & Swartz, L. (2013). "When perhaps the real problem is money itself!": the practical materiality of Bitcoin. *Social Semiotics*, 23. https://doi.org/10.1080/10350330.2013.777594

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). Model of Trust Theory. *The. Academy of Management Review, 20*(3), 709–734.

McAllister, D. (1995). Affect- and cognition-based trust formations for interpersonal cooperation in organizations. *Academy of Management Journal, 38*, 24–59. https://doi.org/10.2307/256727

McCall, M., & McMahon, D. (2016). Customer loyalty program management: what matters to the customer. *Cornell Hospitality Quarterly, 57*(1), 111–115. https://doi.org/10.1177/1938965515614099

McKnight, D. H., & Chervany Norman, L. (2001).). Trust and distrust definitions: One bite at a time. Lecture Notes in Artificial Intelligence (Subseries of Lecture Notes in Computer Science). *2246*, 27–54. https://doi.org/10.1007/3-540-45547-7_3

McKnight, D. H., & Choudhury, V. (2006). Distrust and trust in B2C e-commerce: do they differ? *Proceedings of the ACM Conference on Electronic Commerce*. https://doi.org/10.1145/1151454.1151527

McKnight, D. H., Cummings, L. L., & Chervany, N. L. (1998). Initial trust formation in new organizational relationships. *Academy of Management Review, 23*(3), 473–490. https://doi.org/10.5465/AMR.1998.926622

McKnight, D. H., Lankton, N. K., Nicolaou, A., & Price, J. (2017). Distinguishing the effects of B2B information quality, system quality, and service outcome quality on trust and distrust. *Journal of Strategic Information Systems, 26*(2), 118–141. https://doi.org/10.1016/j.jsis.2017.01.001

Mengelkamp, E., Schlund, D., & Weinhardt, C. (2019). Development and real-world application of a taxonomy for business models in local energy markets. *Applied Energy, 256*, Article 113913. https://doi.org/10.1016/j.apenergy.2019.113913

Merlo, O., Eisingerich, A., Auh, S., & Levstek, J. (2018). The benefits and implementation of performance transparency: the why and how of letting your customers 'see through' your business. *Business Horizons, 61*(1), 73–84. https://doi.org/10.1016/j.bushor.2017.09.007

Mezger, A., Cabanelas, P., López-Miguens, M. J., Cabiddu, F., & Rüdiger, K. (2020). Sustainable development and consumption: the role of trust for switching towards green energy. *Business Strategy and the Environment, 29*(8), 3598–3610. https://doi.org/10.1002/bse.2599

Miles, et al. (2018). *Qualitative data analysis: A methods sourcebook*. SAGE Publications.

Moody, G. D., Galletta, D. F., & Lowry, P. B. (2010). Unifying conflicting models of trust and distrust for enhanced understanding and predictive power in organizational relationships: proposing the unified trust-distrust model (UTDM). *SSRN Electronic Journal, 10*(68). https://doi.org/10.2139/ssrn.2287398

Moody, G. D., Galletta, D. F., & Lowry, P. B. (2014). When trust and distrust collide online: The engenderment and role of consumer ambivalence in online consumer behavior. *Electronic Commerce Research and Applications, 13*(4), 266–282. https://doi.org/10.1016/j.elerap.2014.05.001

Moody, G. D., Lowry, P. B., & Galletta, D. F. (2017). It's complicated: explaining the relationship between trust, distrust, and ambivalence in online transaction relationships using polynomial regression analysis and response surface analysis. *European Journal of Information Systems, 26*(4), 379–413. https://doi.org/10.1057/s41303-016-0027-9

Muzahid, A., & Noorjahan, P. (2009). Impact of service quality, trust and customer satisfaction on cunsumer loyalty. *ABAC Journal* (Vol. 29,(1), 24–38.

Myers, M., & Newman, M. (2007). The qualitative interview in is research: examining the craft. *Information and Organization, 17*, 2–26. https://doi.org/10.1016/j.infoandorg.2006.11.001

Nguyen, N., Leclerc, A., & LeBlanc, G. (2013). The mediating role of customer trust on customer loyalty. *Journal of Service Science and Management, 06*(01), 96–109. https://doi.org/10.4236/jssm.2013.61010

Ning, Y., Feng, M., Feng, J., & Liu, X. (2019). Understanding clients' experience of trust and distrust in dwelling fit-out projects. *Engineering, Construction and Architectural Management, 26*(3), 444–461. https://doi.org/10.1108/ECAM-03-2018-0115

Nunes, J., & Drze, X. (2006). The endowed progress effect: how artificial advancement increases effort. *Journal of Consumer Research, 32*, 504–512. https://doi.org/10.1086/500480

Olsen, S. O., Wilcox, J., & Olsson, U. (2005). Consequences of ambivalence on satisfaction and loyalty. *Psychology and Marketing, 22*(3), 247–269. https://doi.org/10.1002/mar.20057

Ozaki, R. (2011). Adopting sustainable innovation: what makes consumers sign up to green electricity? *Business Strategy and the Environment, 20*(1), 1–17. https://doi.org/10.1002/bse.650

Paymans, T., Lindenberg, J., & Neerincx, M. (2004). Usability trade-offs for adaptive user interfaces: Ease of use and learnability. https://doi.org/10.1145/964442.964512.

Peffers et al. (2012). Design Science Research in Information Systems: Advances in Theory and Practice. Information Systems and Applications, 7th International Conference, DESRIST 2012.

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems, 24*(3), 45–77. https://doi.org/10.2753/MIS0742-1222240302

Peng, L. Y., & Wang, Q. (2006). Impact of relationship marketing tactics (RMTs) on switchers and stayers in a competitive service industry. *Journal of Marketing Management, 22*(1–2), 25–59.

Perrons, R. K., & Cosby, T. (2020). Applying blockchain in the geoenergy domain: the road to interoperability and standards. *Applied Energy, 262*, Article 114545. https://doi.org/10.1016/j.apenergy.2020.114545

Peter, V., Paredes, J., Rivial, M. R., Sepúlveda, E. S., & Astorga, D. A. H. (2019). Blockchain meets energy: digital solutions for a decentralized and decarbonized sector. *German-Mexican Energy Partnership (EP) and Florence School of Regulation (FSR)*, 1–45.

Portes, A., Cases, A.-S., & N'Goala, G. (2020). Should digital marketing practices be more transparent? *An Empirical Investigation on the roles of Consumer digital Literacy and Privacy concerns in self-Service Technologies*, 1–11. https://hal.archives-ouvertes.fr/hal-02502389.

Raadal, H. L., Dotzauer, E., Hanssen, O. J., & Kildal, H. P. (2012). The interaction between electricity disclosure and tradable green certificates. *Energy Policy, 42*, 419–428. https://doi.org/10.1016/j.enpol.2011.12.006

Raspberry Pi Foundation. (2016). Raspberry Pi 3 Model B. https://www.raspberrypi.org/products/raspberry-pi-3-model-b/.

Rieger, A., Lockl, J., Urbach, N., Guggenmos, F., & Fridgen, G. (2019). Building a blockchain application that complies with the EU general data protection regulation. *MIS Quarterly Executive, 18*(4), 263–279. https://doi.org/10.17705/2msqe.00020

Rieger, A., Roth, T., Sedlmeir, J., & Fridgen, G. (2021). The privacy challenge in the race for digital vaccination certificates. *Med, 2*(6), 633–634. https://doi.org/10.1016/j.medj.2021.04.018

Risius, M., & Spohrer, K. (2017). A blockchain research framework - what we (don't) know, where we go from here, and how we will get there. *Business & Information Systems Engineering, 59*(6), 385–409. https://doi.org/10.1007/s12599-017-0506-0

Rosell, J. I., & Ibáñez, M. (2006). Modelling power output in photovoltaic modules for outdoor operating conditions. *Energy Conversion and Management, 47*(15–16), 2424–2430. https://doi.org/10.1016/j.enconman.2005.11.004

Rossi, M., Mueller-Bloch, C., Thatcher, J. B., & Beck, R. (2019). Blockchain research in information systems: current trends and an inclusive future research agenda. *Journal of the Association for Information Systems, 20*(9), 1388–1403. https://doi.org/10.17705/1jais.00571

Roth, T., Stohr, A., Amend, J., Fridgen, G., & Rieger, A. (2022). Blockchain as a driving force for federalism: a theory of cross-organizational task-technology fit. *International Journal of Information Management*, Article 102476.

Saha, S., Ravi, N., Hreinsson, K., Baek, J., Scaglione, A., & Johnson, N. G. (2021). A secure distributed ledger for transactive energy: The Electron Volt Exchange (EVE) blockchain. *Applied Energy, 282*, 1–49. https://doi.org/10.1016/j.apenergy.2020.116208

Sarker, S., Henningsson, S., Jensen, T., & Hedman, J. (2021). The use of blockchain as a resource for combating corruption in global shipping: an interpretive case study. *Journal of Management Information Systems, 38*(2), 338–373.

Sedlmeir, J., Buhl, H. U., Fridgen, G., & Keller, R. (2020). The energy consumption of blockchain technology: beyond myth. *Business and Information Systems Engineering, 62*(6), 599–608. https://doi.org/10.1007/s12599-020-00656-x

Sedlmeir, J., Smethurst, R., Rieger, A., & Fridgen, G. (2021). Digital identities and verifiable credentials. *Business & Information Systems Engineering, 63*(5), 603–613.

Seebacher, S., & Schüritz, R. (2017). *Blockchain Technology as an Enabler of Service Systems: A Structured Literature Review*. https://doi.org/10.1007/978-3-319-56925-3_2

Sousa, T., Soares, T., Pinson, P., Moret, F., Baroche, T., & Sorin, E. (2019). Peer-to-peer and community-based markets: a comprehensive review. *Renewable and Sustainable Energy Reviews, 104*, 367–378. https://doi.org/10.1016/j.rser.2019.01.036

Stathopoulou, A., & Balabanis, G. (2016). The effects of loyalty programs on customer satisfaction, trust, and loyalty toward high- and low-end fashion retailers. *Journal of Business Research, 69*(12), 5801–5808. https://doi.org/10.1016/j.jbusres.2016.04.177

Tams, S., Thatcher, J. B., & Craig, K. (2018). How and why trust matters in post-adoptive usage: The mediating roles of internal and external self-efficacy. *Journal of Strategic Information Systems, 27*(2), 170–190. https://doi.org/10.1016/j.jsis.2017.07.004

Thomas, L., Zhou, Y., Long, C., Wu, J., & Jenkins, N. (2019). A general form of smart contract for decentralized energy systems management. *Nature Energy, 4*(2), 140–149. https://doi.org/10.1038/s41560-018-0317-7

Uncles, M. D., Dowling, G. R., & Hammond, K. (2003). Customer loyalty and customer loyalty programs. *Journal of Consumer Marketing, 20*(4–5), 294–316. https://doi.org/10.1108/07363760310483676

Upadhyay, N. (2020). Demystifying blockchain: a critical analysis of challenges, applications and opportunities. *International Journal of Information Management, 54*, Article 102120. https://doi.org/10.1016/j.ijinfomgt.2020.102120

Vaishnavi, V., & Uechler, W. (2008). Design Science Research Methods and Patterns: Innovating Information and Communication Technology.

van Aken, J. E. (2004). Management research based on the paradigm of the design sciences: the quest for field-tested and grounded technological rules. *Journal of Management Studies, 41*(2), 219–246. https://doi.org/10.1111/joms.2004.41.issue-2

van der Werff, L., Legood, A., Buckley, F., Weibel, A., & de Cremer, D. (2019). Trust motivation: the self-regulatory processes underlying trust decisions. *Organizational Psychology Review, 9*(2–3), 99–123. https://doi.org/10.1177/2041386619873616

Vesel, P., & Zabkar, V. (2009). Managing customer loyalty through the mediating role of satisfaction in the DIY retail loyalty program. *Journal of Retailing and Consumer Services, 16*(5), 396–406. https://doi.org/10.1016/j.jretconser.2009.05.002

Walls, J. G., Widmeyer, G. R., & Sawy, O. (2004). Assessing information system design theory in perspective: How useful was our 1992 initial rendition? *Journal of Information Technology Theory and Application, 6*, 43–58.

Warkentin, M., & Orgeron, C. P. (2020). Using the security triad to assess blockchain technology in public sector applications. *Int. J. Inf. Manag, 52*, Article 102090.

Watanabe, H., Fujimura, S., Nakadaira, A., Miyazaki, Y., Akutsu, A., & Kishigami, J. (2016). Blockchain contract: securing a blockchain applied to smart contracts. *2016 IEEE International Conference on Consumer Electronics, ICCE 2016*, 467–468. https://doi.org/10.1109/ICCE.2016.7430693

Webster, J., & Watson, R. T. (2002). Analysing the past for prepare the future: writing a review. *MIS Quarterly, 26*, 2.

Werbach, K. (2018). The Blockchain and the New Architecture of Trust. https://doi.org/10.7551/mitpress/11449.001.0001.

Wüstenhagen, R., Wolsink, M., & Bürer, M. J. (2007). Social acceptance of renewable energy innovation: an introduction to the concept. *Energy Policy, 35*(5), 2683–2691. https://doi.org/10.1016/j.enpol.2006.12.001

Yen, Y.-S. (2010). Can perceived risks affect the relationship of switching costs and customer loyalty in e-commerce? *Internet Research, 20*, 210–224. https://doi.org/10.1108/10662241011032254

Yi, Y., & Jeon, H. (2003). Effects of loyalty programs on value perception, program loyalty, and brand loyalty. *Journal of the Academy of Marketing Science, 31*(3), Article 229. https://doi.org/10.1177/0092070303031003002.

Zhang, H., Wang, J., & Ding, Y. (2019). Blockchain-based decentralized and secure keyless signature scheme for smart grid. *Energy, 180*, 955–967. https://doi.org/10.1016/j.energy.2019.05.127

Zhang, W., Wei, C.-P., Jiang, Q., Peng, C.-H., & Zhao, J. L. (2021). Beyond the block: a novel blockchain-based technical model for long-term care insurance. *Journal of Management Information Systems, 38*(2), 374–400.

Ziolkowski, R., Miscione, G., & Schwabe, G. (2020). Decision problems in blockchain governance: old wine in new bottles or walking in someone else's shoes? *Journal of Management Information Systems, 37*(2), 316–348. https://doi.org/10.1080/07421222.2020.1759974

Zoerner, T. (2020). GrünstromIndex - Vorhersage von regionalem Ökostrom. https://gruenstromindex.de/.

Manuel Utz (manuel.utz@uni-bayreuth.de) is a researcher at the Faculty of Law, Business and Economics at the University of Bayreuth, Germany. His research focuses on the design and implementation of blockchain-based applications in energy markets.

Simon Johanning (johanning@wifa.uni-leipzig.de) is a researcher in energy economics and works on research infrastructure for blockchain-based peer-to-peer energy trade. His main interest is in the digitalization of energy sectors, with a particular focus on the use of blockchain technology and modeling of energy systems.

Tamara Roth (tamara.roth@uni.lu) is a researcher at the Interdisciplinary Center for Security, Reliability and Trust (SnT) at the University of Luxembourg. Her research interests include the effect of cultural principles on the adoption of cryptographic technologies in the public sector as well as the design of solutions based on cryptographic technologies for the healthcare sector. Prior to joining the SnT, Tamara has been a research assistant at the University of Bayreuth at the Faculty of Biology, Chemistry & Earth Sciences.

Thomas Bruckner (bruckner@wifa.uni-leipzig.de) is the director of the Institute for Infrastructure and Resources Management at Leipzig University, Germany. He also holds the Chair for Energy Management and Sustainability. His research interests are on modeling climate change, liberalized electricity markets and decentralized energy systems.

Jens Strüker (jens.strueker@fim-rc.de) is Professor of Information Systems and Digital Energy Management at the University of Bayreuth and co-director of the Blockchain Lab of Fraunhofer Institute for Applied Information Technology. His research focus is on real-time energy markets and enabling technologies such as IoT and Blockchain.

RP10: Amend, J., Feulner, S., Rieger, A., Roth, T., Fridgen, G., & Guggenberger, T. (2024). **Bringing Government into the Digital Age: Insights from Germany's Asylum Procedure.** *MIS Quarterly Executive (Accepted)*.

Journal Ranking: 10.0 (CiteScore); 1.840 (SNIP)

Bringing Government into the Digital Age: Insights from Germany's Asylum Procedure

ABSTRACT

Governments spend billions to bring their services into the digital age. But government IT projects can be challenging when the law requires cooperation across multiple levels of government while each level must maintain distinct IT systems. This article examines how Germany's Federal Office for Migration and Refugees successfully navigated these challenges when it implemented FLORA, an inter-governmental IT system that supports the coordination of asylum procedures. FLORA improves the exchange and quality of procedural information, accelerates the procedure by up to 50 percent, and mitigates error and data privacy concerns. Based on our insights into the FLORA project, we provide three recommendations for successfully building inter-governmental IT systems.

Keywords: Government services, Government IT systems**,** Decentralized IT architecture, Private blockchain, Asylum management.

Bringing Government into the Digital Age: Insights from Germany's Asylum Procedure

Governments Often Struggle to Build Inter-governmental IT Systems

Governments invest significant effort and resources to move their services into the digital age.[1] The US Federal Government, for instance, had an IT budget of $98.1 billion in 2024, of which $29.1 billion were earmarked for major investments.[2] However, these investments can be difficult to translate into more secure and efficient services. Many government services require that multiple levels of government cooperate, but the law clearly separates competencies, budgets, and – by extension – IT systems. The result are often complex and multi-layered IT architectures that complicate information exchange and are difficult to modernize. Cooperation between federal and state governments is a prime example. The two levels have distinct competencies, and each state has its own IT systems. Introducing new IT systems for their cooperation, in turn, requires all these governments to come together. The same applies to cooperation between other levels of government. [3]

Despite these challenges, governments can bridge the divide. In this article, we describe one such example from Germany, where the federal and state governments introduced FLORA, a system for the coordination of Germany's asylum procedure. FLORA increases

[1] See for example: Bui, Q.N. "Increasing the Relevance of Enterprise Architecture through "Crisitunities" in U.S. State Governments," *MIS Quarterly Executive* (14:4), 2015, pp. 169-179 or Kim, S.L. & Teo, T. "Lessons for Software Development Ecosystems: South Korea's e-Government Open Source Initiative," *MIS Quarterly Executive* (12:2), 2013, pp. 93-108.

[2] More information on the United States' federal IT spending is available here: https://itdashboard.gov/

[3] More insights into the challenges of government IT projects can be found in: Pahlka, J. (2023). Recoding America: Why government is failing in the digital age and how we can do better. Metropolitan Books.

the procedure's quality, reduces its duration by up to 50%, and minimizes the risk of errors and data privacy violations. FLORA is a particularly rich case study because its development was fraught with many of the challenges that too often weigh down inter-governmental IT systems. Below, we describe how Germany's government overcame these challenges. We then elaborate on FLORA's private permissioned blockchain architecture and governance. Based on these insights, we develop three recommendations for building inter-governmental IT systems that can bring multi-level government services into the digital age.

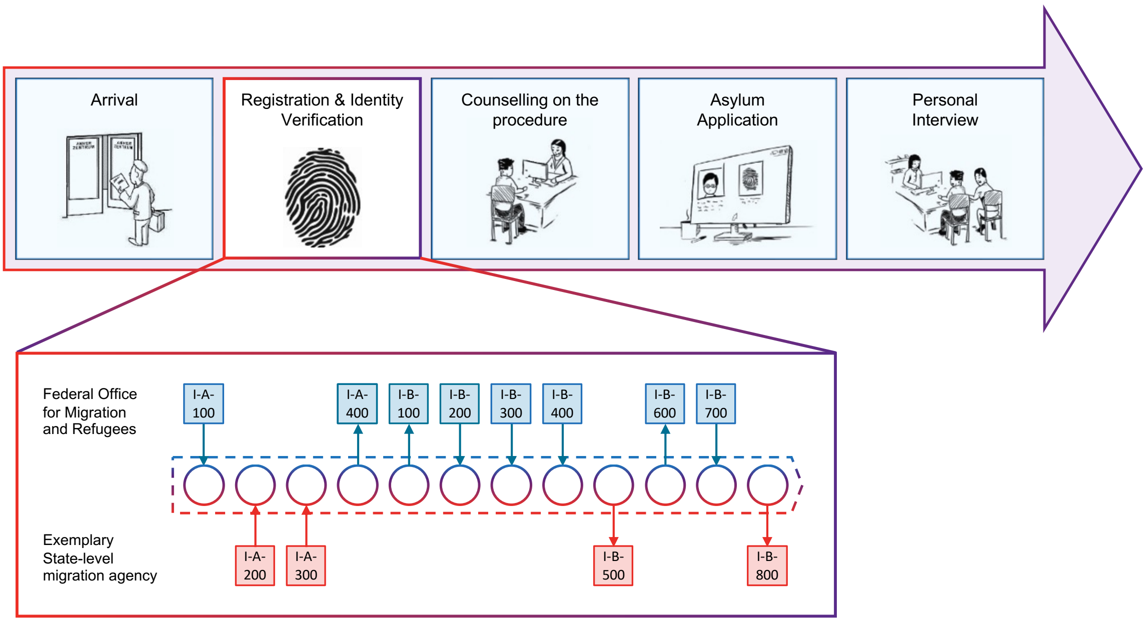
FLORA's Value

In 2023, Germany processed around 352.000 new asylum applications[4]. Its asylum procedure is federally organized and requires various agencies to closely cooperate. The Federal Office for Migration and Refugees is at the core of the procedure and manages and issues decisions on asylum applications. It collaborates closely with state-level migration agencies that are responsible for the initial registration of asylum seekers, and their eventual integration or repatriation. Health agencies are involved in the procedure to provide medical care, translation service providers support interviews, educational service providers offer language courses, and law enforcement agencies complete background checks and facilitate repatriations. Figure 1 provides a drill-down into the first part of the procedure, highlighting its complexity.[5]

[4] For more statistical details, see: https://www.bamf.de/SharedDocs/Meldungen/DE/2024/240108-asylgeschaeftsstatistik-dezember-und-gesamtjahr-2023.html

[5] A full overview of the procedure is available on the Federal Office's website: https://www.bamf.de/EN/Themen/AsylFluechtlingsschutz/AblaufAsylverfahrens/ablaufasylverfahrens-node.html

Figure 1: Drill-down Into the First Part of the Asylum Procedure


Arrival
Registration & Identity Verification
Counselling on the procedure
Asylum Application
Personal Interview
Federal Office for Migration and Refugees
Exemplary State-level migration agency
I-A-100
I-A-400
I-B-100
I-B-200
I-B-300
I-B-400
I-B-600
I-B-700
I-A-200
I-A-300
I-B-500
I-B-800

All involved agencies and partner organizations are subject to a tight legal framework that defines the distribution of responsibilities and rules for the procedure. This framework also mandates that most of these agencies have their own IT systems and processes. The resulting fragmentation of IT systems complicates collaboration and the exchange of procedural information across agency and system boundaries. In most cases, Excel-based lists are manually filled and exchanged via e-mail, which takes a lot of time and is very error-prone.

FLORA's introduction for the first part of the procedure (up to the personal interview) eliminated most Excel-based lists and streamlined the exchange of procedural information. Moreover, FLORA improves the quality of information, speeds up the procedure by up to 50%, and reduces the risks for errors and data privacy violations.[6] Table 1 provides a high-level summary of the value added by FLORA.

Table 1: Overview of the First Part of the Asylum Procedure Before and After the Implementation of FLORA

Parameters	Before FLORA	With FLORA
Sharing of procedural information	• Significant inefficiencies due to Excel-based lists	• More efficient exchange of procedural information across agencies
Quality of procedural information	• Considerable effort to find and retrieve procedural information from different databases and files	• Significantly improved information accuracy and completeness thanks to a 'single procedural source of truth'
Duration of the procedure	• Slow procedures due to long waiting and search times	• Accelerated procedures (up to 50%) through substantial reductions of waiting and search times
Legal compliance	• Elevated risk of procedural errors and difficulties complying with data protection requirements	• Reduced risk of procedural errors and better compliance with data protection requirements

FLORA's Implementation Journey

In response to the European refugee crisis in 2015/2016, the Federal Office substantially increased its investments in digital technologies that would make the procedure more efficient, secure, and scalable. These technologies included advanced validation tools, such as facial recognition to complement the validation of identities with fingerprints, speech recognition to validate claims of origin, and the analysis of

[6] The FLORA project conducted a comprehensive evaluation of the piloting phase:
Amend, J., Arnold, L., Fabri, L., Feulner, S., Fridgen, G., Harzer, L., Karnebogen, P., Koehler, F., Ollig, P., Rieger, A., Schellinger, B., and Schmidbauer-Wolf, G.-M. "Federal Blockchain Infrastructure Asylum (FLORA) - Piloting and evaluation of the FLORA support system in the context of the AnkER facility Dresden," Federal Office for Migration and Refugees, 2023.

smartphone data to validate itineraries. They also involved attempts to standardize, digitize, and automate the exchange of procedural data between the involved agencies with an XML-based standard. Additional efforts focused on creating structures and processes for experimentation with emerging technologies, such as artificial intelligence and blockchain.[7]

Avoiding a Centralized System

The Federal Office became intrigued with blockchain in early 2018 due to its promises of decentralization, data integrity, and transparency. Decentralization was intriguing since centralized IT architectures had proven challenging to implement across the multiple levels of government involved in the procedure. They would usually require new laws to allow for centralized data processing and the redistribution of (technical) competencies. Germany's Central Register of Foreign Nationals ("Ausländerzentralregister," or AZR), with its user base of more than 6000 agencies at the federal, state and local levels, was a painful case in point: any update to the AZR, such as a new data field, requires an update to the federal AZR law.[8] Data integrity was a concern because the AZR had a history of not reliably ensuring that the right data was available in the right quality at the right time. Increasing transparency was essential to the Federal Office because two recent security incidents had highlighted how difficult it was to identify the status of a procedure in real-time. In the words of Marcus Richter, the, at the time, Federal Office's vice-president:

[7] For more details on these initiatives, see the Federal Office's digitalization agenda: https://www.bamf-digitalisierungsagenda.de/en/

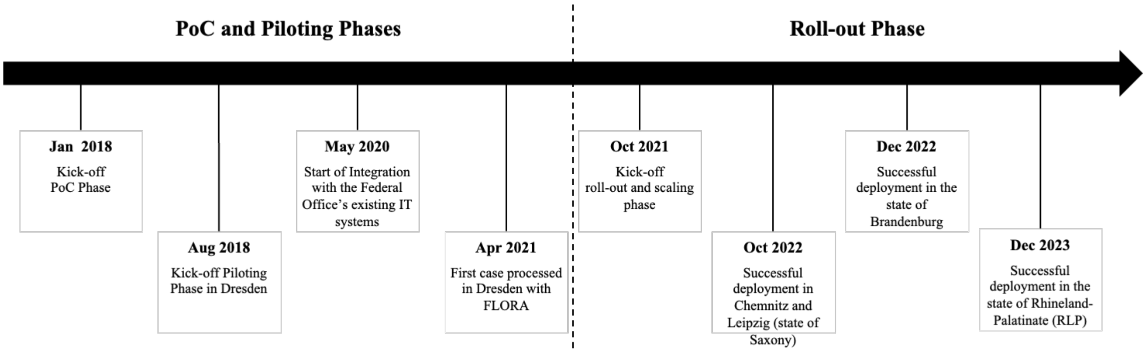
[8] For more details on the AZR, see the Federal Office's website: https://www.bamf.de/EN/Behoerde/Aufgaben/Datenerhebung/datenerhebung-node.html.

For more detail on data processing in Germany's asylum procedure, see: https://www.bamf.de/SharedDocs/Anlagen/EN/EMN/Studien/wp90-datenmanagement.pdf?__blob=publicationFile&v=1.

In recent years, we have had security incidents in Germany where we as the [Federal Office] have always asked ourselves what we can do to prevent such situations. If we have a logging layer, I can basically press a button and […] say exactly which [procedural step of the associated asylum case] took place when. And that has been our guiding idea, so to speak.

Since blockchain promised to realize this vision and reflect the requirements of multi-level, federal data processing,[9] the Federal Office conducted a proof-of-concept during the first half of 2018 (Figure 2).

Figure 2: Timeline of the FLORA Project


PoC and Piloting Phases
Roll-out Phase
Jan 2018
Kick-off PoC Phase
Aug 2018
Kick-off Piloting Phase in Dresden
May 2020
Start of Integration with the Federal Office's existing IT systems
Apr 2021
First case processed in Dresden with FLORA
Oct 2021
Kick-off roll-out and scaling phase
Oct 2022
Successful deployment in Chemnitz and Leipzig (state of Saxony)
Dec 2022
Successful deployment in the state of Brandenburg
Dec 2023
Successful deployment in the state of Rhineland-Palatinate (RLP)

The proof-of-concept implemented a simplified asylum procedure with three agencies. The result of this proof-of-concept was a private blockchain application that had the potential to create substantial value for the Federal Office and its partner agencies. The application could facilitate a 'shared source of truth' of the status and progress of asylum procedures between the involved agencies. It also promised significant efficiency and

[9] Deeper insights into why private blockchains are interesting for Germany's asylum procedure can be found in: Roth, T., Stohr, A., Amend, J., Fridgen, G. & Rieger, A. "Blockchain as a driving force for federalism: A theory of cross-organizational task-technology fit," *International Journal of Information Management* (68), February 2023.

privacy improvements over the use of Excel-based lists.[10] Another quote by Marcus Richter illustrates these expectations:

> *"In the future, we should no longer copy data into large nationwide databases. Rather, we should leave the data where we collect it and use a logging layer to make transparent when and where status changes occurred. With a lightweight blockchain solution, we can more easily implement this logging layer than with an expansion of the existing and already complex IT solutions."*

Developing a Production Pilot with a State-level Migration Agency

Upon successful completion of the proof-of-concept, the Federal Office decided to initiate a pilot project. The overarching goal of this project was to test if the expected value could be realized in day-to-day operations.[11] Moreover, the pilot intended to establish if a private blockchain could be designed to meet the procedure's strict privacy and security requirements. Due to the complexity of the asylum procedure, the Federal Office limited the scope of the pilot project to one state-level migration agency (State Directorate of Saxony (LDS)) and the asylum procedure in Dresden, Saxony.

One challenge for the pilot project was to achieve compliance with the procedure's privacy requirements. First, these requirements restrict the processing of personal data unless there is an explicit legal basis for each act of data processing. Second,

[10] These considerations were detailed in a PoC whitepaper: Fridgen, G., Guggenmos, F., Lockl, J., Rieger, A. and Urbach, N. "Supporting communication and cooperation in the asylum procedure with Blockchain technology – A proof of concept by the Federal Office for Migration and Refugees," Federal Office for Migration and Refugees, 2019.

[11] Further details are available in the pilot whitepaper: Amend, J., Arnold, L., Fabri, L., Feulner, S., Fridgen, G., Harzer, L., Karnebogen, P., Koehler, F., Ollig, P., Rieger, A., Schellinger, B., and Schmidbauer-Wolf, G.-M. "Federal Blockchain Infrastructure Asylum (FLORA) - Piloting and evaluation of the FLORA support system in the context of the AnkER facility Dresden," Federal Office for Migration and Refugees, 2023.

responsibilities for compliance need to be clearly identified and designated, especially when multiple agencies jointly control the processing of personal data through a shared IT system, such as a private blockchain application. Third, all personal data needs to be erased after relevant legal bases expire and corrections have to be made when the data is faulty. These requirements are difficult to reconcile with an append-only database, such as blockchain. The Federal Office nevertheless managed to address all these challenges by combining a joint data processing agreement with a pseudonymization solution that erases the attribution of procedural information to an asylum applicant rather than the information itself.[12]

Another challenge was compliance with federal IT security requirements. Since the federal government's reference framework for IT security did not yet cover decentralized IT systems such as private permissioned blockchains, the Federal Office needed to develop its own IT security framework for FLORA, including a comprehensive survey of potential risks as well as strategies to control or contain these risks.

Further challenges resulted from the limited resources and capabilities of the LDS. Originally, the Federal Office had aimed to jointly develop and host the pilot system. However, the LDS lacked both the financial and personal resources for the project and was not interested in developing blockchain capabilities. The Federal Office thus had to take full responsibility for the development and hosting of FLORA, while the LDS would only support the Federal Office with functional requirements. In the words of a business analyst from the Federal Office:

[12] Further insights into these challenges and the Federal Office's solution strategy can be found in: Rieger, A., Lockl, J., Urbach, N., Guggenmos, F. & Fridgen, G. "Building a blockchain application that complies with the EU general data protection regulation," *MIS Quarterly Executive* (18:4), 2019.

"Sure, Saxony's central immigration agency and any other agency could technically host a blockchain node. But many, including Saxony's central immigration agency, do not really want this. The level of complexity in the governance, not necessarily in the technology, requires a different way of thinking and can be an impediment."

Despite this rather one-sided development and hosting model, the FLORA system met all expectations and project endpoints by September 2021. These positive results encouraged the Federal Office to make FLORA a strategic priority and roll it out across Germany. In the words of Hans-Eckhardt Sommer, president of the Federal Office:

"Projects like FLORA for faster information exchange with the [state-level migration agencies] - a project that is particularly close to my heart because the added value is immense, especially in times of high application numbers - contribute to our good reputation, especially with the [state-level migration agencies]".

Rolling-out FLORA Across Germany's Sixteen States

Most other state-level migration agencies shared the LDS's lack of interest in developing blockchain capabilities and hosting FLORA. Consequently, the Federal Office introduced a Software-as-a-Service (SaaS) model. In this model, the Federal Office hosts FLORA instances for the state-level migration agencies and offers access to these instances through Application Programming Interfaces (APIs) and a web-based FLORA Frontend. A consultant to the project explains this model:

"We currently have a software-as-a-service model, which ultimately means that the Federal Office deploys a productive solution for [the state-level migration agencies]. It doesn't mean, however, that [they] cannot influence the solution, make remarks, or ask for personalization. It just means, from a purely technical perspective, that the Federal Office hosts the solution. Long-term, the aim is to develop [the model more] into the direction of platform-as-a-service [...] to push responsibilities back to the competent state agencies."

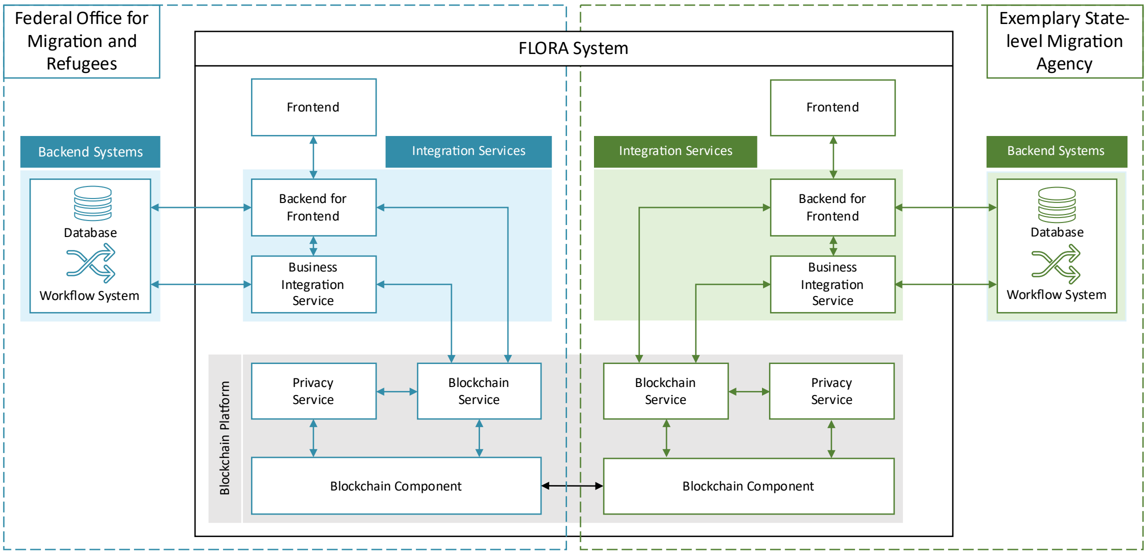
However, the roll-out sometimes proved more difficult than expected. Some employees required significant training and first-line user support to encourage them to adopt the new system. Others were guarded when they did not see immediate benefits for their tasks, even if other users benefitted substantially. A local unit head describes how employees, who perceived substantial benefits, specifically requested a timely roll-out:

> *"As a local unit, we communicate very often and very much with the [state-level migration agencies]. FLORA enables us to exchange a lot of data, which we urgently need for our processes in the local unit, on a daily basis with minimal effort. It is, therefore, a great wish - certainly for all local units - to use the technology as soon as possible."*

FLORA's Architecture

The FLORA system allows the involved agencies to connect their backend databases and workflow management systems. FLORA's architecture has a different FLORA instance for each agency, all of which are currently hosted by the Federal Office. Each FLORA instance, in turn, has two layers: An Integration Services layer and a Blockchain Platform layer (see Figure 3).

Figure 3: FLORA's Architecture



The primary purpose of FLORA is to share procedural information between the involved agencies. It creates a 'shared source of truth' through secure, timely, and reliable distribution and persistent tracking of process status messages.[13] For instance, once the Federal Office has conducted an ID check, its backend systems create a FLORA API call to distribute the status message 'ID check completed' to the other agencies involved in the specific asylum procedure. In cases where backend systems are not yet fully connected to FLORA, status updates can be imported through .csv files or entered via a FLORA Frontend.

The Integration Services establish links between the backend systems, the FLORA Frontend, and the Blockchain Platform layer. The Business Integration Service (BIS) has two functions, it receives API calls from the backend systems, translates these calls into status messages, and forwards these messages to the Blockchain Platform layer. Moreover, it maps the identifiers used in the backend systems to unique procedure identifiers that are consistent across all involved agencies.[14] The Backend for Frontend (BFF) handles user authentication, the population of the Frontend with information from the backend systems and the Blockchain Platform layer, and the writing of status messages resulting from data entry in the FLORA Frontend.

The Blockchain Platform consists of three components. The Blockchain Service acts as a service endpoint between the Integration Services and a Blockchain Component based on

[13] FLORA includes both overarching status messages and sub-process status messages. While overarching status messages map the procedural logic defined by the Federal Asylum Act (and thus are the same in all of Germany's sixteen states), sub-process status messages reflect local differences in the asylum procedure.

[14] To ensure that an asylum procedure can be initially identified by the FLORA system, several identification attributes are transmitted from the backend system of the submitting agency, together with the first status message (e.g., date of birth, personal number, application numbers). The FLORA ID is then generated by the BIS of the submitting agency and exchanged with the responsible partner agencies. These agencies then use their own BISs to map the FLORA ID with the IDs in their backend systems.

the Hyperledger Fabric Framework, which is used for distribution and storage of status messages.[15] Once a submitting agency writes a new status message into its Blockchain Component, it is shared with the Blockchain Component of the other agencies responsible for the specific asylum procedure.[16,17] Furthermore, the Blockchain Component uses smart contracts to validate authentication and compliance with a basic process model of the procedure. However, it does not restrict deviations from the process model, as the asylum procedure is predicated on the accountability of human case handlers.

The Privacy Service addresses an important data privacy requirement, that is, the right to erasure. Compliance with this requirement mandates that no personal data should be written to an 'immutable' blockchain. However, all procedural data processed by the FLORA system is inherently personal. To mitigate this challenge, FLORA employs a pseudonymization approach. The procedural data in the Blockchain Component is not linked to the FLORA ID but to a pseudonymous technical identifier. These technical identifiers are mapped to FLORA IDs in the privacy services. Erasing these mappings allows the anonymization of the procedural data in the Blockchain Component, which is a permissible way of erasure under the GDPR.

In cases where FLORA is not fully integrated with an agency's backend systems, case handlers can use a FLORA Frontend to get tabular overviews of various asylum procedures and their status. Based on this information, they can plan and complete the

[15] The status messages are tamper-evident as all Blockchain Components also hold a copy of the hash values ("fingerprints") of all status messages written by the participating agencies.

[16] Status messages are distributed and stored in so-called 'Private Data Collections'. These collections are special elements of the Hyperledger Fabric Framework and allow to share status messages with a specific subset of participating agencies. All other agencies receive only a hash value of the status message.

[17] As responsibilities in the asylum procedure are clearly delineated and agencies do not have a legal basis for cross-validation, the Blockchain Component does not employ a consensus mechanism but a simple ordering mechanism.

next steps in the procedure. Many of the tabular overviews also allow manual data entry and – by extension – the distribution of a new status message.

FLORA’s Governance

In FLORA’s SaaS model, state-level migration agencies can introduce requirements, propose changes, and participate in the higher-level prioritization of new features. Lower-level prioritization and technical development decisions are privy to the Federal Office. The same applies to technical decisions regarding the hosting of FLORA instances on the Federal Office’s infrastructure. To avoid tensions resulting from this strong centralization of decision rights, the Federal Office goes above and beyond to ensure that the concerns and suggestions of all state-level migration agencies are considered, and their specific requirements reflected. It offers free workshops and trainings, a FLORA support team, ‘office hours’ with FLORA’s project management team, and joint feedback rounds with all participating agencies.

Responsibilities, in turn, are more distributed. In line with the centralized development model, the Federal Office assumes responsibility for FLORA’s privacy, security, and availability. However, the GDPR and relevant asylum laws require that the responsibility for data processing is shared between the Federal Office’s local units and the state-level migration agencies. FLORA’s governance framework extends these responsibilities to first-level support and representing local needs in strategic feature prioritization meetings.

To incentivize the adoption of FLORA, the Federal Office engages in outreach activities to emphasize FLORA’s value for different employee groups and funds customization and initial hosting. Once this ‘honeymoon’ phase is over, costs for hosting are shared between the Federal Office and the respective state-level migration agency. Moreover, the Federal

Office provides technical support for agencies that want to use FLORA's APIs to directly connect their instance with relevant back-end systems.

Positive Outcomes

After initial concerns, FLORA has been fully embraced by the Federal Office's local units and the involved state-level migration agencies. Users typically describe FLORA as a powerful and well-designed application that significantly improves day-to-day operations.

Sharing of procedural information. FLORA significantly reduces the inefficiencies of Excel-based lists. It shares procedural information on the status and progress of individual asylum procedures instantly, even during times of high influx and backlogs. Procedural information can be shared for each individual asylum procedure or entire batches. Where FLORA is integrated with backend systems, procedural information can flow directly between the backend systems of the involved agencies.

Quality of procedural information. Before FLORA's introduction, case handlers often needed to consult different Excel-based lists and databases to obtain the relevant procedural information. This data was sometimes neither complete nor accurate. After the introduction of FLORA, case handlers now have a shared source of truth with complete, accurate, and up-to-date procedural information. This information allows to better complete and plan subsequent steps in the procedure, such as booking transport capacities and interpreters for interviews.

Duration of the procedure. Although FLORA does not automate any of the procedure's steps, it significantly reduces waiting and search times. In some cases, the first part of the procedure could be accelerated by up to 50%. These efficiency gains have a positive impact, especially on state-level migration agencies that are often stretched thin in terms of personnel. With FLORA, they can remain productive even in times of high influx and backlogs.

Legal Compliance. Before FLORA's implementation, the risk of procedural errors was often high, and compliance with data privacy requirements was difficult. Through FLORA, errors owed to missing or false information have become rare, and observing data privacy requirements is easy. For instance, FLORA works with automated timers for deleting procedural information, obviating the need to clear outdated Excel-based lists.

Recommendations for Building Inter-Governmental IT Systems

Government services can be difficult to digitalize when they requires cooperation and coordination between agencies across multiple levels of government but the law requires that these agencies maintain distinct IT systems. While the resulting barriers are daunting, they can be overcome as demonstrated by Germany's FLORA project. In the following section, we draw on the insights from the FLORA project to synthesize three recommendations for successfully building inter-governmental IT systems.

Recommendation 1: Determine the Suitability of Decentralized Over Centralized Solutions.

Introducing new IT systems that support collaboration within and across levels of government is challenging as heterogenous legacy systems often complicate data exchange and coordination. The natural reflex may often be to build a 'cost-effective' centralized system that reduces this complexity. However, creating a new centralized IT system to coordinate multiple agencies can come with substantial hidden costs. In cases where the law prohibits one shared IT system, it would need to be changed before building such as system. Standardization costs can likewise be substantial when local procedures and data models must be compared and aligned, and new data repositories created and maintained.

These hidden costs may often outweigh the higher development, hosting, and maintenance costs of decentralized solutions. Germany’s asylum procedure is a case in point. The Central Register of Foreign Nationals (“Ausländerzentralregister,” or AZR) serves as a constant reminder of the hidden costs of using centralized IT architectures, including substantial ‘law-making' costs for updates and alignment. The FLORA system avoids these costs as it builds on the idea of decentralized data sharing, which obviates the need for new legal bases. Moreover, it comes with low standardization costs as it does not require the alignment of local variants and data models of the procedure. It leaves these variants and models untouched but offers opportunities to selectively adopt best practices from other sites.

Recommendation 2: Advocate for Modularity to Break-up Multi-layered Legacy Architectures.

A second fundamental challenge for building inter-governmental IT systems is the complex, multi-layered nature of many legacy IT systems. New levels of legal requirements are typically mapped with new layers of technology while complexity reduction remains a secondary concern. Too often, these decisions result in legacy IT systems that are more difficult to adapt and extend than the legal frameworks they support. Although updates and new IT systems cannot eliminate legal complexity, they can make an essential contribution to maintainability and updatability by emphasizing loose coupling and modularity over messy, multi-layered architectures and efficient data exchange over redundant storage. Over time, adherence to these principles can successively break down complex IT architectures and encapsulate those parts of legacy systems that are difficult to maintain and replace.

FLORA is an important step in this direction. It emphasizes complementarity and does not replicate legacy system data. Instead, it uses this data to generate procedural updates that can be used to improve the exchange and use of the already available data. Moreover, FLORA is designed to ensure that its individual components can be easily maintained, updated, and replaced with different technologies and frameworks. For instance, FLORA uses the Hyperledger Fabric framework for procedural data sharing and storage as it allows to reflect the demands of multi-level, federal data processing. However, this Blockchain component can be easily replaced if another similarly convenient albeit less complex option becomes available.

Recommendation 3: Start with a Software-as-a-Service Model and then Gradually Move to a Flexible Integration Model.

Funding and organizing the development of shared IT systems for multi-level government services can be difficult. The legal separation of competencies will usually require that technical and financial responsibilities match the legal framework. In the short run, this matching exercise can paralyze digital transformation efforts. Yet, for innovation efforts to progress, it may sometimes be advisable for a single agency to temporarily take the lead and initially assume a large share of the technical and financial responsibilities ('one-for-all' approach). Once the new IT system is mature enough, other agencies can start the required resource allocation and responsibility redistribution processes.

The FLORA project provides an interesting reference for how such a ‘one-for-all’ approach can be implemented. The Federal Office not only assumed the technical and financial responsibility for developing the FLORA system but also introduced an initially free Software-as-a-Service (SaaS) model that allowed its state-level partner agencies to immediately use the system. In due time, each agency can then decide on the desired level of integration with their legacy systems and initiate the requisite budgeting, contracting, and staffing processes. This gradual transition from a SaaS model to flexible integration drastically lowers the usual adoption barriers.

Concluding Comments

FLORA brings together Germany’s Federal Office for Migration and Refugees and its state-level migration agencies. It creates substantial value by improving the exchange and quality of procedural information between these agencies, by reducing search and wait times, and by minimizing the risks of errors and data privacy violations. FLORA’s success hinges on the ability to bridge between legally-separated legacy systems. It is designed in a modular way that leverages the decentralization and controlled information-sharing features of a private, permissioned blockchain but also allows for its replacement should a better technological option become available.

APPENDIX: RESEARCH METHOD

We chose an inductive research design to develop an in-depth understanding of how governments can bring their services into the digital age. Specifically, we conducted a longitudinal single-case study[18] based on Germany's FLORA project for the coordination of asylum procedures.

We chose the FLORA project because it provides valuable insights and rich data for studying how government agencies can successfully collaborate on building inter-governmental IT systems. We directly observed the FLORA project and collected data over six years, from the project's inception in early 2018 to its rollout in several states in Germany by 2024. Three of the co-authors provided academic advisory services to the FLORA project. The first two authors accompanied the projects for about two years and were primarily tasked with conducting an in-depth evaluation of the FLORA pilot system and its later rollout. The third co-author accompanied the project from January 2018 onward and was primarily tasked with advising the conceptualization of the system.

We could gather rich data from multiple sources due to our close involvement with the project. Our primary data were 98 interviews conducted at different points in the project between 2018 and 2024. Since we had closely accompanied and evaluated the project since its inception in January 2018, we were also able to draw on project documentation (1000+ pages) and direct observations to triangulate our findings. Table A1 provides an overview of the collected data sources.

[18] For more information on case study research, see: Yin, R. Case Study Research: Design and Methods, *SAGE Publications*, 2017.

Table A1. Data Sources

Data sources	Description
Semi-structured interviews	98 interviews, recorded, transcribed, and coded using grounded theory methods
Documents	1000+ pages of project documentation: • Conceptual and legal documents (200+ pages) • Meeting minutes, technical documentation, and user support documents (600+ pages) • Whitepapers and evaluation reports (200+ pages)
Observations	Observations from regular sprint reviews, project workshops, management meetings, and events

RP11: Hartwich, E., Hoess, A., Rieger, A., Roth, T., Fridgen, G., & Young, A. (2023). **How Organizations Sustain and Navigate Between (De)centralization Equilibria: A Process Model.** *ICIS 2023 Proceedings*. https://aisel.aisnet.org/icis2023/itadopt/itadopt/10

Conference Ranking: 2 (GGS Class); A- (GGS Rating)

How Organizations Sustain and Navigate Between (De)centralization Equilibria: A Process Model

Completed Research Paper

Eduard Hartwich
SnT-Interdisciplinary Centre for
Security, Reliability and Trust,
University of Luxembourg,
Luxembourg, Luxembourg
eduard.hartwich@uni.lu

Alexandra Hoess
SnT-Interdisciplinary Centre for
Security, Reliability and Trust,
University of Luxembourg,
Luxembourg, Luxembourg
alexandra.hoess@uni.lu

Alexander Rieger
SnT-Interdisciplinary Centre for
Security, Reliability and Trust,
University of Luxembourg,
Luxembourg, Luxembourg
alexander.rieger@uni.lu

Tamara Roth
Sam M. Walton College of Business,
University of Arkansas,
Fayetteville, Arkansas, United States
tr036@uark.edu

Gilbert Fridgen
SnT-Interdisciplinary Centre for
Security, Reliability and Trust,
University of Luxembourg,
Luxembourg, Luxembourg
gilbert.fridgen@uni.lu

Amber Grace Young
Sam M. Walton College of Business,
University of Arkansas,
Fayetteville, Arkansas, United States
AYoung@walton.uark.edu

Abstract

Finding the 'right' balance between centralization and decentralization in organizational processes, governance, and IT can be difficult. To navigate this tension field, organizations need to find (de)centralization equilibria that are often dynamic and depend on organizational strategy and context. However, little is known about how organizations should respond once an old equilibrium is punctuated or breaks down. In this paper, we thus conduct an inductive multiple-case study to investigate how organizations sustain and transition between (de)centralization equilibria. We synthesize our insights into a process model that paints the transition as an iterative recalibration process subject to centralization and decentralization tensions. Often, this process will require local and temporary compromises. Our work contributes a much-needed process perspective to the IS literature on (de)centralization.

Keywords: Centralization, Decentralization, Equilibrium, Punctuation

Introduction

"The real trick in high reliability systems is somehow
to achieve simultaneous centralization and decentralization" (Weick, 1987, p. 124).

The 'golden ratio' between centralization and decentralization is difficult to achieve. While centralized structures can reduce coordination costs of organizational processes and governance mechanisms, they become ineffective once organizations reach a certain size and communication complexity (Mintzberg, 1989; Rediker & Seth, 1995; Siggelkow & Levinthal, 2003). Decentralized structures, in turn, allow organizations to distribute decision-making rights and responsibilities so that 'local' opportunities and requirements can be reflected as they arise (Andersen, 2005; Kahai et al., 2003; Weick, 1987). However, decentralized structures do not come without costs either. Too much decentralization allows subunits to act opportunistically and withhold information from organizational leadership, which not only creates coordination costs (Foss et al., 2010; Grandori, 1997; Rediker & Seth, 1995; Srikanth & Puranam, 2014) but also fuels conflicts of interest (Andersen, 2005; Beck et al., 2018; Wiseman et al., 2012). Larger organizations consequently find themselves in a tension field between centralization and decentralization (Mintzberg, 1989) in which they need to develop a certain (de)centralization equilibrium (Smith & Lewis, 2011).

In today's organizations, it can be difficult to establish such 'equilibria' in organizational processes, governance, and information technology (IT) (Hanelt et al., 2021; Henderson & Venkatraman, 1999; King, 1983). Moreover, organizations are occasionally subject to punctuating events that can challenge stable, existing equilibria and require recalibration or a transition to a new equilibrium (Romanelli & Tushman, 1994; Tushman & Romanelli, 1985). However, organizations often struggle with navigating these changes once an established equilibrium is broken. In particular, there is a need for a greater understanding of how organizations can and should manage the tensions that these recalibrations and transitions bring. We thus ask the following question:

RQ: *How can organizations sustain and navigate between stable (de)centralization equilibria?*

To answer our research question, we conduct an inductive, longitudinal multiple-case study (Eisenhardt & Graebner, 2007; Yin, 2011). Our study focuses on the development and adoption of two cross-organizational IT systems that saw several transitions between centralization and decentralization. The first case revolves around the development and roll-out of Germany's Federal Blockchain Infrastructure Asylum (FLORA), which supports the coordination between the authorities involved in Germany's asylum procedure. The second case studies the development and adoption of the European Blockchain Services Infrastructure (EBSI), which supports the delivery of cross-border public services in Europe. We could gain particularly rich insights into these two cases as authors of this work have been regularly involved with the projects since 2018.

Our contributions are two-fold. First, we derive a process model for the development of stable (de)centralization equilibria, which are characterized by established activity patterns, routines and workflows (Romanelli & Tushman, 1994; Tushman & Romanelli, 1985). Specifically, our model casts the development of equilibria between centralization and decentralization in organizational processes, governance, and IT as an iterative recalibration and transition process that is triggered by punctuating events and shaped by centralization and decentralization tensions. Second, we find that organizational decision-makers can be particularly successful in this process when they allow for local and temporary differences in the degree of (de)centralization.

The rest of the paper is structured as follows. The background section synthesizes the management literature on (de)centralization, the role of IT in supporting (de)centralization equilibria, and the impact of blockchain on (de)centralization. The third section describes our two cases and our data collection and analysis. In the fourth section, we present our emerging process model. The fifth section discusses our model and three complementary conjectures before elaborating on our theoretical contributions, practical implications, and boundary conditions. Section six concludes with a summary of our key insights.

Theoretical Background

Navigating the Tension Field Between Centralization and Decentralization

When organizations start to form, they typically rely on centralized processes and governance mechanisms (Aldrich & Pfeffer, 1976; Mintzberg, 1984). In such centralized structures, decision-making authority is vested with a single entity or a small group of people that also defines and dictates these organizational processes (Ahituv et al., 1989; Mintzberg, 1989; Siggelkow & Levinthal, 2003). As the number of entities with decision-making authority is limited, centralization typically increases operational efficiency and reduces coordination costs (Aulakh & Gencturk, 2000; Mintzberg, 1989; Peppard, 2018; Rediker & Seth, 1995). However, centralization is only practical when the necessary information and competencies reside with or can be transferred to a central authority that is accepted and respected by organizational subunits and when the actions of this authority are transparent (Foss et al., 2010; Grandori, 1997; Mintzberg, 1989; Rediker & Seth, 1995; Srikanth & Puranam, 2014). Once organizations start expanding and grow beyond a certain size (Mintzberg, 1989), centralized organizing often causes overbearing communication costs or even loss of control (Smith & Lewis, 2011).

Unlike centralization, decentralization distributes decision-making authority along an organization's vertical and horizontal dimensions; it leaves decision-making to the discretion of the respective subunits (Mintzberg, 1984, 1989; Siggelkow & Levinthal, 2003). This distributed authority also allows them to define organizational processes locally, foster flexibility, and seize opportunities as they occur (Andersen, 2005; Kahai et al., 2003; Weick, 1987). But decentralized structures come with their own challenges. Organizational subunits may behave opportunistically, create information asymmetries, and are prone to conflicts of interest (Andersen, 2005; Beck et al., 2018; Wiseman et al., 2012). Decentralized structures are also disadvantageous when decentral decision-makers are "incompetent, are not appropriately held to account for their decisions or make decisions that result in problems for other organizational units or for higher management" (King, 1983, p. 321). Decentralized organizing thus typically couples the distribution of decision rights with accountabilities and incentive mechanisms to persuade their decentral subunits to act in a certain way (Moldoveanu & Martin, 2001; Weill, 2004).

What makes things complicated for many organizations is that they are neither fully centralized nor fully decentralized. Instead, they find themselves in a dynamic tension field between centralization and decentralization (Siggelkow & Levinthal, 2003; Smith & Lewis, 2011) that requires the negotiation of equilibria. In these equilibria, organizations can leverage the advantages of both structures and balance out their challenges. Once organizational decision-makers accept this equilibrium thinking, they can create flexible organizations and spur a virtuous relationship between both ends of the (de)centralization spectrum (Smith & Lewis, 2011). More specifically, successful organizational leaders "build the management of change into [their organization's] very structure" (Drucker, 1992, p. 97), allowing them to move between different degrees of centralization and decentralization (King, 1983; Siggelkow & Levinthal, 2003).

Such a level of structural malleability, for instance, can enable organizations to initially organize the processes and governance of their sub-units in a decentral manner. This allows them to quickly introduce advancements and innovation to the market and reap benefits from early-mover advantages. Once these advantages fade or are leveled by competitors, organizations often centralize these units to keep costs at bay and reintegrate them with the processes and governance mechanisms of the parent organization (Uhl-Bien & Arena, 2018). Other reasons to realign (de)centralization equilibria can come from changes in organizational management after extended periods of stability (Brown, 1997; Davis & Eisenhardt, 2011; Smith & Tushman, 2005). Whenever organizational leadership changes, the risk of opportunistic behavior in subunits needs to be re-evaluated and potentially requires recentralization as well as adjustment of organizational processes and governance. The management literature refers to such changes as punctuating events (Lyytinen & Newman, 2008; Tushman & Romanelli, 1985), which "substantively disrupt established activity patterns" (Romanelli & Tushman, 1994, p.1141). They may trigger recalibration and eventually "install the basis for new equilibrium periods" (Romanelli & Tushman, 1994, p.1141) that may provoke new challenges and opportunities (Davis & Eisenhardt, 2011).

The Role of Information Technology for (De)centralization Equilibria

Managing such punctuating events may also require adjustments to an organization's IT (Henderson & Venkatraman, 1999; Lyytinen & Newman, 2008). Many organizational leaders manage these adjustments by translating new processes and governance structures into their IT. That is, when they decide to centralize their organization's processes and governance, they also aim for more centralized (macro)structures in the organization's IT to ensure better control. Efforts to decentralize organizational processes and governance, in contrast, often result in the decentralization of IT to mirror the needs and requirements of empowered organizational subunits (Sambamurthy & Zmud, 1999).

However, aligning organizational processes, governance, and IT does not have to be unilateral. New ways of digital organizing typically work in both directions and also require aligning organizational processes and governance mechanisms to IT (Davis & Eisenhardt, 2011). Digital platform ecosystems, for instance, have developed into one of the most common ways of orchestrating different organizations in the co-creation and appropriation of joint value propositions (Constantinides et al., 2018; de Reuver et al., 2018). These ecosystems are powered by digital platforms that blur organizational and hierarchical boundaries (Hein et al., 2020; Jacobides et al., 2018). When platforms have centralized designs, they also introduce a certain degree of centralization to the processes and governance of the platform ecosystem (Hein et al., 2020; T. L. Huber et al., 2017). Other technologies for cross-organizational cooperation, such as blockchain, emphasize decentralized designs (Lacity, 2018), which promote a certain degree of decentralization on (cross-)organizational processes and governance.

These examples demonstrate that IT is not an exclusively stabilizing element in the development of (de)centralization equilibria but show that it can also enable organizations to establish new equilibria, especially in cross-organizational contexts (Zhao et al., 2020). Organizations should thus "not simply seek to identify and adopt the best available technology to restructure the organization" (Henderson & Venkatraman, 1999, p. 481); IT should rather act as a catalyst in an organization's pursuit of stable (de-)centralization equilibria. For this pursuit, organizational processes, governance, and IT need to be malleable (Hanelt et al., 2021; Henderson & Venkatraman, 1999; King, 1983; Mikalef et al., 2021). Malleability in IT is typically achieved through decomposition and modularization of IT components and the implementation of interfaces between these modules (Hanseth & Lyytinen, 2010; Mikalef et al., 2021). Malleable organizational processes are commonly ensured through exchangeable process steps (Hammer, 2014) while malleable governance is characterized by informal and relational practices within formal structures (Gubitta & Gianecchini, 2002; Lumineau et al., 2021).

The truly challenging part, however, is the use of this malleability in response to punctuating events that challenge or break current equilibria (Romanelli & Tushman, 1994). While the IS literature agrees that this response can require changes to organizational processes, governance, or IT, little guidance is available on how organizations can navigate new (de)centralization equilibria once an established equilibrium can no longer be sustained.

The Impact of Blockchain on (De)centralization

Navigating between (de)centralization equilibria is particularly demanding if the underlying IT prescribes a certain degree of (de)centralization. One such example is blockchain technology. Blockchains are decentralized and replicated databases that allow so-called blockchain nodes to directly communicate and interact without an intermediating server or third party (Halaburda, 2018; Halaburda & Mueller-Bloch, 2019; Nakamoto, 2008). They are quite flexible in the degree of decentralization they support. Private permissioned blockchains, for instance, are often less decentralized as they restrict read and write access to a set of pre-registered nodes. Public permissionless blockchains, in turn, impose neither restriction and are often highly decentralized (Beck et al., 2018).

Although blockchains stipulate a certain degree of IT decentralization, they do not necessarily lead to decentralized equilibria (Chen et al., 2021). In fact, research argues that even permissionless blockchains tend to result in rather centralized IT architectures and governance, whereas persmissioned ones may favor decentralization (Bakos et al., 2021). As such, blockchain projects are interesting examples to study how organizations can manage the resulting (de)centralization tensions, as little is known about how such structures are established and how they evolve.

Method and Case Description

To explore how organizations can sustain and navigate between (de)centralization equilibria, we conducted a multiple-case study on the introduction of two blockchain systems (Eisenhardt, 2021; Eisenhardt & Graebner, 2007; Yin, 2017). We selected the two cases for three reasons: 1) they involved the same IT, 2) they are situated in a similar public sector context, and 3) two members of our research team closely accompanied both projects as academic advisor and observer for over five years. This involvement of our team members provided us with particularly rich insights, including unique participant observations and access to relevant project documentation and interview partners. The two cases are complementary since the first case is dominated by centralization tensions, while the second case places a stronger emphasis on decentralization.

Case 1: Germany's Federal Blockchain Infrastructure Asylum (FLORA)

Our first case is the development and roll-out of the Federal Blockchain Infrastructure Asylum, a blockchain-based system that supports the efficient and secure exchange of procedural information between the authorities involved in Germany's asylum procedure. Work on FLORA started in February 2018, and the first pilot was deployed in 2021. Currently, the Federal Office and its partner authorities are rolling out FLORA across Germany's sixteen federal states. Figure 1 provides an overview of FLORA's development trajectory from January 2018 to September 2023.

The FLORA project builds upon Hyperledger Fabric, a private permissioned blockchain framework that supports private sub-chains for each federal state and location. FLORA's nodes (one node per organization) are hosted centrally by the Federal Office but partner authorities are free to host their own node if desired. Read and write access is defined based on each authority's legal responsibility.

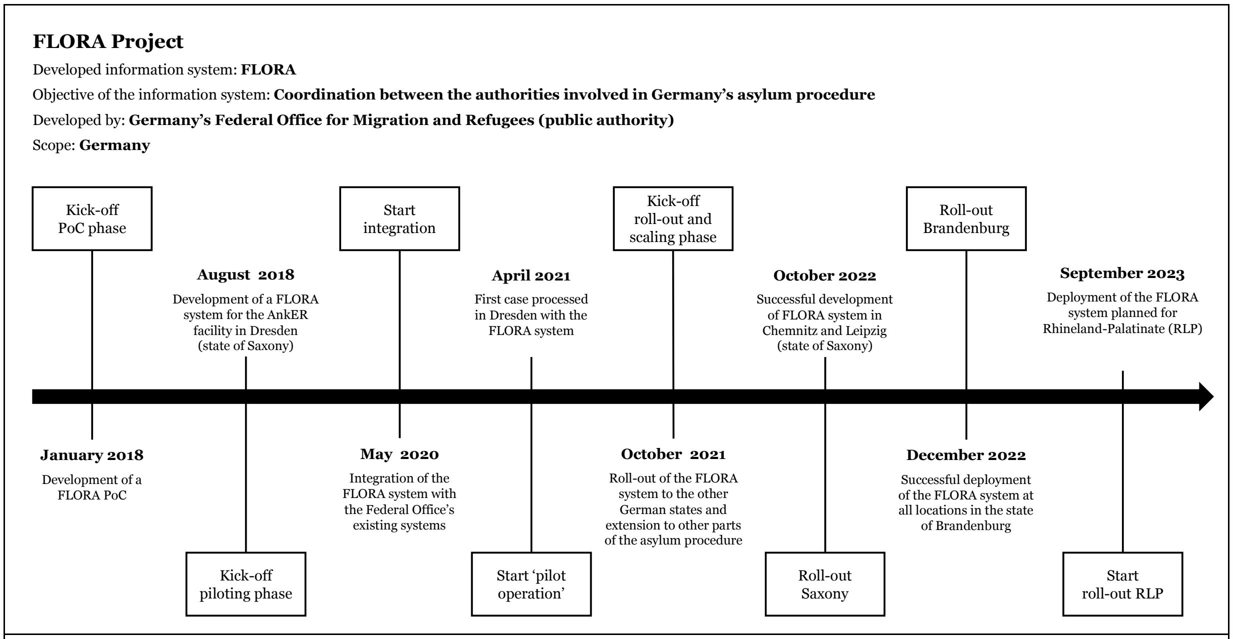

FLORA Project
Developed information system: FLORA
Objective of the information system: Coordination between the authorities involved in Germany's asylum procedure
Developed by: Germany's Federal Office for Migration and Refugees (public authority)
Scope: Germany
Kick-off PoC phase
January 2018
Development of a FLORA PoC
August 2018
Development of a FLORA system for the AnkER facility in Dresden (state of Saxony)
Kick-off piloting phase
Start integration
May 2020
Integration of the FLORA system with the Federal Office's existing systems
April 2021
First case processed in Dresden with the FLORA system
Start 'pilot operation'
Kick-off roll-out and scaling phase
October 2021
Roll-out of the FLORA system to the other German states and extension to other parts of the asylum procedure
October 2022
Successful development of FLORA system in Chemnitz and Leipzig (state of Saxony)
Roll-out Saxony
Roll-out Brandenburg
December 2022
Successful deployment of the FLORA system at all locations in the state of Brandenburg
September 2023
Deployment of the FLORA system planned for Rhineland-Palatinate (RLP)
Start roll-out RLP

Figure 1. Detail and Timeline of the FLORA Project.

Case 2: European Blockchain Services Infrastructure (EBSI)

Our second case is the European Blockchain Services Infrastructure (EBSI), a blockchain system developed and operated by the European Blockchain Partnership (EBP). The EBP was formed in April 2018 between the European Commission and the EU member states, as well as Norway and Liechtenstein with the intent to build a blockchain-based system that would support the efficient and secure delivery of cross-border public services. EBSI currently supports the authentication of digital diploma credentials, and deployment in production is scheduled for the second half of 2023. In parallel, the EBP is working on several other use cases, such as social security passports and document traceability. Figure 2 provides an overview of EBSI's development trajectory from April 2018 to September 2023.

In contrast to FLORA, EBSI is hosted decentrally across more than 20 European member states. EBSI relies on a permissioned blockchain based on Hyperledger Besu. Any organization can read data, but only a subset of pre-authorized organizations can host an EBSI node to obtain write and validation rights.

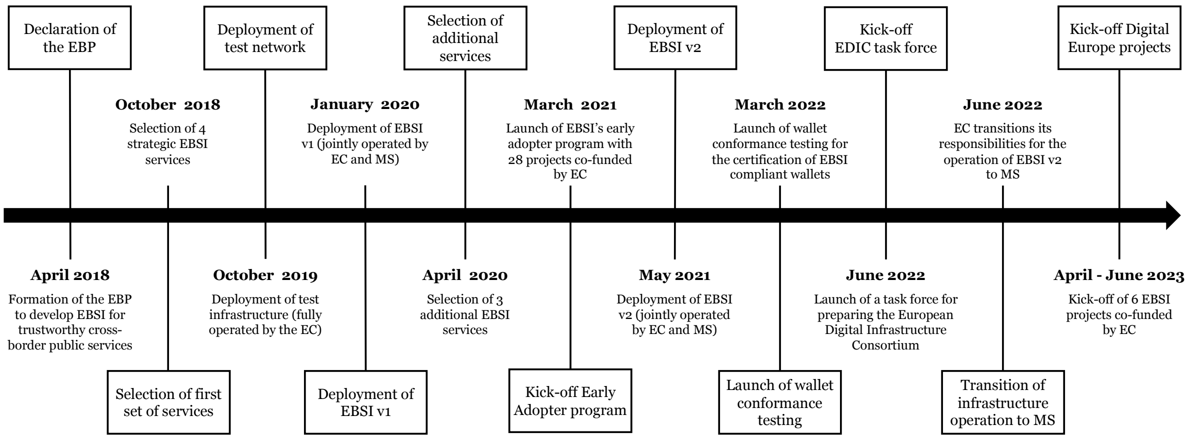
EBSI Project

Developed information system: **EBSI**

Objective of the information system: **Delivering cross-border public services**

Developed by: **European Blockchain Partnership**

Scope: **European Union (including Liechtenstein and Norway)**


Declaration of the EBP
April 2018
Formation of the EBP to develop EBSI for trustworthy cross-border public services
October 2018
Selection of 4 strategic EBSI services
Selection of first set of services
Deployment of test network
October 2019
Deployment of test infrastructure (fully operated by the EC)
January 2020
Deployment of EBSI v1 (jointly operated by EC and MS)
Deployment of EBSI v1
Selection of additional services
April 2020
Selection of 3 additional EBSI services
March 2021
Launch of EBSI's early adopter program with 28 projects co-funded by EC
Kick-off Early Adopter program
Deployment of EBSI v2
May 2021
Deployment of EBSI v2 (jointly operated by EC and MS)
March 2022
Launch of wallet conformance testing for the certification of EBSI compliant wallets
Launch of wallet conformance testing
Kick-off EDIC task force
June 2022
Launch of a task force for preparing the European Digital Infrastructure Consortium
June 2022
EC transitions its responsibilities for the operation of EBSI v2 to MS
Transition of infrastructure operation to MS
Kick-off Digital Europe projects
April - June 2023
Kick-off of 6 EBSI projects co-funded by EC

EC = European Commission
MS = Member States

Figure 2. Detail and Timeline of the EBSI Project.

Data Collection

Our first source of case evidence is semi-structured interviews. As the third author accompanied the FLORA project, he regularly conducted explorative interviews to evaluate the emerging system and identify tensions and best practices for developing blockchain projects. During these interviews, tensions between centralization and decentralization became prominent as the project advanced. When we observed similar tensions in an interview study on EBSI's development, we started to specifically explore the changes between centralization and decentralization in a focused set of interviews between March and May 2023. To select informants for the focused interviews, we followed recommendations for informant selection by Huber & Power (1985).

All interviews were conducted based on interview guides we derived from the respective literature. These were organizational (de)centralization in general (Mintzberg, 1989; Smith & Lewis, 2011; Smith & Tushman, 2005) for the explorative interviews as well as IS-specific (de)centralization (King, 1983; Sambamurthy & Zmud, 1999) for the focused interviews. We audio-recorded and transcribed the interviews using established video conferencing tools. Where interviewees did not consent to be recorded, we took extensive notes. The interviews were conducted in German or English, dependent on the language preferences of the interviewees, and lasted between 30-90 minutes. Table 1 summarizes the explorative and focused interviews on which we built our case study.

Case	Number of Interviews
FLORA	Exploratory Interviews: 15 Focused Interviews: 5
EBSI	Exploratory Interviews: 7 Focused Interviews: 6

Table 1. Interviews

We complemented these interviews with project documentation and direct observations. The third author has been an academic advisor to both the FLORA and the EBSI projects for more than five years. As part of his role in the FLORA project, he regularly participated in meetings on FLORA's technical and strategic development and observed stakeholders in their use of the emerging FLORA system. In the EBSI project, he served as a technical advisor to the EBP. As part of this role, he similarly attended regular meetings related to the technical and strategic development of EBSI. The second author additionally observed the EBSI project for two years (starting in autumn 2021) for research purposes and to inform Luxembourg's national strategy on blockchain and digital identities. She attended meetings related to EBSI's strategic and technical development and the implementation of EBSI's digital diploma use case. Their involvement gave us unique access to relevant documents (source 2) and provided rich participant observations (source 3). Table 2 summarizes these sources.

Case	Project Documentation	Direct Observations
FLORA	1000+ pages	Third author: 3-4 full days per week working on the FLORA project from Jan 2018 to May 2020 2-3 full days per week working on the FLORA project from Jun 2020 to May 2023 1-2 full days per week working on the FLORA project from Jun 2023 to Sep 2023
EBSI	1000+ pages	Second author: 2-3 days per month observing the EBP from Nov 2021 to September 2023 Third author: 2-3 days per month advising the EBP from Feb 2019 to September 2023

Table 2. Overview of Collected Project Documentation and Observations

Data Analysis

To analyze our case evidence, we followed best practices for studying multiple cases and coding qualitative data (Corbin & Strauss, 1990; Eisenhardt, 1989, 2021; Eisenhardt & Graebner, 2007). We started our analysis with a within-case analysis to see how centralization and decentralization developed in each of the two cases. Throughout this analysis, two authors openly coded the project documentation and interview transcripts to understand context factors and get a feeling for the overall case setting. In the first round of axial coding, they aggregated their open codes into higher-level categories. They frequently consulted with the whole author team to discuss their codes and triangulate their findings with the second and third author's project insights. We also used these meetings to iterate between the pertinent theories on organizational and IS (de)decentralization and our case data.

Overall, our within-case analysis revealed that the FLORA project was dominated by centralization compromises, which led to mounting tensions as the project progressed. The EBSI project, in turn, iterated between centralization and decentralization compromises, continuously demanding a recalibration of the equilibrium.

Informed by these insights, we proceeded to a cross-case analysis to compare how the two cases balanced centralization and decentralization over time. For this purpose, two authors conducted a second round of axial coding as well as one round of selective coding. During this second coding process, they again regularly met with their co-authors to discuss the codes, triangulate with the second and third authors' insights, and iterate with the pertinent theories.

Our cross-case analysis produced rich insights into the dynamic nature of (de)centralization equilibria. We found stable equilibria in both projects, i.e., periods characterized by stable activity patterns, routines, and workflows. However, punctuations through changes in organizational strategy or context disrupted these equilibria and demanded new compromises in the degree of (de)centralization that inevitably demanded both projects to establish new equilibria.

Results

Throughout our coding and discussion rounds, a story of recalibration and transition emerged. Both projects started with the vision to establish a decentralized equilibrium that would reflect the federal context of both IT systems. However, the need for quick progress required a certain degree of centralization in various stages of the projects. Some of these centralization 'compromises' needed to be revisited as the projects advanced, creating a dynamic back-and-forth and recalibration of organizational processes, governance, and IT. We now turn to how this back-and-forth played out in each of the two projects.

Navigating (De)centralization in the FLORA Project

Germany's asylum procedure requires close collaboration and information exchange between various organizations at the municipal, state, and federal levels. While the Federal Office for Migration and Refugees plays a pivotal role in issuing decisions about asylum applications, state-level migration, authorities and municipal governments are responsible for the initial registration, distribution, accommodation, care, and eventual integration or repatriation of applicants. Several security agencies conduct background checks, and various health authorities provide medical care. The involved authorities often exchange information via inefficient means such as paper lists, spreadsheets, and fax messages. However, efforts to improve this exchange have proven difficult. Since the federal separation of competencies typically prevents "digital centralization" and redistribution of competencies to a central authority, many authorities involved in the procedure prefer a "decentralized" architecture that requires neither the extension of centralized databases nor the delegation of control to a single authority. An IT service provider to the project explains:

"The decentralization of rights and responsibilities resonates well with the BAMF [...] and the foundation of federal organizing. [In the asylum procedure,] responsibilities must be clearly defined and easy to adapt to the individual cases. More specifically, responsibilities should only be with the competent local authority that is, indeed, responsible and able to assume such responsibilities. This makes the installation of a single authority that first has to delegate responsibilities very unattractive."

To address this need for decentralization, Germany's Federal Office for Migration and Refugees began to explore blockchain technology with a Proof-of-Concept (PoC) in January 2018. The idea was that blockchain could reflect the federal structure of the procedure in a cross-organizational IT architecture. Based on a positive evaluation of the PoC, the BAMF initiated a joint pilot project with Saxony's central immigration authority (LDS) in August 2018 to develop and test the FLORA system in Dresden, Saxony. This part of the project saw the establishment of an equilibrium where governance and especially strategic decision-making was shared between the Federal Office and the LDS. In the words of one of FLORA's project managers:

"We closely collaborated with the LDS from the beginning on, which has been quite special. [...] We had a lot of shared responsibilities and required frequent alignment calls. [...] Ultimately, our AnkER facility in Dresden has been selected for the pilot project [...] since we were convinced of the added value of the FLORA project and all groups, offices, and authorities [within the AnkER facility] saw their visions aligned with the goals of FLORA."

Additionally, the Federal Office envisioned shared development and decentralized hosting of the FLORA system. This vision resonated well with the LDS. However, as the pilot phase progressed, the LDS soon signaled a lack of both the required resources and competencies to participate in the development and hosting of the FLORA system. To not jeopardize the pilot project, the Federal Office's FLORA team ultimately established a compromise. The FLORA team would assume full technical responsibility for the FLORA system and host an LDS instance of the FLORA system on the Federal Office's IT infrastructure. The LDS, in turn, would support the FLORA team with requirements and specifications and participate in strategic decision-making. In the words of a business analyst:

"Sure, the LDS and any other authority could technically host a blockchain node. But many, including the LDS do not really want this. The level of complexity in the governance, not necessarily in the technology, requires a different way of thinking and can be an impediment."

Through this centralized equilibrium, the FLORA team could quickly respond when the COVID pandemic required temporary changes to parts of the procedure. This success did not go unnoticed by partnering authorities as well as the BAMF's leadership. Toward the end of the pilot phase, the BAMF's president participated in a conference with representatives from several other German states who responded positively to the presentation of FLORA's pilot phase and encouraged him to make FLORA's roll-out a strategic priority. With the partnering authorities' increasing interest in adopting the FLORA system, the Federal Office, once again, evaluated options for more decentralized governance and IT. However, these efforts were punctuated when the states asked for a fast roll out of the FLORA system. In effect, the FLORA team decided to further formalize its (de)centralization compromise. In particular, it developed a software-as-a-service (SaaS) model and prioritized the roll-out to German states that were interested in the pilot's centralized development and hosting model. A consultant to the project explains:

"We currently have a software-as-a-service model, which ultimately means that the BAMF deploys a productive solution for other stakeholders. It doesn't mean, however, that other organizations cannot influence the solution, make remarks, or ask for personalization. It just means, from a purely technical perspective, that the Federal Office hosts the solution. Long-term, the aim is to develop [the model] into the direction of platform-as-a-service […] to push responsibilities back to the competent state authorities."

As the roll-out progressed, however, the FLORA team began to experience tensions with the SaaS equilibrium as coordinating with an increasing number of 'customers' slowed down development. To ease these tensions, the FLORA team recalibrated its governance model by pushing more responsibilities to its local offices and their partner authorities at the state level. For instance, they were given full responsibility for local data management and first-level support. However, this recalibration was challenging as not all local offices and partner authorities were interested in assuming this responsibility. One of FLORA's project managers explains:

"On the one hand, [the local offices and their partner authorities] love the thought of assuming their rightful responsibilities. On the other hand, they want us to map their processes. […] They feel overwhelmed when they cannot simply call and say what they want but have to do it themselves. So, we really need to push them to assume their responsibilities."

Further centralization tensions resulted from the hosting of the FLORA instances. Historically, the Federal Office had to cede operation of its IT infrastructure to the Informationstechnikzentrum Bund (ITZBund), the Federal Government's IT service provider. This legacy meant the Federal Office had to repeatedly apply for new infrastructure services as the roll-out proceeded. ITZBund, in turn, was slow to provide these services due to lengthy bureaucratic processes. The FLORA team thus explored various options for becoming more independent and recalibrating the 'centralized' hosting equilibrium. In the words of one of the project's IT architects:

"In the end, the 'latencies' provided the relevant incentive to decide that the system is operated by the Federal Office itself. That is, only the basic infrastructure of the network, such as IP addresses, DNS names, routing, firewall, is provided by the ITZ-Bund and we, the Federal Office, provide the operating system, on which we build virtual machines to operate our application."

Navigating (De)centralization in the EBSI Project

Much like the Federal Office, the EBP started to explore blockchain in 2018 to deliver digital public services. The EBP's objective was to develop a European Blockchain Services Infrastructure that would allow member states to provide cross-border public services through a shared IT infrastructure. The use of blockchain was deemed particularly suitable for such an infrastructure, as it would allow to replicate the EU's federal structure in a decentralized IT architecture. This idea of decentralization was also reflected in the EBP's initial processes and governance structure. Strategic decisions were made by a policy group composed of one representative for each EBP member state. Technical decisions were made by a technical group that was also composed of member state delegates. Specifications and requirements for the supported public services came from working groups for each service. Member states were free to decide whether they wanted to involve themselves in the technical and service groups. This decentralization of responsibilities allowed the EBP to secure member state support and buy-in in the EBP's early stages. One representative from an EBSI network operator explains:

"I think [decentralization of responsibilities to different working groups] is a viable approach. It allows the EBP to bring experts together and enables in-depth discussions. Because if you had such discussions in the EBP's higher-level policy- and technical groups, those discussions would become blurred and probably even politicized. And when we look back at what we have achieved, it shows that this decentralization made sense because we have made good progress on these use cases."

However, first decentralization tensions occurred when higher echelons in the European Commission pushed for a swift development of a working pilot system in 2019. While the member states supported the European Commission's ambition to accelerate the development of an EBSI pilot system, many hesitated to assume the required responsibilities and costs for this system. To break this impasse, the European Commission realized that a recalibration and transition toward a more centralized equilibrium was needed. They offered to step in and take responsibility for developing EBSI's core features and deploying a pilot network. To support this shift, the EBP granted the European Commission's EBSI team a certain degree of decision-making authority in technical development. A quote by a national policy representative illustrates:

"The degree of centralization was not forced by the European Commission. It was a result of a lack of involvement from the member states. [...] The technical development is quite European Commission-centric. Which is, in general, not a good thing. But it's a result of some member states, I don't say, stepping back, but not being so technically committed [...] It's a consequence of the fact that the member states didn't want to take [the responsibility]."

The temporary but relatively centralized equilibrium allowed the EBP to quickly set up a pilot system. However, rolling out the system called for further recalibration, especially for decentralized hosting and development of applications that build on the pilot system. To incentivize and financially support this partial 'redecentralization', the European Commission launched an EBSI funding facility. Many of the submitted tenders focused on applications that would use EBSI to support the issuance and verification of digital diplomas. This focus then led to further decentralization needs as digital diplomas required an additional end-user component, a so-called digital wallet. Soon, the EBSI team felt they did not have the necessary expertise and mandate to develop these wallets. To mitigate these centralization tensions, they created another funding facility and invited private IT companies to contribute the wallets. This decentralized development process required additional control mechanisms. To account for these, the EBSI team defined a set of technical specifications and a certification program. One national EBP policy representative reflects:

"The basic idea is to operate an infrastructure. But for that infrastructure, we had to find a boundary after which we open it [the development of applications] to the market. The important thing is that you find this line and you provide some APIs or other channels for open communication, and then it's a good thing to leave it to the market and to private organizations. It's a good choice because, in this case, competition [...] can really have a good impact. I think, if we wanted to create a unique wallet realized by the European Commission, we had to wait too long. Probably upon release, the wallet would have been technically outdated. It's ok that the infrastructure and the requirements for it have had this [centralized] story. While on the upper-levels, like the wallets and so on, we have to [decentralize] it to the market."

This recalibration allowed the EBP to foster EBSI's adoption and progress on the development of digital diplomas. Consequently, the EBSI team began to work on a rollout strategy for a production-ready system. Once again, this strategic prioritization turned out to punctuate the existing equilibrium. In effect, the EBP realized that launching EBSI in production would require increased operational responsibilities of the member states. Yet, the member states felt unable to take full responsibility for an infrastructure they cannot fully control and that is distributed and operated across different organizations and member states. Given these constraints, the EBP started transitioning to a new equilibrium. That is, they started to incorporate the EBP into a newly established European Digital Infrastructure Consortium (EDIC) that would be co-financed and jointly governed by the participating member states. The EDIC would act as an overarching central entity accountable for the development and operation of EBSI. One representative from the European Commission explains:

"That's why we want to support the follow-up of this initiative [the EBP] through a new instrument [EDIC], where it will be less the European Commission that is in the driving seat [...] We want the member states to continue their cooperation and to be more the driver of this initiative, with the European Commission staying in the role of the policy support and also financial support. But with the member states taking over our responsibilities in this initiative. That's something we are now preparing with the EBP, and we hope that this will be a way to ensure the continuity of EBSI."

Although all EBP member states considered this transition necessary, many refrained from financially committing to EDIC as a founding member. Some member states were particularly concerned about the long-term perspective of EBSI and an investment in a highly controversial technology that has proven over time to have considerable (technical) limitations. Other member states were hesitant to be a 'first mover'. As a result, only one-third of the member states committed to becoming founding members of EDIC. The limited participation in EDIC caused an (unforeseen) centralization of EBSI's governance as compared to the previously decentralized approach – in particular, the EBP policy and technical groups – that governed EBP and EBSI since their inception. One representative from an EBSI network operator describes:

"All member states, almost all, support EDIC. I don't think I've heard any critical voice saying no we don't. Maybe a couple of member states are not decided yet. Everybody supports it [EDIC], but nobody wants to fund it, that's very clear. That's the crux. [...] And there is also the risk that we don't know what will happen after 3 years. That risk exists, of course. But as I understand it, you can join the EDIC and you can also leave again, there is some flexibility."

The IT architecture of EBSI should, in turn, remain decentralized among different node operators in the member states according to detailed service-level agreements, including well-defined terms and conditions for node operation as well as IT security requirements. However, complying with these service-level agreements appeared to be challenging for some pilot network operators who lacked the required IT security certification. Obtaining such a certification can be costly and requires substantial organizational changes. Consequently, the EBSI team feared that a secure and production-grade EBSI would again lead to an unduly centralized network. To mitigate this risk, the EBSI team once again adapted its approach. More specifically, they initiated another funding facility – this time for hosting productive instances and developing complementary productive applications. One national EBP policy representative reflects:

"This is a risk. If these requirements [for the node operation] prove to be too strict and too strong. They impair the enlargement of the number of nodes. This is, of course, an issue. [... And] it's quite expensive to set up and operate a node. This is an issue."

Summary

In both projects, the initial vision was to develop an IT system that follows dominant federal organizing structures and a strict decentralization of responsibilities. However, the Federal Office and the EBP had to compromise on decentralization early on because the (political) need for quick progress required a more centralized approach. Over time, the limitations of these centralization compromises and a range of punctuating events required an iterative recalibration and a transition to new (de)centralization equilibria. The FLORA project opted to maintain and recalibrate its centralization compromise and, ultimately, establish a more centralized equilibrium than initially envisioned. The EBP, in turn, attempted to mitigate mounting (de)centralization tensions by iterating between centralization and decentralization, regularly pushing back temporarily centralized responsibilities to the member states.

Discussion

We started our study by observing that large organizations are trapped in a tension field between centralization and decentralization (Mintzberg, 1984, 1989; Smith & Lewis, 2011; Weick, 1987). While the tension field is well researched, little is known about how organizations can navigate this tension field and establish new stable (de)centralization equilibria in their organizational processes, governance, and IT once an old equilibrium is punctuated. We thus conducted a multiple-case study on two projects that saw the establishment, recalibration, and transition between several such equilibria. Our analysis unpacks how changes in organizational strategy or context will typically punctuate (de)centralization equilibria. These punctuating events make the old equilibrium unstable and require organizations to embark on an iterative recalibration of their organizational processes, governance, and IT to reach a new stable equilibrium.

A Process Model for the Development of Dynamic (De)centralization Equilibria

Our insights can be translated into a process model (Cloutier & Langley, 2020) that captures the dynamic development of (de)centralization equilibria in organizational processes, governance, and IT (Figure 3). Drawing on centralization and decentralization literature in the fields of management (Mintzberg, 1984, 1989; Romanelli & Tushman, 1994; Smith & Lewis, 2011; Smith & Tushman, 2005) and IS (Andersen, 2005; Kahai et al., 2003; King, 1983; Sambamurthy & Zmud, 1999), our model describes the iterative recalibration of organizational processes, governance, and IT in response to punctuating events (Lyytinen & Newman, 2008; Romanelli & Tushman, 1994). It highlights that the recalibration process is guided by observations of centralization or decentralization tensions.

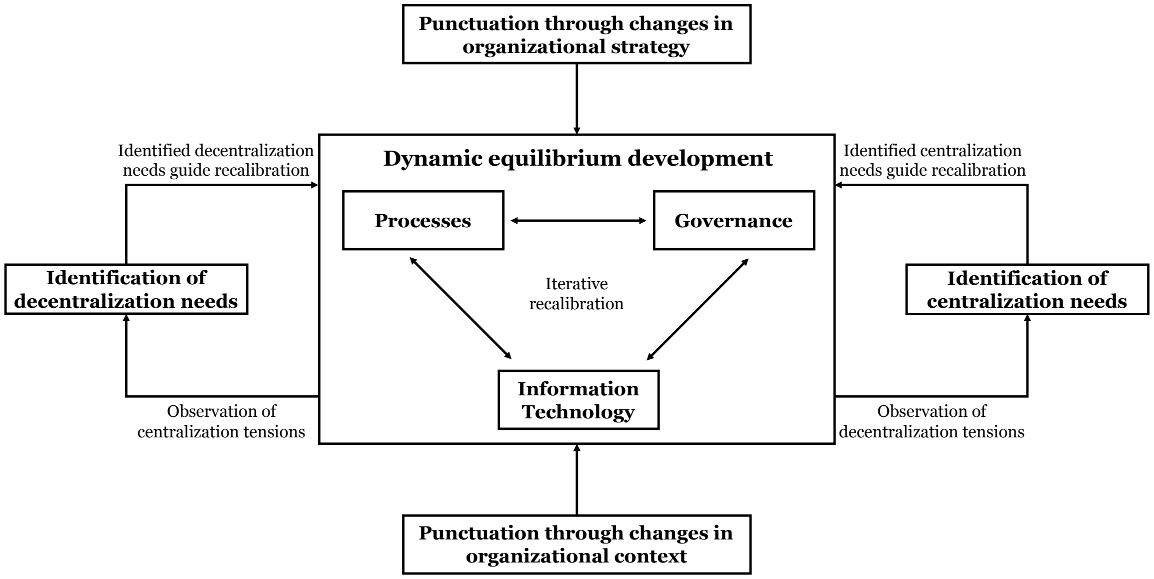

Punctuation through changes in organizational strategy
Dynamic equilibrium development
Processes
Governance
Iterative recalibration
Information Technology
Identified decentralization needs guide recalibration
Identification of decentralization needs
Observation of centralization tensions
Identified centralization needs guide recalibration
Identification of centralization needs
Observation of decentralization tensions
Punctuation through changes in organizational context

Figure 3. A Process Model for the Dynamic Development of (De)centralization Equilibria in Organizational Processes, Governance, and IT.

Successful navigation of such identification and recalibration processes requires organizations to be malleable in their processes, governance, and IT (Hanelt et al., 2021; Henderson & Venkatraman, 1999; King, 1983; Mikalef et al., 2021). This malleability is particularly crucial when organizations need to react quickly to punctuating changes in their strategic direction (Aldrich & Pfeffer, 1976; Smith & Tushman, 2005) or their organizational context (Ahituv et al., 1989; Sambamurthy & Zmud, 1999). Changes in strategic priorities, for example, may necessitate organizations to shift their governance from a centralized to a more decentralized structure or vice versa. For instance, as our cases demonstrate, strategies that call for a rapid system roll-out, may result in centralization needs. Resource constraints of a central entity, in turn, may provoke decentralization needs when the system grows. Such shifts often require adjustments to organizational processes and IT to mirror these new governance structures. However, our cases also demonstrate that such shifts are typically temporary. As time passes, new punctuating events may trigger further recalibration or the transition to new equilibria. Thus, we derive the following conjecture:

Conjecture 1: (De)centralization equilibria are inherently temporary and stability results from the ability to recalibrate and transition between equilibria.

Our cases demonstrate how important it is for organizations to navigate equilibria, recalibrations, and transitions carefully. The nature of the tensions organizations will face during transitions depends on the desired degree of centralization or decentralization (Andersen, 2005; King, 1983; Sambamurthy & Zmud, 1999). If the new equilibrium, for example, is to be characterized by strong centralization in one or multiple elements, these changes may lead to substantial coordination or communication costs across organizational subunits (Andersen, 2005; Kahai et al., 2003; Mikalef et al., 2021; Sambamurthy & Zmud, 1999). Identifying such tensions will guide the redesign of the new equilibrium in a more decentralized way and initiate an iterative process of recalibration and re-evaluation. Similar tensions occur when a target equilibrium is situated at the decentralized end of the spectrum. Tensions related to the loss of control over subunits (Beck et al., 2018; Moldoveanu & Martin, 2001; Weill, 2004) or a void in accountabilities as in the cases of FLORA and EBSI, in turn, can emphasize the need to centralize and push for a recalibration of the equilibrium. Hence, we propose as our second conjecture:

Conjecture 2: Punctuations or imbalances in the equilibrium create (un)foreseen needs for counterbalancing organizational processes, governance, and/ or IT.

To accommodate the dynamic recalibration of organizational processes, organizations must allow for local and temporary nuances in their (de)centralization equilibria. Decentralized organizations that aim to establish a decentralized IT system cannot always rely on their existing structures from the onset, as subunits may often be unable or unwilling to take the lead (Andersen, 2005; Beck et al., 2018; Wiseman et al., 2012). In such cases, centralization may not only be essential for filling accountability voids but also for proceeding quickly (Aulakh & Gencturk, 2000; Mintzberg, 1989; Peppard, 2018; Rediker & Seth, 1995). In effect, decentralized organizations may accept local or temporary centralization compromises to enable a transition to a more decentralized equilibrium later. Finding the right time for this transition, however, is essential to avoid undue centralization tensions. Centralized development, for instance, may increasingly impede the roll-out and extension once decentralized IT systems exceed a certain size. Moreover, increased decentralized use can make it hard to maintain centralized accountability. When (de)centralization compromises lead to escalating tensions, organizations may re-evaluate their local and temporal compromises. Accordingly, we derive our third conjecture:

Conjecture 3: To achieve stable (de)centralization equilibria, organizations must allow for dynamism and regularly revisit local and temporary compromises.

Theoretical Contributions

Our research first contributes to the IS literature on (de)centralization by demonstrating that sustaining (de)centralization equilibria in organizational processes, governance, and IT is inherently dynamic. More specifically, our work emphasizes that organizations evolve in response to punctuating events that require an iterative recalibration and transition to a new temporary equilibrium. This process perspective builds on insights into the realization of stable decentralized IT structures and the relevance of malleability (Henderson & Venkatraman, 1999; King, 1983; Mikalef et al., 2021; Sambamurthy & Zmud, 1999). At the same time, it extends these insights by examining the process, i.e., dynamic transitions between (de)centralization equilibria, organizations use to resolve tensions. Moreover, our process perspective highlights that (de)centralization equilibria are not persistent. We explain how organizations can work toward a new equilibrium by making changes to organizational processes, governance, or IT when changes in organizational strategy or context destabilize the old equilibrium (Romanelli & Tushman, 1994).

Secondly, our research adds to management literature on decentralization by demonstrating that the establishment of (de)centralization equilibria requires an IT perspective (Ahituv et al., 1989; Siggelkow & Levinthal, 2003). We emphasize that IT does and should play an important role in sustaining desirable (de)centralization equilibria in today's organizations. However, this does not establish IT as more important than organizational processes or governance. All three are of equal importance and require careful individual and joint consideration in the pursuit of stable equilibria (Romanelli & Tushman, 1994; Smith & Tushman, 2005). Yet, we observe that the selection of the underlying IT can create baseline tensions and impact the development of (de)centralization equilibria. Blockchains, for example, stipulate a certain degree of decentralization, which may conflict with centralized processes and governance structures. This may require compromises and frequent recalibration.

Third, our research contributes both to the IS and management literature on (de)centralization by connecting the two literatures and unpacking *how* organizations can successfully navigate the recalibration and transition between old and new equilibria. Our study demonstrates that organizations must allow and embrace temporary compromises in these processes. Moreover, organizations will often not be able to apply the same degree of (de)centralization to all units, since not all units possess the same maturity or competence level. As such, we confirm and corroborate the insights of Smith & Tushman (2005) and Smith & Lewis (2011) that dynamic compromises between centralization and decentralization can be utilized to benefit organizations.

Practical Implications

The practical implications of our study are two-fold. First, our research sheds light on how organizational leaders can rebalance the degree of (de)centralization in their organization's processes, governance, and IT in response to changes in strategy or the organizational context. Additionally, our work highlights that any change in the degree of (de)centralization can entail an iterative recalibration or transition process. Organizational leaders should be careful when choosing overly centralized or decentralized structures, as either choice will introduce tensions that may require costly recalibration or transition at a later point. Moreover, organizational leaders are well advised to minimize the number of punctuating events that require an iterative recalibration.

Second, our paper provides organizational leaders with decision support on how to navigate these iterative recalibration and transition processes best. We highlight that organizational leaders should avoid applying a one-size-fits-all approach. Instead, they should consider, allow, and accept local and temporary differences. Especially temporary compromises may be essential to build a stable equilibrium. However, organizational leaders should be aware that such compromises will not be tolerated indefinitely and that other changes in strategy or organizational context may occur that will demand resolving such compromises earlier than expected. Thus, temporal compromises need to be constantly re-evaluated. This minimizes the risk of organizational leaders to mismanage their organizations and create long-term imbalances in their (de)centralization equilibria, which might result in more frequent and costly recalibration.

Boundary Conditions

Boundary conditions are essential to theoretical insights, including those developed from multiple-case study research, as they help define the scope and applicability of the developed theoretical insights (Eisenhardt, 2021). We identify three such boundary conditions for our process model and conjectures in terms of domain, prevalent organizational structures, and technology.

First, both cases are public sector projects, which might limit the generalizability and transferability of our insights. Public organizations are typically not driven by profitability considerations and market pressure. As such, they might have more margin for maneuvering when allowing for local and temporary differences between their organizational subunits while trying to find a (de)centralization equilibrium. Companies might not always have this level of freedom as market pressures may restrict them and stifle attempts to 'experiment' with different levels of centralization (Weick, 1987).

Second, both cases are situated in a federally organized context, which naturally places them between centralized and decentralized structures. This second boundary condition emphasizes the transferability of our findings to strongly centralized or strongly decentralized organizations. Our model cannot predict whether organizations that find themselves on one end of the (de)centralization continuum would be willing to – at least temporarily – commit (de)centralization compromises and search for new stable equilibria. Yet as both centralized and decentralized structures each present opportunities and limitations, we argue that organizations at either end of the (de)centralization continuum will sooner or later face punctuating events that may cause them to compromise on parts of their existing structures to ensure successful organizing (Smith & Lewis, 2011; Smith & Tushman, 2005).

Third, both projects focus on developing blockchain-based systems, which naturally imposes a certain degree of decentralization. This third boundary condition, thus, affects the transferability of our results to equilibria build around more inherently centralized IT. However, a closer look at both cases suggests that our model may not be limited to blockchain. While both systems were initially built around blockchain, the blockchain components have become less important over time and have been complemented by various other components and technologies as development proceeds. Furthermore, many of the observed (de)centralization tensions occurred independently of blockchain technology. This leads us to surmise that our insights can also be transferred to IT systems that do not build on blockchain.

Conclusion

Our study demonstrates that establishing a (de-)centralization equilibrium in organizational processes, governance, and IT is a dynamic process that requires constant recalibration and sometimes transitions to new equilibria. Based on insights from two blockchain projects, we derive a process model that describes this recalibration and transition. Our model details that punctuations through changes in organizational strategies and context, as well as tensions inherent to centralization and decentralization, can trigger an iterative recalibration process and the transition to a new (de)centralization equilibrium. Navigating this transition can require local or temporal compromises.

Acknowledgements

This research was funded in part by the Luxembourg National Research Fund (FNR) and PayPal, PEARL grant reference *13342933/Gilbert Fridgen*, as well as the Luxembourg National Research Fund (FNR) in the FiReSpARX (grant reference *14783405*) project, and Luxembourg's Ministry for Digitalisation. We also acknowledge the support of the European Union (EU) within its Horizon 2020 programme, project MDOT (Medical Device Obligations Taskforce), grant agreement *814654,* that made this paper possible. For the purpose of open access, the authors have applied a Creative Commons Attribution 4.0 International (CC BY 4.0) license to any Author Accepted Manuscript version arising from this submission.

References

Ahituv, N., Neumann, S., & Zviran, M. (1989). Factors affecting the policy for distributing computing resources. *MIS Quarterly*, *13*(4), 389–401. **https://doi.org/10.2307/248722**

Aldrich, H. E., & Pfeffer, J. (1976). Environments of organizations. *Annual Review of Sociology*, *2*(1), 79–105. **https://doi.org/10.1146/annurev.so.02.080176.000455**

Andersen, T. J. (2005). The performance effect of computer-mediated communication and decentralized strategic decision making. *Journal of Business Research*, *58*(8), 1059–1067. **https://doi.org/10.1016/j.jbusres.2004.02.004**

Aulakh, P. S., & Gencturk, E. F. (2000). International principal–agent relationships: Control, governance and performance. *Industrial Marketing Management*, *29*(6), 521–538. **https://doi.org/10.1016/S0019-8501(00)00126-7**

Bakos, Y., Halaburda, H., & Mueller-Bloch, C. (2021). When permissioned blockchains deliver more decentralization than permissionless. *Communications of the ACM*, *64*(2), 20–22. **https://doi.org/10.1145/3442371**

Beck, R., Müller-Bloch, C., & King, J. (2018). Governance in the Blockchain Economy: A Framework and Research Agenda. *Journal of the Association for Information Systems*, *19*(10). **https://aisel.aisnet.org/jais/vol19/iss10/1/**

Brown, C. V. (1997). Examining the emergence of hybrid IS governance solutions: Evidence from a single case site. *Information Systems Research*, *8*(1), 69–94. **https://doi.org/10.1287/isre.8.1.69**

Chen, Y., Richter, J. I., & Patel, P. C. (2021). Decentralized Governance of Digital Platforms. *Journal of Management*, *47*(5), 1305–1337. **https://doi.org/10.1177/0149206320916755**

Cloutier, C., & Langley, A. (2020). What makes a process theoretical contribution? *Organization Theory*, *1*(1), 1–32. **https://doi.org/10.1177/2631787720902473**

Constantinides, P., Henfridsson, O., & Parker, G. G. (2018). Introduction—Platforms and Infrastructures in the Digital Age. *Information Systems Research*, *29*(2), 381–400. **https://doi.org/10.1287/isre.2018.0794**

Corbin, J. M., & Strauss, A. (1990). Grounded theory research: Procedures, canons, and evaluative criteria. *Qualitative Sociology*, *13*(1), 3–21. **https://doi.org/10.1007/BF00988593**

Davis, J. P., & Eisenhardt, K. M. (2011). Rotating leadership and collaborative innovation: Recombination processes in symbiotic relationships. *Administrative Science Quarterly*, *56*(2), 159–201. **https://doi.org/10.1177/0001839211428131**

de Reuver, M., Sørensen, C., & Basole, R. C. (2018). The Digital Platform: A Research Agenda. *Journal of Information Technology*, *33*(2), 124–135. **https://doi.org/10.1057/s41265-016-0033-3**

Drucker, P. F. (1992). The New Society of Organizations. *Harvard Business Review*, *20*(7), 281–293.

Eisenhardt, K. M. (1989). Building Theories from Case Study Research. *Academy of Management Review*, *14*(4), 532–550. **https://doi.org/10.5465/amr.1989.4308385**

Eisenhardt, K. M. (2021). What is the Eisenhardt Method, really? *Strategic Organization*, *19*(1), 147–160. **https://doi.org/10.1177/1476127020982866**

Eisenhardt, K. M., & Graebner, M. E. (2007). Theory Building From Cases: Opportunities And Challenges. *Academy of Management Journal*, *50*(1), 25–32. **https://doi.org/10.5465/amj.2007.24160888**

Foss, N. J., Husted, K., & Michailova, S. (2010). Governing knowledge sharing in organizations: Levels of analysis, governance mechanisms, and research directions. *Journal of Management Studies*, *47*(3), 455–482. **https://doi.org/10.1111/j.1467-6486.2009.00870.x**

Grandori, A. (1997). Governance structures, coordination mechanisms and cognitive models. *Journal of Management & Governance*, *1*(1), 29–47. **https://doi.org/10.1023/A:1009977627870**

Gubitta, P., & Gianecchini, M. (2002). Governance and flexibility in family-owned SMEs. *Family Business Review*, *15*(4), 277–297. **https://doi.org/10.1111/j.1741-6248.2002.00277.x**

Halaburda, H. (2018). Blockchain revolution without the blockchain? *Communications of the ACM*, *61*(7), 27–29. **https://doi.org/10.1145/3225619**

Halaburda, H., & Mueller-Bloch, C. (2019). *Will We Realize Blockchain's Promise of Decentralization?* **https://hbr.org/2019/09/will-we-realize-blockchains-promise-of-decentralization**

Hammer, M. (2014). What is business process management? In *Handbook on business process management 1: Introduction, methods, and information systems* (pp. 3–16). Springer. **https://doi.org/10.1007/978-3-642-45100-3_1**

Hanelt, A., Bohnsack, R., Marz, D., & Antunes Marante, C. (2021). A systematic review of the literature on digital transformation: Insights and implications for strategy and organizational change. *Journal of Management Studies*, *58*(5), 1159–1197. **https://doi.org/10.1111/joms.12639**

Hanseth, O., & Lyytinen, K. (2010). Design theory for dynamic complexity in information infrastructures: The case of building internet. *Journal of Information Technology*, *25*, 1–19. **https://doi.org/10.1057/jit.2009.19**

Hein, A., Schreieck, M., Riasanow, T., Setzke, D. S., Wiesche, M., Böhm, M., & Krcmar, H. (2020). Digital platform ecosystems. *Electronic Markets*, *30*(1), 87–98. **https://doi.org/10.1007/s12525-019-00377-4**

Henderson, J. C., & Venkatraman, H. (1999). Strategic alignment: Leveraging information technology for transforming organizations. *IBM Systems Journal*, *38*(2.3), 472–484. **https://doi.org/10.1147/SJ.1999.5387096**

Huber, G. P., & Power, D. J. (1985). Retrospective Reports of Strategic-Level Managers: Guidelines for Increasing Their Accuracy. *Strategic Management Journal*, *6*(2), 171–180. **https://doi.org/10.1002/smj.4250060206**

Huber, T. L., Kude, T., & Dibbern, J. (2017). Governance practices in platform ecosystems: Navigating tensions between cocreated value and governance costs. *Information Systems Research*, *28*(3), 563–584. **https://doi.org/10.1287/isre.2017.0701**

Jacobides, M. G., Cennamo, C., & Gawer, A. (2018). Towards a theory of ecosystems. *Strategic Management Journal*, *39*(8), 2255–2276. **https://doi.org/10.1002/smj.2904**

Kahai, P. S., Carr, H. H., & Snyder, C. A. (2003). Technology and the decentralization of information systems. *Information Systems Management*, *20*(3), 51–60. **https://doi.org/10.1201/1078/43205.20.3.20030601/43073.6**

King, J. L. (1983). Centralized versus decentralized computing: Organizational considerations and management options. *ACM Computing Surveys (CSUR)*, *15*(4), 319–349. **https://doi.org/10.1145/289.290**

Lacity, M. C. (2018). Addressing key challenges to making enterprise blockchain applications a reality. *MIS Quarterly Executive*, *17*(3), 201–222. **https://aisel.aisnet.org/misqe/vol17/iss3/3**

Lumineau, F., Wang, W., & Schilke, O. (2021). Blockchain Governance—A New Way of Organizing Collaborations? *Organization Science*, *32*(2), 500–521. **https://doi.org/10.1287/orsc.2020.1379**

Lyytinen, K., & Newman, M. (2008). Explaining information systems change: A punctuated socio-technical change model. *European Journal of Information Systems*, *17*, 589–613. **https://doi.org/10.1057/ejis.2008.50**

Mikalef, P., Pateli, A., & van de Wetering, R. (2021). IT architecture flexibility and IT governance decentralisation as drivers of IT-enabled dynamic capabilities and competitive performance: The moderating effect of the external environment. *European Journal of Information Systems*, *30*(5), 512–540. **https://doi.org/10.1080/0960085X.2020.1808541**

Mintzberg, H. (1984). Who should control the corporation? *California Management Review*, *27*(1), 90–115. **https://doi.org/10.2307/41165115**

Mintzberg, H. (1989). *The structuring of organizations*. Springer. **https://doi.org/10.1007/978-1-349-20317-8_23**

Moldoveanu, M., & Martin, R. (2001). Agency theory and the design of efficient governance mechanisms (Joint Committee on Corporate Governance). *Toronto: Rotman School of Management, University of Toronto.*, *3*(5), 430.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Decentralized Business Review.

Peppard, J. (2018). Rethinking the concept of the IS organization. *Information Systems Journal*, *28*(1), 76–103. **https://doi.org/10.1111/isj.12122**

Rediker, K. J., & Seth, A. (1995). Boards of directors and substitution effects of alternative governance mechanisms. *Strategic Management Journal*, *16*(2), 85–99. **https://doi.org/10.1002/smj.4250160202**

Romanelli, E., & Tushman, M. L. (1994). Organizational transformation as punctuated equilibrium: An empirical test. *Academy of Management Journal*, *37*(5), 1141–1166. **https://doi.org/10.5465/256669**

Sambamurthy, V., & Zmud, R. W. (1999). Arrangements for information technology governance: A theory of multiple contingencies. *MIS Quarterly*, *23*(2), 261–290. **https://doi.org/10.2307/249754**

Siggelkow, N., & Levinthal, D. A. (2003). Temporarily divide to conquer: Centralized, decentralized, and reintegrated organizational approaches to exploration and adaptation. *Organization Science*, *14*(6), 650–669. **https://doi.org/10.1287/orsc.14.6.650.24840**

Smith, W. K., & Lewis, M. W. (2011). Toward a theory of paradox: A dynamic equilibrium model of organizing. *Academy of Management Review*, *36*(2), 381–403. **https://doi.org/10.5465/amr.2009.0223**

Smith, W. K., & Tushman, M. L. (2005). Managing strategic contradictions: A top management model for managing innovation streams. *Organization Science*, *16*(5), 522–536. **https://doi.org/10.1287/orsc.1050.0134**

Srikanth, K., & Puranam, P. (2014). The firm as a coordination system: Evidence from software services offshoring. *Organization Science*, *25*(4), 1253–1271. **https://doi.org/10.1287/orsc.2013.0886**

Tushman, M. L., & Romanelli, E. (1985). Organizational evolution: A metamorphosis model of convergence and reorientation. *Research in Organizational Behavior*, *7*, 171–222.

Uhl-Bien, M., & Arena, M. (2018). Leadership for organizational adaptability: A theoretical synthesis and integrative framework. *The Leadership Quarterly*, *29*(1), 89–104. **https://doi.org/10.1016/j.leaqua.2017.12.009**

Weick, K. E. (1987). Organizational culture as a source of high reliability. *California Management Review*, *29*(2), 112–127. **https://doi.org/10.2307/41165243**

Weill, P. (2004). Don't just lead, govern: How top-performing firms govern IT. *MIS Quarterly Executive*, *3*(1), 1–17. **https://aisel.aisnet.org/misqe/vol3/iss1/3**

Wiseman, R. M., Cuevas-Rodríguez, G., & Gomez-Mejia, L. R. (2012). Towards a social theory of agency. *Journal of Management Studies*, *49*(1), 202–222. **https://doi.org/10.1111/j.1467-6486.2011.01016.x**

Yin, R. K. (2011). *Applications of case study research* (3rd ed). Sage Publications.

Yin, R. K. (2017). *Case Study Research and Applications* (6th Edition). Sage Publications.

Zhao, Y., von Delft, S., Morgan-Thomas, A., & Buck, T. (2020). The evolution of platform business models: Exploring competitive battles in the world of platforms. *Long Range Planning*, *53*(4), 101892. **https://doi.org/10.1016/j.lrp.2019.101892**

RP12: Roth, T., Rieger, A., Utz, M., & Young, A. (2022). **The Role of Cultural Fit in the Adoption of Fashionable IT: A Blockchain Case Study.** *ICIS 2022 Proceedings*.
https://aisel.aisnet.org/icis2022/blockchain/blockchain/17
Conference Ranking: 2 (GGS Class); A- (GGS Rating)

ICIS 2022 Proceedings | Blockchain, DLT, and FinTech

Dec 12th, 12:00 AM

The Role of Cultural Fit in the Adoption of Fashionable IT: A Blockchain Case Study

Tamara Roth
University of Luxembourg, tamara.roth@uni.lu

Alexander Rieger
University of Luxembourg, alexander.rieger@uni.lu

Manuel Utz
Faculty, of Law, Business, and Economics, University of Bayreuth, Germany, manuel.utz@hs-fresenius.de

Amber Grace Young
University of Arkansas, ayoung@walton.uark.edu

Recommended Citation

Roth, Tamara; Rieger, Alexander; Utz, Manuel; and Young, Amber Grace, "The Role of Cultural Fit in the Adoption of Fashionable IT: A Blockchain Case Study" (2022). *ICIS 2022 Proceedings*. 17.
https://aisel.aisnet.org/icis2022/blockchain/blockchain/17

The Role of Cultural Fit in the Adoption of Fashionable IT: A Blockchain Case Study

Completed Research Paper

Tamara Roth
Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg, Luxembourg
tamara.roth@uni.lu

Alexander Rieger
Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg, Luxembourg
alexander.rieger@uni.lu

Manuel Utz
Faculty, of Law, Business, and Economics, University of Bayreuth, Bayreuth, Germany
manuel.utz@uni-bayreuth.de

Amber Grace Young
Sam M. Walton College of Business, University of Arkansas
Fayetteville, United States
ayoung@walton.uark.edu

Abstract

Investments in fashionable IT do not make organizations more successful than investments in less fashionable alternatives. Many organizations nevertheless associate with fashionable IT to signal compliance with norms of progress and rationality. These decisions can be risky as they require the ability to navigate hype narratives and fit the new technology into the adopting organization. In this paper, we explore a so far understudied fit perspective: cultural fit between the values attributed to the fashionable IT and those of the recipient organizational context. Through an interpretivist case study of two blockchain projects, we find that cultural sensemaking and dissonance reduction can be important determinants for successful adoption of fashionable IT. Moreover, we identify two recursive paths for how organizations can reduce cultural dissonance. They can adapt their implementation and the narratives surrounding the fashionable IT or they can transform their local or overarching organizational culture.

Keywords: Blockchain, Cultural fit, Cultural sensemaking, Fashionable IT

Introduction

Certain digital technologies go through a veritable fad and fashion phase. Prominent examples include e-commerce technologies at the turn of this millennium (Baskerville & Myers, 2009) and blockchain in more recent years (Lacity, 2022; Rossi et al., 2019). IT fashions describe a "relatively transitory collective belief, that an information technology is new, efficient, and at the forefront of practice" (Wang, 2010). Like more traditional fashions, IT fashions are a temporary phenomenon with sharp up- and down-swings (Baskerville & Myers, 2009; Wang, 2010; Wang & Ramiller, 2009).

Organizational leaders are often eager to embrace fashionable IT over less-fashionable alternatives despite evidence that investments in fashionable versus non-fashionable IT tend to result in similar increases in organizational performance (Wang, 2010). These decisions may be largely driven by a desire to enhance an organization's short-term legitimacy, as well as the reputation and compensation of organizational leaders (Baskerville & Myers, 2009; Wang, 2010). Yet, they are not without risk. While organizational leaders have a certain degree of control over ‘sensemaking’ for non-fashionable IT, sensemaking of fashionable IT is often driven by narratives in the ‘fashion market’. These narratives are typically outside of an organization’s control and complicate the task of sensemaking (Wang & Ramiller, 2009).

While much work has been dedicated to how organizations can navigate the sensemaking process from a political and technical perspective, less is known about how organizations may promote cultural fit (Ansari et al., 2010; Canato et al., 2013; Piazza & Abrahamson, 2020). Yet, in contexts that are replete with beliefs, values, and norms, cultural fit can be an essential factor for successful adoption (Alavi et al., 2005; Kappos & Rivard, 2008; Koch et al., 2013; Leidner & Kayworth, 2006). In this study, we seek to investigate the establishment of this fit and employ a theory-building study to address the research question:

How do organizations establish fit between their organizational culture and fashionable IT?

To build our theory, we conduct an inductive case study on two successful blockchain projects: one in the context of asylum management and one in the context of a customer loyalty program. Since members of the author team have closely accompanied each of the two projects, we could collect particularly rich insights into how the projects created cultural fit.

Our emerging theoretical insights are twofold. Firstly, we find strong evidence for a process of cultural sensemaking and dissonance reduction between the values attributed to the fashionable IT and those of the adopting organization's culture. Secondly, we find that cultural dissonance may be iteratively reduced along two paths: Fashionable IT systems and the narratives surrounding them can be adapted to match organizational culture, and organizational culture can be transformed to match narratives surrounding the fashionable IT. Our paper contributes to the literature on fashionable IT by demonstrating the importance of cultural fit. Moreover, we develop a theoretical model of cultural sensemaking and dissonance reduction for fashionable IT.

The rest of the paper is organized as follows. The subsequent section provides an overview of challenges associated with the adoption of fashionable management practices and IT . Moreover, the section discusses the role of organizational culture in the adoption of IT. Next, we present details on our case-study design, data collection, and data analysis. In the fourth section, we present the theoretical model that emerged from our analysis of the two cases. The fifth section discusses our theoretical contribution, offers practical implications, and presents boundary conditions of our theorizing. The paper concludes with a summary of key insights from our analysis, limitations, and an outlook on future research.

Theoretical Background

Fashionable management practices and IT

The management literature defines fashionable management practices as a "relatively transitory collective belief, disseminated by management fashion setters, that a management technique leads rational management progress" (Abrahamson, 1996). The idea of fashions was introduced as an explanation for two phenomena that rational choice theories failed to properly explain: the successful diffusion of inefficient innovations and the poor diffusion of certain efficient innovations. The theory of management fashions offers a sociological lens to study and explain these phenomena as the result of imitation and legitimacy-seeking processes (Abrahamson, 1991, 1996; Ansari et al., 2010; Piazza & Abrahamson, 2020).

Fashionable management practices can be characterized as the product of management fashion markets with a 'supply' side of fashion-setters (e.g., consulting firms or business schools) and a 'demand side' of adopting organizations (Abrahamson, 1991; Piazza & Abrahamson, 2020). Fashionable practices typically go through four stages: innovation, fashion broadcast, faddish contagion, and retention or abandonment (Abrahamson, 1996; Piazza & Abrahamson, 2020). All these phases are typically accompanied by different fashion narratives (Abrahamson & Fairchild, 1999; van Grinsven et al., 2016). These narratives tend to be positive, emotional, and uncritical in the up-swing phase and somewhat negative, guarded, and critical in the downswing phase (Abrahamson & Fairchild, 1999). Fashion narratives are integral enablers for fashionable management practices as they allow to create and disseminate the relatively transitory, collective belief that the practice leads rational management progress (Ansari et al., 2010; Piazza & Abrahamson, 2020; van Grinsven et al., 2016).

During adoption of a fashionable management practice, 'demand-side' organizations will typically try to leverage the interpretative viability of the practice to translate it to their recipient context (Ansari et al., 2010; van Grinsven et al., 2016). This 'structural' translation focusses on increasing political, technical, and cultural fit between the characteristics of the practice and those of the adopting organization (Ansari et al., 2010). Political fit defines alignment between the normative characteristics of the practice and the interests and agendas of adopting organizations and their leaders. Technical fit, in turn, describes the degree to which technical foundations and characteristics match. Lastly, cultural fit is concerned with matching cultural values and meaning structures embedded into the practice to those of the recipient organization. Quality circles, for instance, were initially seen as a Japanese innovation that was hard to reconcile with values of individualism in American corporate culture. This perception led to modifications of the practice to match American "participatory management" styles (Ansari et al., 2010; Strang & Kim, 2006). Narratives again play an important part in the adoption of fashionable practices as their re-framing allows organizations to signal structural fit in general and cultural fit in particular (van Grinsven et al., 2016; Zilber, 2006).

Fashionable IT has many commonalities with fashionable management practices (Baskerville & Myers, 2009; Wang, 2010; Wang & Ramiller, 2009). First, fashionable IT goes through similar fashion cycles and is the product of similar fashion markets (Baskerville & Myers, 2009). Second, organizations equally associate with fashionable IT to increase legitimacy (Wang & Ramiller, 2009). More specifically, engagement with fashionable IT can lead to both higher external legitimacy (reputational gains) and internal legitimacy (higher executive compensation). This legitimacy-enhancing effect exists both for material engagement – i.e., actual implementation of the fashionable technology, and informational engagement in press – and public discourse. Of the two, informational engagement appears to have a higher effect on legitimacy. Third, fashion narratives are also pivotal for creating and disseminating fashionable IT (Baskerville & Myers, 2009; Gal et al., 2022; Wang & Ramiller, 2009). They are important sources for adopting organizations to learn about new and fashionable IT. They can, however, become sources of misinformation as many narratives are replete with wishful and unbalanced claims, especially in the upswing phase (Wang & Ramiller, 2009).

While fashionable practices and IT have much in common, there are also differences. Fashionable IT, for instance, is substantially more material than practices (Baskerville & Myers, 2009; Wang, 2010). This difference in materiality has various implications, such as a broader pool of potential fashion setters, like IT companies and developer communities, and a higher likelihood of institutionalization, that is, long-term productive use (Wang, 2010). Yet, favoring fashionable IT does not automatically give adopting organizations a clear edge. On the contrary, fashionable IT can require substantial political work and technical integration effort without clear performance gains over non-fashionable IT (Wang, 2010; Wang & Ramiller, 2009). Moreover, fashionable IT may require particular attention to cultural fit because value-laden fashion narratives bear a high risk of dissonance with organizational culture and increases the chances of IT culture conflict (Kappos & Rivard, 2008; Su, 2015)

The role of organizational culture for the adoption of IT

Organizational culture is a concept with many conceptualizations and perspectives (Kappos & Rivard, 2008; Schein, 1996, 2016). In this work, we follow Schein (2016) and define it as a “a pattern or system of beliefs, values, and behavioral norms that come to be taken for granted as basic assumptions and eventually drop out of awareness”. Organizational culture is typically conceived as a hierarchical construct with different levels that range from less-material basic assumptions to more material cultural artifacts, such as practices (Canato et al., 2013; Leidner & Kayworth, 2006; Schein, 2016). To balance observability and interpretability, studies of organizational culture typically focus on local and overarching organizational values (Alavi et al., 2005; Koch et al., 2013; Leidner & Kayworth, 2006).

Organizational culture can be an important factor in developing, adopting, and using IT. Yet, cultural dissonance or ‘conflicts’ can arise when three types of values are not aligned: (1) organizational values, (2) values related to an IT system in question, either embedded through work behaviors that the IT is designed to enable or attributed through association, and (3) values ascribed to IT in general. 0/0/00 0:00:00 AM'Systemic conflict’ between organizational values and the values related to a particular IT can be especially problematic (Alavi et al., 2005; Koch et al., 2013; Leidner & Kayworth, 2006).

Systemic conflict can be resolved either by adapting the design or use of an IT system (Alavi et al., 2005; Kappos & Rivard, 2008; Leidner & Kayworth, 2006) or by changing the organizational culture and its values (Kappos & Rivard, 2008; Koch et al., 2013; Leidner & Kayworth, 2006). In this work, we aim to explore how these two approaches play out for fashionable IT. We are particularly interested in how organizations can resolve systemic conflicts between their organizational values and those values attributed to fashionable IT through narratives in the fashion market. For this purpose, we focus our analysis on blockchain technology, which has garnered a reputation as a veritable hype technology in recent years and which is surrounded by various value-laden narratives (Lacity, 2022; Rossi et al., 2019).

Research Method

As cultural fit is poorly explored for fashionable IT, we chose a theory-building from cases approach. Case studies allow for an 'in-depth' investigation of a socially embedded phenomenon and can support the emergence of new theory (Eisenhardt, 1989, 2021; Eisenhardt & Graebner, 2007; Yin, 2017). Case study research is particularly fruitful for investigating an under-studied phenomenon or an "under-represented perspective in a well-researched literature" (Eisenhardt, 2021). As our study explores such an under-represented perspective, a case-study design appears conducive and appropriate. To allow for cross-case synthesis and more generalizable and parsimonious insights, we chose a multiple-case approach with a common-process design. This design emphasizes the selection of cases "about the same focal phenomenon in purposefully different settings, thus improving generalizability (i.e., transferability) of the emergent theory across settings" (Eisenhardt, 2021).

Case setting and selection

The setting for our case study is the adoption of blockchain in different organizational contexts. Blockchains are distributed databases hosted jointly by a network of so-called nodes. Blockchains group data in a block structure, hence the name 'blockchain'. These blocks are connected cryptographically, making it hard to change entries once the network has distributed a new block and added it to the chain (Beck et al., 2018; Rieger, Roth, Sedlmeir, & Fridgen, 2022; Ziolkowski et al., 2020).

Blockchain was initially introduced as a distributed database technology for processing cryptocurrency transactions but became broadly fashionable in 2016/2017 when blockchains with so-called "smart contract" features took hold (Lacity, 2022; Rossi et al., 2019). These blockchains enabled the automated execution of predefined logic, ranging from asylum management (Rieger et al., 2019; Roth, Stohr, et al., 2022) to verification of identity-related documents (Rieger et al., 2021; Rieger, Roth, Sedlmeir, Weigl, et al., 2022; Sedlmeir et al., 2021), and process models in supply chain management (Jensen et al., 2019; Mattke et al., 2019; Sarker et al., 2021).

Blockchain continues to be a fashionable technology, to which Gartner offers testament with a special hype cycle for blockchain use cases (Litan, 2022). Blockchain technology is typically associated with various fashion narratives (Lacity, 2022; Roth, Utz, et al., 2022; Utz et al., 2022). These firmly center around arguments of trust, disintermediation, and decentralization. Specifically, blockchain is marketed as being able to establish trust in contexts where parties do not trust each other (Lacity, 2022; Utz et al., 2022). Moreover, blockchain systems are often described as enabling decentralized processes (Rieger et al., 2019; Roth, Stohr, et al., 2022) or as agents of disintermediation (Beck et al., 2018; Lacity, 2022; Roth, Utz, et al., 2022).

To select suitable blockchain projects, we followed common recommendations for theoretical sampling of cases (Eisenhardt, 1989, 2021; Eisenhardt & Graebner, 2007) and employed three sampling criteria. In line with our interpretivist stance, we firstly focused on cases in which at least one co-author was deeply involved to ensure in-depth and first-hand insights. Secondly, we concentrated on early-adopter organizations in their respective contexts to control for the effect of conformity pressures from other organizations and potentially limited adoption in response (Ansari et al., 2010). Thirdly, we selected cases in which organizations engaged with blockchain materially and informationally to catch the effects of both types of engagement (Wang, 2010). Overall, our case selection led to a sample of two cases: one in asylum management and one in customer loyalty management. In both cases, blockchain was adopted successfully even though this success was not evident from the get-go. This initial ambiguity offers highly fertile ground for an analysis of the adoption process.

The first case revolves around the use of blockchain by Germany's federal government to support the coordination of authorities involved in the asylum procedure with a system called FLORA. Germany's asylum procedure is federally organized, which means that many authorities at different levels need to cooperate to successfully complete the procedure. These authorities are subject to a tight legal framework and belief-system that influence the distribution of competencies, rules, and processes. The FLORA system aims to bridge the gap between the fragmented IT systems of the involved authorities by sharing essential procedural updates and information between the systems. Moreover, it uses smart contracts to automatically check compliance with the standard procedure and issue warning messages when it detects deviations. The project began relatively early during the initial blockchain hype in January 2018 as an innovative flagship project of Germany's federal government and was piloted successfully in 2021. The FLORA system is currently being rolled out across several German states.

The second case investigates how the Stadtwerke Leipzig, a private German energy provider, uses blockchain to establish a customer loyalty system called NexoEnergy. The system was developed for customers with Green Electricity Tariffs (GET). GET customers tend to have strong belief systems and often distrust their energy utilities due to fears of 'greenwashing'. The NexoEnergy system addresses these concerns by tracking the share of renewable energy in the grid and rewarding customers with 'green' loyalty tokens on a blockchain. Customers can freely control these tokens to invest into green generation facilities of the Stadwerke Leipzig, reduce their energy bill, or have them redeemed for cash. The NexoEnergy project started in December 2018 and made the step to productive use in February 2020. It is currently being rolled out across different other energy providers.

Data collection

For our case study, we collected three types of data: interviews, participant observations, and documentation (Yin, 2017). In line with our interpretivist stance, interviews and participant observations represented our primary data source, whereas documentation helped us triangulate when we iterated between data and theory. We summarize these sources in Table 1.

Case	Number of interviews	Participant Observation	Project Documentation
FLORA	45	3-4 days per week from Jan 2018 to May 2020 2-3 days per week from Jun 2020 to Sep 2022	750+ pages
NexoEnergy	21	4 days per week from Dec 2018 to Dec 2020 1 day per week from Jan 2021 to Dec 2021 1 day per month from Jan 2022 to Sep 2022	250+ pages

Table 1. Overview of collected data sources

For each of the cases, we conducted interviews at different points during the project to trace the adoption process. The initial purpose of these interviews was to examine factors for successful blockchain adoption. But - as it happens often in qualitative research (Graebner et al., 2012) – cultural fit emerged as a dominant theme over the course of our study, refocusing our data collection and analysis. Cultural fit had been an important theme in both projects early on. However, its significance only became evident to us when cultural issues appeared consistently in a large round of interviews with members of the FLORA project during the second half of 2020. When we compared these findings to the NexoEnergy project, we found that cultural issues were equally prominent. This insight drove a redesign of our study and we began to concentrate on cultural fit. For the FLORA project, we included more explicit questions on cultural fit as we accompanied the roll-out of the FLORA system until September 2022. In the NexoEnergy case, we collected a second set of interviews in April and May 2022 with an explicit focus on cultural fit.

Our informants were either directly involved with the projects or closely connected to them. Table 2 presents an overview of those interviews that held statements related to issues of cultural fit on which we could build our analysis. We group these interviews based on an Schein's (1996) classification of culture types in organizations. Specifically, we interviewed organizational leaders, project managers, and their support ('executives'); IT managers, developers, and IT consultants ('engineers'), and business staff and consultants ('operators'). Table 2 provides a classification of our interviews across these types.

	Number of interviews		
Case	**Organizational leaders, project managers, and their support**	**IT managers, developers, and IT consultants**	**Business staff and business consultants**
FLORA	6	11	28
NexoEnergy	8	6	7

Table 2. Classification of interview partners

We adopted a semi-structured design with an interview guide to ensure broad coverage of our focal phenomenon (Yin, 2017). We conducted each interview with one or two interviewers, took notes, and audio recorded what was discussed. We subsequently transcribed our audio recordings for further analysis and reference. The interviews lasted between thirty minutes and one hour. We used a semi-structured protocol to encourage interviewee engagement and elicit stories about the two cases. We began each interview with an introduction by the interviewer(s) and an explanation of the interview context. In a second part, we asked interviewees to briefly discuss their relevant backstory and current organizational position. Next, we fostered rapport by encouraging interviewees to talk about their involvement in the case context and their experiences with the respective blockchain system. To reduce dissonance, we mirrored the tone and vocabulary of our interviewees and allowed them to take the conversation in any direction that they chose. In several cases, we contacted the interviewee again after the interview to clarify open questions and fill blank spots.

We built our interviews with the 'executives' and 'engineers' groups around how they (intend to) use blockchain, how it affects performance, and how blockchain fits into the project's organizational context. Moreover, we asked about challenges with its implementation and how they were resolved. Lastly, we left room for interviewees to offer their opinion on the necessity of using blockchain over other technologies. In our interviews with 'operators', we focused on expected benefits from the systems and their perspective on using blockchain in these systems.

To complement our interview data set, we sat in a vast range of project meetings, such as strategic meetings, conceptual workshops, and bi- or tri-weekly developer meetings. In the FLORA case, the second author was additionally tasked with advising the conceptualization of the system and an evaluation of the FLORA pilot system and its later roll out. In the NexoEnergy case, the third author similarly advised conceptualization and accompanied verification of the system with test customers.

To enable triangulation, we added various project documents to our evidence base, such as project presentations, conceptual documents, and marketing material. Given that we had access to almost all project documents, we selected only those documents that held explicit statements related to cultural issues.

Data analysis

The focal units of our analysis were the narratives woven around the blockchain systems and the adopting organizations' culture. More specifically, we examined how the values attributed to blockchain and those of the recipient cultural context evolved over the course of the two projects. We chose to focus on values in line with other studies on the effect of cultural context, given their easier observability than basic assumptions or artifacts (Alavi et al., 2005; Koch et al., 2013; Leidner & Kayworth, 2006).

We began our analysis with a review of (industry) reports, white papers, and academic literature on the use of blockchain in the two case contexts. This review was based on a two-step coding process (Corbin & Strauss, 1990) and produced overall 5800 codes that helped us identify common narratives in each of the fashion (sub-)markets.

We then analyzed each of the cases individually. For this analysis, the first author of this work sat down with each of the involved authors and analyzed the interview transcripts and project documents following a two-stage coding process in line with Corbin and Strauss' (1990) recommendations for grounded theory building. We coded openly and focused on early theme discovery in the initial stage. We then continued with a first round of axial coding, exploring relevant constructs, relationships, and theoretical explanations.

The involved authors would complement the open and axial coding with insights from their participant observations. We recorded emerging themes and theoretical elements in memos and organized our around 7000 codes in data trees. To support coding and manage data volume, we used the MAXQDA software toolkit.

The case-specific analysis allowed us to understand how blockchain was used in each project and how cultural fit evolved in each case. The FLORA project was strongly concerned with aligning its blockchain system with the federal organizing structure of Germany's asylum procedure. The NexoEnergy project, in turn, focused on rebuilding customer trust, reducing distrust, and eliminating ambivalence. Moreover, both cases turned out to be serendipitous for our analysis, as we could observe substantial adaptations of common blockchain narratives and the IT system in the FLORA project and clear signs of cultural transformation for the Stadwerke Leipzig in response to the NexoEnergy project.

We then moved to cross-case analysis. For this purpose, the three authors involved in the individual case analysis first sat down and discussed insights from each case. Armed with these cross-case insights, the two coding teams then did a second axial coding and alignment round. During this phase, we began to iterate between theory and data to fine-tune construct definitions, clarify relationships between constructs, and sharpen theoretical explanations (Eisenhardt, 1989, 2021; Eisenhardt & Graebner, 2007). In the last step, we applied selective coding to "construct and fill the storyline around the core phenomenon" (Corbin & Strauss, 1990). We again iterated between data and theory to establish differences and similarities of our emerging theoretical model with existing literature on fashionable IT and cultural fit.

The cross-case analysis sharpened our understanding of different ways cultural fit could evolve for fashionable IT. We found that the FLORA project established cultural fit mainly by fitting its blockchain system and the attached narratives to its organizational culture. In the NexoEnergy project, we could observe the opposite. We also found marked differences in pivotal values. For instance, trust was a secondary concern in the FLORA case but played a very important role for the NexoEnergy project. Yet, there were also similarities in values. For instance, transparency was a very important value in both projects.

Emergent Theoretical Model

We now turn to the theoretical model that emerged during our analysis and describe the role of cultural fit during the observed adoption processes. We found that both projects went through a process of cultural sensemaking. Moreover, both struggled with cultural dissonance and iteratively worked on establishing cultural fit. This cultural dissonance reduction process went both ways. In an iterative *adaptation* process, the blockchain systems and the narratives surrounding them were fitted to organizational values. In a second *transformation* process, organizational values were edited to match those values in the narratives surrounding the blockchain systems.

Adaptation of narratives and systems

A recurring pattern throughout the two cases was that the blockchain systems and the narratives surrounding them were matched to organizational values (Table 3). In the FLORA case, this *adaptation of the fashionable IT system and narratives* was the dominant dissonance reduction process. In the NexoEnergy case, they were dominated by cultural changes but still apparent.

FLORA. The German asylum procedure is replete with federal values that regularly complicate the adoption of new IT systems. The FLORA project team thus decided to develop the FLORA system in a way that supported federal organizing principles. Moreover, it dropped certain narratives and reframed others to fit these federal values. Specifically, it wove 'federalism' narratives around the FLORA system that emphasized blockchain's ability to support federal values, organizing structures and processes. Narratives that could not be reconciled with this federalism perspective were discarded.

A core blockchain narrative that the FLORA project team chose to discard was the 'distrust mediation' narrative. This narrative is rooted in the common fashion narrative that blockchain systems can digitize processes that have so far resisted the introduction of alternative IT systems due to concerns about sharing sensitive data and mutual distrust. Authorities involved in the Germany asylum procedure, on the other hand, are required by law to cooperate and share information. Moreover, they are connected by a strong network of trustful ties. Framing blockchain as an ideal technology for 'low-trust' environments was thus unwelcome and discarded accordingly. A quote by one of FLORA's project managers illustrates:

"Blockchain offers a technological solution to create trust where trust does not exist or no longer exists at a sufficient level to drive interactions or even data exchange. What's my point? Well, I have a hard time with the argument that we need blockchain to instill trust within public administration. I, indeed, reject this argument."

A related narrative that underwent substantial reframing and re-implementation was one that we term 'automated validation'. In many blockchain systems. smart contracts are used to verify the validity of a transaction. In a cryptocurrency network, this could be that a transaction was signed by the holder of a certain balance and that the transaction does not exceed this balance. The FLORA system also makes use of smart contracts to check compliance with the default procedure. However, numerous constellations exists where a digression from the default procedure is justified. Moreover, organizational culture in most of the authorities involved in the asylum procedure emphasizes employee empowerment. Accordingly, the FLORA system was relegated to a support application that could return warning messages but not reject digressions from the default procedure. As one of FLORA's project managers explains:

"It is important that blockchain is flexible. Sure, smart contracts and automated process steps are helpful and even warning messages for digressions from the regular procedure. But in the end, it is vital that the employee, the user, still has the decision-making authority. They may be warned if they deviate in any way from the standard process, but ultimately, they still have the power to decide or the decision-making authority of how they want to proceed."

Other narratives were partly reframed and re-implemented. A representative example is the 'transparency' narrative. Many blockchain systems are hyped as establishing transparency as the blockchain is replicated on several nodes in a blockchain network. Transparency is also an essential value for the authorities involved in Germany's asylum procedure. However, it is narrowly bounded by legal limits and data minimization requirements. Thus, the FLORA team was open to maintaining transparency but in a 'selective' way. In the words of one of FLORA's developers:

"Blockchain enables to work transparently, to disclose everything as is relevant for the users. At the same time, [...] blockchain enables to work together, to share the data that should be shared, while making sure that data can only be viewed by who is authorized, responsible and involved."

A narrative that was kept and implemented mostly unchanged was the 'decentralization' narrative. Blockchain is typically marketed as a technological means to establish or maintain decentralized structures. For asylum management in Germany, centralized IT systems are often undesirable as their introduction and modification may require changes to the federal separation of competencies. Moreover, they often lead to unbalanced data control arrangements and fall short in supporting local differences and particularities. Accordingly, the project team began to strongly emphasize the FLORA system's ability to mediate these concerns. A quote by one of FLORA's project managers illustrates:

"Blockchain offers the possibility to map regional differences, leaves enough room for flexibility and still allows for standardization. Thus, the technology strengthens local autonomy, preserves federal structures, and even strengthens the latter. People retain their responsibility and, using this solution, also take on joint responsibility for the task."

NexoEnergy. Energy providers are inherently concerned with ensuring reliable supply. These concerns often limit the adoption of new IT systems until they have undergone various testing and certification cycles. Moreover, new IT systems are typically designed to support the existing regulatory framework with its centralized structure, roles, and responsibilities. As such, blockchain's 'disintermediation' narrative was not welcome to the NexoEnergy team. This narrative originated from the area of cryptocurrencies and decentralized finance and presents blockchain as a technical means to eliminate banks and other intermediaries in traditional financial systems. For NexoEnergy's purposes, this narrative was not helpful as the blockchain system was not meant to disintermediate the energy provider but mediate a trustful relationship with its customers. Accordingly, the narrative was dropped. In the words of the Stadtwerke's lead blockchain developer:

"One of the [Stadwerke's] main competitive advantages is that they are [a] local [company] and that they are reliable in supplying electricity. [...] The Stadtwerke Leipzig are perceived as a trusted electricity

supplier. While NexoEnergy can certainly encourage behavioral changes, customers still see added value in the fact that electricity is being delivered by the Stadtwerke in a dependable manner.“

A narrative that was kept and implemented in an adapted way was the ‘transparency’ narrative. Green Electricity Tariffs had been a bone of contention for the Stadtwerke Leipzig over several years. GET customers had felt irritated when their aggregated electricity demand was covered by so-called green electricity certificates. These certificates offer proof that a certain amount of green electricity has been fed into the grid. However, these certificates do not proof that this occurred when GET customers consumed electricity. The NexoEnergy team took up these concerns and used blockchain to transparently track when green supply coincided with customer demand. One of the Stadtwerke’s software developers and the NexoEnergy product owner explain:

"Customers today are much more interested in data transparency. It is a competitive advantage for energy providers to use NexoEnergy to make transparent where electricity comes from and what ‘color’ it has."

“NexoEnergy was the answer to one of the biggest challenges that [the] Stadtwerke Leipzig have, which is how to engage with customers to reduce churn rates. So, the biggest value-added was to use [fashionable] IT to bind customers. We used blockchain to track changes in user behavior [towards more green electricity consumption] and level up the engagement by increasing data transparency.”

Summary. In both cases, the adopting organizations engaged not just blockchain as a technology but also the narratives woven around it. They tried to align these narratives and the values attributed to blockchain with their organizational values. The FLORA project became particularly active in this regard once the project team had recognized that promoting blockchain as an ‘enabler of federalism’ earned the FLORA system considerable traction both internally and with partner authorities. The NexoEnergy project, in turn, focused on dropping narratives that were hard to reconcile with basic assumptions and values in the electric power industry.

Case	**Blockchain narratives in the fashion market**	**Adaptation of blockchain narratives and systems**	**Pivotal value**
FLORA	Distrust mediation: Blockchain can mediate distrust in low trust environments	Dropped: Authorities involved in the German asylum procedure trust each other	Trust
	Automated validation: Blockchain enables automated data validation	Reframed and reimplemented: The FLORA system supports employees with automated checks and warning messages	Empowerment
	Transparency: Blockchain supports data sharing and transparency	Reframed and reimplemented: The FLORA system supports controlled data sharing and ‘selective’ transparency	Transparency
	Decentralization: Blockchain enables decentralized structures and processes	Reframed and reimplemented: The FLORA system enables authorities involved in the German asylum procedure to use a shared system and avoid the shortcomings of centralized systems	Separation of competencies
NexoEnergy	Disintermediation: Blockchain allows to replace intermediaries	Dropped: Most actors in electric power systems have well-defined roles and responsibilities, and their replacement may threaten system stability	Reliability
	Transparency:	Reframed and reimplemented:	Transparency

	Blockchain supports data sharing and transparency	The NexoEnergy system supports controlled data sharing and 'selective' transparency	

Table 3. Observed adaptation of blockchain narratives and systems (selection)

Transformation of organizational culture

In both the FLORA and NexoEnergy case, we could observe not just an adaptation of the blockchain systems and narratives woven around them but also a transformation of certain local and overarching organizational values (Table 4). This transformation process was less pronounced in the FLORA project but dominant in the NexoEnergy project.

FLORA. Although the adaptation process strongly dominated in the FLORA case, we could also identify changes to beliefs over the course of the project. One such change was the increased emphasis on 'cooperation'. While cooperation between authorities plays an important role for the German asylum procedure, it often follows rigid structures that can limit adaptive and joint innovation. The FLORA project helped to recast these structures and engage in local innovation efforts between offices of the federal government and competent state authorities. Several project members traced this increased readiness to collaborate directly to 'cooperation' narratives that surround blockchain. One quote by a manager at one of FLORA's partner authorities illustrates:

"Blockchain is exactly what we need to enable digital collaboration between the federal government and the states. That's when you can see that a technology has an overall impact and doesn't just mediate between two units, two groups, or two departments."

NexoEnergy. In the NexoEnergy case, cultural transformation processes dominated the adaptation of the blockchain system and the narratives woven around it. Cooperation was again a pivotal value, but cultural changes went further. More specifically, the Stadwerke Leipzig re-thought its approaches to customer loyalty, IT projects, and IT infrastructure, and transferred several values embedded in blockchain narratives to its organizational culture.

'Cooperation' was strengthened especially between the business and the IT department. Although these departments had cooperated on projects in the past, their cooperation had followed rigid structures that defined departments as clearly separated units that communicated according to well-defined rules. The NexoEnergy project, however, required more flexible structures and rules. For instance, flexibility was important to reach a common understanding of blockchain and how it could be used to facilitate customer loyalty. Moreover, agile development was instrumental in aligning customer needs with the perspectives of the business and IT departments. Several of the involved project members pinned this increased readiness to cooperate on blockchain technology and the mobilizing effect of its fashionable character. Quotes by one of the Stadtwerke's software developers and the CTO of their IT service partner illustrate:

"Each department was initially afraid of the unknown technology. However, by creating a joint understanding of the technology, the fear was quickly reduced, and agile collaboration was established. The departments entered into a constructive dialog in which problems could be named more precisely through the prior creation of a common understanding."

"The new way of cooperation between departments was quite the opposite to the existing culture at the Stadtwerke Leipzig. Traditionally, the business departments came up with an idea, created requirements and commissioned the IT department to implement them. This one-way channel was broken up by the NexoEnergy project. [....] These changes all started with Blockchain as the CIO said "Blockchain is popular, let´s find a use case for it at the Stadtwerke Leipzig."

Besides cooperation, the NexoEnergy project also effected the inclusion of 'customer agency' in its organizational beliefs. In the past, the Stadtwerke had focused on developing products and services that required little customer agency and that shielded customers from complexity. The NexoEnergy project, however, showed that customers were interested in more responsibility and more complex products. For instance, the test customers requested a wallet for their loyalty tokens that only they could access even if this meant that the tokens would be lost if they forgot their log-in credentials. Moreover, they asked for more control over their token transactions, even though the purchase and sale of tokens can be complex.

These requests led the Stadtwerke Leipzig to re-think its approach to product and service design: customers should be given more responsibility and more complex products. This belief in customer agency persisted after the introduction of NexoEnergy and many project members attributed it to discussions about blockchain and the innovativeness it embodied. In the words of a developer and the CTO of the Stadtwerke's IT service partner:

"NexoEnergy changed the [Stadtwerke's] approach to customer management from [offering] standard electricity tariffs to offering a real product with a compelling story. With NexoEnergy, the Stadtwerke enabled their customers to interact with their source of electricity. [...] NexoEnergy is the first product of the Stadtwerke that really made customers aware of their electricity: it really loaded electricity with emotions. NexoEnergy is more like a lifestyle choice than an electricity product and has a high level of customer engagement."

"First of all, NexoEnergy is a whole new product with a significantly higher level of complexity for the customer. It is thus also very new in terms of communication. Why? New technologies are used that need to be explained to customers. [...] This higher level of complexity was not only understood by the customers. The project also showed that by sending price signals at times of green electricity surplus, it was possible to create a completely different, more partnership-based relationship [with customers]."

A third transformation occurred in relation to 'control'. More specifically, the NexoEnergy project led the Stadtwerke Leipzig to re-think its approach to data control. Before the project, data control was understood in a narrow physical sense – all data had to be stored on company premises. NexoEnergy broadened the conceptualization of control. Blockchain networks typically replicate data on several blockchain nodes, which complicates data control in the narrow physical sense. At the same time, private blockchains allow a high degree of non-physical control through hard-coded rules for read and write access. The realization that data control was possible even when deployed on third party IT infrastructure, was instrumental in developing a cloud strategy and establishing readiness to cooperate with cloud service providers. Several decision-makers at the Stadtwerke re-traced the origins of these changes to the NexoEnergy project and discussions about blockchain. The CIO of the Stadtwerke Leipzig explains:

"NexoEnergy has clearly brought about a rethinking of our data silos. Where in 2018 everyone was still storing and hoarding data [in their own silos], in 2022 we are now using cloud infrastructures and systems-of-systems approaches. This [change] was necessary and important because the data volume of [our] municipal utilities is already no longer manageable and this type of infrastructure [...] is thus indispensable."

A fourth transformation was related to the product and service development process. Before, products and services were matched to requirements of the business department, which in turn were based on market research. The NexoEnergy project, in turn, introduced a community approach that involved customers, external partners, researchers, and freelancers in the product and service development process. This approach was adapted from blockchain's 'community' narrative. Many blockchain projects are developed by heterogenous groups with a strong community mindset. These groups combine different perspectives to develop blockchain frameworks and systems that meet both technical and social, 'community acceptance' criteria. Although the adoption of this community approach turned out to be more time-consuming than in previous projects, it increased customer acceptance substantially and it was retained in subsequent projects. In the words of the COO of the Stadtwerke's IT service partner and the NexoEnergy Product Owner:

"By involving customer groups in product development at an early stage, it was possible to determine very quickly how the product works and what problems arise in everyday use. Furthermore, the feedback loops allowed us to quickly determine the level of complexity customers can be expected to accept, which in turn had a positive effect on customer acceptance. [Our] customers' level of trust also grew as they realized 'I'm working on something bigger for my city here.' This led to a significant change in the [Stadtwerke's] product development process. [...] The exchange and handling of information over the product development process has improved thanks to NexoEnergy."

"The cooperation between [various] different stakeholders such as developers, universities, and early customers in NexoEnergy changed the product development for the better as the exchange of information from different perspectives was possible and needed."

Summary. In both cases, the adopting organizations transformed their organizational culture based on values embedded in the narratives surrounding blockchain technology. The FLORA project was especially successful in encouraging more local cooperation. The NexoEnergy project, in turn, effected local and overarching changes organizational values. These changes were triggered when the project team realized that blockchain narratives had a high degree of cultural dissonance with its organizational culture yet held desirable values that could be transplanted to its organizational culture. Blockchain's fashionable character was an important enabler because it increased readiness to innovate and reconsider existing structures and practices.

Case	**Blockchain narratives in the fashion market**	**Transformation of organizational culture**	**Pivotal value**
FLORA	Cooperation: Blockchain enables cooperation between participants of a blockchain network	Emphasized: The FLORA project strengthened local readiness to cooperate and innovate across organizational boundaries	Cooperation
NexoEnergy	Cooperation: Blockchain enables cooperation between participants of a blockchain network	Emphasized: The NexoEnergy project strengthened readiness to cooperate across departmental boundaries	Cooperation
	Participant agency: Blockchain enables read and write access without the need for a 3rd party	Recast: The NexoEnergy project encouraged the emphasis of customer agency in the design of new products and services	Empowerment
	Data sovereignty: Blockchain networks replicate data on several nodes, but private networks enable strict rules for read and write access.	Recast: The NexoEnergy project encouraged a non-physical conceptualization of data control and paved the way for an off-premise cloud strategy	Control
	Community: Blockchain networks are developed and maintained according to community principles	Recast: The NexoEnergy project introduced and popularized a community approach to product and service development	Involvement
	Cooperation: Blockchain enables cooperation between participants of a blockchain network	Emphasized: The FLORA project strengthened local readiness to cooperate and innovate across organizational boundaries	Cooperation

Table 4. Observed transformation of organizational culture (selection)

Discussion

We began our study with the observation that the literature on (fashionable) management practices emphasizes cultural fit as an important factor for adoption (Ansari et al., 2010; Canato et al., 2013; Piazza & Abrahamson, 2020; van Grinsven et al., 2016). However, the literature on fashionable IT remains silent on this type of fit - even though organizational values can be important determinants of IT adoption (Alavi et al., 2005; Koch et al., 2013; Leidner & Kayworth, 2006).

By studying two blockchain projects, we provide corroborative evidence that cultural sensemaking and dissonance reduction can indeed play an important role in the adoption of fashionable IT. Moreover, we develop a tentative process model that explains how cultural fit can be promoted through a two-way process of cultural dissonance reduction between fashionable IT and organizational culture.

The importance of cultural fit for the adoption of fashionable IT

We contribute to the literature on fashionable IT by adding cultural fit as a third dimension relevant for successful adoption. Prior research on fashionable IT has already identified the importance of legitimacy and performance considerations as well as political and technical fit (Wang, 2010). What is missing is an in-depth analysis of cultural fit as suggested in the literature on (fashionable) management practices (Ansari et al., 2010; Canato et al., 2013; Piazza & Abrahamson, 2020). Our analysis corroborates the existence and relevance of this fit for fashionable IT.

Secondly, we offer empirical support for the existence and resolution of what Leidner & Kayworth (2006) proposed as cultural dissonance or 'system conflict'. The reasoning behind this conflict is that technologies can be embedded or attributed with values and that these values can conflict with organizational culture, which complicates adoption. We offer support for this notion of conflict in fashionable IT adoption, highlighting how the fashion market attributes various values to fashionable IT, which then require cultural sensemaking and dissonance reduction by adopting organizations. What is more, we find strong evidence that the dissonance reduction process can play out both ways. Organization culture can adapt fashionable IT systems and the narratives woven around them (Alavi et al., 2005; Kappos & Rivard, 2008; Leidner & Kayworth, 2006). In turn, values embodied in fashionable IT narratives can 'reorient' organizational values (Kappos & Rivard, 2008; Koch et al., 2013; Leidner & Kayworth, 2006). An interesting implication of our work - albeit one that our evidence remains inconclusive on - is that fashionable IT may require more cultural sensemaking and dissonance reduction than conventional IT.

Thirdly, we broaden the discussion of what makes innovation with fashionable IT different from innovation with non-fashionable IT. One core characteristic of IT is its 're-programmability' which enables generativity and interpretative variability (Gal et al., 2022; Yoo et al., 2010, 2012). Interpretative variability is especially high when IT has a highly nonmaterial character (Gal et al., 2022). Fashionable IT may thus be different from non-fashionable IT not just because it affords legitimacy but also because the narratives surrounding it are nonmaterial and offer high degrees of interpretative flexibility.

A tentative model of cultural sensemaking and dissonance reduction for fashionable IT

Our core contribution is a tentative theoretical model of 'cultural sensemaking' (Gioia & Chittipeddi, 1991; Su, 2015) and dissonance reduction for fashionable IT. Our model (Figure 1) builds on theories of cultural fit in the (fashionable) management practice literature (Ansari et al., 2010; Canato et al., 2013; Piazza & Abrahamson, 2020) as well as related theories on cultural conflict in organizational IT adoption (Alavi et al., 2005; Kappos & Rivard, 2008; Koch et al., 2013; Leidner & Kayworth, 2006). The theory of cultural fit describes the alignment of management practices with the organizational values of the recipient organization (Ansari et al., 2010; Canato et al., 2013; Piazza & Abrahamson, 2020). Cultural conflicts in organizational IT adoption result from diverging values embedded or attributed to technology and those of the recipient context. Our framework combines these two theoretical perspectives and makes them available for the study of fashionable IT.

Our emergent theoretical model argues that cultural conflict can be created and mediated through the narratives surrounding fashionable IT. More specifically, our framework suggests that these narratives facilitate attributing values to fashionable IT. However, this interpretative viability (Ansari et al., 2010) also means that adopting organizations will face narratives woven around values that digital fashion setters and other adopting organizations have attributed to fashionable IT.

These values may not match those of the adopting organization and require actions that reduce cultural dissonance. This sensemaking and dissonance reduction process is iterative and can occur both ways. Fashionable IT systems and the narratives surrounding them can be adapted to fit organizational culture. Organizational values, in turn, can be transformed to capitalize on values embodied in digital fashion narratives. These changes to organizational culture may be local or overarching (Alavi et al., 2005; Kappos & Rivard, 2008).

Successful cultural sensemaking and dissonance reduction can earn fashionable IT projects considerable momentum and effect cultural changes that would not be possible with non-fashionable IT. However, the process can be complex when the 'fashion market' has attributed values that conflict with the culture of the recipient organization. While organizations can choose to drop or reframe these values in the narratives surrounding the fashionable IT, their adaptation may lead to a loss of the "collective belief, that an information technology is new, efficient, and at the forefront of practice" (Wang, 2010). So, while the long-term goal of adopting fashionable IT may be performance gains and institutionalization, caution is required in the short term to avoid losing the perception of conformance with norms of rationality and progress. Certain fashionable IT projects may require multiple smaller sensemaking and dissonance reduction cycles to balance legitimacy and performance considerations.

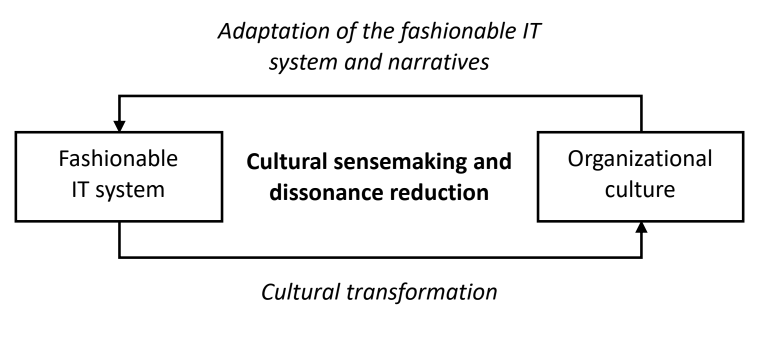

Adaptation of the fashionable IT system and narratives
Fashionable IT system
Cultural sensemaking and dissonance reduction
Organizational culture
Cultural transformation

Figure 1. A tentative model of cultural sensemaking and dissonance reduction for fashionable IT

Practical Implications

Our findings suggest that organizational leaders interested in associating with fashionable IT would do well to not just focus on hyping their investments and projects with the hottest IT and fitting it to their organization's existing IT systems. They should be equally concerned with the cultural aspect of these investments and projects. More specifically, organizational leaders should develop a sense of the values associated with the fashionable IT they want to invest in. They should then evaluate these values for their fit with those of their organizations and work on adjusting the fashionable IT and the narratives surrounding it, and sometimes their organizational values to make such cultural fit apparent. If such a fit is not given, they will risk that their organizations will have a hard time adopting the fashionable IT and moving from proofs-of-concept to productive systems that offer performance gains.

Establishing cultural fit may also be something fashion setters like consultants can and should support only to a certain degree. Instead, projects with fashionable IT may require 'cultural entrepreneurship' from both organizational leaders and members of the adopting organization. Conveniently, management and IS research already offer insights into how cultural fit can be created (Alavi et al., 2005; Canato et al., 2013; Koch et al., 2013; Leidner & Kayworth, 2006).

However, this is not to say that IS researchers do not have a role to play – on the contrary. IS researchers, especially those with a deep understanding of cultural theories, are well-positioned to guide the fashion adoption process. They can do more than just shape the fashion-setting process or offer post-hoc critique (Baskerville & Myers, 2009).

Boundary conditions

Boundary conditions are important for all research, especially theories built from cases (Eisenhardt, 2021). One such condition is establishing the valence of cultural fit compared to political and technical fit. Our framework demonstrates the existence of and importance of cultural fit for the adoption of fashionable IT, but it does not support any statements on its relative valence. Moreover, our framework remains silent on the importance of cultural fit in contexts with a higher or lesser emphasis on values, norms, and belief systems.

Another boundary condition is the existence of 'interpretative viability' of a fashionable IT and the narratives surrounding it, and the ability of recipient organizations to use this viability. Ansari et al. (2010), for instance, argue that earlier adopters of a fashionable management practice may have more leeway in establishing cultural fit than later adopters who feel more conformity pressures. Given the limited scope of our study, our evidence naturally stays silent if such an observation also holds true for fashionable IT.

A third potential boundary condition is the generalizability of our findings to IT that is non-fashionable. Since narratives and IT culture conflicts are not limited to fashionable IT, the core ideas of our framework might also hold for non-fashionable IT. In other words, cultural sensemaking and dissonance reduction may be an important process to explicate values "assumed in the work behaviors that the IT is designed to enable" (Leidner & Kayworth, 2006) and support the adoption of new technologies in organizational contexts.

The last boundary condition arises from whether fashionable management practices and fashionable IT are separate phenomena. This question builds on the observation that many management practices are supported by IT, which affords these practices a certain degree of materiality. Many fashionable information technologies, in turn, support changes in management practices, which blurs the line between management practice and IT (Wang, 2010). While this argument may be legitimate, our two cases provide strong reason to believe it does not hold in all cases. Neither the FLORA project nor the NexoEnergy project were concerned with re-organizing administrative procedures. Accordingly, we believe that fashionable IT is a separate phenomenon requiring independent investigation and theories.

Conclusion

In this study, we investigate the role of cultural fit for the successful adoption of fashionable IT. Based on insights from two blockchain projects, we derive a tentative theoretical model that explains the establishment of cultural fit between fashionable IT and adopting organizations. We find that this fit can be established through a process of cultural sensemaking and dissonance reduction. Dissonance reduction occurs iteratively and reduces the cultural distance between organizational values and the values attributed to the fashionable IT.

Naturally, our study is not free from limitations. For instance, two cases may be too limited to cover all aspects of the phenomenon in question. We have thus started to collect evidence on a third case that will examine the use of the European Union's European Blockchain Services Infrastructure (EBSI) in the context of digital diploma management. Tentative evidence from this investigation corroborates both the adaptation and transformation processes. Another limit may originate from the selection of our cases. We had opted to focus on blockchain technology which is typically replete with value-laden narratives. Moreover, both examined contexts are characterized by strong values and belief systems. While this does not mean that cultural fit may be irrelevant for other fashionable technologies and contexts, their effect may be less pronounced.

Lastly, our model is still tentative. It only unpacks the ‘sensemaking’ part of the process and does not yet cover the proceeding process of ‘cultural sensegiving’ by the fashion market and the subsequent process of ‘giving back sense to the market’. In the proceeding process, the fashionable IT is attributed with values outside of the adopting organization’s control. These ‘diffuse cultural loadings’ complicate cultural sensegiving by organization leaders as well as sensemaking by organizational members. In the subsequent process, informational engagement with the fashionable IT can shape the discourse in the fashion market. Moreover, our model does not yet fully unpack the interplay of material and discursive changes.

Acknowledgements

This work was supported by PayPal and the Luxembourg National Research Fund FNR (P17/IS/13342933/PayPal-FNR/Chair in DFS/Gilbert Fridgen). Moreover, we would like to acknowledge the support of the European Union (EU) within its Horizon 2020 programme, project MDOT (Medical Device Obligations Taskforce), Grant agreement 814654.

References

Abrahamson, E. (1991). Managerial fads and fashions: The diffusion and rejection of innovations. *Academy of Management Review*, *16*(3), 586–612. https://doi.org/10.1177/135050840181001

Abrahamson, E. (1996). Management fashion. *Academy of Management Review*, *21*(1), 254–285. https://doi.org/10.5465/amr.1996.9602161572

Abrahamson, E., & Fairchild, G. (1999). Management fashion: Lifecycles, triggers, and collective learning processes. *Administrative Science Quarterly*, *44*(4), 708–740. https://doi.org/10.2307/2667053

Alavi, M., Kayworth, T. R., & Leidner, D. E. (2005). An empirical examination of the influence of organizational culture on knowledge management practices. *Journal of Management Information Systems*, *22*(3), 191–224. https://doi.org/10.2753/MIS0742-1222220307

Ansari, S. M., Fiss, P. C., & Zajac, E. J. (2010). Made to fit: How practices vary as they diffuse. *Academy of Management Review*, *35*(1), 67–92. https://doi.org/10.5465/amr.35.1.zok67

Baskerville, R. L., & Myers, M. D. (2009). Fashion waves in information systems research and practice. *Mis Quarterly*, 647–662. https://doi.org/10.2307/20650319

Beck, R., Müller-Bloch, C., & King, J. L. (2018). Governance in the blockchain economy: A framework and research agenda. *Journal of the Association for Information Systems*, *19*(10), 1. https://aisel.aisnet.org/jais/vol19/iss10/1

Canato, A., Ravasi, D., & Phillips, N. (2013). Coerced Practice Implementation in Cases of Low Cultural Fit: Cultural Change and Practice Adaptation During the Implementation of Six Sigma at 3M. *Academy of Management Journal*, *56*(6), 1724–1753. https://doi.org/10.5465/amj.2011.0093

Corbin, J. M., & Strauss, A. (1990). Grounded theory research: Procedures, canons, and evaluative criteria. *Qualitative Sociology*, *13*(1), 3–21. https://doi.org/10.1007/BF00988593

Eisenhardt, K. M. (1989). Building Theories from Case Study Research. *Academy of Management Review*, *14*(4), 532–550. https://doi.org/10.2307/258557

Eisenhardt, K. M. (2021). What is the Eisenhardt Method, really? *Strategic Organization*, *19*(1), 147–160. https://doi.org/10.1177/1476127020982866

Eisenhardt, K. M., & Graebner, M. E. (2007). Theory Building From Cases: Opportunities And Challenges. *Academy of Management Journal*, *50*(1), 25–32. https://doi.org/10.5465/amj.2007.24160888

Gal, U., Berente, N., & Chasin, F. (2022). *Technology Lifecycles and Digital Technologies: Patterns of Discourse across Levels of Materiality*. https://doi.org/10.17705/1jais.00761

Gioia, D. A., & Chittipeddi, K. (1991). Sensemaking and sensegiving in strategic change initiation. *Strategic Management Journal*, *12*(6), 433–448. https://doi.org/10.1002/smj.4250120604

Graebner, M. E., Martin, J. A., & Roundy, P. T. (2012). Qualitative data: Cooking without a recipe. *Strategic Organization*, *10*(3), 276–284. https://doi.org/10.1177/1476127012452821

Jensen, T., Hedman, J., & Henningsson, S. (2019). How tradelens delivers business value with blockchain technology. *MIS Quarterly Executive*, *18*(4). https://aisel.aisnet.org/misqe/vol18/iss4/5

Kappos, A., & Rivard, S. (2008). A three-perspective model of culture, information systems, and their development and use. *MIS Quarterly*, *32*(3), 601–634.

Koch, H., Leidner, D. E., & Gonzalez, E. S. (2013). Digitally enabling social networks: Resolving IT–culture conflict. *Information Systems Journal*, *23*(6), 501–523. https://doi.org/10.1111/isj.12020

Lacity, M. C. (2022). Blockchain: From Bitcoin to the Internet of Value and beyond. *Journal of Information Technology*, 02683962221086300. https://doi.org/10.1177/02683962221086300

Leidner, D. E., & Kayworth, T. (2006). Review: A Review of Culture in Information Systems Research: Toward a Theory of Information Technology Culture Conflict. *MIS Quarterly*, *30*(2), 357–399. https://doi.org/10.2307/25148735

Litan, A. (2022). *Gartner Hype Cycle for Blockchain and Web3, 2022*. https://blogs.gartner.com/avivah-litan/2022/07/22/gartner-hype-cycle-for-blockchain-and-web3-2022/

Mattke, J., Hund, A., Maier, C., & Weitzel, T. (2019). How an Enterprise Blockchain Application in the US Pharmaceuticals Supply Chain is Saving Lives. *MIS Quarterly Executive*, *18*(4). https://aisel.aisnet.org/misqe/vol18/iss4/6

Piazza, A., & Abrahamson, E. (2020). Fads and fashions in management practices: Taking stock and looking forward. *International Journal of Management Reviews*, *22*(3), 264–286. https://doi.org/10.1111/ijmr.12225

Rieger, A., Lockl, J., Urbach, N., Guggenmos, F., & Fridgen, G. (2019). Building a blockchain application that complies with the EU General Data Protection Regulation. *MIS Quarterly Executive*, *18*(4).

https://doi.org/10.17705/2msqe.00020

Rieger, A., Roth, T., Sedlmeir, J., & Fridgen, G. (2021). The privacy challenge in the race for digital vaccination certificates. *Med*, *2*(6), 633–634. https://doi.org/10.1016/j.medj.2021.04.018

Rieger, A., Roth, T., Sedlmeir, J., & Fridgen, G. (2022). We need a broader debate on the sustainability of blockchain. *Joule*, *6*(6), 1137–1141. https://doi.org/10.1016/j.joule.2022.04.013

Rieger, A., Roth, T., Sedlmeir, J., Weigl, L., & Fridgen, G. (2022). Not yet another digital identity. *Nature Human Behaviour*, *6*(1), 3–3. https://doi.org/10.1038/s41562-021-01243-0

Rossi, M., Mueller-Bloch, C., Thatcher, J. B., & Beck, R. (2019). Blockchain research in information systems: Current trends and an inclusive future research agenda. *Journal of the Association for Information Systems*, *20*(9), 14. https://doi.org/10.17705/1jais.00571

Roth, T., Stohr, A., Amend, J., Fridgen, G., & Rieger, A. (2022). Blockchain as a driving force for federalism: A theory of cross-organizational task-technology fit. *International Journal of Information Management*, 102476. https://doi.org/10.1016/j.ijinfomgt.2022.102476

Roth, T., Utz, M., Baumgarte, F., Rieger, A., Sedlmeir, J., & Strüker, J. (2022). Electricity powered by blockchain: A review with a European perspective. *Applied Energy*, *325*, 119799. https://doi.org/10.1016/j.apenergy.2022.119799

Sarker, S., Henningsson, S., Jensen, T., & Hedman, J. (2021). The use of blockchain as a resource for combating corruption in global shipping: An interpretive case study. *Journal of Management Information Systems*, *38*(2), 338–373. https://doi.org/10.1080/07421222.2021.1912919

Schein, E. H. (1996). Culture: The Missing Concept in Organization Studies. *Administrative Science Quarterly*, *41*(2), 229–240. https://doi.org/10.2307/2393715

Schein, E. H. (2016). *Organizational culture and leadership* (5th ed.). John Wiley & Sons.

Sedlmeir, J., Smethurst, R., Rieger, A., & Fridgen, G. (2021). Digital identities and verifiable credentials. *Business & Information Systems Engineering*, *63*(5), 603–613. https://doi.org/10.1007/s12599-021-00722-y

Strang, D., & Kim, Y.-M. (2006). The Diffusion and Domestication of Managerial Innovations: The spread of scientific management, quality circles, and TQM between the United States and Japan. In *The Oxford handbook of work and organization* (pp. 177–199). Oxford University Press.

Su, N. (2015). Cultural sensemaking in offshore information technology service suppliers. *Mis Quarterly*, *39*(4), 959–984.

Utz, M., Johanning, S., Roth, T., Bruckner, T., & Strüker, J. (2022). From ambivalence to trust: Using blockchain in customer loyalty programs. *International Journal of Information Management*, 102496. https://doi.org/10.1016/j.ijinfomgt.2022.102496

van Grinsven, M., Heusinkveld, S., & Cornelissen, J. (2016). Translating management concepts: Towards a typology of alternative approaches. *International Journal of Management Reviews*, *18*(3), 271–289.

Wang, P. (2010). Chasing the hottest IT: Effects of information technology fashion on organizations. *MIS Quarterly*, 63–85. https://doi.org/10.2307/20721415

Wang, P., & Ramiller, N. C. (2009). Community learning in information technology innovation. *MIS Quarterly*, 709–734. https://doi.org/10.2307/20650324

Yin, R. K. (2017). *Case study research: Design and methods* (6th ed.). SAGE Publications, Inc.

Yoo, Y., Boland Jr, R. J., Lyytinen, K., & Majchrzak, A. (2012). Organizing for innovation in the digitized world. *Organization Science*, *23*(5), 1398–1408.

Yoo, Y., Henfridsson, O., & Lyytinen, K. (2010). Research Commentary—The New Organizing Logic of Digital Innovation: An Agenda for Information Systems Research. *Information Systems Journal*, *21*(4), 724–735. https://doi.org/10.1287/isre.1100.0322

Zilber, T. B. (2006). The Work of the Symbolic in Institutional Processes: Translations of Rational Myths in Israeli High Tech. *Academy of Management Journal*, *49*(2), 281–303. https://doi.org/10.5465/amj.2006.20786073

Ziolkowski, R., Miscione, G., & Schwabe, G. (2020). Decision problems in blockchain governance: Old wine in new bottles or walking in someone else's shoes? *Journal of Management Information Systems*, *37*(2), 316–348. https://doi.org/10.1080/07421222.2020.1759974

RP13: Roth, T., Rieger, A., Fridgen, G., & Young, A. (2023). **How IS Affect Social Justice Tensions: A Case Study of Asylum Management.** In B. Shishkov (Ed.), *Business Modeling and Software Design (pp. 268–277)*. Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-36757-1_18

How is Affect Social Justice Tensions: A Case Study of Asylum Management

Tamara Roth[1,2](✉), Alexander Rieger[1], Gilbert Fridgen[1], and Amber Young[2]

[1] Interdisciplinary Centre for Security, Reliability, and Trust at the University of Luxembourg, Kirchberg, Luxembourg
{tamara.roth,alexander.rieger,gilbert.fridgen}@uni.lu, tr036@uark.edu

[2] Sam M. Walton College of Business at the University of Arkansas, Fayetteville, USA
ayoung@walton.uark.edu

Abstract. Asylum management is rife with questions surrounding social justice. The use of information systems in this context is often complex and fosters social injustices instead of promoting social justice. The reason for this complexity may be the result of conflicting conceptualizations of social justice. By conducting an inductive and embedded single-case study of one blockchain systems for asylum management, we find that such conflicts can occur across and within the individual, group, and supra-group levels, and result in tensions. These tensions can be addressed through the implementation of information systems in four ways: reinforcement, stabilization, mediation, and resolution. This dynamic negotiation through information systems may prevent the materialization of one specific social justice conceptualization and distributes the quest for social justice across multiple levels.

1 Introduction

In 2015, refugees fleeing war and terrorism in their home countries poured into Germany and surrounding countries [1, 2]. As more than a million new asylum applications came in, Germany struggled to coordinate the asylum procedure in a socially just but efficient manner. Paperwork was lost, processes were delayed, and life-altering mistakes were made as Excel spreadsheets were passed back and forth across and within government agencies inside of and beyond state borders [2]. In addition to the coordination challenges, competing interests and conflicting conceptualizations of justice across stakeholders and levels of organizing proved difficult to manage. Government representatives were interested balancing the rights of refugees and concerns of German citizens [3]. German states were interested in distributing the responsibility such that each state contributed equitably [4]. Refugees were interested in transparency and equal opportunities [5]. The European Union aimed to redistribute responsibilities to not overburden single nations and improve opportunities for asylum seekers [3].

Difficulties in aligning these various goals, in addition to the large number of incoming asylum seekers, created a strong need for more efficient, secure, and just handling of asylum procedures. This need extended to how the involved authorities managed

B. Shishkov (Ed.): BMSD 2023, LNBIP 483, pp. 268–277, 2023.
https://doi.org/10.1007/978-3-031-36757-1_18

their internal processes and how they coordinated work across organizational boundaries [2]. In a first step, Germany's Federal Government modernized and expanded its IT infrastructure to allow for full digitalization of its processes and effective handling and coordination of an increasing number of applications [18, 19]. These investments increased information availability and helped the Federal Government develop its internal processes. Yet, coordinating with state authorities proved more difficult to digitalize. In particular, the creation of a joint IT system for cross-organizational process coordination was complicated by the federal separation of competencies. To mediate these challenges, the federal and state governments began to investigate a blockchain system that could reflect the organizing principles of federal procedures [19]. In late 2021, the rollout of the national FLORA system across Germany began.

While any blockchain system in a federally structured environment provides opportunity to observe the struggle for a dominant social justice conceptualization [6], asylum management, which is replete with cross-organizational procedures, provides opportunity for particularly rich insights. Procedures in asylum management often reach across national borders [5] challenging traditional conceptualizations of distributive social justice. These are typically bounded within a society, i.e., nation-states that share a cultural identity and political ideology, and possess the relevant structures to enforce social justice rules [7, 8]. To understand social justice in an asylum management context, a broader perspective is needed, one that includes more universal conceptualizations of social justice, such as egalitarian social justice or – to redress injustices – elements of commutative social justice. Employing a theory-building approach, we investigate the following research questions:

How does strategic use of information systems to negotiate concurrent but divergent conceptualizations of social justice shape social justice outcomes?

To build our theory, we conduct a single-case study [9] of the FLORA system and the subprojects that surrounded its development. Our investigation reveals how tensions emerge from different social justice conceptualizations at the individual, group, and supra-group levels of organizing. Information systems can be implemented strategically to influence these tensions in four different ways: they can exacerbate (reinforcement strategy), maintain (stabilization strategy), reduce (mediation strategy), and eliminate (resolution strategy) tensions. When tensions occur at levels of organizing with asymmetric resources, resources can be leveraged to increase the chances of success and, ultimately, which social justice conceptualization will dominate.

The rest of the paper is organized as follows. The next section provides an overview of the research on social justice and IT. Next, we present details of our case study design, data collection, and data analysis. We then present the theoretical framework that emerged from our analysis of the case. The paper concludes with a summary of key insights from our analysis and an outlook on future research.

2 Theoretical Background

The search for a uniform conceptualization of justice has a longstanding tradition. First approaches date back to Aristotle and Plato, and even old religious texts, such as the Talmud and the Bible, elaborate on problems of just distribution of resources [7, 8]. This most fundamental type of justice, termed distributive justice, attempts to find answers to the question of "how a society or group should allocate its scarce resources or products among individuals with competing needs or claims" [10]. While this question is still a key issue in contemporary theories of justice, the specific term "social justice" entered political discourse only after the advent of socialist movements and the industrial revolution, which brought about substantial socioeconomic changes [7, 8]. As a rather young concept tied to socioeconomic development, social justice received particular attention in the early years of the 20th century. Principles resulting from these modern debates—such as need, merit, and equality—are still central to theorizing about social justice today [8].

An exemplary context for the visibility of social justice challenges at different levels of social organizing is asylum. While the reasons for asylum typically extend beyond national borders, the social justice negotiations that surround it occur within the boundaries of host nations [11]. To understand social justice in an asylum management context, a broader perspective is needed, beyond distributive social justice, such as egalitarian social justice or – to redress injustices – elements of commutative social justice [7]. In line with distributive social justice conceptualizations [7], nations first aim to ensure the well-being and safety of their own citizens [12]. This becomes particularly visible in the various containment and immigration policies, which distinguish legal from illegal or unwanted migration. Such distinction puts most asylum seekers outside of the national community of their host country and promotes a citizen–noncitizen relationship [11]. A lack of ties to the national community and being regarded as an outsider may not only affect asylum seekers' well-being, but also raises social justice concerns. Despite a potential outsider perspective, a basic level of justice is ensured by mandates of procedural social justice, i.e., due process and transparent as well as verifiable and lawful processes [8].

A yet-understudied possibility to foster and improve on social justice at different levels of social organizing is the use of information systems. More specifically, many new technologies have emerged in recent years that may possess characteristics that can help improve social justice. One such development, which has been hyped by libertarians for its high degree of decentralization and redistribution of digital power to the individual, is blockchain technology. Blockchains are databases that store transactions in a distributed network [13, 14]. Consisting of a chronologically ordered chain of blocks, blockchains provide a high degree of tamper resistance and transparency. More specifically, each new block references information from its predecessor, making retrospective changes to the order of blocks easy to detect. The comparatively quick detection of fraudulent behavior and the high degree of transparency is often perceived to contribute to an equal distribution of power and information among involved actors. This perceived democratization of information and power—although blockchains may also be designed in a way that they allow for a certain degree of inequality, for instance, regarding the availability of sensitive information [15, 19] – may add to social justice at all levels.

While social justice plays a major role at the individual level, where individuals measure the degree of equity by comparing themselves with a referent, equality perceptions may also play an important role at the group and supra-group levels [12].

3 Research Method

As theorizing on the effects of information systems on social justice negotiations is limited, we chose a theory-building case study approach. Case studies allow for an "in-depth" investigation of a socially embedded phenomenon and can support the emergence of new theory [9, 17]. Case study research is particularly fruitful for investigating an under-explored phenomenon or an "under-represented perspective in a well-researched literature" [16]. As social justice negotiations are often multifaceted and highly context-specific [7, 8, 12], we opted against a multiple-case design. Instead, we built our investigation around a comprehensive case that would foster depth and richness [3, 9]. This reasoning led us to select the FLORA project, a revelatory and longitudinal case that balances depth and breadth and allows for cross-synthesis [9].

3.1 Case Description

We study the FLORA project, which is developing a blockchain-based system for the exchange of process information between German authorities involved in German and European asylum procedures. To address the coordination and justice challenges introduced by the wave of refugees in 2015, the federal and some state governments began to invest heavily into new IT systems. However, these efforts were often limited by the bureaucratic structure of Germany's asylum procedure. The procedure's completion requires close collaboration and information exchange between various authorities at the local, state, and federal levels.

The federal government has thus explored 'decentralized' technical alternatives that can accommodate the bureaucratic nature of the asylum procedure and are compatible with government IT systems. As part of this exploration, the federal government developed a blockchain enabled system for the exchange of important process information between federal and cooperating state governments. The government also partnered with academe and contracted, among others, the second and fourth author of this study to ensure the design of the system was appropriate and promoted justice for stakeholders at multiple levels of organizing. The system started as a proof-of-concept (PoC) in January 2018, was subsequently piloted in the German state of Saxony, and has been rolled out across other German states in a step-by-step manner since the end of 2021. In 2020, it also motivated the European Blockchain Partnership (EBP) to establish a working group headed by Germany and France that will extend the European Blockchain Service Infrastructure (EBSI) to support the transfer of refugees between European member states.

3.2 Data Collection

Our inductive analysis draws on 45 semi-structured interviews with partners directly and indirectly involved with the FLORA project as well as 20 semi-structured interviews with asylum applicants and support organizations. These were conducted using an interview guide which helped to ensure comprehensive coverage of the subject area [3, 9]. The protocol of our semi-structured interviews involved a brief introduction followed by questions on interviewees' perceptions of social justice tensions, and on the opportunities, challenges, and success factors for the blockchain project. During the interviews, we adapted the questions to shift the focus depending on the respective interviewee's knowledge and interactions with the system [3, 9]. We mirrored the interviewees' verbal posture and vocabulary and allowed the interviewees to go in directions that they found interesting [9]. In selecting our interviewees, we focused on incorporating a broad variety of perspectives. That is, we selected interviewees with technical expertise and in-depth knowledge of the asylum procedure. Likewise, we included the perspectives of governmental employees, external consultants and IT service providers, refugees, and refugee support organizations. Our interviews lasted between 30 and 60 min, were audio-recorded and, afterward, fully transcribed. To increase construct validity, we also obtained interviewees' feedback on the draft case study reports.

We also draw from a comprehensive database of historical project information to triangulate our findings. We analyzed over 400 pages of documentation on the collaboration software Confluence and over 200 pages of technical concepts and functional specifications. Moreover, we gathered field observations from bi-weekly sprint reviews and management meetings, as well as over 50 project workshops with different departments, authorities, and organizations.

We used qualitative analysis techniques and the analysis software MAXQDA to analyze our data. We undertook three stages of data analysis: open, axial, and selective coding [16]. The codes were either based on our theoretical lens (deductive coding) or emerged during data collection (inductive coding) [17].

4 Preliminary Findings

Reinforcement occurred where the FLORA systems were strategically used to impose higher-level conceptualizations of social justice at the expense of lower-level ones. In these instances, the systems contributed to the amplification of social justice tensions. The reinforcement effect was prominent between the group and the individual levels. In the national procedure, Germany's asylum laws emphasize equitable distribution of refugees across German states in line with federal and state quota systems. These quota systems are based on tax revenue and population numbers, and typically support supra-group- and group-level conceptualizations of social justice. Consequently, many refugees fear that the strategic use of the FLORA system to enforce quotas disadvantages them. For instance, some believe that rural areas offer fewer opportunities to demonstrate their readiness to integrate, such as internships and vocational trainings. One refugee explains this "fair-procedure" tension between the group and individual levels:

> "*The law says that you cannot work somewhere else from where you live. The law also says that you cannot move to another municipality. At the same time, they require you to get […] an internship to show your willingness to integrate. […] This puts me in a position where I cannot move forward and show my willingness to integrate.*"

The national FLORA system exacerbates this 'fair procedure' tension by enforcing a federal and state conceptualization of quotas as a means to social justice. Federal and state representatives strategically implemented FLORA to better manage "hand-overs" in case the quota systems demand relocation. FLORA also helps federal and state representatives identify refugees who have gone missing during hand-overs.

Stabilization was possible where the two FLORA systems facilitated a compromise. These compromises helped stabilize existing tensions and prevented their further exacerbation. A particular prominent stabilization example is information access. The General Data Protection Regulation and other pertinent laws grant refugees the right to know how their personal information is processed. Yet, refugees or their lawyers must direct a formal request to the competent authorities before such information is disclosed. Authorities are cautious about these requests, as some refugees use this information to anticipate repatriation or transfer actions and "disappear." A quote by one refugee assistant illustrates this 'information access' tension:

> *"Quicker and less error-prone processes would, of course, also lead to quicker repatriations. It would only increase the value for asylum seekers who are rightfully in this country. You cannot have a solution that benefits everyone. [...] But it could well be that asylum seekers who learn in advance of a pending repatriation simply go underground for a while."*

FLORA has an ambiguous effect in this regard. On one hand, it increases the level of detail of the available information that refugees can request. Moreover, refugees can petition more authorities for information because the systems ensure consistent sharing of process information between all authorities involved in a refugee's asylum procedure. Yet, FLORA does not change the status quo in that this information is shared with refugees only reactively, and refugees still need to petition involved authorities for disclosure of the processed information. A quote by one of the government officials working with FLORA illustrates:

> *I don't think that FLORA makes much of a difference regarding our work with asylum seekers. [...] Status updates and appointments are still issued over the provincial headquarters [...] and refugee asylum seekers have to ask for this information, [...] especially their status. [It's more] the internal way of dealing with their applications instead of or rather in addition of the lists."*

In some instances, the FLORA systems could be strategically implemented in ways that aligned social-justice conceptualizations and reduced tensions. ***Mediation*** effects were especially apparent for FLORA at the group and individual levels. One prominent example for mediation between the group and individual levels was faster, more secure procedures. Before the introduction of the national FLORA system, process information was often exchanged using e-mails and Excel files, and sometimes fax messages and phone calls. These communication channels were slow and prone to errors, as they involved many manual steps, such as copying data from and into the Excel files. Slow and faulty procedures not only place undue mental strain on refugees and workers, but also could lead to grave errors, such as unlawful repatriations. One of our FLORA project managers explains this "lawfulness of the procedure" tension:

> *"Above all, asylum applications should not only be processed efficiently, but efficiently and correctly. At that time, there was the scandal in Bremen—let's call it 'scandal' because it was one—where wrongful asylum decisions were made and people [were] deported who should have been allowed to stay. At that point, there was agreement that we need a more transparent solution, to avoid similar mistakes in the future."*

The introduction of the national FLORA system perceptibly improved the exchange of process information. Waiting times between process steps were reduced by almost half and Excel files were retired. Moreover, the system decreased the risk of procedural errors and unlawful actions. These changes were positively received by the involved authorities, as well as many refugee assistants and refugees.

Finally, the FLORA systems were strategically implemented to settle social-justice tensions. We found evidence for these **resolution** effects across the supra-group and group levels, as well as between different conceptualizations at the group level. A prominent resolution effect occurred in relation to the federal nature of Germany's asylum procedure. This nature means that the overall procedure is standardized, but that many authorities with regional differences are involved. Federal organizing principles empower regional branches of the federal government and their partner authorities at the state and municipal levels to foster social justice locally. Yet, they also complicate standardization efforts at the federal level, as well as the introduction of shared IT systems that would make the procedure more just globally. One of FLORAs project managers explains this "separation of competencies" tension between the supra-group and group levels:

> *"We have tasks at the federal level. We have tasks at the state level, the municipal level, and all kinds of areas where not everyone is always allowed to see everything. That's why many processes are not so well connected. Everyone has their own responsibilities."*

The national FLORA system was strategically implemented to successfully resolve this tension. It standardizes the exchange of process information and encourages the use of a single IT system. At the same time, it permits regional branches and their partner authorities to maintain their regional subprocesses. This perception that the FLORA system could be used as an enabler of federalism is an essential motivator for state governments to adopt the system.

> *"Blockchain offers the possibility to map regional differences, leaves enough room for flexibility, and still allows for standardization. Thus, the technology strengthens local autonomy, preserves federal structures, and even strengthens the latter. People retain their responsibility and, using [the FLORA system], also take on joint responsibility for the task."*

Resources played an important role in determining how the FLORA systems were strategically implemented to address social justice tensions. We found that the systems tended to be implemented in ways that strategically advantaged those with greater resources. This pattern was observed across levels. Because the EU, federal, and state authorities control the FLORA systems, they were often implemented in a way that privileged higher-level conceptualizations of social justice. Yet, strategic use of the FLORA systems for mediation was more common when procedural errors and resulting injustices at the individual-level warranted action, and when states and municipalities with diverging resources quarreled about just distribution.

5 Discussion

We contribute to the literature on social justice by unpacking how social justice negotiations can be complicated by conceptual differences. These negotiations typically occur at three conceptual levels: individual, group, and supra-group. At the individual level it is about being materially right in finding a just solution for the individual cases. For the group level, solutions that collectively do justice to the social groups involved ensure being materially right on the aggregate level. The supra-group level mandates the upholding of rules to be formally right. While the literature on social justice already indirectly distinguishes between these levels [7, 8] our case study allows us to directly observe their distinctness and arising tensions. As observed tensions between the levels show, social justice negotiations cannot be simplified by providing a common definition; it is paramount to account for their messiness by allowing for their coexistence, even if the hierarchical model complicates negotiations that span cultural and group boundaries. More specifically, the negotiation of different social justice conceptualizations may deliver more socially just outcomes than the enforcement of one universal definition (Fig. 1).

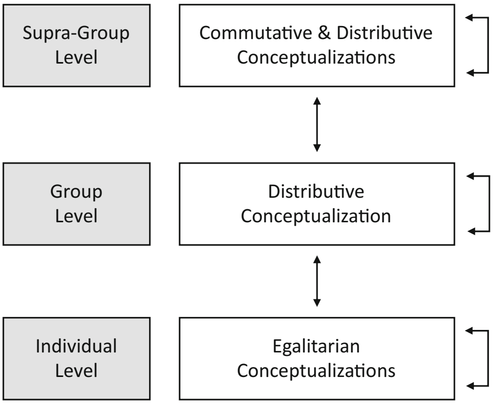

Supra-Group Level
Commutative & Distributive Conceptualizations
Group Level
Distributive Conceptualization
Individual Level
Egalitarian Conceptualizations

Fig. 1. Emergence of social justice tensions from different conceptualizations

This research contributes also to the IS literature by describing four ways information systems can be implemented to shape negotiations of meaning around social justice (Fig. 2). We term the first strategy reinforcement. When an information system is implemented to impose a particular conceptualization, the effect is amplified tensions. The second strategy, which we call stabilization, facilitates compromise and maintenance of the status quo and helps to avoid exacerbation of existing tensions. The third strategy, mediation, aligns different social justice conceptualizations and aims to reduce tensions. Finally, information systems can be strategically implemented toward resolution, or to settle social justice tensions.

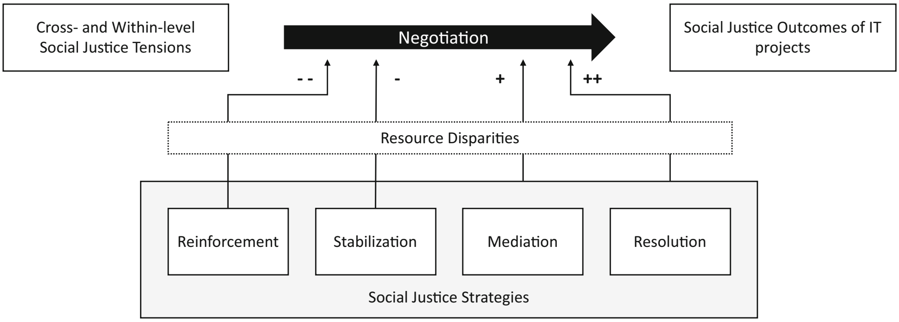

Cross- and Within-level Social Justice Tensions
Negotiation
Social Justice Outcomes of IT projects
- -
-
+
++
Resource Disparities
Reinforcement
Stabilization
Mediation
Resolution
Social Justice Strategies

Fig. 2. Social Justice Strategies for IT projects

Information systems can be powerful tools for the negotiation of social justice. When they are used judiciously, they do not limit the complexity of these negotiations. Instead, they support navigation through the plethora of tensions that define social justice negotiations. Some of these tensions can be resolved, others mediated or stabilized. At still other times, a reinforcement strategy may be adopted to promote a higher-level social justice objective. In such cases, the risk of unjustly favoring dominant conceptualizations of social justice is high. Reinforcement strategies reduce complexity, which can lead to performance gains and facilitate a straighter course. Yet, such an approach may oversimplify social justice in an unjust manner.

6 Conclusion

Information systems can be strategically implemented to promote social justice in the face of societal challenges, such as the ongoing global refugee crisis [1]. Yet, conflicting social justice conceptualizations can make it difficult to promote social justice through information systems. Through an embedded case study of a blockchain system for asylum management, we find that such conflicts can at the individual, group, and supra-group levels, and lead to social justice tensions. Information systems can be strategically implemented in four ways to address these tensions: reinforcement, stabilization, mediation, and resolution. The effectiveness of each of these strategies depends on the extent to which negotiating parties leverage financial and technical resources to champion their conceptualization of social justice.

Acknowledgements. This research was funded in part by: the Luxembourg National Research Fund (FNR) grant reference 14783405; FNR and PayPal, PEARL grant reference 13342933/Gilbert Fridgen; and the European Union (EU) within its Horizon 2020 programme, project MDOT (Medical Device Obligations Taskforce) grant agreement 814654. For the purpose

References

1. AbuJarour, S., et al.: ICT-enabled refugee integration: A research agenda. Commun. AIS, **44**(1), 874–891 (2019). https://doi.org/10.17705/1CAIS.04440
2. Dittmer, C., Lorenz, D.F.: Disaster situation and humanitarian emergency – in-between responses to the refugee crisis in Germany. Int. Migr. **59**(3), 96–112 (2021). https://doi.org/10.1111/imig.12679
3. Aligica, P.D., Savidge, T.: The European Migrant Crisis: a case study in failure of governmental and supra-governmental responses. In: Haeffele, S., Storr, V.H. (eds.) Government Responses to Crisis. Mercatus Studies in Political and Social Economy, pp. 129–141. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-39309-0_8
4. Ericson, R.E., Zeager, L.A.: Coordination and fair division in refugee responsibility sharing. J. Conflict Resolution **66**, 00220027221080985 (2019). https://doi.org/10.1177/00220027221080985
5. Andrade, A.D., Doolin, B.: Information and communication technology and the social inclusion of refugees. MIS Q. **40**(2), 405–416 (2016)
6. Moreau, M.-A.: Labour relations and the concept of Social Justice in the European Union. In: Micklitz, H.-W. (ed.) The Many Concepts of Social Justice in European Private Law. Edward Elgar Publishing (2011). https://doi.org/10.4337/9780857935892.00024
7. Jackson, B.: The conceptual history of social justice. Political Stud. Rev. **3**(3), 356–373 (2005). https://doi.org/10.1111/j.1478-9299.2005.00028.x
8. Miller, D.: Principles of social justice. Harvard University Press (1999)
9. Yin, R.K.: Case study research: design and methods (6th ed.) SAGE Publications, Inc. (2017)
10. Roemer, J.E.: Theories of distributive justice. Harvard University Press (1996)
11. Pisani, M.: 'Illegal bodies' on the move: a critical look at forced migration towards social justice for young asylum seekers. In: Council of Europe (ed.), Healthy Europe: Confidence and uncertainty for young people in contemporary Europe, pp. 83–98 (2016)
12. Pogge, T.W.: An egalitarian law of peoples. Philos. Public Aff. **23**(3), 195–224 (1994). https://doi.org/10.1111/j.1088-4963.1994.tb00011.x
13. Beck, R., Müller-Bloch, C., King, J.L.: Governance in the blockchain economy: a framework and research agenda. J. Assoc. Inf. Syst. **19**(10), 1 (2018). https://aisel.aisnet.org/jais/vol19/iss10/1
14. Chanson, M., Bogner, A., Bilgeri, D., Fleisch, E., Wortmann, F.: Blockchain for the IoT: privacy-preserving protection of sensor data. J. Assoc. Inf. Syst. **20**(9), 1274–1309 (2019). https://doi.org/10.17705/1jais.00567
15. Lumineau, F., Wang, W., Schilke, O.: Blockchain governance—a new way of organizing collaborations? Organ. Sci. **32**(2), 500–521 (2021). https://doi.org/10.1287/orsc.2020.1379
16. Eisenhardt, K.M.: What is the Eisenhardt Method, really? Strateg. Organ. **19**(1), 147–160 (2021). https://doi.org/10.1177/1476127020982866
17. Corbin, J.M., Strauss, A.: Grounded theory research: Procedures, canons, and evaluative criteria. Qualitat. Sociol. **13**(1), 3–21 (1990).https://doi.org/10.1007/BF00988593

RP14: Hartwich, E., Roth, T., Rieger, A., Zavolokina, L., & Fridgen, G. (2024). **Negotiation and Translation Between Discursive Fields: A Study of the Diffusion of Decentralized Finance.** *ECIS 2024 Proceedings.*

Conference Ranking: 3 (GGS Class); B (GGS Rating)

How Organizations Sustain and Navigate Between (De)centralization Equilibria: A Process Model

Completed Research Paper

Eduard Hartwich
SnT-Interdisciplinary Centre for Security, Reliability and Trust,
University of Luxembourg,
Luxembourg, Luxembourg
eduard.hartwich@uni.lu

Alexandra Hoess
SnT-Interdisciplinary Centre for Security, Reliability and Trust,
University of Luxembourg,
Luxembourg, Luxembourg
alexandra.hoess@uni.lu

Alexander Rieger
SnT-Interdisciplinary Centre for Security, Reliability and Trust,
University of Luxembourg,
Luxembourg, Luxembourg
alexander.rieger@uni.lu

Tamara Roth
Sam M. Walton College of Business,
University of Arkansas,
Fayetteville, Arkansas, United States
tr036@uark.edu

Gilbert Fridgen
SnT-Interdisciplinary Centre for Security, Reliability and Trust,
University of Luxembourg,
Luxembourg, Luxembourg
gilbert.fridgen@uni.lu

Amber Grace Young
Sam M. Walton College of Business,
University of Arkansas,
Fayetteville, Arkansas, United States
AYoung@walton.uark.edu

Abstract

Finding the 'right' balance between centralization and decentralization in organizational processes, governance, and IT can be difficult. To navigate this tension field, organizations need to find (de)centralization equilibria that are often dynamic and depend on organizational strategy and context. However, little is known about how organizations should respond once an old equilibrium is punctuated or breaks down. In this paper, we thus conduct an inductive multiple-case study to investigate how organizations sustain and transition between (de)centralization equilibria. We synthesize our insights into a process model that paints the transition as an iterative recalibration process subject to centralization and decentralization tensions. Often, this process will require local and temporary compromises. Our work contributes a much-needed process perspective to the IS literature on (de)centralization.

Keywords: Centralization, Decentralization, Equilibrium, Punctuation

Introduction

*"The real trick in high reliability systems is somehow
to achieve simultaneous centralization and decentralization"* (Weick, 1987, p. 124).

The 'golden ratio' between centralization and decentralization is difficult to achieve. While centralized structures can reduce coordination costs of organizational processes and governance mechanisms, they become ineffective once organizations reach a certain size and communication complexity (Mintzberg, 1989; Rediker & Seth, 1995; Siggelkow & Levinthal, 2003). Decentralized structures, in turn, allow organizations to distribute decision-making rights and responsibilities so that 'local' opportunities and requirements can be reflected as they arise (Andersen, 2005; Kahai et al., 2003; Weick, 1987). However, decentralized structures do not come without costs either. Too much decentralization allows subunits to act opportunistically and withhold information from organizational leadership, which not only creates coordination costs (Foss et al., 2010; Grandori, 1997; Rediker & Seth, 1995; Srikanth & Puranam, 2014) but also fuels conflicts of interest (Andersen, 2005; Beck et al., 2018; Wiseman et al., 2012). Larger organizations consequently find themselves in a tension field between centralization and decentralization (Mintzberg, 1989) in which they need to develop a certain (de)centralization equilibrium (Smith & Lewis, 2011).

In today's organizations, it can be difficult to establish such 'equilibria' in organizational processes, governance, and information technology (IT) (Hanelt et al., 2021; Henderson & Venkatraman, 1999; King, 1983). Moreover, organizations are occasionally subject to punctuating events that can challenge stable, existing equilibria and require recalibration or a transition to a new equilibrium (Romanelli & Tushman, 1994; Tushman & Romanelli, 1985). However, organizations often struggle with navigating these changes once an established equilibrium is broken. In particular, there is a need for a greater understanding of how organizations can and should manage the tensions that these recalibrations and transitions bring. We thus ask the following question:

RQ: *How can organizations sustain and navigate between stable (de)centralization equilibria?*

To answer our research question, we conduct an inductive, longitudinal multiple-case study (Eisenhardt & Graebner, 2007; Yin, 2011). Our study focuses on the development and adoption of two cross-organizational IT systems that saw several transitions between centralization and decentralization. The first case revolves around the development and roll-out of Germany's Federal Blockchain Infrastructure Asylum (FLORA), which supports the coordination between the authorities involved in Germany's asylum procedure. The second case studies the development and adoption of the European Blockchain Services Infrastructure (EBSI), which supports the delivery of cross-border public services in Europe. We could gain particularly rich insights into these two cases as authors of this work have been regularly involved with the projects since 2018.

Our contributions are two-fold. First, we derive a process model for the development of stable (de)centralization equilibria, which are characterized by established activity patterns, routines and workflows (Romanelli & Tushman, 1994; Tushman & Romanelli, 1985). Specifically, our model casts the development of equilibria between centralization and decentralization in organizational processes, governance, and IT as an iterative recalibration and transition process that is triggered by punctuating events and shaped by centralization and decentralization tensions. Second, we find that organizational decision-makers can be particularly successful in this process when they allow for local and temporary differences in the degree of (de)centralization.

The rest of the paper is structured as follows. The background section synthesizes the management literature on (de)centralization, the role of IT in supporting (de)centralization equilibria, and the impact of blockchain on (de)centralization. The third section describes our two cases and our data collection and analysis. In the fourth section, we present our emerging process model. The fifth section discusses our model and three complementary conjectures before elaborating on our theoretical contributions, practical implications, and boundary conditions. Section six concludes with a summary of our key insights.

Theoretical Background

Navigating the Tension Field Between Centralization and Decentralization

When organizations start to form, they typically rely on centralized processes and governance mechanisms (Aldrich & Pfeffer, 1976; Mintzberg, 1984). In such centralized structures, decision-making authority is vested with a single entity or a small group of people that also defines and dictates these organizational processes (Ahituv et al., 1989; Mintzberg, 1989; Siggelkow & Levinthal, 2003). As the number of entities with decision-making authority is limited, centralization typically increases operational efficiency and reduces coordination costs (Aulakh & Gencturk, 2000; Mintzberg, 1989; Peppard, 2018; Rediker & Seth, 1995). However, centralization is only practical when the necessary information and competencies reside with or can be transferred to a central authority that is accepted and respected by organizational subunits and when the actions of this authority are transparent (Foss et al., 2010; Grandori, 1997; Mintzberg, 1989; Rediker & Seth, 1995; Srikanth & Puranam, 2014). Once organizations start expanding and grow beyond a certain size (Mintzberg, 1989), centralized organizing often causes overbearing communication costs or even loss of control (Smith & Lewis, 2011).

Unlike centralization, decentralization distributes decision-making authority along an organization's vertical and horizontal dimensions; it leaves decision-making to the discretion of the respective subunits (Mintzberg, 1984, 1989; Siggelkow & Levinthal, 2003). This distributed authority also allows them to define organizational processes locally, foster flexibility, and seize opportunities as they occur (Andersen, 2005; Kahai et al., 2003; Weick, 1987). But decentralized structures come with their own challenges. Organizational subunits may behave opportunistically, create information asymmetries, and are prone to conflicts of interest (Andersen, 2005; Beck et al., 2018; Wiseman et al., 2012). Decentralized structures are also disadvantageous when decentral decision-makers are "incompetent, are not appropriately held to account for their decisions or make decisions that result in problems for other organizational units or for higher management" (King, 1983, p. 321). Decentralized organizing thus typically couples the distribution of decision rights with accountabilities and incentive mechanisms to persuade their decentral subunits to act in a certain way (Moldoveanu & Martin, 2001; Weill, 2004).

What makes things complicated for many organizations is that they are neither fully centralized nor fully decentralized. Instead, they find themselves in a dynamic tension field between centralization and decentralization (Siggelkow & Levinthal, 2003; Smith & Lewis, 2011) that requires the negotiation of equilibria. In these equilibria, organizations can leverage the advantages of both structures and balance out their challenges. Once organizational decision-makers accept this equilibrium thinking, they can create flexible organizations and spur a virtuous relationship between both ends of the (de)centralization spectrum (Smith & Lewis, 2011). More specifically, successful organizational leaders "build the management of change into [their organization's] very structure" (Drucker, 1992, p. 97), allowing them to move between different degrees of centralization and decentralization (King, 1983; Siggelkow & Levinthal, 2003).

Such a level of structural malleability, for instance, can enable organizations to initially organize the processes and governance of their sub-units in a decentral manner. This allows them to quickly introduce advancements and innovation to the market and reap benefits from early-mover advantages. Once these advantages fade or are leveled by competitors, organizations often centralize these units to keep costs at bay and reintegrate them with the processes and governance mechanisms of the parent organization (Uhl-Bien & Arena, 2018). Other reasons to realign (de)centralization equilibria can come from changes in organizational management after extended periods of stability (Brown, 1997; Davis & Eisenhardt, 2011; Smith & Tushman, 2005). Whenever organizational leadership changes, the risk of opportunistic behavior in subunits needs to be re-evaluated and potentially requires recentralization as well as adjustment of organizational processes and governance. The management literature refers to such changes as punctuating events (Lyytinen & Newman, 2008; Tushman & Romanelli, 1985), which "substantively disrupt established activity patterns" (Romanelli & Tushman, 1994, p.1141). They may trigger recalibration and eventually "install the basis for new equilibrium periods" (Romanelli & Tushman, 1994, p.1141) that may provoke new challenges and opportunities (Davis & Eisenhardt, 2011).

The Role of Information Technology for (De)centralization Equilibria

Managing such punctuating events may also require adjustments to an organization's IT (Henderson & Venkatraman, 1999; Lyytinen & Newman, 2008). Many organizational leaders manage these adjustments by translating new processes and governance structures into their IT. That is, when they decide to centralize their organization's processes and governance, they also aim for more centralized (macro)structures in the organization's IT to ensure better control. Efforts to decentralize organizational processes and governance, in contrast, often result in the decentralization of IT to mirror the needs and requirements of empowered organizational subunits (Sambamurthy & Zmud, 1999).

However, aligning organizational processes, governance, and IT does not have to be unilateral. New ways of digital organizing typically work in both directions and also require aligning organizational processes and governance mechanisms to IT (Davis & Eisenhardt, 2011). Digital platform ecosystems, for instance, have developed into one of the most common ways of orchestrating different organizations in the co-creation and appropriation of joint value propositions (Constantinides et al., 2018; de Reuver et al., 2018). These ecosystems are powered by digital platforms that blur organizational and hierarchical boundaries (Hein et al., 2020; Jacobides et al., 2018). When platforms have centralized designs, they also introduce a certain degree of centralization to the processes and governance of the platform ecosystem (Hein et al., 2020; T. L. Huber et al., 2017). Other technologies for cross-organizational cooperation, such as blockchain, emphasize decentralized designs (Lacity, 2018), which promote a certain degree of decentralization on (cross-)organizational processes and governance.

These examples demonstrate that IT is not an exclusively stabilizing element in the development of (de)centralization equilibria but show that it can also enable organizations to establish new equilibria, especially in cross-organizational contexts (Zhao et al., 2020). Organizations should thus "not simply seek to identify and adopt the best available technology to restructure the organization" (Henderson & Venkatraman, 1999, p. 481); IT should rather act as a catalyst in an organization's pursuit of stable (de-)centralization equilibria. For this pursuit, organizational processes, governance, and IT need to be malleable (Hanelt et al., 2021; Henderson & Venkatraman, 1999; King, 1983; Mikalef et al., 2021). Malleability in IT is typically achieved through decomposition and modularization of IT components and the implementation of interfaces between these modules (Hanseth & Lyytinen, 2010; Mikalef et al., 2021). Malleable organizational processes are commonly ensured through exchangeable process steps (Hammer, 2014) while malleable governance is characterized by informal and relational practices within formal structures (Gubitta & Gianecchini, 2002; Lumineau et al., 2021).

The truly challenging part, however, is the use of this malleability in response to punctuating events that challenge or break current equilibria (Romanelli & Tushman, 1994). While the IS literature agrees that this response can require changes to organizational processes, governance, or IT, little guidance is available on how organizations can navigate new (de)centralization equilibria once an established equilibrium can no longer be sustained.

The Impact of Blockchain on (De)centralization

Navigating between (de)centralization equilibria is particularly demanding if the underlying IT prescribes a certain degree of (de)centralization. One such example is blockchain technology. Blockchains are decentralized and replicated databases that allow so-called blockchain nodes to directly communicate and interact without an intermediating server or third party (Halaburda, 2018; Halaburda & Mueller-Bloch, 2019; Nakamoto, 2008). They are quite flexible in the degree of decentralization they support. Private permissioned blockchains, for instance, are often less decentralized as they restrict read and write access to a set of pre-registered nodes. Public permissionless blockchains, in turn, impose neither restriction and are often highly decentralized (Beck et al., 2018).

Although blockchains stipulate a certain degree of IT decentralization, they do not necessarily lead to decentralized equilibria (Chen et al., 2021). In fact, research argues that even permissionless blockchains tend to result in rather centralized IT architectures and governance, whereas persmissioned ones may favor decentralization (Bakos et al., 2021). As such, blockchain projects are interesting examples to study how organizations can manage the resulting (de)centralization tensions, as little is known about how such structures are established and how they evolve.

Method and Case Description

To explore how organizations can sustain and navigate between (de)centralization equilibria, we conducted a multiple-case study on the introduction of two blockchain systems (Eisenhardt, 2021; Eisenhardt & Graebner, 2007; Yin, 2017). We selected the two cases for three reasons: 1) they involved the same IT, 2) they are situated in a similar public sector context, and 3) two members of our research team closely accompanied both projects as academic advisor and observer for over five years. This involvement of our team members provided us with particularly rich insights, including unique participant observations and access to relevant project documentation and interview partners. The two cases are complementary since the first case is dominated by centralization tensions, while the second case places a stronger emphasis on decentralization.

Case 1: Germany's Federal Blockchain Infrastructure Asylum (FLORA)

Our first case is the development and roll-out of the Federal Blockchain Infrastructure Asylum, a blockchain-based system that supports the efficient and secure exchange of procedural information between the authorities involved in Germany's asylum procedure. Work on FLORA started in February 2018, and the first pilot was deployed in 2021. Currently, the Federal Office and its partner authorities are rolling out FLORA across Germany's sixteen federal states. Figure 1 provides an overview of FLORA's development trajectory from January 2018 to September 2023.

The FLORA project builds upon Hyperledger Fabric, a private permissioned blockchain framework that supports private sub-chains for each federal state and location. FLORA's nodes (one node per organization) are hosted centrally by the Federal Office but partner authorities are free to host their own node if desired. Read and write access is defined based on each authority's legal responsibility.

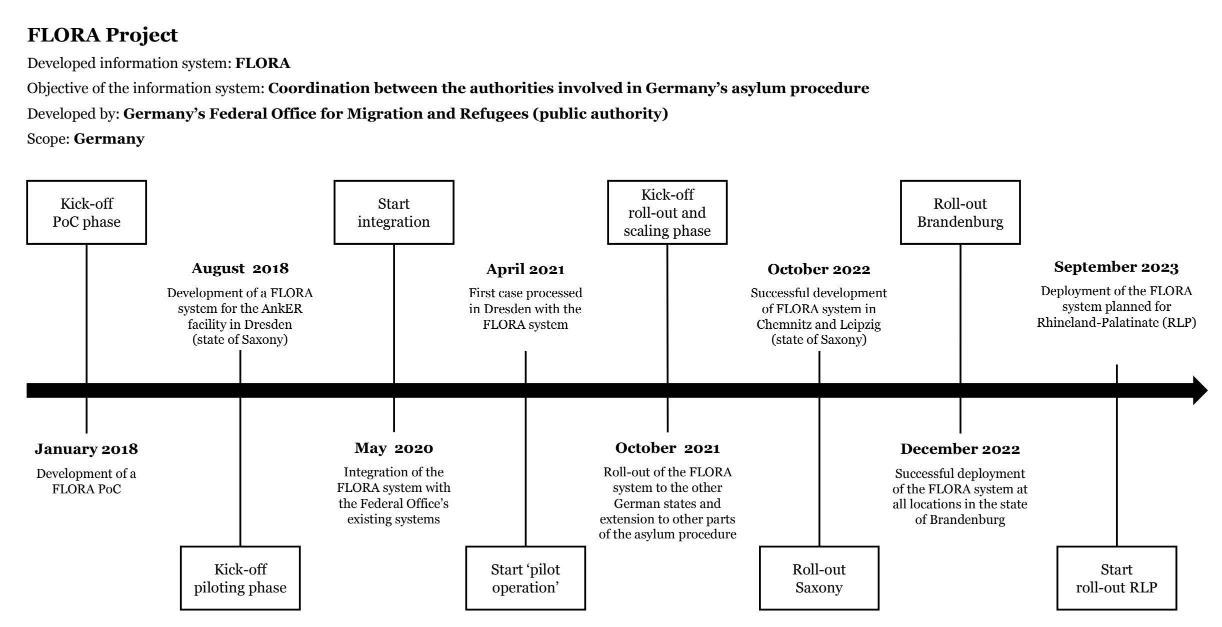

FLORA Project
Developed information system: FLORA
Objective of the information system: Coordination between the authorities involved in Germany's asylum procedure
Developed by: Germany's Federal Office for Migration and Refugees (public authority)
Scope: Germany
Kick-off PoC phase
January 2018
Development of a FLORA PoC
August 2018
Development of a FLORA system for the AnkER facility in Dresden (state of Saxony)
Kick-off piloting phase
Start integration
May 2020
Integration of the FLORA system with the Federal Office's existing systems
April 2021
First case processed in Dresden with the FLORA system
Start 'pilot operation'
Kick-off roll-out and scaling phase
October 2021
Roll-out of the FLORA system to the other German states and extension to other parts of the asylum procedure
October 2022
Successful development of FLORA system in Chemnitz and Leipzig (state of Saxony)
Roll-out Saxony
Roll-out Brandenburg
December 2022
Successful deployment of the FLORA system at all locations in the state of Brandenburg
September 2023
Deployment of the FLORA system planned for Rhineland-Palatinate (RLP)
Start roll-out RLP

Figure 1. Detail and Timeline of the FLORA Project.

Case 2: European Blockchain Services Infrastructure (EBSI)

Our second case is the European Blockchain Services Infrastructure (EBSI), a blockchain system developed and operated by the European Blockchain Partnership (EBP). The EBP was formed in April 2018 between the European Commission and the EU member states, as well as Norway and Liechtenstein with the intent to build a blockchain-based system that would support the efficient and secure delivery of cross-border public services. EBSI currently supports the authentication of digital diploma credentials, and deployment in production is scheduled for the second half of 2023. In parallel, the EBP is working on several other use cases, such as social security passports and document traceability. Figure 2 provides an overview of EBSI's development trajectory from April 2018 to September 2023.

In contrast to FLORA, EBSI is hosted decentrally across more than 20 European member states. EBSI relies on a permissioned blockchain based on Hyperledger Besu. Any organization can read data, but only a subset of pre-authorized organizations can host an EBSI node to obtain write and validation rights.

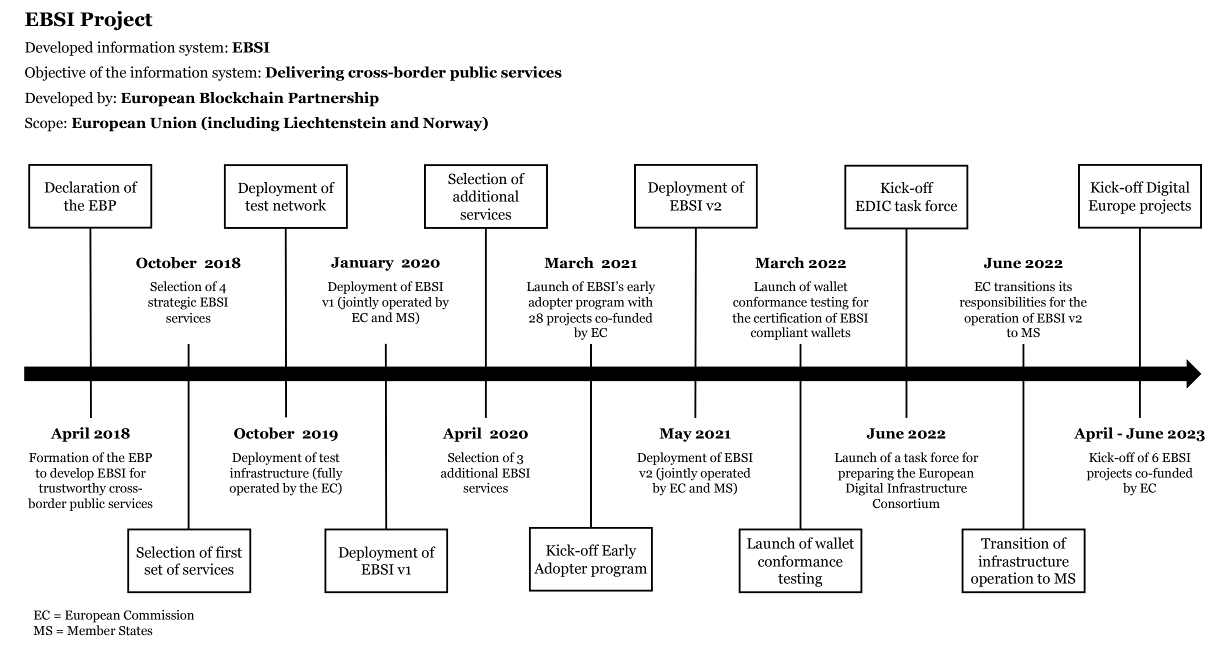

EBSI Project
Developed information system: EBSI
Objective of the information system: Delivering cross-border public services
Developed by: European Blockchain Partnership
Scope: European Union (including Liechtenstein and Norway)
Declaration of the EBP
Deployment of test network
Selection of additional services
Deployment of EBSI v2
Kick-off EDIC task force
Kick-off Digital Europe projects
October 2018
Selection of 4 strategic EBSI services
January 2020
Deployment of EBSI v1 (jointly operated by EC and MS)
March 2021
Launch of EBSI's early adopter program with 28 projects co-funded by EC
March 2022
Launch of wallet conformance testing for the certification of EBSI compliant wallets
June 2022
EC transitions its responsibilities for the operation of EBSI v2 to MS
April 2018
Formation of the EBP to develop EBSI for trustworthy cross-border public services
October 2019
Deployment of test infrastructure (fully operated by the EC)
April 2020
Selection of 3 additional EBSI services
May 2021
Deployment of EBSI v2 (jointly operated by EC and MS)
June 2022
Launch of a task force for preparing the European Digital Infrastructure Consortium
April - June 2023
Kick-off of 6 EBSI projects co-funded by EC
Selection of first set of services
Deployment of EBSI v1
Kick-off Early Adopter program
Launch of wallet conformance testing
Transition of infrastructure operation to MS
EC = European Commission
MS = Member States

Figure 2. Detail and Timeline of the EBSI Project.

Data Collection

Our first source of case evidence is semi-structured interviews. As the third author accompanied the FLORA project, he regularly conducted explorative interviews to evaluate the emerging system and identify tensions and best practices for developing blockchain projects. During these interviews, tensions between centralization and decentralization became prominent as the project advanced. When we observed similar tensions in an interview study on EBSI's development, we started to specifically explore the changes between centralization and decentralization in a focused set of interviews between March and May 2023. To select informants for the focused interviews, we followed recommendations for informant selection by Huber & Power (1985).

All interviews were conducted based on interview guides we derived from the respective literature. These were organizational (de)centralization in general (Mintzberg, 1989; Smith & Lewis, 2011; Smith & Tushman, 2005) for the explorative interviews as well as IS-specific (de)centralization (King, 1983; Sambamurthy & Zmud, 1999) for the focused interviews. We audio-recorded and transcribed the interviews using established video conferencing tools. Where interviewees did not consent to be recorded, we took extensive notes. The interviews were conducted in German or English, dependent on the language preferences of the interviewees, and lasted between 30-90 minutes. Table 1 summarizes the explorative and focused interviews on which we built our case study.

Case	Number of Interviews
FLORA	Exploratory Interviews: 15 Focused Interviews: 5
EBSI	Exploratory Interviews: 7 Focused Interviews: 6

Table 1. Interviews

We complemented these interviews with project documentation and direct observations. The third author has been an academic advisor to both the FLORA and the EBSI projects for more than five years. As part of his role in the FLORA project, he regularly participated in meetings on FLORA's technical and strategic development and observed stakeholders in their use of the emerging FLORA system. In the EBSI project, he served as a technical advisor to the EBP. As part of this role, he similarly attended regular meetings related to the technical and strategic development of EBSI. The second author additionally observed the EBSI project for two years (starting in autumn 2021) for research purposes and to inform Luxembourg's national strategy on blockchain and digital identities. She attended meetings related to EBSI's strategic and technical development and the implementation of EBSI's digital diploma use case. Their involvement gave us unique access to relevant documents (source 2) and provided rich participant observations (source 3). Table 2 summarizes these sources.

Case	Project Documentation	Direct Observations
FLORA	1000+ pages	Third author: 3-4 full days per week working on the FLORA project from Jan 2018 to May 2020 2-3 full days per week working on the FLORA project from Jun 2020 to May 2023 1-2 full days per week working on the FLORA project from Jun 2023 to Sep 2023
EBSI	1000+ pages	Second author: 2-3 days per month observing the EBP from Nov 2021 to September 2023 Third author: 2-3 days per month advising the EBP from Feb 2019 to September 2023

Table 2. Overview of Collected Project Documentation and Observations

Data Analysis

To analyze our case evidence, we followed best practices for studying multiple cases and coding qualitative data (Corbin & Strauss, 1990; Eisenhardt, 1989, 2021; Eisenhardt & Graebner, 2007). We started our analysis with a within-case analysis to see how centralization and decentralization developed in each of the two cases. Throughout this analysis, two authors openly coded the project documentation and interview transcripts to understand context factors and get a feeling for the overall case setting. In the first round of axial coding, they aggregated their open codes into higher-level categories. They frequently consulted with the whole author team to discuss their codes and triangulate their findings with the second and third author's project insights. We also used these meetings to iterate between the pertinent theories on organizational and IS (de)decentralization and our case data.

Overall, our within-case analysis revealed that the FLORA project was dominated by centralization compromises, which led to mounting tensions as the project progressed. The EBSI project, in turn, iterated between centralization and decentralization compromises, continuously demanding a recalibration of the equilibrium.

Informed by these insights, we proceeded to a cross-case analysis to compare how the two cases balanced centralization and decentralization over time. For this purpose, two authors conducted a second round of axial coding as well as one round of selective coding. During this second coding process, they again regularly met with their co-authors to discuss the codes, triangulate with the second and third authors' insights, and iterate with the pertinent theories.

Our cross-case analysis produced rich insights into the dynamic nature of (de)centralization equilibria. We found stable equilibria in both projects, i.e., periods characterized by stable activity patterns, routines, and workflows. However, punctuations through changes in organizational strategy or context disrupted these equilibria and demanded new compromises in the degree of (de)centralization that inevitably demanded both projects to establish new equilibria.

Results

Throughout our coding and discussion rounds, a story of recalibration and transition emerged. Both projects started with the vision to establish a decentralized equilibrium that would reflect the federal context of both IT systems. However, the need for quick progress required a certain degree of centralization in various stages of the projects. Some of these centralization 'compromises' needed to be revisited as the projects advanced, creating a dynamic back-and-forth and recalibration of organizational processes, governance, and IT. We now turn to how this back-and-forth played out in each of the two projects.

Navigating (De)centralization in the FLORA Project

Germany's asylum procedure requires close collaboration and information exchange between various organizations at the municipal, state, and federal levels. While the Federal Office for Migration and Refugees plays a pivotal role in issuing decisions about asylum applications, state-level migration, authorities and municipal governments are responsible for the initial registration, distribution, accommodation, care, and eventual integration or repatriation of applicants. Several security agencies conduct background checks, and various health authorities provide medical care. The involved authorities often exchange information via inefficient means such as paper lists, spreadsheets, and fax messages. However, efforts to improve this exchange have proven difficult. Since the federal separation of competencies typically prevents "digital centralization" and redistribution of competencies to a central authority, many authorities involved in the procedure prefer a "decentralized" architecture that requires neither the extension of centralized databases nor the delegation of control to a single authority. An IT service provider to the project explains:

"The decentralization of rights and responsibilities resonates well with the BAMF [...] and the foundation of federal organizing. [In the asylum procedure,] responsibilities must be clearly defined and easy to adapt to the individual cases. More specifically, responsibilities should only be with the competent local authority that is, indeed, responsible and able to assume such responsibilities. This makes the installation of a single authority that first has to delegate responsibilities very unattractive."

To address this need for decentralization, Germany's Federal Office for Migration and Refugees began to explore blockchain technology with a Proof-of-Concept (PoC) in January 2018. The idea was that blockchain could reflect the federal structure of the procedure in a cross-organizational IT architecture. Based on a positive evaluation of the PoC, the BAMF initiated a joint pilot project with Saxony's central immigration authority (LDS) in August 2018 to develop and test the FLORA system in Dresden, Saxony. This part of the project saw the establishment of an equilibrium where governance and especially strategic decision-making was shared between the Federal Office and the LDS. In the words of one of FLORA's project managers:

"We closely collaborated with the LDS from the beginning on, which has been quite special. [...] We had a lot of shared responsibilities and required frequent alignment calls. [...] Ultimately, our AnkER facility in Dresden has been selected for the pilot project [...] since we were convinced of the added value of the FLORA project and all groups, offices, and authorities [within the AnkER facility] saw their visions aligned with the goals of FLORA."

Additionally, the Federal Office envisioned shared development and decentralized hosting of the FLORA system. This vision resonated well with the LDS. However, as the pilot phase progressed, the LDS soon signaled a lack of both the required resources and competencies to participate in the development and hosting of the FLORA system. To not jeopardize the pilot project, the Federal Office's FLORA team ultimately established a compromise. The FLORA team would assume full technical responsibility for the FLORA system and host an LDS instance of the FLORA system on the Federal Office's IT infrastructure. The LDS, in turn, would support the FLORA team with requirements and specifications and participate in strategic decision-making. In the words of a business analyst:

"Sure, the LDS and any other authority could technically host a blockchain node. But many, including the LDS do not really want this. The level of complexity in the governance, not necessarily in the technology, requires a different way of thinking and can be an impediment."

Through this centralized equilibrium, the FLORA team could quickly respond when the COVID pandemic required temporary changes to parts of the procedure. This success did not go unnoticed by partnering authorities as well as the BAMF's leadership. Toward the end of the pilot phase, the BAMF's president participated in a conference with representatives from several other German states who responded positively to the presentation of FLORA's pilot phase and encouraged him to make FLORA's roll-out a strategic priority. With the partnering authorities' increasing interest in adopting the FLORA system, the Federal Office, once again, evaluated options for more decentralized governance and IT. However, these efforts were punctuated when the states asked for a fast roll out of the FLORA system. In effect, the FLORA team decided to further formalize its (de)centralization compromise. In particular, it developed a software-as-a-service (SaaS) model and prioritized the roll-out to German states that were interested in the pilot's centralized development and hosting model. A consultant to the project explains:

"We currently have a software-as-a-service model, which ultimately means that the BAMF deploys a productive solution for other stakeholders. It doesn't mean, however, that other organizations cannot influence the solution, make remarks, or ask for personalization. It just means, from a purely technical perspective, that the Federal Office hosts the solution. Long-term, the aim is to develop [the model] into the direction of platform-as-a-service [...] to push responsibilities back to the competent state authorities."

As the roll-out progressed, however, the FLORA team began to experience tensions with the SaaS equilibrium as coordinating with an increasing number of 'customers' slowed down development. To ease these tensions, the FLORA team recalibrated its governance model by pushing more responsibilities to its local offices and their partner authorities at the state level. For instance, they were given full responsibility for local data management and first-level support. However, this recalibration was challenging as not all local offices and partner authorities were interested in assuming this responsibility. One of FLORA's project managers explains:

"On the one hand, [the local offices and their partner authorities] love the thought of assuming their rightful responsibilities. On the other hand, they want us to map their processes. [...] They feel overwhelmed when they cannot simply call and say what they want but have to do it themselves. So, we really need to push them to assume their responsibilities."

Further centralization tensions resulted from the hosting of the FLORA instances. Historically, the Federal Office had to cede operation of its IT infrastructure to the Informationstechnikzentrum Bund (ITZBund), the Federal Government's IT service provider. This legacy meant the Federal Office had to repeatedly apply for new infrastructure services as the roll-out proceeded. ITZBund, in turn, was slow to provide these services due to lengthy bureaucratic processes. The FLORA team thus explored various options for becoming more independent and recalibrating the 'centralized' hosting equilibrium. In the words of one of the project's IT architects:

"In the end, the 'latencies' provided the relevant incentive to decide that the system is operated by the Federal Office itself. That is, only the basic infrastructure of the network, such as IP addresses, DNS names, routing, firewall, is provided by the ITZ-Bund and we, the Federal Office, provide the operating system, on which we build virtual machines to operate our application."

Navigating (De)centralization in the EBSI Project

Much like the Federal Office, the EBP started to explore blockchain in 2018 to deliver digital public services. The EBP's objective was to develop a European Blockchain Services Infrastructure that would allow member states to provide cross-border public services through a shared IT infrastructure. The use of blockchain was deemed particularly suitable for such an infrastructure, as it would allow to replicate the EU's federal structure in a decentralized IT architecture. This idea of decentralization was also reflected in the EBP's initial processes and governance structure. Strategic decisions were made by a policy group composed of one representative for each EBP member state. Technical decisions were made by a technical group that was also composed of member state delegates. Specifications and requirements for the supported public services came from working groups for each service. Member states were free to decide whether they wanted to involve themselves in the technical and service groups. This decentralization of responsibilities allowed the EBP to secure member state support and buy-in in the EBP's early stages. One representative from an EBSI network operator explains:

"I think [decentralization of responsibilities to different working groups] is a viable approach. It allows the EBP to bring experts together and enables in-depth discussions. Because if you had such discussions in the EBP's higher-level policy- and technical groups, those discussions would become blurred and probably even politicized. And when we look back at what we have achieved, it shows that this decentralization made sense because we have made good progress on these use cases."

However, first decentralization tensions occurred when higher echelons in the European Commission pushed for a swift development of a working pilot system in 2019. While the member states supported the European Commission's ambition to accelerate the development of an EBSI pilot system, many hesitated to assume the required responsibilities and costs for this system. To break this impasse, the European Commission realized that a recalibration and transition toward a more centralized equilibrium was needed. They offered to step in and take responsibility for developing EBSI's core features and deploying a pilot network. To support this shift, the EBP granted the European Commission's EBSI team a certain degree of decision-making authority in technical development. A quote by a national policy representative illustrates:

"The degree of centralization was not forced by the European Commission. It was a result of a lack of involvement from the member states. [...] The technical development is quite European Commission-centric. Which is, in general, not a good thing. But it's a result of some member states, I don't say, stepping back, but not being so technically committed [...] It's a consequence of the fact that the member states didn't want to take [the responsibility]."

The temporary but relatively centralized equilibrium allowed the EBP to quickly set up a pilot system. However, rolling out the system called for further recalibration, especially for decentralized hosting and development of applications that build on the pilot system. To incentivize and financially support this partial 'redecentralization', the European Commission launched an EBSI funding facility. Many of the submitted tenders focused on applications that would use EBSI to support the issuance and verification of digital diplomas. This focus then led to further decentralization needs as digital diplomas required an additional end-user component, a so-called digital wallet. Soon, the EBSI team felt they did not have the necessary expertise and mandate to develop these wallets. To mitigate these centralization tensions, they created another funding facility and invited private IT companies to contribute the wallets. This decentralized development process required additional control mechanisms. To account for these, the EBSI team defined a set of technical specifications and a certification program. One national EBP policy representative reflects:

"The basic idea is to operate an infrastructure. But for that infrastructure, we had to find a boundary after which we open it [the development of applications] to the market. The important thing is that you find this line and you provide some APIs or other channels for open communication, and then it's a good thing to leave it to the market and to private organizations. It's a good choice because, in this case, competition [...] can really have a good impact. I think, if we wanted to create a unique wallet realized by the European Commission, we had to wait too long. Probably upon release, the wallet would have been technically outdated. It's ok that the infrastructure and the requirements for it have had this [centralized] story. While on the upper-levels, like the wallets and so on, we have to [decentralize] it to the market."

This recalibration allowed the EBP to foster EBSI's adoption and progress on the development of digital diplomas. Consequently, the EBSI team began to work on a rollout strategy for a production-ready system. Once again, this strategic prioritization turned out to punctuate the existing equilibrium. In effect, the EBP realized that launching EBSI in production would require increased operational responsibilities of the member states. Yet, the member states felt unable to take full responsibility for an infrastructure they cannot fully control and that is distributed and operated across different organizations and member states. Given these constraints, the EBP started transitioning to a new equilibrium. That is, they started to incorporate the EBP into a newly established European Digital Infrastructure Consortium (EDIC) that would be co-financed and jointly governed by the participating member states. The EDIC would act as an overarching central entity accountable for the development and operation of EBSI. One representative from the European Commission explains:

"That's why we want to support the follow-up of this initiative [the EBP] through a new instrument [EDIC], where it will be less the European Commission that is in the driving seat [...] We want the member states to continue their cooperation and to be more the driver of this initiative, with the European Commission staying in the role of the policy support and also financial support. But with the member states taking over our responsibilities in this initiative. That's something we are now preparing with the EBP, and we hope that this will be a way to ensure the continuity of EBSI."

Although all EBP member states considered this transition necessary, many refrained from financially committing to EDIC as a founding member. Some member states were particularly concerned about the long-term perspective of EBSI and an investment in a highly controversial technology that has proven over time to have considerable (technical) limitations. Other member states were hesitant to be a 'first mover'. As a result, only one-third of the member states committed to becoming founding members of EDIC. The limited participation in EDIC caused an (unforeseen) centralization of EBSI's governance as compared to the previously decentralized approach – in particular, the EBP policy and technical groups – that governed EBP and EBSI since their inception. One representative from an EBSI network operator describes:

"All member states, almost all, support EDIC. I don't think I've heard any critical voice saying no we don't. Maybe a couple of member states are not decided yet. Everybody supports it [EDIC], but nobody wants to fund it, that's very clear. That's the crux. [...] And there is also the risk that we don't know what will happen after 3 years. That risk exists, of course. But as I understand it, you can join the EDIC and you can also leave again, there is some flexibility."

The IT architecture of EBSI should, in turn, remain decentralized among different node operators in the member states according to detailed service-level agreements, including well-defined terms and conditions for node operation as well as IT security requirements. However, complying with these service-level agreements appeared to be challenging for some pilot network operators who lacked the required IT security certification. Obtaining such a certification can be costly and requires substantial organizational changes. Consequently, the EBSI team feared that a secure and production-grade EBSI would again lead to an unduly centralized network. To mitigate this risk, the EBSI team once again adapted its approach. More specifically, they initiated another funding facility – this time for hosting productive instances and developing complementary productive applications. One national EBP policy representative reflects:

"This is a risk. If these requirements [for the node operation] prove to be too strict and too strong. They impair the enlargement of the number of nodes. This is, of course, an issue. [... And] it's quite expensive to set up and operate a node. This is an issue."

Summary

In both projects, the initial vision was to develop an IT system that follows dominant federal organizing structures and a strict decentralization of responsibilities. However, the Federal Office and the EBP had to compromise on decentralization early on because the (political) need for quick progress required a more centralized approach. Over time, the limitations of these centralization compromises and a range of punctuating events required an iterative recalibration and a transition to new (de)centralization equilibria. The FLORA project opted to maintain and recalibrate its centralization compromise and, ultimately, establish a more centralized equilibrium than initially envisioned. The EBP, in turn, attempted to mitigate mounting (de)centralization tensions by iterating between centralization and decentralization, regularly pushing back temporarily centralized responsibilities to the member states.

Discussion

We started our study by observing that large organizations are trapped in a tension field between centralization and decentralization (Mintzberg, 1984, 1989; Smith & Lewis, 2011; Weick, 1987). While the tension field is well researched, little is known about how organizations can navigate this tension field and establish new stable (de)centralization equilibria in their organizational processes, governance, and IT once an old equilibrium is punctuated. We thus conducted a multiple-case study on two projects that saw the establishment, recalibration, and transition between several such equilibria. Our analysis unpacks how changes in organizational strategy or context will typically punctuate (de)centralization equilibria. These punctuating events make the old equilibrium unstable and require organizations to embark on an iterative recalibration of their organizational processes, governance, and IT to reach a new stable equilibrium.

A Process Model for the Development of Dynamic (De)centralization Equilibria

Our insights can be translated into a process model (Cloutier & Langley, 2020) that captures the dynamic development of (de)centralization equilibria in organizational processes, governance, and IT (Figure 3). Drawing on centralization and decentralization literature in the fields of management (Mintzberg, 1984, 1989; Romanelli & Tushman, 1994; Smith & Lewis, 2011; Smith & Tushman, 2005) and IS (Andersen, 2005; Kahai et al., 2003; King, 1983; Sambamurthy & Zmud, 1999), our model describes the iterative recalibration of organizational processes, governance, and IT in response to punctuating events (Lyytinen & Newman, 2008; Romanelli & Tushman, 1994). It highlights that the recalibration process is guided by observations of centralization or decentralization tensions.

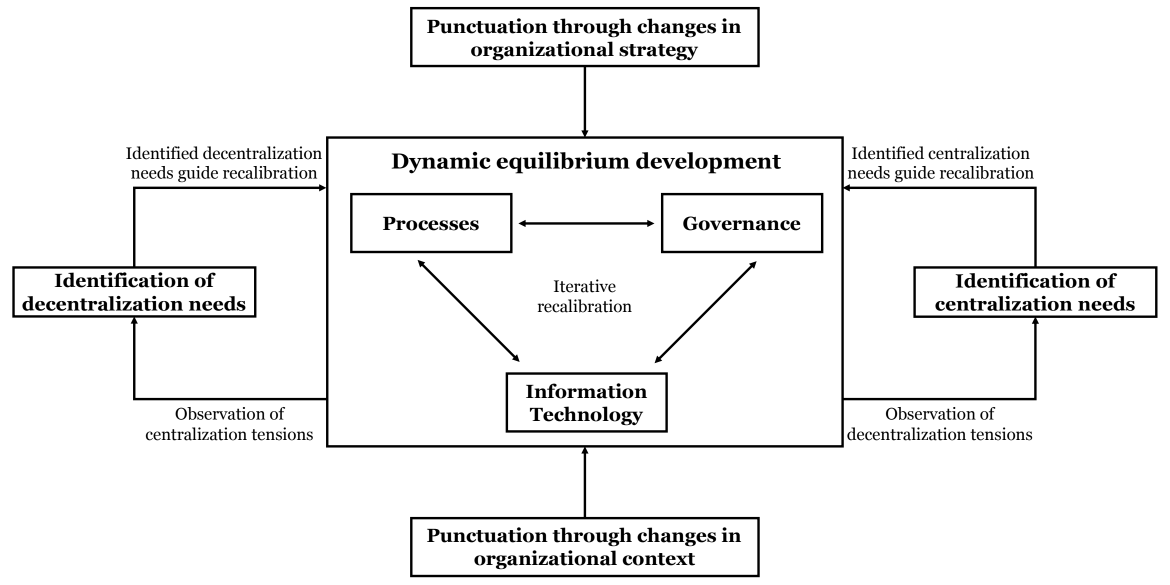

Punctuation through changes in organizational strategy
Dynamic equilibrium development
Processes
Governance
Iterative recalibration
Information Technology
Identified decentralization needs guide recalibration
Identification of decentralization needs
Observation of centralization tensions
Identified centralization needs guide recalibration
Identification of centralization needs
Observation of decentralization tensions
Punctuation through changes in organizational context

Figure 3. A Process Model for the Dynamic Development of (De)centralization Equilibria in Organizational Processes, Governance, and IT.

Successful navigation of such identification and recalibration processes requires organizations to be malleable in their processes, governance, and IT (Hanelt et al., 2021; Henderson & Venkatraman, 1999; King, 1983; Mikalef et al., 2021). This malleability is particularly crucial when organizations need to react quickly to punctuating changes in their strategic direction (Aldrich & Pfeffer, 1976; Smith & Tushman, 2005) or their organizational context (Ahituv et al., 1989; Sambamurthy & Zmud, 1999). Changes in strategic priorities, for example, may necessitate organizations to shift their governance from a centralized to a more decentralized structure or vice versa. For instance, as our cases demonstrate, strategies that call for a rapid system roll-out, may result in centralization needs. Resource constraints of a central entity, in turn, may provoke decentralization needs when the system grows. Such shifts often require adjustments to organizational processes and IT to mirror these new governance structures. However, our cases also demonstrate that such shifts are typically temporary. As time passes, new punctuating events may trigger further recalibration or the transition to new equilibria. Thus, we derive the following conjecture:

Conjecture 1: (De)centralization equilibria are inherently temporary and stability results from the ability to recalibrate and transition between equilibria.

Our cases demonstrate how important it is for organizations to navigate equilibria, recalibrations, and transitions carefully. The nature of the tensions organizations will face during transitions depends on the desired degree of centralization or decentralization (Andersen, 2005; King, 1983; Sambamurthy & Zmud, 1999). If the new equilibrium, for example, is to be characterized by strong centralization in one or multiple elements, these changes may lead to substantial coordination or communication costs across organizational subunits (Andersen, 2005; Kahai et al., 2003; Mikalef et al., 2021; Sambamurthy & Zmud, 1999). Identifying such tensions will guide the redesign of the new equilibrium in a more decentralized way and initiate an iterative process of recalibration and re-evaluation. Similar tensions occur when a target equilibrium is situated at the decentralized end of the spectrum. Tensions related to the loss of control over subunits (Beck et al., 2018; Moldoveanu & Martin, 2001; Weill, 2004) or a void in accountabilities as in the cases of FLORA and EBSI, in turn, can emphasize the need to centralize and push for a recalibration of the equilibrium. Hence, we propose as our second conjecture:

Conjecture 2: Punctuations or imbalances in the equilibrium create (un)foreseen needs for counterbalancing organizational processes, governance, and/ or IT.

To accommodate the dynamic recalibration of organizational processes, organizations must allow for local and temporary nuances in their (de)centralization equilibria. Decentralized organizations that aim to establish a decentralized IT system cannot always rely on their existing structures from the onset, as subunits may often be unable or unwilling to take the lead (Andersen, 2005; Beck et al., 2018; Wiseman et al., 2012). In such cases, centralization may not only be essential for filling accountability voids but also for proceeding quickly (Aulakh & Gencturk, 2000; Mintzberg, 1989; Peppard, 2018; Rediker & Seth, 1995). In effect, decentralized organizations may accept local or temporary centralization compromises to enable a transition to a more decentralized equilibrium later. Finding the right time for this transition, however, is essential to avoid undue centralization tensions. Centralized development, for instance, may increasingly impede the roll-out and extension once decentralized IT systems exceed a certain size. Moreover, increased decentralized use can make it hard to maintain centralized accountability. When (de)centralization compromises lead to escalating tensions, organizations may re-evaluate their local and temporal compromises. Accordingly, we derive our third conjecture:

Conjecture 3: To achieve stable (de)centralization equilibria, organizations must allow for dynamism and regularly revisit local and temporary compromises.

Theoretical Contributions

Our research first contributes to the IS literature on (de)centralization by demonstrating that sustaining (de)centralization equilibria in organizational processes, governance, and IT is inherently dynamic. More specifically, our work emphasizes that organizations evolve in response to punctuating events that require an iterative recalibration and transition to a new temporary equilibrium. This process perspective builds on insights into the realization of stable decentralized IT structures and the relevance of malleability (Henderson & Venkatraman, 1999; King, 1983; Mikalef et al., 2021; Sambamurthy & Zmud, 1999). At the same time, it extends these insights by examining the process, i.e., dynamic transitions between (de)centralization equilibria, organizations use to resolve tensions. Moreover, our process perspective highlights that (de)centralization equilibria are not persistent. We explain how organizations can work toward a new equilibrium by making changes to organizational processes, governance, or IT when changes in organizational strategy or context destabilize the old equilibrium (Romanelli & Tushman, 1994).

Secondly, our research adds to management literature on decentralization by demonstrating that the establishment of (de)centralization equilibria requires an IT perspective (Ahituv et al., 1989; Siggelkow & Levinthal, 2003). We emphasize that IT does and should play an important role in sustaining desirable (de)centralization equilibria in today's organizations. However, this does not establish IT as more important than organizational processes or governance. All three are of equal importance and require careful individual and joint consideration in the pursuit of stable equilibria (Romanelli & Tushman, 1994; Smith & Tushman, 2005). Yet, we observe that the selection of the underlying IT can create baseline tensions and impact the development of (de)centralization equilibria. Blockchains, for example, stipulate a certain degree of decentralization, which may conflict with centralized processes and governance structures. This may require compromises and frequent recalibration.

Third, our research contributes both to the IS and management literature on (de)centralization by connecting the two literatures and unpacking *how* organizations can successfully navigate the recalibration and transition between old and new equilibria. Our study demonstrates that organizations must allow and embrace temporary compromises in these processes. Moreover, organizations will often not be able to apply the same degree of (de)centralization to all units, since not all units possess the same maturity or competence level. As such, we confirm and corroborate the insights of Smith & Tushman (2005) and Smith & Lewis (2011) that dynamic compromises between centralization and decentralization can be utilized to benefit organizations.

Practical Implications

The practical implications of our study are two-fold. First, our research sheds light on how organizational leaders can rebalance the degree of (de)centralization in their organization's processes, governance, and IT in response to changes in strategy or the organizational context. Additionally, our work highlights that any change in the degree of (de)centralization can entail an iterative recalibration or transition process. Organizational leaders should be careful when choosing overly centralized or decentralized structures, as either choice will introduce tensions that may require costly recalibration or transition at a later point. Moreover, organizational leaders are well advised to minimize the number of punctuating events that require an iterative recalibration.

Second, our paper provides organizational leaders with decision support on how to navigate these iterative recalibration and transition processes best. We highlight that organizational leaders should avoid applying a one-size-fits-all approach. Instead, they should consider, allow, and accept local and temporary differences. Especially temporary compromises may be essential to build a stable equilibrium. However, organizational leaders should be aware that such compromises will not be tolerated indefinitely and that other changes in strategy or organizational context may occur that will demand resolving such compromises earlier than expected. Thus, temporal compromises need to be constantly re-evaluated. This minimizes the risk of organizational leaders to mismanage their organizations and create long-term imbalances in their (de)centralization equilibria, which might result in more frequent and costly recalibration.

Boundary Conditions

Boundary conditions are essential to theoretical insights, including those developed from multiple-case study research, as they help define the scope and applicability of the developed theoretical insights (Eisenhardt, 2021). We identify three such boundary conditions for our process model and conjectures in terms of domain, prevalent organizational structures, and technology.

First, both cases are public sector projects, which might limit the generalizability and transferability of our insights. Public organizations are typically not driven by profitability considerations and market pressure. As such, they might have more margin for maneuvering when allowing for local and temporary differences between their organizational subunits while trying to find a (de)centralization equilibrium. Companies might not always have this level of freedom as market pressures may restrict them and stifle attempts to 'experiment' with different levels of centralization (Weick, 1987).

Second, both cases are situated in a federally organized context, which naturally places them between centralized and decentralized structures. This second boundary condition emphasizes the transferability of our findings to strongly centralized or strongly decentralized organizations. Our model cannot predict whether organizations that find themselves on one end of the (de)centralization continuum would be willing to – at least temporarily – commit (de)centralization compromises and search for new stable equilibria. Yet as both centralized and decentralized structures each present opportunities and limitations, we argue that organizations at either end of the (de)centralization continuum will sooner or later face punctuating events that may cause them to compromise on parts of their existing structures to ensure successful organizing (Smith & Lewis, 2011; Smith & Tushman, 2005).

Third, both projects focus on developing blockchain-based systems, which naturally imposes a certain degree of decentralization. This third boundary condition, thus, affects the transferability of our results to equilibria build around more inherently centralized IT. However, a closer look at both cases suggests that our model may not be limited to blockchain. While both systems were initially built around blockchain, the blockchain components have become less important over time and have been complemented by various other components and technologies as development proceeds. Furthermore, many of the observed (de)centralization tensions occurred independently of blockchain technology. This leads us to surmise that our insights can also be transferred to IT systems that do not build on blockchain.

Conclusion

Our study demonstrates that establishing a (de-)centralization equilibrium in organizational processes, governance, and IT is a dynamic process that requires constant recalibration and sometimes transitions to new equilibria. Based on insights from two blockchain projects, we derive a process model that describes this recalibration and transition. Our model details that punctuations through changes in organizational strategies and context, as well as tensions inherent to centralization and decentralization, can trigger an iterative recalibration process and the transition to a new (de)centralization equilibrium. Navigating this transition can require local or temporal compromises.

Acknowledgements

This research was funded in part by the Luxembourg National Research Fund (FNR) and PayPal, PEARL grant reference *13342933/Gilbert Fridgen*, as well as the Luxembourg National Research Fund (FNR) in the FiReSpARX (grant reference *14783405*) project, and Luxembourg's Ministry for Digitalisation. We also acknowledge the support of the European Union (EU) within its Horizon 2020 programme, project MDOT (Medical Device Obligations Taskforce), grant agreement *814654,* that made this paper possible. For the purpose of open access, the authors have applied a Creative Commons Attribution 4.0 International (CC BY 4.0) license to any Author Accepted Manuscript version arising from this submission.

References

Ahituv, N., Neumann, S., & Zviran, M. (1989). Factors affecting the policy for distributing computing resources. *MIS Quarterly*, *13*(4), 389–401. **https://doi.org/10.2307/248722**

Aldrich, H. E., & Pfeffer, J. (1976). Environments of organizations. *Annual Review of Sociology*, *2*(1), 79–105. **https://doi.org/10.1146/annurev.so.02.080176.000455**

Andersen, T. J. (2005). The performance effect of computer-mediated communication and decentralized strategic decision making. *Journal of Business Research*, *58*(8), 1059–1067. **https://doi.org/10.1016/j.jbusres.2004.02.004**

Aulakh, P. S., & Gencturk, E. F. (2000). International principal–agent relationships: Control, governance and performance. *Industrial Marketing Management*, *29*(6), 521–538. **https://doi.org/10.1016/S0019-8501(00)00126-7**

Bakos, Y., Halaburda, H., & Mueller-Bloch, C. (2021). When permissioned blockchains deliver more decentralization than permissionless. *Communications of the ACM*, *64*(2), 20–22. **https://doi.org/10.1145/3442371**

Beck, R., Müller-Bloch, C., & King, J. (2018). Governance in the Blockchain Economy: A Framework and Research Agenda. *Journal of the Association for Information Systems*, *19*(10). **https://aisel.aisnet.org/jais/vol19/iss10/1/**

Brown, C. V. (1997). Examining the emergence of hybrid IS governance solutions: Evidence from a single case site. *Information Systems Research*, *8*(1), 69–94. **https://doi.org/10.1287/isre.8.1.69**

Chen, Y., Richter, J. I., & Patel, P. C. (2021). Decentralized Governance of Digital Platforms. *Journal of Management*, *47*(5), 1305–1337. **https://doi.org/10.1177/0149206320916755**

Cloutier, C., & Langley, A. (2020). What makes a process theoretical contribution? *Organization Theory*, *1*(1), 1–32. **https://doi.org/10.1177/2631787720902473**

Constantinides, P., Henfridsson, O., & Parker, G. G. (2018). Introduction—Platforms and Infrastructures in the Digital Age. *Information Systems Research*, *29*(2), 381–400. **https://doi.org/10.1287/isre.2018.0794**

Corbin, J. M., & Strauss, A. (1990). Grounded theory research: Procedures, canons, and evaluative criteria. *Qualitative Sociology*, *13*(1), 3–21. **https://doi.org/10.1007/BF00988593**

Davis, J. P., & Eisenhardt, K. M. (2011). Rotating leadership and collaborative innovation: Recombination processes in symbiotic relationships. *Administrative Science Quarterly*, *56*(2), 159–201. **https://doi.org/10.1177/0001839211428131**

de Reuver, M., Sørensen, C., & Basole, R. C. (2018). The Digital Platform: A Research Agenda. *Journal of Information Technology*, *33*(2), 124–135. **https://doi.org/10.1057/s41265-016-0033-3**

Drucker, P. F. (1992). The New Society of Organizations. *Harvard Business Review*, *20*(7), 281–293.

Eisenhardt, K. M. (1989). Building Theories from Case Study Research. *Academy of Management Review*, *14*(4), 532–550. **https://doi.org/10.5465/amr.1989.4308385**

Eisenhardt, K. M. (2021). What is the Eisenhardt Method, really? *Strategic Organization*, *19*(1), 147–160. **https://doi.org/10.1177/1476127020982866**

Eisenhardt, K. M., & Graebner, M. E. (2007). Theory Building From Cases: Opportunities And Challenges. *Academy of Management Journal*, *50*(1), 25–32. **https://doi.org/10.5465/amj.2007.24160888**

Foss, N. J., Husted, K., & Michailova, S. (2010). Governing knowledge sharing in organizations: Levels of analysis, governance mechanisms, and research directions. *Journal of Management Studies*, *47*(3), 455–482. **https://doi.org/10.1111/j.1467-6486.2009.00870.x**

Grandori, A. (1997). Governance structures, coordination mechanisms and cognitive models. *Journal of Management & Governance*, *1*(1), 29–47. **https://doi.org/10.1023/A:1009977627870**

Gubitta, P., & Gianecchini, M. (2002). Governance and flexibility in family-owned SMEs. *Family Business Review*, *15*(4), 277–297. **https://doi.org/10.1111/j.1741-6248.2002.00277.x**

Halaburda, H. (2018). Blockchain revolution without the blockchain? *Communications of the ACM*, *61*(7), 27–29. **https://doi.org/10.1145/3225619**

Halaburda, H., & Mueller-Bloch, C. (2019). *Will We Realize Blockchain's Promise of Decentralization?* **https://hbr.org/2019/09/will-we-realize-blockchains-promise-of-decentralization**

Hammer, M. (2014). What is business process management? In *Handbook on business process management 1: Introduction, methods, and information systems* (pp. 3–16). Springer. **https://doi.org/10.1007/978-3-642-45100-3_1**

Hanelt, A., Bohnsack, R., Marz, D., & Antunes Marante, C. (2021). A systematic review of the literature on digital transformation: Insights and implications for strategy and organizational change. *Journal of Management Studies*, *58*(5), 1159–1197. **https://doi.org/10.1111/joms.12639**

Hanseth, O., & Lyytinen, K. (2010). Design theory for dynamic complexity in information infrastructures: The case of building internet. *Journal of Information Technology, 25*, 1–19. **https://doi.org/10.1057/jit.2009.19**

Hein, A., Schreieck, M., Riasanow, T., Setzke, D. S., Wiesche, M., Böhm, M., & Krcmar, H. (2020). Digital platform ecosystems. *Electronic Markets*, *30*(1), 87–98. **https://doi.org/10.1007/s12525-019-00377-4**

Henderson, J. C., & Venkatraman, H. (1999). Strategic alignment: Leveraging information technology for transforming organizations. *IBM Systems Journal*, *38*(2.3), 472–484. **https://doi.org/10.1147/SJ.1999.5387096**

Huber, G. P., & Power, D. J. (1985). Retrospective Reports of Strategic-Level Managers: Guidelines for Increasing Their Accuracy. *Strategic Management Journal*, *6*(2), 171–180. **https://doi.org/10.1002/smj.4250060206**

Huber, T. L., Kude, T., & Dibbern, J. (2017). Governance practices in platform ecosystems: Navigating tensions between cocreated value and governance costs. *Information Systems Research*, *28*(3), 563–584. **https://doi.org/10.1287/isre.2017.0701**

Jacobides, M. G., Cennamo, C., & Gawer, A. (2018). Towards a theory of ecosystems. *Strategic Management Journal*, *39*(8), 2255–2276. **https://doi.org/10.1002/smj.2904**

Kahai, P. S., Carr, H. H., & Snyder, C. A. (2003). Technology and the decentralization of information systems. *Information Systems Management*, *20*(3), 51–60. **https://doi.org/10.1201/1078/43205.20.3.20030601/43073.6**

King, J. L. (1983). Centralized versus decentralized computing: Organizational considerations and management options. *ACM Computing Surveys (CSUR)*, *15*(4), 319–349. **https://doi.org/10.1145/289.290**

Lacity, M. C. (2018). Addressing key challenges to making enterprise blockchain applications a reality. *MIS Quarterly Executive*, *17*(3), 201–222. **https://aisel.aisnet.org/misqe/vol17/iss3/3**

Lumineau, F., Wang, W., & Schilke, O. (2021). Blockchain Governance—A New Way of Organizing Collaborations? *Organization Science*, *32*(2), 500–521. **https://doi.org/10.1287/orsc.2020.1379**

Lyytinen, K., & Newman, M. (2008). Explaining information systems change: A punctuated socio-technical change model. *European Journal of Information Systems*, *17*, 589–613. **https://doi.org/10.1057/ejis.2008.50**

Mikalef, P., Pateli, A., & van de Wetering, R. (2021). IT architecture flexibility and IT governance decentralisation as drivers of IT-enabled dynamic capabilities and competitive performance: The moderating effect of the external environment. *European Journal of Information Systems*, *30*(5), 512–540. **https://doi.org/10.1080/0960085X.2020.1808541**

Mintzberg, H. (1984). Who should control the corporation? *California Management Review*, *27*(1), 90–115. **https://doi.org/10.2307/41165115**

Mintzberg, H. (1989). *The structuring of organizations*. Springer. **https://doi.org/10.1007/978-1-349-20317-8_23**

Moldoveanu, M., & Martin, R. (2001). Agency theory and the design of efficient governance mechanisms (Joint Committee on Corporate Governance). *Toronto: Rotman School of Management, University of Toronto.*, *3*(5), 430.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Decentralized Business Review.

Peppard, J. (2018). Rethinking the concept of the IS organization. *Information Systems Journal*, *28*(1), 76–103. **https://doi.org/10.1111/isj.12122**

Rediker, K. J., & Seth, A. (1995). Boards of directors and substitution effects of alternative governance mechanisms. *Strategic Management Journal*, *16*(2), 85–99. **https://doi.org/10.1002/smj.4250160202**

Romanelli, E., & Tushman, M. L. (1994). Organizational transformation as punctuated equilibrium: An empirical test. *Academy of Management Journal*, *37*(5), 1141–1166. **https://doi.org/10.5465/256669**

Sambamurthy, V., & Zmud, R. W. (1999). Arrangements for information technology governance: A theory of multiple contingencies. *MIS Quarterly*, *23*(2), 261–290. **https://doi.org/10.2307/249754**

Siggelkow, N., & Levinthal, D. A. (2003). Temporarily divide to conquer: Centralized, decentralized, and reintegrated organizational approaches to exploration and adaptation. *Organization Science*, *14*(6), 650–669. **https://doi.org/10.1287/orsc.14.6.650.24840**

Smith, W. K., & Lewis, M. W. (2011). Toward a theory of paradox: A dynamic equilibrium model of organizing. *Academy of Management Review*, *36*(2), 381–403. **https://doi.org/10.5465/amr.2009.0223**

Smith, W. K., & Tushman, M. L. (2005). Managing strategic contradictions: A top management model for managing innovation streams. *Organization Science*, *16*(5), 522–536. **https://doi.org/10.1287/orsc.1050.0134**

Srikanth, K., & Puranam, P. (2014). The firm as a coordination system: Evidence from software services offshoring. *Organization Science*, *25*(4), 1253–1271. **https://doi.org/10.1287/orsc.2013.0886**

Tushman, M. L., & Romanelli, E. (1985). Organizational evolution: A metamorphosis model of convergence and reorientation. *Research in Organizational Behavior*, *7*, 171–222.

Uhl-Bien, M., & Arena, M. (2018). Leadership for organizational adaptability: A theoretical synthesis and integrative framework. *The Leadership Quarterly*, *29*(1), 89–104. **https://doi.org/10.1016/j.leaqua.2017.12.009**

Weick, K. E. (1987). Organizational culture as a source of high reliability. *California Management Review*, *29*(2), 112–127. **https://doi.org/10.2307/41165243**

Weill, P. (2004). Don't just lead, govern: How top-performing firms govern IT. *MIS Quarterly Executive*, *3*(1), 1–17. **https://aisel.aisnet.org/misqe/vol3/iss1/3**

Wiseman, R. M., Cuevas-Rodríguez, G., & Gomez-Mejia, L. R. (2012). Towards a social theory of agency. *Journal of Management Studies*, *49*(1), 202–222. **https://doi.org/10.1111/j.1467-6486.2011.01016.x**

Yin, R. K. (2011). *Applications of case study research* (3rd ed). Sage Publications.

Yin, R. K. (2017). *Case Study Research and Applications* (6th Edition). Sage Publications.

Zhao, Y., von Delft, S., Morgan-Thomas, A., & Buck, T. (2020). The evolution of platform business models: Exploring competitive battles in the world of platforms. *Long Range Planning*, *53*(4), 101892. **https://doi.org/10.1016/j.lrp.2019.101892**

RP15: Weigl, L., Roth, T., Amard, A., & Zavolokina, L. (2023). **When Public Values and User-Centricity in e-Government Collide – A Systematic Review.** *Government Information Quarterly (Minor Revisions).*

Journal Rating: 17.3 (CiteScore); 3.309 (SNIP)

When Public Values and User-Centricity in e-Government Collide – a Systematic Review

Abstract

User-centricity in e-Government is a double-edged sword. While it helps governments design digital services tailored to the needs of citizens, it may also increase the burden on users and deepen the digital divide. From an institutional perspective, these fundamental conflicts are inevitable. To better understand the role and effect of user-centricity in e-Government, this paper analyses academic literature on user-centricity and public values. The analysis leads to three main insights: First, there is a conflict in citizen representation that may result from the normative dominance of decision-makers. Second, we identify an accountability conflict that can prevent user-centric innovation from thriving in a highly institutionalized environment. Third, we identify a pluralism conflict that emerges from a clash between the reality of a diverse society and the assumed homogeneity of actors. The need to address these conflicts increases with rapid technological innovation, such as distributed ledger technologies, artificial intelligence, and trust infrastructures. These technologies put the user at the center stage and permeate aspects of social life beyond government. In response to these insights, we outline suggestions for further research and practice.

Keywords: User-centricity, citizen-centricity, public values, e-Government, literature review

1. Introduction

Public administrations worldwide embrace citizen-centricity as a key component of their organizational strategy (OECD & Asian Development Bank, 2019; Vesnic-Alujevic et al., 2019). This new strategy also reflects governments' eagerness to explore new technologies that may help improve public services (Dwivedi et al., 2011) and better incorporate the needs of citizens as users (Codagnone et al., 2020; Sevaldson, 2018; Zavolokina et al., 2023). In e-Government, the new focus on citizens as users has evolved into 'user-centricity'. This construct encompasses the involvement and participation of users in the *design* of digital public services applications – also referred to as *co-design* – and the adaption of digital systems to users' preferences at the *implementation* stage.

Despite their goal to improve the delivery of public services, some user-centric implementations assume an ambitious level of digital skills that not all users possess. A lack of these skills and relevant knowledge of underlying public procedures could, for instance, exclude citizens from the co-creation of digital public services in collaborative design approaches. The resulting intention-reality gap creates tensions that materialize in the so-called digital divide, i.e., a state in which significant portions of the population either lack the necessary digital skills or access to otherwise available technology (Robinson et al., 2003). Governments focused on user-centricity for their delivery of public services risk oppressing these already marginalized groups further by assuming a common level of digital skills and not accounting for socio-economic differences. At the same time, the implementation of user-centricity can be a powerful tool to empower citizens and better reflect their needs (Weigl et al., 2022).

However, putting citizens' needs and expectations center stage is difficult and requires a holistic approach beyond mere revision of government processes. User-centric e-Government affects the foundation of public service delivery and necessitates carefully balancing values introduced by user-centricity with established public values. We define public value(s) in line with Moore (1995), who posits that public value encapsulates the shared expectations of citizens regarding government and public services. He argues that public organizations pursue public value to effectively address public needs. A common ground for all public value frames is that public values are often ambiguous, hybrid, contrasting, and overlapping (Stoker, 2006). That is, the support and fulfillment of values introduced or championed by user-centricity may clash with established public value frames. Resulting value conflicts are clear signs of value pluralism and require careful management of user-centric implementations (van der Wal & van Hout, 2009). Weigl et al. (2022), for instance, find that user-centricity is strongly aligned with values such as efficiency, innovation, transparency, or accountability to the public. While these values reflect government institutions' general pursuit of legitimacy, reputation, and a democratic ethos, they introduce economic rationality, which is not typically at the core of public organizing (Mignerat & Rivard, 2015; Wiredu, 2012). To anticipate conflicts and best leverage the possibilities introduced by user-centricity, governments need to deepen their understanding of *how* user-centricity may align and conflict with established public values, and *what* causes these conflicts. Current studies either focus on general public value conflicts or the design of different approaches to user-centric digital services in e-Government. Only few studies explore value conflicts between user-centric and public values in a digital government context (Weigl et al., 2022). The existing fragmented literature and often contradictory research results also do not elaborate on how potentially conflicting values can be reconciled in user-centric designs, projects, and initiatives. The consequences and sources of such value conflicts for e-Government services are yet to be systematically analyzed (Ingrams, 2019).

Given the relevance of user-centric applications in eGovernment and the advancement of relevant technologies to facilitate such applications, the needs of service providers and recipients need to be better integrated into user-centric designs. The resulting reconciliation of user-centric with public values may support more inclusive services and inform the development of technologies for social good. Efforts to integrate user-centricity into public value frames include the identification of conflict areas and, most importantly, their sources. These efforts are relevant to avoid deviations from core public values post-implementation, which can carry an elevated risk of exacerbating societal disparities, eroding trust in governance, and compromising privacy. Moreover, without identifying the sources of conflicts between user-centricity and public values, those conflicts will be difficult to tackle or reduce.

Thus, our study aims to provide a systematic overview of the *status quo* on interactions between user-centricity and established public values. We identify value conflicts and their sources based on an abductive analysis of our data. These serve as the foundation for recommendations to support the integration of user-centric digital services with public values. We also outline future research directions at the intersection of public value theory and user-centricity in IS and digital government. Since our study intends to deliver a systematic overview and actionable recommendations on how emerging user-centric technologies across many levels of social organizing, such as digital identities and artificial intelligence, (Ølnes et al., 2017), can be best integrated, we ask the following research questions:

RQ1. What value conflicts emerge in user-centric approaches to e-Government?

RQ2. Why do these value conflicts between user-centric values and public values emerge?

To address these research questions, we first conduct a systematic literature review to synthesize literature in IS, computer science, and public administration. The synthesis helps us understand the interplay between user-centric and public values as well as emerging value conflicts. Based on abductive analyses, we explore underlying conflict sources, i.e., emerging or contextual factors that influence or exacerbate value conflicts. Second, we outline opportunities for further research to address the identified conflicts and assist the implementation of future user-centric government-to-citizen initiatives. Our study may also serve as a roadmap for user-centric approaches with new technological applications in e-Government.

The remainder of the paper is structured as follows. The second section discusses the concepts of user-centricity and public policy, public values for e-Government, and conflict literature. The third section outlines the research approach including literature identification, selection, relevance, quality assessment, and data extraction and analysis. The fourth section provides an overview of our findings. It describes the conflicts identified in our systematic literature review and integrates an analysis of their underlying sources. The fifth section discusses the research contributions and proposes areas for future research. The paper ends with a summary of our key findings, the paper's limitations, and an outline of future research directions.

2. Background

2.1. User-centricity and public policy

With the advent of digital transformation efforts at different governmental levels and the introduction of new technologies to improve public services, such as data analytics, AI, or novel identity management applications (Bhargav-Spantzel et al., 2006; Niglia & Tangi, 2024), user-centricity has become a primary goal for policy-makers (European Commission, 2023; OECD, 2009). While user-centric approaches were initially limited to human-computer interaction research in the 1980s, they have gained more widespread attention with the rise of software development projects. User-centric approaches commonly focus on users' needs, expectations and preferences (Jarke, 2021; Kurdi et al., 2010). They also resonate well with software designers' X-centered designs, such as healthcare with patient-centered design (Morales Rodriguez et al., 2007), workplace with employee-centered design (Spurlock & O'Neil, 2009), or public administration with citizen-centric design (van Velsen et al., 2009a). Policy-makers and practitioners seized the advancement of user-centricity by developing national and international policies. For example, international organizations such as the OECD directly link user-centric digital public services to citizen well-being (Welby, 2019) and propose tailored guidance for the public (OECD, 2009). Extensive funding up to hundreds of millions of dollars[1] for projects targeting user-centricity further pushes these approaches. Many countries successfully embedded user-centricity in their service design, such as the U.S.A. (U. S. General Services Administration, 2023) and the U.K. (Government Digital Service, 2023). Some governments either directly support service designers aiming for user-centric designs or propose dedicated training (Government Digital Service, 2020). It is particularly relevant that service designers understand the importance of development and evaluation phases to achieve user-centric outcomes. IT develops rapidly, expecting citizens to catch up quickly. This is only possible when service designers can reflect different levels of digital skills and heterogenous needs in their applications to, for instance, accommodate an aging population (Lee, 2022).

The new focus on citizens as users may also affect policy-makers who need to consider the influences of user-centricity on policy-making and vice versa (Othman et al., 2020). Current considerations of this relationship have primarily focused on systems development. In this

[1] See, for instance, the projects listed on the website of the World Bank: https://projects.worldbank.org/en/projects-operations/project-detail/P168425

context, user-centricity appears as a multidimensional concept composed of four pillars (Iivari & Iivari, 2011): (1) user-centricity as user focus, (2) user-centricity as work-centeredness, (3) user-centricity as user involvement, and (4) user-centricity as system personalization. Each of these four pillars provides a different, albeit complementary, dimension to the concept. First, user focus addresses users' needs based on their activities or tasks and characteristics (such as skills or personal preferences). Second, work-centeredness provides insights into users' work activities, context, and dominant work practices. Third, user involvement reflects the importance and relevance users attach to a given system. Iivari et al. (2011) additionally distinguish between user involvement and user participation. The latter is a type of user involvement, in which users actively participate in the design process. Fourth, system personalization reflects the adaptability or adaptivity of the system's content structure, presentation, and functionalities to individual preferences or behaviors.

User-centric values steer how governments manage and integrate digital technologies into processes and interactions with citizens. However, the reconciliation between user-centric values in e-government and established public values has not been well-researched. Current work is focused on the benefits of user-centricity and primarily explores adoption mechanisms to overcome the challenges of e-Government (Al-Hujran et al., 2015; Alzahrani et al., 2017; Rana et al., 2012; Van Velsen et al., 2008; van Velsen et al., 2009a), presenting user-centricity as a panacea. In practice, however, the proposed panacea has neither mitigated implementation struggles nor improved the acceptance of digital technologies in public administration.

The origin of user-centric approaches may explain their limited effect in practice. User-centricity is rooted in market-oriented principles, such as customer-centric relationships, and does not necessarily focus on users' 'true needs'. Instead, user-centricity considers, for instance, profit-maximizing strategies. This casts doubt on its representation of citizens' multifaceted needs and expectations and its contribution to social good in eGovernment contexts.

2.2.Public values for e-Government

Maintaining or improving services and policies of system designs during digital transformation reflects the "inherently democratic mission [of public administration that] rely on support from citizens and institutions of government for their viability" (Ventriss et al., 2019, p. 276). However, this mission is not necessarily reflected in the efficiency- and effectiveness-maximization principles of IS implementation (Mignerat & Rivard, 2015).

IS research typically adopts a rational perspective and considers managers as efficiency-seeking decision-makers, whose choices are based on cost-benefit analyses (Avgerou, 2000; Teo et al., 2003; Tingling & Parent, 2002). Going beyond the ideal of a homo economicus in public administration (Avgerou, 2000; Orlikowski & Barley, 2001; Teo et al., 2003), would require actors to endorse public values as they seek legitimacy over efficiency (Jansen & Tranvik, 2011; Mignerat & Rivard, 2015). According to institutional theory, legitimacy is crucial for government actors to 'survive' long-term, that is, retain the support of their voters and be re-elected (Meyer & Rowan, 1977; Mignerat & Rivard, 2015).

Despite the clear focus on legitimacy in public administration, public management systems have changed over time and not all systems intrinsically prioritize 'public sector ethos' (Stoker, 2006). Traditional public administration, for instance, follows Weberian principles that position bureaucratic oversight as a central element to satisfying citizens' demands on the state (ibid.). The New Public Management (NPM) approach portrays citizens as 'customers' and heavily draws on private sector management models and market-based mechanisms

(Ferlie et al., 1996; Hood, 1995; Pollitt & Bouckaert, 2017). To achieve a more user-centric focus, Digital Era Governance (DEG) emerged as an attempt to re-aggregate public services around users' needs (Dunleavy, 2005). At the same time, the public value management paradigm (Stoker, 2006) highlights strategic objectives, such as enhancing efficiency in public services, ensuring equality, social inclusion, transparency, and upholding accountability (Cordella & Bonina, 2012; Moore, 1995). While these models and paradigms already try to anticipate values introduced by information technologies (IT), the complex relationship between ICT and citizen-centered governance warrants further analyses.

Bannister et al. (2014) have explored this intricate relationship by developing a typology of how technology implementation impacts a range of public values (Table 1). They refer to public values as "a mode of behavior [or] a way of doing things […] that is held to be right […] by the public, citizens or the so-called 'reasonable man'" (Bannister & Connolly, 2014, p. 120). This definition builds on 'public value' within the public value management paradigm and describes the shared expectations of citizens for government and public services (Moore, 1995). In their typology, Bannister et al. (2014) also identify several public values and categorize them into three domains: duty-oriented, service-oriented, and socially oriented. Duty-oriented values describe values related to the duties of the civil servant vis-à-vis the government. Service-oriented values reflect the responsibility of the civil servant to provide high-quality service to citizens as customers of public administration. Socially oriented values exhibit a broader set of social goods. The resulting typology can be mapped with other syntheses of public values in e-government. For instance, Rose et al. (2015) highlight the ideals of professionalism, efficiency, service, and engagement. The ideal of professionalism builds on traditional bureaucratic values, also called 'foundational values' (Dobel, 2007), which are firmly established in democratic Western countries. Values of the professionalism ideal combine Bannister et al.'s (2014) socially and duty-oriented values. The efficiency ideal (Rose et al., 2015) draws on private sector management practice and shares similarities with industry-oriented and entrepreneurial governance approaches, such as NPM. It aims to encourage responsible spending of public resources and aligns with Bannister et al.'s service-oriented values. The service ideal follows a similar goal but takes a less market-oriented approach. Instead, it focuses on improving government services for citizens. Finally, the engagement ideal, which builds on Bannister et al.'s (2014) socially oriented values, highlights the involvement of citizens to strengthen a democratic approach to policy development.

Bannister et al.'s (2014) framework was updated as a result of changes to the government-citizens relationship through user-centric digitization (Weigl et al., 2022). The current study builds on a refined version of the extended public values typology by Weigl et al. (ibid.), specifically focusing on public values relevant for user-centricity in e-Government projects.

Table 1. Extended taxonomy of public values for user-centricity (based on Bannister et al. 2014 and Weigl et al. 2022). * Marks the public values that we additionally identified in our systematic review.

Duty-oriented	**Service-oriented**	**Socially oriented**
Responsibility to the citizen / political neutrality*	Service to the citizen in his or her different roles	Inclusiveness
Compliance with the law	Respect for the individual	Justice
Efficient use of public funds	Responsiveness / proactivity* / flexible service delivery	Fairness / equity*
Facilitating the democratic will	Effectiveness	Equality of treatment and access
Accountability to government	Efficiency	Respect for the citizen
Economy of public funds	Transparency	Due process
Rectitude	Productivity	Protecting citizen privacy
Legitimacy	Innovation	Protecting citizens from exploitation
Representation of citizens' will and needs		Protecting citizen security
Sustainability*		Accountability to the public
		Consultation / participation* / engagement*
		Impartiality
		Pluralism / diversity*
		Trust / confidence* / reliability*

2.3.Conflict literature

Public values, like the ones identified and catalogued by Bannister et al. (2014), are pervasive in public administration. Although largely invisible in daily practice, they shape the core of organizational behavior and routines. What is commonly referred to as organizational culture, comprises “a pattern or system of beliefs, values, and behavioral norms” (Schein, 2016, p. 88) that operate out of conscious awareness. They often materialize in the form of cultural artifacts like norms and practices (Leidner & Kayworth, 2006; Schein, 2016). As the organizational sociologist Lynne Zucker (1977) put it, “once institutionalized, [organizational culture] exists as a fact, as a part of objective reality” (p. 726). This renders organizational culture largely uncontested if not confronted with impulses from outside of the organizational context (Canato et al., 2013).

Organizational culture is particularly challenged in the context of public administration, where a push for more ‘user democracy’ and ‘user-centricity’ introduces change (de Graaf et al., 2014) through processes adaptation and the adoption of IT (Sevaldson, 2018; van Velsen et al., 2009a). Many novel IT emphasize values conveyed by the concept of user-centricity, which often clash with established organizational values (de Graaf et al., 2014). Such conflicts between the adopted technology and organizational culture are commonly called cultural dissonance (Canato et al., 2013; Leidner & Kayworth, 2006).

However, value conflicts surrounding user-centricity do not only pertain to conflicts between IT-transferred/IT-inherent and organizational values. They can be a natural by-product of the value-laden exogenous political landscape (Aschhoff & Vogel, 2018; de Graaf et al., 2014). The resulting value pluralism leads to some values being championed over others, especially when values appear incompatible (Andersen et al., 2013; Spicer, 2001). Incompatibilities occur in connection with six central dimensions that are “neither […] superior to the other, nor are they equal in value" (Lukes, 1989, p. 125): (1) the purpose and role of government, (2) societal trends, (3) changing technologies, (4) information management, (5) human elements, and (6) interaction and complexity (Dawes, 2009, 2010). The first dimension focuses primarily on the definition of appropriate legal frameworks and performance evaluation methods to better distribute governmental responsibilities. Conflicts often occur between accountability, responsibility, transparency, stewardship, efficiency, effectiveness, and stakeholder values. The second conflict dimension involves demographic variables, such as economic background, ethnicity, and age, that greatly influence participation, the digital divide, and distributive social justice. Possibilities and risks tied to the implementation of novel IT characterize the third conflict dimension. The fourth dimension covers management issues ranging from quality assurance and the accuracy of information to accessibility and usability. The fifth conflict dimension elaborates on the human element, particularly the readiness for change and relevant skills. Finally, the sixth conflict dimension focuses on interaction and complexity, bringing together a cluster of elements that cross the technical, organizational, institutional and personal boundaries. 'Cross-boundary interactions', such as interoperability, collaboration, and cooperation, are particularly important because they rely on complex communication, management and governance dynamics (Dawes, 2009).

Value conflicts in public governance have already been researched extensively (Aschhoff & Vogel, 2018; Costa et al., 2016; de Graaf et al., 2014; Jørgensen & Bozeman, 2007; Nabatchi, 2017; Thacher & Rein, 2004; Ventriss et al., 2019). Yet, research often does not comprehensively address contradictions between established public values and IT-driven, emerging governance approaches like user-centricity. With increasing digitization of governments, this gap needs to be closed to avoid stalemates in public policy-making and to achieve normative consensus (Vogel, 2018). More specifically, it is important to understand interactions between established democratic values and IT-based contemporary governance paradigms to establish feasible compromises. The relevance of this research becomes particularly apparent as new technologies, such as surveillance tools, blockchain, and AI, attract decision-makers' attention, and challenge established public values and democratic norms.

3. Research approach

To uncover dominant value conflicts between public values and values championed or introduced by user-centricity, and their conflict sources, we conduct a qualitative systematic literature review (Templier & Pare, 2018). This method helps us to systematically synthesize existing knowledge on public values in the context of user-centricity from different disciplines. At the same time, it enables us to understand the interplay between public values and prominent values of user-centricity. Since we primarily focus on academic literature, we may not capture current value conflicts that may have occurred in grey literature, industry reports, or case studies. Yet, many of our analyzed papers draw on practical examples so that we catch the most discussed value conflicts in e-Government.

We follow a five-step systematic literature review approach focused on concepts as defined by Kitchenham (2004). We chose this concept-centric perspective over narrative, critical or realist approaches (Paré et al., 2015) to ensure replicability, rigor, and objectivity of the review process (Boell & Cecez-Kecmanovic, 2015). Concept-centricity also enabled us to focus specifically on public values in the context of user-centricity and not the overall public value discourse. Kitchenham's (2004) describes five distinct steps: (1) study identification, (2) study selection, (3) study relevance and quality assessment, (4) data extraction, and (5) data synthesis. For step three, we used the Preferred Reporting Items for Systematic Reviews and

Meta-Analyses (PRISMA) protocol by Moher et al. (2009). Moreover, we included a snowball sampling step to saturate our data set to the best of our knowledge (Webster & Watson, 2002). The following subsections provide a more comprehensive overview of how we applied Kitchenham's (2004) five steps.

3.1.Study identification

We conducted a keyword search (see Table 2) across five databases (IEEE Xplore, ScienceDirect, SAGE Journals, SCOPUS, and Taylor and Francis). We used speech and spelling variants of our key concepts, such as "user-centricity", "user-centric", "user centric" and "user-centered", or "eGovernment" and "e-Government" to avoid language bias. We also determined inclusion and exclusion criteria for our literature search according to discipline, topics, publication type, language and publication year (see Table 3).

Table 2. Search strings for the systematic literature review.

#	Search String						
A	"User-centricity"	AND	"Government"	OR	"Public sector"	OR	"Public administration"
B	"Citizen-centricity"	AND	"Government"	OR	"Public sector"	OR	"Public administration"
C	"Values"	AND	"e-Government"	OR	"Digital government"	OR	"Digital transformation"

As indicated in Table 3, we targeted publications from various disciplines. We avoided research on the early stages of e-Government, which mainly explored the design of government portals and websites, by including only articles published in 2012 or later. We collected the initial data until February 2022. During the writing process of our paper, we conducted another data collection iteration to include recent publications. The last search was conducted in January 2023.

Table 3. Literature search selection criteria. * Marks the criteria that had to be re-applied in the title and abstract selection procedure.

	Inclusion criteria	Exclusion criteria
Discipline*	Information Systems Library and Information Science Public Administration Economics and Sociology Public Policy Business, Management and Accounting Marketing and Sales	Engineering Computer Science and Security Mathematics Natural and Life Sciences
Topics*	User-centricity; citizen-centricity; e-Government; emerging technologies; public values	Architecture; systems, government portals and websites; social media; survey studies from 2012 or before; value creation
Publication type	Book chapters Peer reviewed articles Doctoral theses Conference articles	Books Bachelor or Master theses
Language	English	Non-English
Publication year	2012 – 2023	Articles published before 2012

3.2.Study selection

For the second step of Kitchenham's (2004) approach, we used the PRISMA protocol by Moher et al. (2009) in combination with the citation-chaining approach recommended by Webster and Watson (2002) (Figure 1). PRISMA follows four steps – (1) identification, (2) screening, (3) eligibility, and (4) inclusion. During the identification stage, we collected 7,168 potentially relevant scientific contributions after removing duplicates and books[2]. All identified literature was exported into the bibliographic reference manager Zotero. In the second phase, two authors independently screened the various papers based on a thorough assessment of their titles and narrowed the selection to 228 articles. The authors first presented their selection to each other and compared their results. After thorough discussion, only

[2] The search operators were usually applied to full text and metadata. However, in cases where our search yielded more than 700 publication results, we restricted the search fields to key words, abstract or introduction, depending on the available filters of each database.

studies selected by both authors were considered for closer examination. During this exclusion procedure, we re-applied our pre-defined search selection criteria (Table 3)[3]. In a sub-step of the screening phase, the two authors discussed selected publications based on their abstracts, which reduced the selection to 158 articles. In a further refinement exercise, we grouped the 158 articles according to the timeliness of their data and central foci (Kitchenham, 2004). After the exclusion of an additional 24 publications, we retained overall 134 articles. The excluded publications presented cases of digital transformation that we considered outdated or did not focus on technologies in the public sector. Examples include studies that analyzed social media, as well as studies with survey data from before 2012, or non-English publications. When retrieving full-text articles, eight papers were inaccessible, which reduced our number of studies to 126.

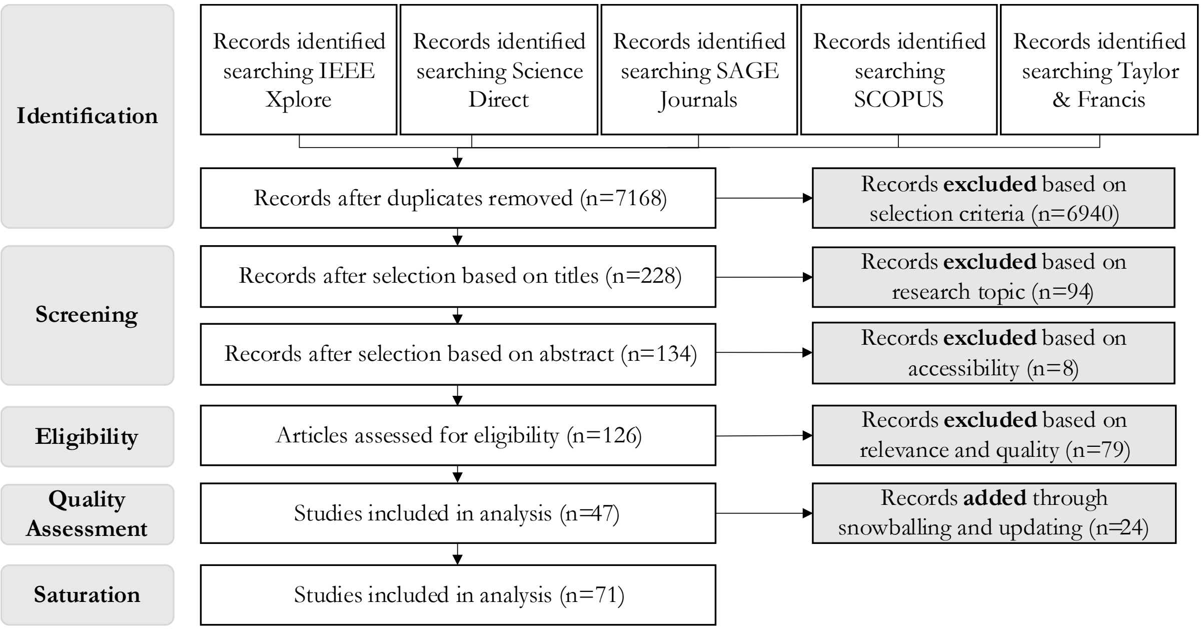

Identification
Records identified searching IEEE Xplore
Records identified searching Science Direct
Records identified searching SAGE Journals
Records identified searching SCOPUS
Records identified searching Taylor & Francis
Records after duplicates removed (n=7168)
Records excluded based on selection criteria (n=6940)
Screening
Records after selection based on titles (n=228)
Records excluded based on research topic (n=94)
Records after selection based on abstract (n=134)
Records excluded based on accessibility (n=8)
Eligibility
Articles assessed for eligibility (n=126)
Records excluded based on relevance and quality (n=79)
Quality Assessment
Studies included in analysis (n=47)
Records added through snowballing and updating (n=24)
Saturation
Studies included in analysis (n=71)

Figure 1. Adapted PRISMA flow diagram (Moher et al. 2009, Kitchenham, 2004; Webster and Watson, 2002)

[3] As the heterogenous search tools of the respective databases also yielded studies which were not related to our key concepts, we had to re-assess the selection criteria manually regarding the topic and discipline of the articles.

3.3.Study relevance and quality assessment

After reading the full papers, 47 out 126 articles were selected for our qualitative analysis. We selected these articles based on their relevance and usefulness in analyzing public values in the context of user-centricity. The quality of the papers is assessed through the articles' citations per year and the journal's impact factor (Coombes and Nicholson 2013). The snowball sampling added another 23 papers to our dataset. The update of our literature review in January 2023 yielded 1 paper that was not included in our literature search from the first cycle. This led to overall 71 papers eligible for qualitative analysis. The complete list of papers can be found in the Appendix.

Our selected papers are evenly distributed between 2012 and 2021. The data collection took place first in 2022 and later in 2023, which might explain the drop in analyzed articles from these 2 years.

Table 4. Number of papers based on their publication year

Year of publication	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**	**2021**	**2022**	**2023**
Number of papers	6	11	7	8	9	3	7	6	4	8	1	1

50 papers were published in peer-reviewed journals, 16 in conference proceedings, and 5 in book chapters. This distribution highlights the overall high-quality level of our selected papers.

Table 5. Number of papers based on their type

Type of article	**Book chapters**	**Conference articles**	**Peer-reviewed journal articles**
Number of articles	5	16	50

Most articles were based on qualitative approaches, but 15 followed quantitative methods, and 7 used a mixed-method approach. Only 3 papers employed a design research method and 2 used formal methods.

Table 6. Number of papers based on the research method used

Research method used	Design research	Formal	Mixed	Qualitative	Quantitative
Number of articles	3	2	7	44	15

Our selected papers covered a wide geographic range, with a satisfying mix of local, regional and worldwide foci. All continents were represented, which not only highlights the topic's relevance but also confirms our methodological rigor. For more details, the table below provides a holistic summary. The number of papers, however, is not absolute since some studies had several countries as focal points. Where studies covered too many countries or were not specific enough, we listed them for the bigger geographical delimitation, i.e., Europe or Worldwide.

Table 7. Number of papers based on the origin of their data or focus of their analysis

Data origin / analysis focus	Number of articles
Australia	1
Canada	2
Denmark	1
Egypt	1
Europe	3
Finland	3
France	1
Germany	3
Greece	1
Hong Kong	1
India	6
Iran	1
Jordan	1
Kazakhstan	1
Mexico	3
Namibia	1
Netherlands	3

New Zealand	1
Norway	1
Peru	1
Qatar	1
Rwanda	1
Singapore	1
Taiwan	1
Tanzania	1
Thailand	1
Turkey	1
UAE	1
Uganda	1
United Kingdom	1
United States	5
Worldwide	29

3.4.Data extraction

We have already extracted the metadata from our literature while selecting studies using a spreadsheet. This helped us skim through titles and abstracts. Once the final set of literature was determined, the 71 downloaded articles were imported to MAXQDA, the software program used for our analysis (Mayring, 2014; Rädiker & Kuckartz, 2018).

3.5.Data synthesis

We performed a qualitative document analysis to synthesize and analyze our data. We manually coded 71 papers in two separate coding teams following a three-stage coding process (Figure 2) of inductive and deductive coding (Saldaña, 2021). We began with open, inductive coding to identify general principles of user-centricity, which we define as first-order concepts (Gioia et al., 2012) in our literature. In a second axial coding cycle, we coded deductively by referring back to the three user-centricity dimensions and the public value framework by Bannister et al. (2014). During this second coding process, we re-grouped and allocated, where possible, some of the codes from the first cycle into given dimensions and emerging framework, i.e., second-order themes (Gioia et al., 2012).

This process led to 5,369 coded segments. To identify conflicts between public values and user-centricity as well as their context, we inductively re-analyzed the coded statements in a third cycle. During this third coding round, we summarized and aggregated our findings to identify the most salient conflict areas. The aggregation of our findings reduced the total number of coded segments to 5,070 (Miles et al., 2014). In a repetition of the third cycle, we synthesized our set of codes by refining and reducing it to the most critical and useful concepts and categories. This cut the number of coded segments to 2,504.

We performed a code relation analysis followed by a qualitative content analysis to identify the most dominant conflicts between user-centricity characteristics and public values (Mayring, 2014). The code relation analysis helped us observe co-occurrences in close proximity (in the same paragraph, for example) between codes that were assigned to one of the two main concepts. An additional qualitative coding query allowed us to investigate which co-occurrences indicate conflicts between established public values and values introduced or championed by user-centricity. Once we identified our main conflicts, two coders bilaterally discussed the allocated codes to contextualize dominant value conflicts.

This contextualization required a more abductive approach to identify concrete conflict sources as influencing factors. Abductive analysis typically "involves a recursive process of double-fitting data and theories" (Timmermans & Tavory, 2012, p .179). That is, the author team met and discussed the coded segments that indicated a conflict source. We focused on recurring themes in different contexts across several of our analyzed papers. Our 'revisiting of the phenomenon' (Timmermans & Tavory, 2012) helped us discern the most salient conflict sources in our coded segments. Close observation of potential conflict sources also spurred 'defamiliarization', i.e., identifying "objects that were relegated to the background of our experience, as they were too taken for granted to be given a second thought" (Timmermans & Tavory, 2012, p .177) Since many public values are a natural part of our status quo, they are difficult to identify even in a conflict situation. By deconstructing the status quo, we could alienate ourselves from the familiar and observe the causes of emerging conflict patterns. Our knowledge of relevant papers and theories in public administration, in addition to the occurrence of the same conflict sources across different cases, helped us to facilitate 'alternate casing' (Timmermans & Tavory, 2012) and discern our third-order codes. These codes indicated important insights behind the emergence of conflicting values and user-centricity characteristics in e-Government. We also repeatedly met to interpret the interplay between existing theories and their surfacing third-order codes. This included discussions about the differences and overlaps between our second-order themes and the aggregate dimensions (Gioia et al., 2012) until we reached an overall consensus.

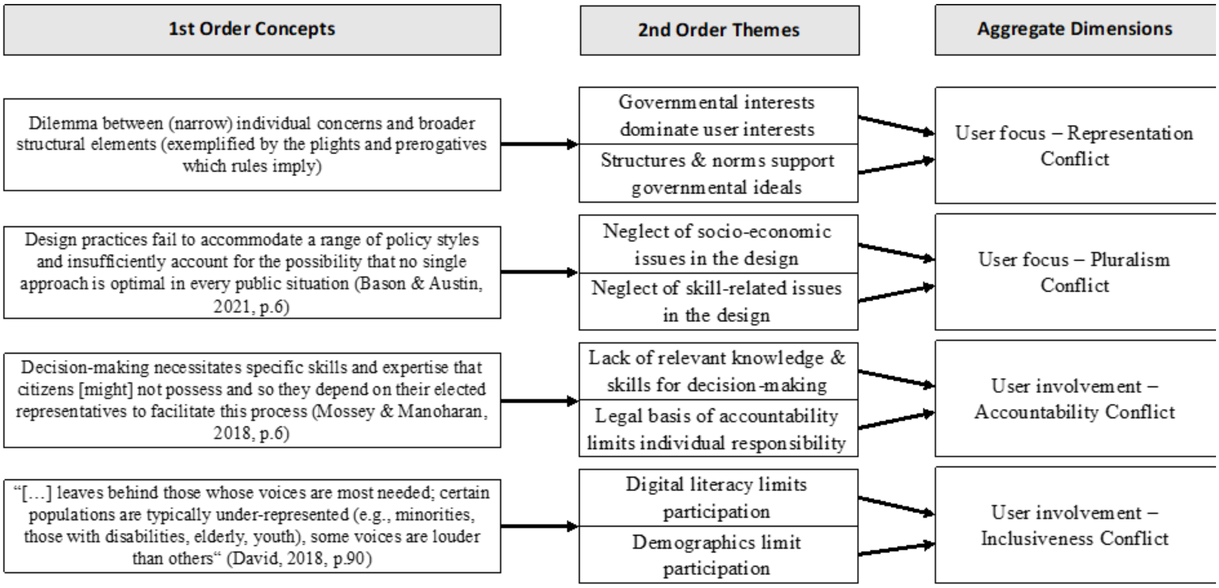

1st Order Concepts
2nd Order Themes
Aggregate Dimensions
Dilemma between (narrow) individual concerns and broader structural elements (exemplified by the plights and prerogatives which rules imply)
Governmental interests dominate user interests
Structures & norms support governmental ideals
User focus – Representation Conflict
Design practices fail to accommodate a range of policy styles and insufficiently account for the possibility that no single approach is optimal in every public situation (Bason & Austin, 2021, p.6)
Neglect of socio-economic issues in the design
Neglect of skill-related issues in the design
User focus – Pluralism Conflict
Decision-making necessitates specific skills and expertise that citizens [might] not possess and so they depend on their elected representatives to facilitate this process (Mossey & Manoharan, 2018, p.6)
Lack of relevant knowledge & skills for decision-making
Legal basis of accountability limits individual responsibility
User involvement – Accountability Conflict
"[…] leaves behind those whose voices are most needed; certain populations are typically under-represented (e.g., minorities, those with disabilities, elderly, youth), some voices are louder than others" (David, 2018, p.90)
Digital literacy limits participation
Demographics limit participation
User involvement – Inclusiveness Conflict

Figure 2. Conflicts between public values in the context of user-centric e-Government approaches.

4. Value conflicts and their causes

Our abductive coding helped us contextualize the dominant conflicts and identify the most plausible conflict sources by revisiting possible conflict sources in different contexts and actively deconstructing our own taken-for-granted status quo. This "iterative dialogue […] between data and an amalgam of existing and new conceptualizations" of value conflicts in e-Government, allowed us to "cull […] and narrow […] possible theoretical leads" (Timmermans & Tavory, 2012, p. 180). More specifically, the revisiting of similar value conflicts and the defamiliarization of the public value context showed that not all identified conflicts in literature have their roots in values of user-centricity. It is rather the *implementation* of user-centric systems and services that introduces new and highlights specific public values over others. Alternate casing with different theories that pinpoint value deficiencies in either the user-centric system or the environment showed that the source of conflict is not the presence or absence of a certain public value, but value pluralism. Value pluralism occurs when several values are relevant but not equally prioritized. The simultaneous fulfillment of particular or multiple public values automatically (sometimes unintentionally) sacrifices or diminishes other non-negotiable public values, which leads to value conflicts. We specifically identified conflicts between established public values and values introduced or championed by user-centricity.

In this section, we elaborate on the abductive analysis of the value conflicts that have been identified between the user-centricity dimensions and public values in e-Government. Since many user-centric values appear naturally aligned with values in public administration, many conflicts were unexpected. Overall, we found four dominant conflicts (see Table 8): (1) a user focus-representation conflict based on the assumption that citizens and governments have diverging interests and needs; (2) a user focus-pluralism conflict, which posits that users are not automatically the target group of young, educated, and technology-conscious people; (3) a user involvement-accountability conflict that contrasts the compatibility of active citizen participation with the accountability of public officials; (4) a user involvement-inclusiveness conflict that illustrates the selective representation of citizens through digital channels. After identifying the four dominant conflicts from the literature, we wanted to better understand their embeddedness in their specific context and identify potential causal links. Revisiting these conflicts and sources provided the ground for a deeper, more nuanced discussion among the author team. During the subsequent defamiliarization phase, we aimed to find plausible explanations and sources from which the identified conflicts materialized by deconstructing the moral foundations of the conflict environment. Moreover, we iterated our emerging conflict sources with existing theories in public administration. This alternate casing allowed for a more holistic analysis of the possible conflict sources and helped us add nuance while ensuring a relevant degree of generalization (Timmermans & Tavory, 2012). In total, five conflict sources emerged (see Table 8): (1) the decision-dominance issue that encumbers decision-making processes due to power and information asymmetries; (2) the degree of participation issue that raises the question how citizens can and want to participate in collaborative design; (3) the resource deficit issue that refers to knowledge, literacy, and financial gaps; (4) the establishment-innovation issue that contrasts established organizational structures in public administration with organizational flexibility needed enable technological innovation; (5) the multistakeholder issue emerges from the challenge of uniting various stakeholder interests from governmental, industry and civic sector at regional or national level.

Table 8. Summary of value conflicts and conflict sources identified in the literature.

Value conflict	Conflict dynamic
User focus-representation	Citizens and governments have diverging interests and needs. Due to this divergence, governments cannot represent users' needs to the extent prescribed by user-centricity.

User focus-pluralism	The implementation of a user-centric technology can face the possibility that no single approach is optimal in every public situation in a pluralistic society that tolerates and supports diversity.
User involvement-accountability	Incompatibility between the active participation of citizens on the one hand, and the accountability of public officials at the government level on the other.
User involvement-inclusiveness	Inclusiveness in the collaborative design stage might be impaired due to citizens involvement through online channels and platforms.

Conflict source	**Conflict source dynamic**
Decision-making dominance	Pertains to the power imbalance between experienced decision-makers (facilitators, experts, community members) and other involved stakeholders, such as IT professionals and research consultants. In case of doubt, decision-makers can overrule suggestions and prioritize their desired values in the system's design choices. Consequentially, decision-makers can countermand findings from user research and/or user-centric design approaches.
Degree of participation	Pertains to the extent to which citizens can arguably be involved in collaborative design. Oftentimes, the diverging interests of different social groups cannot be equally respected in a consolidated system design. Thus, due to a lack of resources, individual citizens can only participate up to a certain degree. In other words, some voices are not heard because the people who would express them lack the resources, including knowledge and awareness, or their participation is not sufficiently effective.
Resource deficit	Refers to two main elements: (1) The lack of technical information and digital literacy among the providers or recipients of digitized public services in an information society that relies on continuous learning, and technological knowledge. (2) Lacking financial means to be able to acquire the necessary devices or access to a network in order to make use of a digital service, and non-existent infrastructure, which hampers connection and thereby access to public services provided through digital channels.
Establishment-innovation issue	Results from novelty-averse, hierarchical and bureaucratic structures, as well as budgetary constraints in the public sector, and the dynamic, risk tolerant and agile nature of innovation. Service providers governance structure and cultures are thus too slow and stiff to embrace the fast and iterative methods required for user-centricity
Multistakeholder issue	Stems from problems arising from multistakeholder governance in which many, possibly conflicting interests are incorporated in the dialogue, decision-making, design and implementation. Simply put, within a service provider organization, different groups have conflicting interests that must be accounted for. User-centric design is overlapping with co-design or participatory design. This does not only refer to the involvement of users, but also to the representation of different stakeholders, such as the government itself, consulting experts, and citizens. Therefore, governments face complexities when trying to integrate users into the design of digital services. The multistakeholder issue also involves risks undermining the participatory nature of the user-centric ideal due to public mind manipulation by lobby groups if such co-design processes are not overseen properly.

Since our findings reported in relation to the co-occurrence of conflicts and conflict sources emerged during an abductive analysis, we cannot speak of statistical causation or correlation. Whenever we refer to some of these contextual factors as *conflict sources*, we intend to provide a theory (Timmermans & Tavory, 2012) for the identified conflicts from a qualitative abductive point of view.

The table below displays the level of co-occurrence between conflicts and their sources based on our systematic literature review and subsequent abductive analysis. A detailed list of articles at the intersection of these concepts can be found in the Appendix in Table 11.

Table 9. Co-occurrence between conflicts and their sources

Conflict source \ **Conflict**	User focus-representation	User focus-pluralism	User involvement-accountability	User involvement-inclusiveness
Decision-making Dominance	**High**	*None*	**High**	Low
Degree of Participation	Low	Low	Low	**High**
Resource Deficit	Low	**High**	Low	**High**
Establishment-Innovation	Low	**High**	**High**	Low
Multistakeholder	**High**	Low	Low	*None*

4.1. User focus-representation conflict

The *user focus-representation conflict* describes the divergent interests and needs of citizens and governments that culminate in the governments' inability to represent users' needs compatible with principles of user-centricity (Berg et al., 2021; Clark, 2021; de Graaf et al., 2014; Grube, 2013; Ingrams, 2019; Kassen, 2021; Kotamraju & van der Geest, 2012; Kyakulumbye et al., 2019; Miniaoui et al., 2020; Mossey et al., 2018; Nabatchi, 2012; Park & Humphry, 2019; Sigwejo & Pather, 2016; Sorn-in et al., 2015). Central to this claim are three main issues.

Firstly, governments typically focus on accountability as defined by law or on "fulfilling […] requirements rather than trying to understand the needs of their users" (Kotamraju & van der Geest, 2012, p. 1; Kyakulumbye et al., 2019; Miniaoui et al., 2020; Sorn-in et al., 2015). The narrow definition of accountability binds them to specific legally defined standards, which can result in a "dilemma between […] individual concerns and broader structural elements (exemplified by the plights and prerogatives which rules imply)" (de Graaf et al., 2014, p. 17; Grube, 2013). This dilemma is particularly highlighted in implementations of user-centricity where infamously complex and inflexible bureaucratic procedures prove difficult to align with users' preferences, such as simplicity, efficiency and anonymity. Such misalignment with user needs appears to stand in the way of more user-centric e-Governments that desire "serious, long-term committed relationships with their citizens and inhabitants. [U]sers, on the other hand, particularly when they are in information-seeking mode, want a quick foray into e-Government" and consider complex processes and long wait times tedious (Kotamraju & van der Geest, 2012, p. 11). These conflicting visions of a productive citizen-government relationship encumber a further integration of user-centric values into the design of e-Governments (ibid.).

Secondly, even in less bureaucratic structures, service designers are "generally unaware of how their values influence the ability to achieve desired values of public participation, such as legitimacy, justice, and effective administration" (Clark, 2021, p. 5; Ingrams, 2019; Kotamraju & van der Geest, 2012; Sorn-in et al., 2015). They typically "choose to downplay the normative element of e-Government and […] design and develop services based on their ideal, rather than the actual relationship between governments and citizens. [This naturally] has adverse consequences for e-Government's user-centricity and, ultimately, its adoption and use" (Kotamraju & van der Geest, 2012, p. 3). Socio-technical dynamics of technology adoption and integration into social systems and processes are particularly affected. They are typically "inscribed with the rules, values and interests of typically dominant groups" (Park & Humphry, 2019, p. 935).

Thirdly, it is difficult to ensure that the quality, validity and representation of such multidimensional public opinion and user-generated data is not contested (Berg et al., 2021, p.

232; Kassen, 2021; Kotamraju & van der Geest, 2012; Mossey et al., 2018; Nabatchi, 2012; Park & Humphry, 2019). Dominant decision-making, i.e., "where the individual will [is] superseded by the collective will" (Grube, 2013, p. 2) is the underlying conflict source in observed *user focus-representation conflicts.* It appears to be rooted in the challenges arising from increasing multistakeholder dynamics of user-centricity implementation, and the negligence of minority opinions in user-centric e-Government designs.

4.2. User focus-pluralism conflict

The second critical conflict is the so-called *user focus-pluralism conflict* (Aschhoff & Vogel, 2018; Bason & Austin, 2022; Berg et al., 2021; Bokayev et al., 2021; Brown, 2021; Cordella & Bonina, 2012; de Graaf et al., 2014; Gupta, Bhaskar, et al., 2016; Gupta et al., 2018; Gupta, Singh, et al., 2016; Kotamraju & van der Geest, 2012; Larsson, 2020; Madan & Ashok, 2022; Mariën & Amon Prodnik, 2014; Park & Humphry, 2019; Scott et al., 2016). Here, pluralism does not refer to classical pluralism in political decision-making theory but relates to a pluralistic society that tolerates and supports diversity. The strong focus on technology in user-centric e-Government approaches may jeopardize pluralism if primarily young, educated, affluent, and technology-conscious people can use the system (Aschhoff & Vogel, 2018; Berg et al., 2021; Bokayev et al., 2021; Brown, 2021; de Graaf et al., 2014; Gupta et al., 2018; Kotamraju & van der Geest, 2012). Design practices without the conscious integration of pluralism and different policy styles would counter user-centric ideals to equally include all members of society (Bason & Austin, 2022, p. 6; Cordella & Bonina, 2012; Park & Humphry, 2019).

At the same time, it is recommended "not to design for a very specific nonrepresentative target group or task" (Kotamraju & van der Geest, 2012, p. 8) since such a narrow focus can be costly and inefficient even in user-centric designs. “Good practice demands that design […] supports […] the most commonly performed tasks or requests, for the largest or most important target groups” (Aschhoff & Vogel, 2018; Kotamraju & van der Geest, 2012, p. 8). Thus, “social challenges such as language barriers, low digital literacy, low user-friendliness of government websites, inability to access internet and lack of awareness in citizens” should be tackled before shifting to public service formats that are only available to a select few (Gupta, Singh, et al., 2016, p. 162). Digitally less literate citizens, or people with restricted access to technological devices and connectivity cannot be passed over. Dismissing their needs is morally questionable and would “disproportionally affect citizens with low socio-economic status and demographic groups already suffering from other types of discrimination” (Gupta et al., 2018; Larsson, 2020, p. 2; Mariën & Amon Prodnik, 2014; Park & Humphry, 2019).

The establishment-innovation issue and resource deficits explain the existence and saliency of this conflict in user-centric approaches (Aschhoff & Vogel, 2018; Bason & Austin, 2022; de Graaf et al., 2014; Grube, 2013). Different from private services, government services need to be relevant and available for all (Kotamraju & van der Geest, 2012). This is a complex endeavor and “runs counter to user-centricity” (ibid, p. 11). At the same time, governments cannot let their digital transformation be driven by market logic. Such logic would risk enforcing socio-economic discrimination and goes against public values of impartiality and equality. Kotamraju et al. (2012, p.8) describe the establishment-innovation issue by summarizing some of the key challenges in user-centered designs for e-Government: (1) users and governments hold contradicting visions of a task, (2) governments cannot choose the audience to which their services should be tailored, (3) users and governments have different commitments to legal rules and regulations, while (4) both have different desires about the nature of their relationship. Governments typically strive for a long-term and proactive relationship with their citizens, while users prefer a transactional relationship with their public service providers.

4.3. User involvement-accountability conflict

In the *user involvement-accountability conflict*, literature questioned the compatibility between the active participation of citizens in digital services design as envisioned by user-centric e-Government and the required accountability for public officials (Aschhoff & Vogel, 2018; Bason & Austin, 2022; Berg et al., 2021; de Graaf et al., 2014; Ghosh Roy & Upadhyay, 2017; Grube, 2013; Ingrams, 2019; König, 2021; Kotamraju & van der Geest, 2012; Mossey et al., 2018). The ideal of user involvement, typically highlighted in the context of user-centricity, encompasses the "tradition of participatory democracy […], including […] user democracy, listening to public opinion, and dialogue" (Aschhoff & Vogel, 2018, p. 10). Professional accountability, or what Bannister et al. (2014) term 'accountability to government', entails the "compliance of public managers with professional standards and formal rules and regulations" (Aschhoff & Vogel, 2018, p. 10; Kotamraju & van der Geest, 2012). Even if forced into user-centric approaches, these values are difficult to reconcile and often result in two conflicts.

First, public servants must comply with a complex set of standards and rules that citizens are unaware of (Aschhoff & Vogel, 2018; de Graaf et al., 2014; Grube, 2013; Kotamraju & van der Geest, 2012). These standards and rules limit citizen involvement to areas that do not require tight regulation. Thus, "all […] proactiveness of citizens and end users may be of little use or even get nullified" where they would be legally accountable for their involvement (Ghosh Roy & Upadhyay, 2017, p. 76). Bason and Austin (2022) further contrast this *classical* ‘accountability’ approach, which values ‘scientific-ness’ and fair outcomes, with *human-centered* (here user-centered) approaches, which propagate user empowerment. They argue that human-centered designs fail to sufficiently account for several requirements of public sector design, such as capacity constraints, different policy styles, and the reality of policy mixes (Bason & Austin, 2022).

Secondly, representative theory suggests that “decision-making necessitates specific skills and expertise that citizens [might] not possess” (Berg et al., 2021; Grube, 2013; Mossey et al., 2018, p. 6). Despite the desirability of citizen participation in user-centric e-Government designs, there are risks that strong user involvement may swing “the pendulum […] too far from the rightly criticized technocratic vision of a smart city” (König, 2021, p. 6).

Power dynamics between decision-makers and stakeholders may further exacerbate the *user involvement-accountability conflict*. Government officials can overrule external stakeholder decisions that would not comply with regulations to ensure fairness and avoid arbitrary rulings. Yet, this power dynamic already foreshadows the establishment-innovation conflict, in which governmental structures determine to what extent user-centricity can be reconciled with existing hierarchies.

4.4. User involvement-inclusiveness conflict

User-centricity foresees the involvement of citizens in the design stage primarily online, which impairs inclusivity (Berg et al., 2021; Clark, 2021; David, 2018; Kassen, 2021; König, 2021; Kotamraju & van der Geest, 2012; Mariën & Amon Prodnik, 2014; Park & Humphry, 2019). This infringement manifests in a *user involvement-inclusiveness conflict*. Citizen involvement “often leaves behind those whose voices are most needed [as it] it takes time, patience, and resources [as well as specifically trained] administrators and decision makers

[…] to deal with citizens" (David, 2018, p. 90). For example, digitally less literate citizens may face neglect in participatory e-Government initiatives (Kassen, 2021; König, 2021; Mariën & Amon Prodnik, 2014; Park & Humphry, 2019). Yet, this conflict does not only unilaterally emerge from the physical, financial, educational, or other socio-economic obstacles and barriers citizens might encounter. A focus on user involvement can further "[affect] inclusiveness, since deliberation can be a demanding form of participation" (Berg et al., 2021, p. 233), and "might reinforce existing inequalities in political participation" (ibid.; König, 2021; Mariën & Amon Prodnik, 2014; Park & Humphry, 2019).

The degree of participation in user-centric designs, therefore, has a strong influence on the *user involvement-inclusiveness conflict.* User involvement and citizen engagement are often "neither realistic nor necessary" even if digital channels were available for all (König, 2021, p. 6). Participating citizens typically have the relevant knowledge and skills to interact with government technology (Berg et al., 2021; Bokayev et al., 2021; David, 2018; Gupta et al., 2018; Gupta, Singh, et al., 2016; Park & Humphry, 2019), and can access their network and financial resources (David, 2018). The latter also often coincides with the readiness to adopt new technologies and ownership of digital devices (Gupta et al., 2018; Larsson, 2020; Mariën & Amon Prodnik, 2014). These characteristics systematically exclude user groups whose voices are already underrepresented in current eGovernment approaches (David, 2018; Mariën & Amon Prodnik, 2014). As such, the dimension of the *user involvement-inclusiveness conflict* shares similarities with *the user focus-pluralism conflict.* Both conflicts exacerbate the marginalization of user groups either at the collaborative design or the application and implementation stage.

5. Discussion and opportunities for further research

Integrating user-centricity into e-Government services is not only a popular design approach, but also a widely recognized and desired requirement (Kujala, 2003; van Velsen et al., 2009b). Our systematic review of the academic literature shows that values introduced or championed by user-centricity designs sometimes conflict with established public values. According to the reviewed and synthesized literature on user-centricity and public values from 2012 to 2023, value conflicts occur in different contexts. Current research shows that they can either be core dynamics of user-centricity, causing a clash between user-centric approaches and public values, or they can occur as a result of user-centric implementations. To further elaborate on why these conflicts arise, we identified conflict sources through an iterative process of abduction in the selected literature. While our analysis provides plausible theories, further research will be required to empirically determine conflict sources or contextual factors and provide mitigation strategies. A potential starting point for empirical research is Dawes' (2009, 2010) six central conflict dimensions. We present how the dimensions may interact in Figure 3.

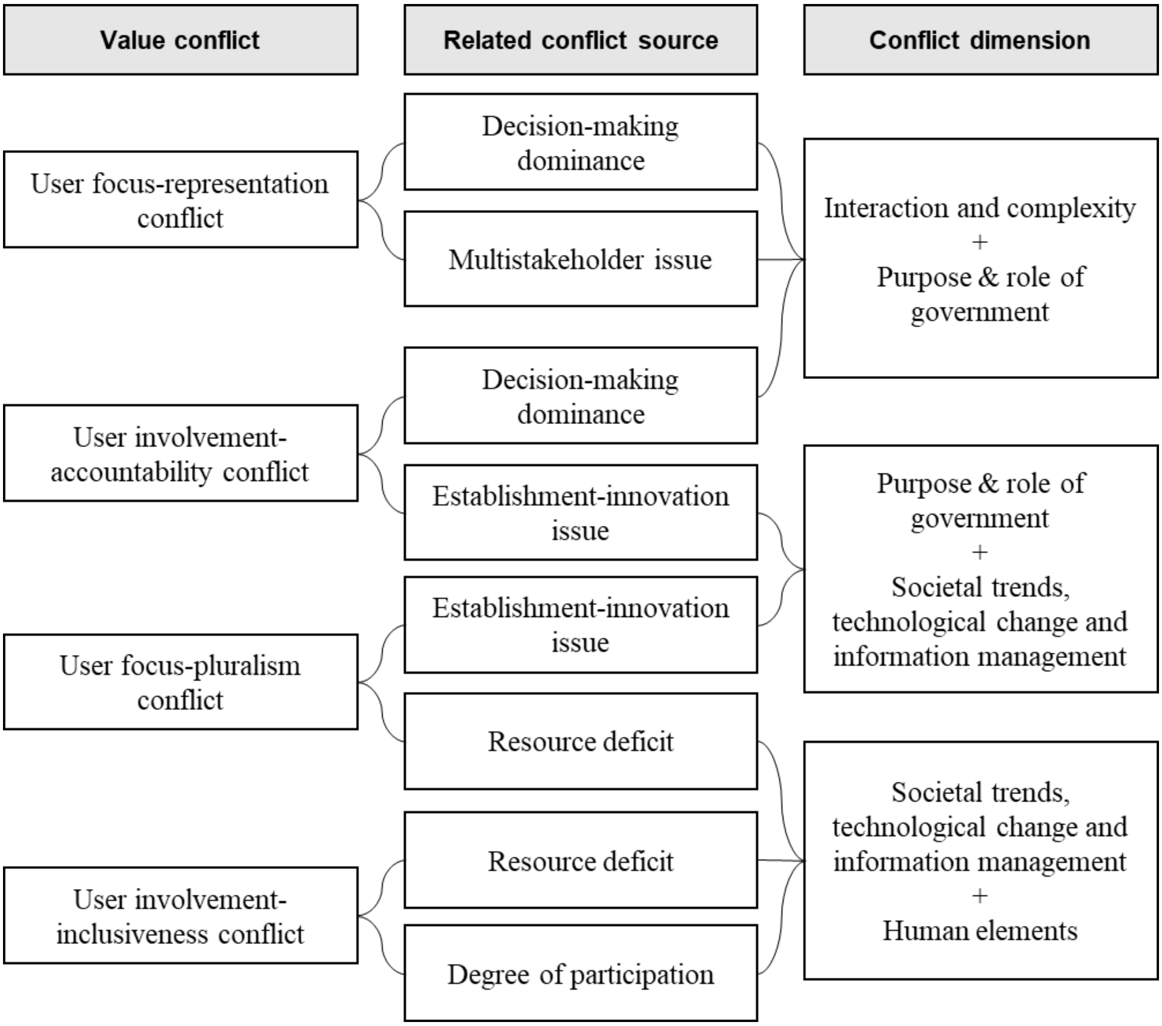

Value conflict
Related conflict source
Conflict dimension
User focus-representation conflict
Decision-making dominance
Multistakeholder issue
Interaction and complexity
+
Purpose & role of government
User involvement-accountability conflict
Decision-making dominance
Establishment-innovation issue
Purpose & role of government
+
Societal trends, technological change and information management
User focus-pluralism conflict
Establishment-innovation issue
Resource deficit
User involvement-inclusiveness conflict
Resource deficit
Degree of participation
Societal trends, technological change and information management
+
Human elements

Figure 3. Embedding public value conflicts in user-centric e-Government, their sources and Dawes' central conflict dimensions (2009, 2010).

In the remainder of the section, we focus only on the most relevant contributions for research and the path forward to furthering our understanding of the dynamics at play. That is, we elaborate on decision-making dominance in the context of user representation (5.1.), and the difficulty of bridging the gap between established government structures and innovation based on user-centric ideals while upholding the principles of government accountability (5.2.). We also touch on the problem of resource deficits to highlight the need for inclusive participation in user-centric e-Government (5.3.). Our research presents a first step in closing the gap of translating values introduced or championed by user-centricity into public policies and service design.

5.1.Decision-making dominance and the representation conflict

The representation of citizens as users is challenging when institutional structures require decision-makers to prioritize certain preferences over others. This raises questions of how user-centric design can ensure that participation is more equally distributed and how government can integrate user-centric values into the delivery of services (Vigoda-Gadot, 2002). Most importantly, research should explore the establishment of normative pluralism and prevent adverse effects for representation through the implementation of user-centric designs. This may also entail investigating if institutional structures would allow for an increased user focus, and if such a focus would yield promised benefits. Due to the involvement of different actors, which challenges the balance between optimal representation and efficient decision-making, we see a substantial overlap with Dawes' (2009) *interaction and complexity dimension*. Moreover, considering the influence of governmental decision-making on this balance warrants a deeper analysis of Dawes' (2009) first dimension – *the purpose and role of government* – concerned with governmental responsibility. Other research has started shedding light on these dynamics and deserves further exploration in this context. For example, the extent to which competent civil society representatives can support the design process and counterbalance unilateral decision-making (Pozzebon et al., 2016; Yang & Pandey, 2011), and their capacity to bring consensus, trustworthiness and legitimacy (OECD, 2022; Porumbescu, 2016).

5.2.Establishment-innovation issue and the accountability conflict

Embedding accountability conflicts in user-centric approaches with the establishment-innovation issue presents a continuation of existing public administration paradigms. Where the NPM approach adopted market logic and private sector management models, the DEG and public value management paradigm emphasize citizen engagement in digital government initiatives and advocate for public values beyond performance-based indicators (Bryson et al., 2014). The latter two thus accommodate key values of user-centricity to a greater extent than NPM. Yet, the accountability conflict shows that it is difficult for such new values to thrive in a highly institutionalized environment. Despite efforts to encourage a more innovative and user-centric mindset in public administration, more research will be required on how the relationship between citizens and public administrations in e-Government can be designed. Drawing on Dawes' (2009) conflict dimensions, we see an overlap with four dimensions: (1) *role and purpose of government*, which encompasses the legal, administrative and bureaucratic processes of the public institutions and their accountability; (2) *changing technologies*, which centers around the implementation of novel IT in institutions and organizations; (3) *information management*, which concerns information quality, accessibility and usability as part of a functioning innovation process; and (4) *societal trends*, which highlights the demographics of society, such as socio-economic status, income, age or education.

Relevant research to better apprehend these complex dynamics includes Fung (2015), who highlights the difficulty for public officials or public service providers to take responsibility for user-driven design choices – especially when users' preferences clash or are not reconcilable with established institutional rules and incentive systems. They suggest that policy-makers need to pay attention to the way they integrate user-centric IT into their interaction with citizens, and consider the "full menu of design choices" available to them

(Fung, 2015; OECD, 2022). The role of specific agencies or ministerial branches – such as GovTech labs – that work at the intersection of public administration and industry has also been researched (Bharosa, 2022). In this context, their capacity to keep the balance between innovation and institutional norms has been highlighted. In fact, multidisciplinary teams encompassing innovative companies, academia and government, with a shared objective for innovating and the relevant budget to reach prototyping stages rapidly, have been suggested to support innovation without sacrificing governmental accountability (Tõnurist et al., 2017). Moreover, the integration of emerging innovations into value-sensitive design principles can ensure ethical alignment and user-centered development (Friedman & Hendry, 2019). This research angle deserves to be further explored so that adequate solutions can be found that strike a balance between fostering experimentation and ensuring responsible innovation.

5.3.Resource deficit and the pluralism and inclusiveness conflict

The conflict contrasts the reality of a diverse society with society's ideal of the digitally literate individual. The inclusiveness conflict with its focus on the pursuit of user engagement and the simultaneous discriminatory exclusion of individuals, is closely related (Mariën & Amon Prodnik, 2014). Both conflicts can be attributed to resource deficits, which encompass a lack of digital skills, a lack of financial resources, and insufficient access to digital infrastructure in rural areas. A lack of awareness among service designers, who are often unaware of inclusiveness challenges or do not know how to address them, can exacerbate the conflict (Bär, 2017). Yet, the much-needed involvement of citizens as stakeholders in the design process is often inhibited by the above-mentioned resource deficits.

Thus, a third path for future research is to analyze the impact of user-centricity on resource-based technological discrimination and exclusion, and on ways to mitigate these effects in practice. Continuing the work of Alomari et al. (2014) at a larger scale, the distinction of the impact in different geographical areas might be particularly interesting to evaluate. This would enable a more nuanced approach to account for different demographics and technological maturity across countries. Further research is also needed to better understand how government measures can impact individual resource deficits. It has been proposed, for instance, that developing digital literacy and digital skills alongside general educational objectives can be an effective means to this end (Choudhary & Bansal, 2022; Méndez-Domínguez et al., 2023). These encompass the deployment of community officers to provide technology advice and support for digital public services (Suchowerska & McCosker, 2022), and investments into better affordability and coverage of digital public infrastructure (Shenglin et al., 2017). Research on the impact of non-digital alternatives as mitigation measures (see e.g., Reddick & Anthopoulos, 2014) also contributes to a better understanding of this challenge. This research can be grounded in four dimensions of Dawes' framework: (1) *changing technologies*; (2) *information management*; (3) *societal trends*; and (4) *human elements*.

6. Conclusion

User-centric principles in e-Government garner support from different governments worldwide that seek to improve their public services. Aimed at benefiting the user, user-centricity is often assumed to naturally complement established public values. Governments typically build on public values to deliver services and interact with citizens. Our study challenges this assumption and deconstructs emerging conflicts between the implementation of values introduced or championed by user-centricity and established public values. We ground our analysis in a systematic literature review of user-centricity in e-Government and gather evidence of value conflicts as well as their underlying sources. Our analysis included more than 7,000 articles from an eleven-year period, out of which we qualitatively coded 71 articles in two separate coding teams. Following this extensive review, we synthesized the knowledge from three different disciplines and identified emerging patterns from individual observations.

We show that user-centricity and public values conflict in four notable areas: the conflict between *user focus* and the citizen *representation* and *pluralism*, and the conflict between *user involvement* and government *accountability* and societal *inclusiveness*. Abductive reasoning helped us discern why these conflicts emerge. We postulate five main influencing factors: the *decision-making dominance issue*, the *degree of participation issue*, the *resource deficit issue*, the *establishment-innovation issue* and the *multistakeholder issue*. The prevalence of these issues within service delivery environments proves that they are not isolated or tangential. Instead, they pose a serious threat to user-centric e-Government service provision success, which warrants further research in the following three areas: the detection of other types of conflicts that were not found in the existing literature; the evidence-based identification of causal relationships between prevalent issues in service delivery environments and these conflicts; and the elaboration and testing of mitigating measures that can alleviate or remove the conflicts themselves, or their outcome.

Our proposed future research also hints at the main limitations of this study. We currently focus primarily on academic literature within particular disciplines and do not consider grey literature, industry reports, or case studies. This selection of specific criteria may bias our analysis. Moreover, expanding the range of sources for analysis could deliver results on emerging conflicts. These results may also support the establishment of causation between conflicts and issues beyond abduction. A more systematic approach to causation may also deliver insights into the nature of our influencing factors. That is, if they are conflict sources, aggravating factors, or have other types of influencing relationships. In addition, our research is limited with regard to deriving practical implications for the public, as the literature analysis focuses on synthesizing existing research rather than prescribing actions or policies. Finally, a systematic literature review is always tied to a pre-defined scope. While our research approaches the concept of user-centricity from a broad angle, thereby increasing the potential for generalization of our findings, it inevitably limits the potential to provide specific recommendations or instructions for practitioners to a specific problem, context, or technology.

7. References

Al-Hujran, O., Al-Debei, M., Chatfield, A., & Migdadu, M. (2015). The imperative of influencing citizen attitude toward e-government adoption and use. *Computers in Human Behavior*, *53*, 189–203. https://doi.org/10.1016/j.chb.2015.06.025

Alomari, M. K., Sandhu, K., & Woods, P. (2014). Exploring citizen perceptions of barriers to e-government adoption in a developing country. *Transforming Government: People, Process and Policy*, *8*(1), 131–150. https://doi.org/10.1108/TG-05-2013-0013

Alzahrani, L., Al-Karaghouli, W., & Weerakkody, V. (2017). Analysing the critical factors influencing trust in e-government adoption from citizens' perspective: A systematic review and a conceptual framework. *International Business Review*, *26*(1), 164–175. Scopus. https://doi.org/10.1016/j.ibusrev.2016.06.004

Andersen, L. B., Jørgensen, T. B., Kjeldsen, A. M., Pedersen, L. H., & Vrangbæk, K. (2013). Public Values and Public Service Motivation: Conceptual and Empirical Relationships. *The American Review of Public Administration*, *43*(3), 292–311. https://doi.org/10.1177/0275074012440031

Aschhoff, N., & Vogel, R. (2018). Value conflicts in co-production: Governing public values in multi-actor settings. *International Journal of Public Sector Management*, *31*(7), 775–793. https://doi.org/10.1108/IJPSM-08-2017-0222

Avgerou, C. (2000). Recognising Alternative Rationalities in the Deployment of Information Systems. *The Electronic Journal of Information Systems in Developing Countries*, *3*(1), 1–15. https://doi.org/10.1002/j.1681-4835.2000.tb00021.x

Bannister, F., & Connolly, R. (2014). ICT, public values and transformative government: A framework and programme for research. *Government Information Quarterly*, *31*(1), 119–128. https://doi.org/10.1016/j.giq.2013.06.002

Bär, F. (2017). *Tackling Knowledge Gaps in Digital Service Delivery*.

Bason, C., & Austin, R. D. (2022). Design in the public sector: Toward a human centred model of public governance. *Public Management Review*, *24*(11), 1727–1757. https://doi.org/10.1080/14719037.2021.1919186

Berg, J., Lindholm, J., & Högväg, J. (2021). How do we know that it works? Designing a digital democratic innovation with the help of user-centered design. *Information Polity*, *26*(3), 221–235. https://doi.org/10.3233/IP-200282

Bhargav-Spantzel, A., Camenisch, J., Gross, T., & Sommer, D. (2006). User centricity: A taxonomy and open issues. *Proceedings of the Second ACM Workshop on Digital Identity Management*, 1–10. https://doi.org/10.1145/1179529.1179531

Bharosa, N. (2022). The rise of GovTech: Trojan horse or blessing in disguise? A research agenda. *Government Information Quarterly*, *39*, 101692. https://doi.org/10.1016/j.giq.2022.101692

Boell, S., & Cecez-Kecmanovic, D. (2015). On being 'Systematic' in Literature Reviews in IS. *Journal of Information Technology*, *30*. https://doi.org/10.1057/jit.2014.26

Bokayev, B., Davletbayeva, Z., Amirova, A., Rysbekova, Z., Torebekova, Z., & Jussupova, G. (2021). *Transforming E-government in Kazakhstan: A Citizen-Centric Approach*. *26*.

Brown, P. R. (2021). Public Value Measurement vs. Public Value Creating Imagination – the Constraining Influence of Old and New Public Management Paradigms. *International Journal of Public Administration*, *44*(10), 808–817. https://doi.org/10.1080/01900692.2021.1903498

Bryson, J. M., Crosby, B. C., & Bloomberg, L. (2014). Public Value Governance: Moving Beyond Traditional Public Administration and the New Public Management. *Public Administration Review*, *74*(4), 445–456. https://doi.org/10.1111/puar.12238

Canato, A., Ravasi, D., & Phillips, N. (2013). Coerced Practice Implementation in Cases of Low Cultural Fit: Cultural Change and Practice Adaptation During the Implementation of Six Sigma at 3M. *The Academy of Management Journal*. https://doi.org/10.5465/amj.2011.0093

Choudhary, H., & Bansal, N. (2022). Addressing Digital Divide through Digital Literacy Training Programs: A Systematic Literature Review. *Digital Education Review*, *41*, 224–248. https://doi.org/10.1344/der.2022.41.224-248

Clark, J. K. (2021). Public Values and Public Participation: A Case of Collaborative Governance of a Planning Process. *The American Review of Public Administration*, *51*(3), 199–212. https://doi.org/10.1177/0275074020956397

Codagnone, C., Misuraca, G., Gineikyte, V., & Barcevicius, E. (2020). Exploring digital government transformation: A literature review. *ICEGOV 2020: 13th International Conference on Theory and Practice of Electronic Governance*, 502–509. Scopus. https://doi.org/10.1145/3428502.3428578

Cordella, A., & Bonina, C. M. (2012). A public value perspective for ICT enabled public sector reforms: A theoretical reflection. *Government Information Quarterly*, *29*(4), 512–520. https://doi.org/10.1016/j.giq.2012.03.004

Costa, A., Caldas, J. C., Coelho, R., Ferreiro, M. de F., & Gonçalves, V. (2016). The Building of a Dam: Value Conflicts in Public Decision-Making. *Environmental Values*, *25*(2), 215–234. https://doi.org/10.3197/096327116X14552114338909

David, N. (2018). Democratizing Government: What We Know About E-Government and Civic Engagement. In *International E-Government Development: Policy, Implementation and Best Practice* (pp. 73–96). https://doi.org/10.1007/978-3-319-63284-1_4

Dawes, S. S. (2009). Governance in the digital age: A research and action framework for an uncertain future. *Government Information Quarterly*, *26*(2), 257–264. https://doi.org/10.1016/j.giq.2008.12.003

Dawes, S. S. (2010). Stewardship and usefulness: Policy principles for information-based transparency. *Government Information Quarterly*, *27*(4), 377–383. https://doi.org/10.1016/j.giq.2010.07.001

de Graaf, G., Huberts, L., & Smulders, R. (2014). Coping With Public Value Conflicts. *Administration & Society*, *48*(9), 1101–1127. https://doi.org/10.1177/0095399714532273

Dobel, J. P. (2007). Public management as ethics. In E. Ferlie, L. E. Lynn, & C. Pollitt, *The Oxford Handbook of Public Management* (pp. 156–181). Oxford University Press.

Dunleavy, P. (2005). New Public Management Is Dead—Long Live Digital-Era Governance. *Journal of Public Administration Research and Theory*, *16*(3), 467–494. https://doi.org/10.1093/jopart/mui057

Dwivedi, Y., Williams, M., Mitra, A., Niranjan, S., & Weerakkody, V. (2011). Understanding advances in Web technologies: Evolution from Web 2.0 to WEB 3.0. In *19th European Conference on Information Systems, ECIS 2011*.

European Commission. (2023). *eGovernment Benchmark 2023 Insight Report—Connecting Digital Governments*. Publications Office of the European Union.

Ferlie, E., Ashburner, L., & Fitzgerald, L. (1996). *The New Public Management in Action*. Oxford University Press.

Friedman, B., & Hendry, D. G. (2019). *Value Sensitive Design: Shaping Technology with Moral Imagination*. MIT Press.

Fung, A. (2015). Putting the Public Back into Governance: The Challenges of Citizen Participation and Its Future. *Public Administration Review*, *75*(4), 513–522. https://doi.org/10.1111/puar.12361

Ghosh Roy, S., & Upadhyay, P. (2017). Does e-readiness of citizens ensure better adoption of government's digital initiatives? A case based study. *Journal of Enterprise Information Management*, *30*, 65–81. https://doi.org/10.1108/JEIM-01-2016-0001

Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2012). Seeking Qualitative Rigor in Inductive Research: Notes on the Gioia Methodology. *Organizational Research Methods*, *16*(1), 15–31. https://doi.org/10.1177/1094428112452151

Government Digital Service. (2020). *User-centred design: Training and events*. Gov.Uk. https://www.gov.uk/service-manual/design/user-centred-design-training-and-events

Government Digital Service. (2023). *Design—Service Manual*. Gov.Uk. https://www.gov.uk/service-manual/design

Grube, D. (2013). In Search of Society? The Limitations of Citizen-Centred Governance. *The Political Quarterly*, *84*. https://doi.org/10.1111/j.1467-923X.2013.12024.x

Gupta, K., Bhaskar, P., & Singh, S. (2016). Critical Factors Influencing E-Government Adoption in India: An Investigation of the Citizens' Perspectives. *Journal of Information Technology Research*, *9*, 28–44. https://doi.org/10.4018/JITR.2016100103

Gupta, K., Singh, S., & Bhaskar, P. (2016). Citizen adoption of e-government: A literature review and conceptual framework. *Electronic Government, an International Journal*, *12*, 160. https://doi.org/10.1504/EG.2016.076134

Gupta, K., Singh, S., & Bhaskar, P. (2018). Citizens' perceptions on benefits of e-governance services. *International Journal of Electronic Governance*, *10*, 24. https://doi.org/10.1504/IJEG.2018.091261

Hood, C. (1995). The “new public management” in the 1980s: Variations on a theme. *Accounting, Organizations and Society*, *20*(2), 93–109. https://doi.org/10.1016/0361-3682(93)E0001-W

Iivari, J., & Iivari, N. (2011). Varieties of user-centredness: An analysis of four systems development methods. *Information Systems Journal*, *21*(2), 125–153. https://doi.org/10.1111/j.1365-2575.2010.00351.x

Ingrams, A. (2019). Public Values in the Age of Big Data: A Public Information Perspective. *Policy & Internet*, *11*(2), 128–148. https://doi.org/10.1002/poi3.193

Jansen, A., & Tranvik, T. (2011). *The State of IT Governance: Patterns of Variation at the Central Government Level in Norway*. *6846*. https://doi.org/10.1007/978-3-642-22878-0_14

Jarke, J. (2021). Co-Creating Digital Public Services. In J. Jarke (Ed.), *Co-creating Digital Public Services for an Ageing Society: Evidence for User-centric Design* (pp. 15–52). Springer International Publishing. https://doi.org/10.1007/978-3-030-52873-7_3

Jørgensen, T. B., & Bozeman, B. (2007). Public Values: An Inventory. *Administration & Society*, *39*(3). https://doi.org/10.1177/0095399707300

Kassen, M. (2021). Understanding decentralized civic engagement: Focus on peer-to-peer and blockchain-driven perspectives on e-participation. *Technology in Society*, *66*, 101650. https://doi.org/10.1016/j.techsoc.2021.101650

Kitchenham, B. (2004). Procedures for Performing Systematic Reviews. *Keele, UK, Keele University*, *33*, 1–26.

Koch, H., Leidner, D. E., & Gonzalez, E. S. (2013). Digitally enabling social networks: Resolving IT–culture conflict. *Information Systems Journal*, *23*(6), 501–523. https://doi.org/10.1111/isj.12020

König, P. D. (2021). Citizen-centered data governance in the smart city: From ethics to accountability. *Sustainable Cities and Society*, *75*, 103308. https://doi.org/10.1016/j.scs.2021.103308

Kotamraju, N. P., & van der Geest, T. M. (2012). The tension between user-centred design and e-government services. *Behaviour & Information Technology*, *31*(3), 261–273. https://doi.org/10.1080/0144929X.2011.563797

Krumbholz, M., Galliers, J., Coulianos, N., & Maiden, N. A. M. (2000). Implementing Enterprise Resource Planning Packages in Different Corporate and National Cultures. *Journal of Information Technology*, *15*(4), 267–279. https://doi.org/10.1177/026839620001500403

Kujala, S. (2003). User involvement: A review of the benefits and challenges. *Behaviour & Information Technology*, *22*(1), 1–16. https://doi.org/10.1080/01449290301782

Kurdi, H., Li, M., & Al-Raweshidy, H. S. (2010). Taxonomy of Grid Systems. In *Handbook of Research on P2P and Grid Systems for Service-Oriented Computing: Models, Methodologies and Applications* (pp. 20–43). IGI Global. https://doi.org/10.4018/978-1-61520-686-5.ch002

Kyakulumbye, S., Pather, S., & Jantjies, M. (2019). *Towards design of citizen centric e-government projects in developing country context: The design-reality gap in Uganda*. 55–73. https://doi.org/10.12821/ijispm070403

Larsson, K. (2020). Digitization or equality: When government automation covers some, but not all citizens. *Government Information Quarterly*, *38*, 101547. https://doi.org/10.1016/j.giq.2020.101547

Lee, C. (2022). Technology and aging: The jigsaw puzzle of design, development and distribution. *Nature Aging*, *2*(12), Article 12. https://doi.org/10.1038/s43587-022-00325-6

Leidner, D., & Kayworth, T. (2006). Review: A Review of Culture in Information Systems Research: Toward a Theory of Information Technology Culture Conflict. *MIS Quarterly*, *30*, 357–399. https://doi.org/10.2307/25148735

Lukes, S. (1989). Making Sense of Moral Conflict. In N. L. Rosenblum (Ed.), *Liberalism and the Moral Life* (pp. 127–142).

Madan, R., & Ashok, M. (2022). AI adoption and diffusion in public administration: A systematic literature review and future research agenda. *Government Information Quarterly*, *40*. https://doi.org/10.1016/j.giq.2022.101774

Mariën, I., & Amon Prodnik, J. (2014). Digital inclusion and user (dis)empowerment: A critical perspective. *Info*, *16*, 35–47. https://doi.org/10.1108/info-07-2014-0030

Mayring, P. (2014). *Qualitative Content Analysis: Theoretical foundation, Basic Procedures and Software Solution*. Open Access Repository.

Méndez-Domínguez, P., Carbonero Muñoz, D., Raya Díez, E., & Castillo De Mesa, J. (2023). Digital inclusion for social inclusion. Case study on digital literacy. *Frontiers in Communication*, *8*. https://doi.org/10.3389/fcomm.2023.1191995

Meyer, J. W., & Rowan, B. (1977). Institutionalized Organizations: Formal Structure as Myth and Ceremony. *American Journal of Sociology*, *83*(2), 340–363. https://doi.org/10.1086/226550

Mignerat, M., & Rivard, S. (2015). Positioning the institutional perspective in information systems research. In L. P. Willcocks, C. Sauer, & M. C. Lacity (Eds.), *Formulating Research Methods for Information Systems: Volume 2* (pp. 79–126). Palgrave Macmillan UK. https://doi.org/10.1057/9781137509888_4

Miles, M. B., Huberman, A. M., & Saldaña, J. (2014). *Qualitative data analysis: A methods sourcebook* (Third edition). SAGE Publications, Inc.

Miniaoui, S., Hashim, K., Atalla, S., Hashim, N. L., & Ismail, S. (2020). *Citizen Readiness to Adopt the New Emerging Technologies in Dubai Smart Government Services*. https://doi.org/10.1109/ICSITech49800.2020.9392071

Moher, D., Liberati, A., Tetzlaff, J., Altman, D. G., & for the PRISMA Group. (2009). Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. *BMJ*, *339*(jul21 1), b2535–b2535. https://doi.org/10.1136/bmj.b2535

Moore, M. H. (1995). *Creating public value: Strategic management in government*. Harvard University Press.

Morales Rodriguez, M., Casper, G., & Brennan, P. F. (2007). Patient-centered design. The potential of user-centered design in personal health records. *Journal of AHIMA*, *78*(4), 44–46; quiz 49–50.

Mossey, S., Manoharan, A., & Bennett, L. (2018). *Exploring Citizen-Centric E-Government Using a Democratic Theories Framework* (pp. 1–32). https://doi.org/10.4018/978-1-5225-5999-3.ch001

Nabatchi, T. (2012). Putting the "Public" Back in Public Values Research: Designing Participation to Identify and Respond to Values. *Public Administration Review*, *72*(5), 699–708. https://doi.org/10.1111/j.1540-6210.2012.02544.x

Nabatchi, T. (2017). Public Values Frames in Administration and Governance. *Perspectives on Public Management and Governance*, *1*. https://doi.org/10.1093/ppmgov/gvx009

Niglia, F., & Tangi, L. (2024). Measuring user-centricity in AI-enabled European public services: A proposal for enabling maturity models. In *Research Handbook on Public Management and Artificial Intelligence* (pp. 97–117). Edward Elgar Publishing. https://www.elgaronline.com/edcollchap/book/9781802207347/book-part-9781802207347-15.xml

OECD. (2009). *Rethinking e-Government Services: User-Centred Approaches*. Organisation for Economic Co-operation and Development. https://www.oecd-ilibrary.org/governance/rethinking-e-government-services_9789264059412-en

OECD. (2022). *OECD Guidelines for citizen participation processes*. https://www.oecd.org/gov/oecd-guidelines-for-citizen-participation-processes-highlights.pdf

OECD & Asian Development Bank. (2019). *Government at a Glance Southeast Asia 2019*. OECD. https://doi.org/10.1787/9789264305915-en

Ølnes, S., Ubacht, J., & Janssen, M. (2017). Blockchain in Government: Benefits and Implications of Distributed Ledger Technology for Information Sharing. *Government Information Quarterly*, *34*(3), 355–364. https://doi.org/10.1016/j.giq.2017.09.007

Orlikowski, W. J., & Barley, S. R. (2001). Technology and Institutions: What Can Research on Information Technology and Research on Organizations Learn from Each Other? *MIS Quarterly*, *25*(2), 145–165. https://doi.org/10.2307/3250927

Othman, M. H., Razali, R., & Nasrudin, M. (2020). *Key Factors for E-Government towards Sustainable Development Goals*. *29*, 2864–2876.

Paré, G., Trudel, M.-C., Jaana, M., & Kitsiou, S. (2015). Synthesizing information systems knowledge: A typology of literature reviews. *Information & Management*, *52*(2), 183–199. https://doi.org/10.1016/j.im.2014.08.008

Park, S., & Humphry, J. (2019). Exclusion by design: Intersections of social, digital and data exclusion. *Information, Communication & Society*, *22*(7), 934–953. https://doi.org/10.1080/1369118X.2019.1606266

Pollitt, C., & Bouckaert, G. (2017). *Public Management Reform: A Comparative Analysis - Into The Age of Austerity*. Oxford University Press.

Porumbescu, G. A. (2016). Linking public sector social media and e-government website use to trust in government. *Government Information Quarterly*, *33*(2), 291–304. https://doi.org/10.1016/j.giq.2016.04.006

Pozzebon, M., Cunha, M. A., & Coelho, T. R. (2016). Making sense to decreasing citizen eParticipation through a social representation lens. *Information and Organization*, *26*(3), 84–99. https://doi.org/10.1016/j.infoandorg.2016.07.002

Rädiker, S., & Kuckartz, U. (2018). *Analyse qualitativer Daten mit MAXQDA: Text, Audio und Video* (1. Aufl. 2019 edition). Springer VS.

Rana, Williams, Dwivedi, & Williams. (2012). Theories and Theoretical Models for Examining the Adoption of E-Government Services. *E-Service Journal*, *8*(2), 26. https://doi.org/10.2979/eservicej.8.2.26

Reddick, C., & Anthopoulos, L. (2014). Interactions with e-government, new digital media and traditional channel choices: Citizen-initiated factors. *Transforming Government: People, Process and Policy*, *8*(3), 398–419. Scopus. https://doi.org/10.1108/TG-01-2014-0001

Robinson, J. P., Dimaggio, P., & Hargittai, E. (2003). New Social Survey Perspectives on the Digital Divide. *IT & Society*, *1*(5), 22.

Rose, J., Persson, J. S., Heeager, L. T., & Irani, Z. (2015). Managing e-Government: Value positions and relationships. *Information Systems Journal*, *25*(5), 531–571. https://doi.org/10.1111/isj.12052

Saldaña, J. (2021). The Coding Manual for Qualitative Researchers. *The Coding Manual for Qualitative Researchers*, 1–440.

Schein, E. H. (2016). *Organizational Culture and Leadership, 5th Edition* (5. edition). Wiley.

Scott, M., DeLone, W., & Golden, W. (2016). Measuring eGovernment success: A public value approach. *European Journal of Information Systems*, *25*(3), 187–208. https://doi.org/10.1057/ejis.2015.11

Sevaldson, B. (2018). Beyond User-Centric Design. *Relating Systems Thinking and Design Symposium*. https://rsdsymposium.org/beyond-user-centric-design/

Shenglin, B., Simonelli, F., Ruidong, Z., Bosc, R., & Wenwei, L. (2017). *Digital Infrastructure: Overcoming Digital Divide in Emerging Economies*. https://pdfs.semanticscholar.org/a513/de546a8c8ceda79fb4e8492c15cd84c7f983.pdf

Sigwejo, A., & Pather, S. (2016). A Citizen-Centric Framework For Assessing E-Government Effectiveness. *Electronic Journal of Information Systems in Developing Countries*, *74*(1), 1–27. https://doi.org/10.1002/j.1681-4835.2016.tb00542.x

Sorn-in, K., Tuamsuk, K., & Chaopanon, W. (2015). Factors affecting the development of e-government using a citizen-centric approach. *Journal of Science and Technology Policy Management*, *6*, 206–222. https://doi.org/10.1108/JSTPM-05-2014-0027

Spicer, M. W. (2001). Value Pluralism and Its Implications for American Public Administration. *Administrative Theory & Praxis*, *23*(4), 507–528.

Spurlock, B., & O'Neil, J. (2009). Designing an Employee-Centered Intranet and Measuring Its Impact on Employee Voice and Satisfaction. *Public Relations Journal*, *3*(2), 1–20.

Stoker, G. (2006). Public value management: A new narrative for networked governance? *American Review of Public Administration*, *36*(1), Article 1. https://doi.org/10.1177/0275074005282583

Suchowerska, R., & McCosker, A. (2022). Governance networks that strengthen older adults' digital inclusion: The challenges of metagovernance. *Government Information Quarterly*, *39*(1), 101649. https://doi.org/10.1016/j.giq.2021.101649

Templier, M., & Pare, G. (2018). Transparency in literature reviews: An assessment of reporting practices across review types and genres in top IS journals. *European Journal of Information Systems*, *27*, 503–550. https://doi.org/10.1080/0960085X.2017.1398880

Teo, H. H., Wei, K. K., & Benbasat, I. (2003). Predicting Intention to Adopt Interorganizational Linkages: An Institutional Perspective. *MIS Quarterly*, *27*(1), 19–49. https://doi.org/10.2307/30036518

Thacher, D., & Rein, M. (2004). Managing Value Conflict in Public Policy. *Governance: An International Journal of Policy, Administration and Institutions*, *17*(4). https://doi.org/10.1111/j.0952-1895.2004.00254.x

Timmermans, S., & Tavory, I. (2012). Theory Construction in Qualitative Research: From Grounded Theory to Abductive Analysis. *Sociological Theory*, *30*(3).

Tingling, P., & Parent, M. (2002). Mimetic Isomorphism and TechnologyEvaluation: Does Imitation TranscendJudgment? *Journal of the Association for Information Systems*, *3*(1). https://doi.org/10.17705/1jais.00025

Tõnurist, P., Kattel, R., & Lember, V. (2017). Innovation Labs in the Public Sector: What they are and what they do? *Public Management Review*, *19*. https://doi.org/10.1080/14719037.2017.1287939

U. S. General Services Administration. (2023). *A collection of tools to bring human-centered design into your project*. 18F. https://methods.18f.govhttps://methods.18f.gov/

van der Wal, Z., & van Hout, E. Th. J. (2009). Is Public Value Pluralism Paramount? The Intrinsic Multiplicity and Hybridity of Public Values. *International Journal of Public Administration*, *32*(3–4), 220–231. https://doi.org/10.1080/01900690902732681

Van Velsen, L., Van der Geest, T., Klaassen, R., & Steehouder, M. (2008). User-centered evaluation of adaptive and adaptable systems: A literature review. *The Knowledge Engineering Review*, *23*(3), 261–281.

van Velsen, L., van der Geest, T., ter Hedde, M., & Derks, W. (2009a). Requirements engineering for e-Government services: A citizen-centric approach and case study. *Government Information Quarterly*, *26*(3), 477–486. https://doi.org/10.1016/j.giq.2009.02.007

van Velsen, L., van der Geest, T., ter Hedde, M., & Derks, W. (2009b). Requirements engineering for e-Government services: A citizen-centric approach and case study. *Government Information Quarterly*, *26*(3), 477–486. https://doi.org/10.1016/j.giq.2009.02.007

Ventriss, C., Perry, J. L., Nabatchi, T., Milward, H. B., & Johnston, J. M. (2019). Democracy, Public Administration, and Public Values in an Era of Estrangement. *Perspectives on Public Management and Governance*, *2*(4), 275–282. https://doi.org/10.1093/ppmgov/gvz013

Vesnic-Alujevic, L., Stoermer, E., Rudkin, J.-E., Scapolo, F., & Kimbell, L. (2019). *The Future of Government 2030+*. Publications Office of the European Union. https://doi.org/10.2760/145751

Vigoda-Gadot, E. (2002). From Responsiveness to Collaboration: Governance, Citizens, and the Next Generation of Public Administration. *Public Administration Review*, *62*, 527–540. https://doi.org/10.1111/1540-6210.00235

Webster, J., & Watson, R. T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. *Management Information Systems Quarterly*, *26*(2), 12.

Weigl, L., Amard, A., Marxen, H., Roth, T., & Zavolokina, L. (2022). User-centricity and Public Values in E-government: Friend or Foe? *30th European Conference on Information Systems*, 18.

Welby, B. (2019). *The impact of digital government on citizen well-being* (32; OECD Working Papers on Public Governance). 10.1787/24bac82f-en.

Wiredu, G. (2012). Information systems innovation in public organisations: An institutional perspective. *Information Technology & People*, *25*, 188–206. https://doi.org/10.1108/09593841211232703

Yang, K., & Pandey, S. K. (2011). Further Dissecting the Black Box of Citizen Participation: When Does Citizen Involvement Lead to Good Outcomes? *Public Administration Review*, *71*(6), 880–892. https://doi.org/10.1111/j.1540-6210.2011.02417.x

Zavolokina, L., Sprenkamp, K., & Schenk, B. (2023). *Citizens' Expectations about Achieving Public Value and the Role of Digital Technologies: It Takes Three to Tango!* https://hdl.handle.net/10125/102873

Zucker, L. G. (1977). The Role of Institutionalization in Cultural Persistence. *American Sociological Review*, *42*(5), 726–743. https://doi.org/10.2307/2094862

8. Appendix

Table 10. List of coded publications during the literature review process and their main characteristics.

Item Type	Publ. Year	Author	Title	Publication Title	Scope of analysis	Research type
Conference article	2013	Abdellatif, Ahmed; Ben Amor, Nahla; Mellouli, Sehl	An intelligent framework for e-government personalized services	Proceedings of the 14th Annual International Conference on Digital Government Research	Worldwide	Design research
Peer-reviewed journal article	2012	Alomari, Mohammad; Woods, Peter; Sandhu, Kuldeep	Predictors for e-government adoption in Jordan: Deployment of an empirical evaluation based on a citizen-centric approach	Information Technology & People	Jordan	Quantitative
Peer-reviewed journal article	2013	Andersen, Lotte Bøgh; Jørgensen, Torben Beck; Kjeldsen, Anne Mette; Pedersen, Lene Holm; Vrangbæk, Karsten	Public Values and Public Service Motivation: Conceptual and Empirical Relationships	The American Review of Public Administration	Denmark	Quantitative
Peer-reviewed journal article	2018	Aschhoff, Nils; Vogel, Rick	Value conflicts in co-production: governing public values in multi-actor settings	International Journal of Public Sector Management	Germany	Qualitative
Peer-reviewed journal article	2022	Bason, Christian; Austin, Robert D.	Design in the public sector: Toward a human centred model of public governance	Public Management Review	Worldwide	Qualitative
Peer-reviewed journal article	2021	Berg, Janne; Lindholm, Jenny; Högväg, Joachim	How do we know that it works? Designing a digital democratic innovation with the help of user-centered design	Information Polity	Finland	Quantitative
Conference article	2013	Berntzen, Lasse	Citizen-centric eGovernment Services	Proceedings of CENTRIC 2013: The Sixth International Conference on Advances in Human-oriented and Personalized Mechanisms, Technologies, and Services	Europe	Quantitative
Peer-reviewed journal article	2021	Bokayev, Baurzhan; Davletbayeva, Zhuldyz; Amirova, Aigerim; Rysbekova, Zhanar; Torebekova,	Transforming E-government in Kazakhstan: A Citizen-Centric Approach	The Innovation Journal: The Public Sector Innovation Journal	Kazakhstan	Quantitative

		Zulfiya; Jussupova, Gul				
Peer-reviewed journal article	2013	Borah, Sri Keshabananda	Implementation of citizen-centric e-Governance projects in Assam	IOSR Journal of Humanities and Social Science	India	Qualitative
Peer-reviewed journal article	2021	Brown, Prudence R.	Public Value Measurement vs. Public Value Creating Imagination – the Constraining Influence of Old and New Public Management Paradigms	International Journal of Public Administration	Worldwide	Qualitative
Peer-reviewed journal article	2014	Bryson, John M.; Crosby, Barbara C.; Bloomberg, Laura	Public Value Governance: Moving Beyond Traditional Public Administration and the New Public Management	Public Administration Review	USA	Qualitative
Peer-reviewed journal article	2021	Clark, Jill K.	Public Values and Public Participation: A Case of Collaborative Governance of a Planning Process	The American Review of Public Administration	USA	Qualitative
Peer-reviewed journal article	2014	Clarke, Amanda; Margetts, Helen	Governments and Citizens Getting to Know Each Other? Open, Closed, and Big Data in Public Management Reform: Open, Closed, and Big Data in Public Management Reform	Policy & Internet	Canada; United Kingdom; USA	Qualitative
Peer-reviewed journal article	2012	Cordella, Antonio; Bonina, Carla M.	A public value perspective for ICT enabled public sector reforms: A theoretical reflection	Government Information Quarterly	Worldwide	Qualitative
Book chapter	2018	David, Nina	Democratizing Government: What We Know About E-Government and Civic Engagement	International E-Government Development	Worldwide	Qualitative
Peer-reviewed journal article	2016	De Graaf, Gjalt; Huberts, Leo; Smulders, Remco	Coping With Public Value Conflicts	Administration & Society	Worldwide	Qualitative
Peer-reviewed journal article	2016	Degbelo, Auriol; Granell, Carlos; Trilles, Sergio; Bhattacharya, Devanjan; Casteleyn, Sven; Kray, Christian	Opening up Smart Cities: Citizen-Centric Challenges and Opportunities from GIScience	ISPRS International Journal of Geo-Information	Worldwide	Qualitative
Conference article	2019	E. Luna, Dolores; Picazo-Vela, Sergio; Ramon Gil-Garcia, J.; Puron-Cid, Gabriel;	Public Value Creation through Digital Service Delivery from a Citizens' Perspective	Proceedings of the 20th Annual International Conference on Digital Government Research	Mexico	Qualitative

		Sandoval-Almazan, Rodrigo; F. Luna-Reyes, Luis				
Peer-reviewed journal article	2016	Ebbers, Wolfgang E.; Jansen, Marloes G.M.; Van Deursen, Alexander J.A.M.	Impact of the digital divide on e-government: Expanding from channel choice to channel usage	Government Information Quarterly	Netherlands	Quantitative
Conference article	2017	Frohlich, Karin	Evaluating the effects of e-government initiatives on citizen-centric goals at selected Namibian Government Ministry	2017 IST-Africa Week Conference (IST-Africa)	Namibia	Qualitative
Peer-reviewed journal article	2015	Gable, Matt	Efficiency, Participation, and Quality: Three Dimensions of E-Government?	Social Science Computer Review	Worldwide	Qualitative
Conference article	2016	Garcia-Garcia, Luz Maria	User Centric e-Government: the Modernization of the National Institute of Migration at Mexico's Southern Border	Proceedings of the 9th International Conference on Theory and Practice of Electronic Governance	Mexico	Qualitative
Conference article	2014	Garcia-Garcia, Luz Maria; Gil-Garcia, J. Ramon; Gómez, Victor	Citizen-centered e-government: towards a more integral approach	Proceedings of the 15th Annual International Conference on Digital Government Research	Worldwide	Qualitative
Conference article	2015	Garcia-Garcia, Luz Maria; Gil-Garcia, J. Ramon; Gómez, Victor	Citizen centered e-government?: the case of National Migration Institute in the Southern Mexican border	Proceedings of the 16th Annual International Conference on Digital Government Research	Mexico	Qualitative
Peer-reviewed journal article	2017	Ghosh Roy, Saikat; Upadhyay, Parijat	Does e-readiness of citizens ensure better adoption of government's digital initiatives? A case based study	Journal of Enterprise Information Management	India	Mixed
Peer-reviewed journal article	2015	Gjermundrød, Harald; Dionysiou, Ioanna	A conceptual framework for configurable privacy-awareness in a citizen-centric eGovernment	Electronic Government, an International Journal	Worldwide	Design research
Peer-reviewed journal article	2013	Grube, Dennis	In Search of Society? The Limitations of Citizen-Centred Governance	The Political Quarterly	Worldwide	Qualitative
Peer-reviewed journal article	2016	Gupta, Kriti Priya; Bhaskar, Preeti; Singh, Swati	Critical Factors Influencing E-Government Adoption in India: An Investigation of the Citizens' Perspectives	Journal of Information Technology Research	India	Quantitative
Peer-reviewed	2016	Gupta, Kriti Priya; Singh,	Citizen adoption of e-government: a literature	Electronic Government, an	India	Mixed

journal article		Swati; Bhaskar, Preeti	review and conceptual framework	International Journal		
Peer-reviewed journal article	2018	Gupta, Kriti Priya; Singh, Swati; Bhaskar, Preeti	Citizens' perceptions on benefits of e-governance services	International Journal of Electronic Governance	India	Quantitative
Conference article	2015	Haider, Muhammad; Khan, Muhammad Umer; Farooq, Sumbal	e-Government: An empirical analysis of current literature	2015 International Conference on Information and Communication Technologies (ICICT)	Worldwide	Qualitative
Conference article	2020	Hashim, Kamarul Faizal; Hashim, Nor Laily; Ismail, Solahudin; Miniaoui, Sami; Atalla, Shadi	Citizen Readiness to Adopt the New Emerging Technologies in Dubai Smart Government Services	2020 6th International Conference on Science in Information Technology (ICSITech)	UAE	Quantitative
Peer-reviewed journal article	2012	Hung, Mei Jen	Building Citizen-centred E-government in Taiwan: Problems and Prospects: Building Citizen-centred E-government in Taiwan	Australian Journal of Public Administration	Taiwan	Qualitative
Peer-reviewed journal article	2019	Ingrams, Alex	Public Values in the Age of Big Data: A Public Information Perspective: Public Values in the Age of Big Data	Policy & Internet	Germany; Netherlands	Qualitative
Peer-reviewed journal article	2018	Janssen, Marijn; Helbig, Natalie	Innovating and changing the policy-cycle: Policy-makers be prepared!	Government Information Quarterly	Worldwide	Qualitative
Peer-reviewed journal article	2015	Jho, Whasun; Song, Kyong Jae	Institutional and technological determinants of civil e-Participation: Solo or duet?	Government Information Quarterly	Worldwide	Quantitative
Conference article	2013	Kamaruddin, Kamalia Azma; Noor, Nor Laila Md	Citizen-driven model in citizen-centric t-government	Proceedings of the 7th International Conference on Theory and Practice of Electronic Governance	Worldwide	Qualitative
Peer-reviewed journal article	2021	Kassen, Maxat	Understanding decentralized civic engagement: Focus on peer-to-peer and blockchain-driven perspectives on e-participation	Technology in Society	Finland; France; Germany	Qualitative
Peer-reviewed journal article	2021	König, Pascal D.	Citizen-centered data governance in the smart city: From ethics to accountability	Sustainable Cities and Society	Worldwide	Qualitative
Peer-reviewed journal article	2012	Kotamraju, Nalini P.; Van Der Geest, Thea M.	The tension between user-centred design and e-government services	Behaviour & Information Technology	Netherlands	Qualitative
Peer-reviewed	2019	Kumar, Avanish	Citizen-centric model of governmental	Transforming Government:	India	Qualitative

journal article			entrepreneurship: Transforming public service management for the empowerment of marginalized women	People, Process and Policy		
Peer-reviewed journal article	2021	Kyakulumbye, Stephen; Pather, Shaun; Jantjies, Mmaki	Towards design of citizen centric e-government projects in developing country context: the design-reality gap in Uganda	International Journal of Information Systems and Project Management	Uganda	Qualitative
Conference article	2015	Lappas, Georgios; Triantafillidou, Amalia; Kleftodimos, Alexandras; Yannas, Prodromos	Evaluation framework of local e-government and e-democracy: A citizens' perspective	2015 IEEE Conference on e-Learning, e-Management and e-Services (IC3e)	Greece	Quantitative
Peer-reviewed journal article	2021	Larsson, Karl Kristian	Digitization or equality: When government automation covers some, but not all citizens	Government Information Quarterly	Norway	Qualitative
Conference article	2020	Liva, Giovanni; Codagnone, Cristiano; Misuraca, Gianluca; Gineikyte, Vaida; Barcevicius, Egidijus	Exploring digital government transformation: a literature review	Proceedings of the 13th International Conference on Theory and Practice of Electronic Governance	Worldwide	Qualitative
Peer-reviewed journal article	2023	Madan, Rohit; Ashok, Mona	AI adoption and diffusion in public administration: A systematic literature review and future research agenda	Government Information Quarterly	Worldwide	Qualitative
Peer-reviewed journal article	2014	Mariën, Ilse; A. Prodnik, Jernej	Digital inclusion and user (dis)empowerment: a critical perspective	Digital Policy, Regulation and Governance	Worldwide	Qualitative
Book chapter	2018	Mossey, Sean; Manoharan, A.P.; Bennett, Lamar Vernon	New Approaches, Methods, and Tools in Urban E-Planning	New Approaches, Methods, and Tools in Urban E-Planning:	USA	Mixed
Peer-reviewed journal article	2013	Mostafa, Mohamed M.; El-Masry, Ahmed A.	Citizens as consumers: Profiling e-government services' users in Egypt via data mining techniques	International Journal of Information Management	Egypt	Quantitative
Peer-reviewed journal article	2012	Nabatchi, Tina	Putting the "Public" Back in Public Values Research: Designing Participation to Identify and Respond to Values	Public Administration Review	Worldwide	Qualitative
Peer-reviewed journal article	2018	Nabatchi, Tina	Public Values Frames in Administration and Governance	Perspectives on Public Management and Governance	Worldwide	Qualitative

Book chapter	2018	Osborne, Stephen P.; Strokosch, Kirsty; Radnor, Zoe	Co-Production and the Co-Creation of Value in Public Services	Co-Production and Co-Creation	Worldwide	Qualitative
Peer-reviewed journal article	2014	Osman, Ibrahim H.; Anouze, Abdel Latef; Irani, Zahir; Al-Ayoubi, Baydaa; Lee, Habin; Balcı, Asım; Medeni, Tunç D.; Weerakkody, Vishanth	COBRA framework to evaluate e-government services: A citizen-centric perspective	Government Information Quarterly	Turkey	Mixed
Peer-reviewed journal article	2019	Panagiotopoulos, Panos; Klievink, Bram; Cordella, Antonio	Public value creation in digital government	Government Information Quarterly	Worldwide	Qualitative
Peer-reviewed journal article	2014	Pang, Min-Seok; Lee, Gwanhoo; DeLone, William H	IT Resources, Organizational Capabilities, and Value Creation in Public-Sector Organizations: A Public-Value Management Perspective	Journal of Information Technology	Worldwide	Qualitative
Peer-reviewed journal article	2019	Park, Sora; Humphry, Justine	Exclusion by design: intersections of social, digital and data exclusion	Information, Communication & Society	Australia	Qualitative
Conference article	2020	Parra, Raul Diaz; Saenz, Christian Fernando Libaque	The Influence of Digital Transformation of the Peruvian Public Sector on Citizen Trust	AMCIS 2020 Proceedings	Peru	Quantitative
Peer-reviewed journal article	2020	Pérez-Morote, Rosario; Pontones-Rosa, Carolina; Núñez-Chicharro, Montserrat	The effects of e-government evaluation, trust and the digital divide in the levels of e-government use in European countries	Technological Forecasting and Social Change	Europe	Quantitative
Peer-reviewed journal article	2013	Persaud, Ajax; Persaud, Priya	Rethinking E-Government Adoption: A User-Centered Model	International Journal of Electronic Government Research	Canada	Mixed
Book chapter	2013	Purao, Sandeep; Seng, Teo Chin; Wu, Alfred	Modeling Citizen-Centric Services in Smart Cities	Conceptual Modeling	Worldwide	Formal
Conference article	2013	Purao, Sandeep; Wu, Alfred	Towards Values-inspired Design: The Case of Citizen-Centric Services	Proceedings of the Thirty Fourth International Conference on Information Systems, Milan 2013	Worldwide	Formal
Peer-reviewed	2015	Rose, Jeremy; Persson, John Stouby;	Managing e-Government: value	Information Systems Journal	Worldwide	Qualitative

journal article		Heeager, Lise Tordrup; Irani, Zahir	positions and relationships			
Peer-reviewed journal article	2016	Scott, Murray; DeLone, William; Golden, William	Measuring eGovernment success: a public value approach	European Journal of Information Systems	USA	Quantitative
Peer-reviewed journal article	2019	Sepasgozar, Samad M.E.; Hawken, Scott; Sargolzaei, Sharifeh; Foroozanfa, Mona	Implementing citizen centric technology in developing smart cities: A model for predicting the acceptance of urban technologies	Technological Forecasting and Social Change	Iran	Mixed
Peer-reviewed journal article	2016	Sharma, Ravi; Fantin, Arul-Raj; Prabhu, Navin; Guan, Chong; Dattakumar, Ambica	Digital literacy and knowledge societies: A grounded theory investigation of sustainable development	Telecommunications Policy	Finland; Hong Kong; Qatar; New Zealand; Singapore	Qualitative
Peer-reviewed journal article	2016	Sigwejo, Annastellah; Pather, Shaun	A Citizen-Centric Framework For Assessing E-Government Effectiveness	The Electronic Journal of Information Systems in Developing Countries	Tanzania	Qualitative
Peer-reviewed journal article	2015	Sorn-in, Kanda; Tuamsuk, Kulthida; Chaopanon, Wasu	Factors affecting the development of e-government using a citizen-centric approach	Journal of Science & Technology Policy Management	Thailand	Mixed
Book chapter	2014	Synnes, Kåre; Kranz, Matthias; Rana, Juwel; Schelén, Olov; Nilsson, Michael	User-Centric Social Interaction for Digital Cities	Creating Personal, Social, and Urban Awareness through Pervasive Computing:	Worldwide	Qualitative
Peer-reviewed journal article	2013	Thomas, John Clayton	Citizen, Customer, Partner: Rethinking the Place of the Public in Public Management	Public Administration Review	Worldwide	Qualitative
Conference article	2012	Tsohou, Aggeliki; Lee, Habin; Irani, Zahir; Weerakkody, Vishanth; Osman, Ibrahim; Latif, Abdel Anuz; Medeni, Tunc	Evaluating e-government services from a citizens' perspective: a reference process	European, Mediterranean & Middle Eastern Conference on Information Systems 2012	Europe	Design research
Conference article	2017	Twizeyimana, Jean Damascene	User-centeredness and usability in e-government: a reflection on a case study in Rwanda	Proceedings of the Internationsl Conference on Electronic Governance and Open Society: Challenges in Eurasia	Rwanda	Qualitative

Table 11. Value conflicts and conflict sources found in literature.

	User focus-representation	User focus-pluralism	User involvement-accountability	User involvement-inclusiveness
Decision-making Dominance	Grube, 2013; Ingrams, 2019; Kassen, 2021; Kotamraju & van der Geest, 2012; Park & Humphry, 2019		de Graaf et al., 2016; Ingrams, 2019; Kotamraju & van der Geest, 2012; Mossey et al., 2018	David, 2018; Kotamraju & van der Geest, 2012; Mariën & Amon Prodnik, 2014
Degree of Participation	Berg et al., 2021; Grube, 2013; Kassen, 2021; Kotamraju & van der Geest, 2012; Nabatchi, 2012	Aschhoff & Vogel, 2018; Gupta, Singh, et al., 2016; Kotamraju & van der Geest, 2012; Mariën & Amon Prodnik, 2014	Aschhoff & Vogel, 2018; Berg et al., 2021; de Graaf et al., 2016; König, 2021; Kotamraju & van der Geest, 2012; Mossey et al., 2018	David, 2018; König, 2021; Kotamraju & van der Geest, 2012; Mariën & Amon Prodnik, 2014, 2014
Resource Deficit	Kotamraju & van der Geest, 2012; Kyakulumbye et al., 2019; Sigwejo & Pather, 2016	Berg et al., 2021; Bokayev et al., 2021; Gupta et al., 2018; Gupta, Singh, et al., 2016; Kotamraju & van der Geest, 2012; Larsson, 2020; Mariën & Amon Prodnik, 2014; Park & Humphry, 2019	Kotamraju & van der Geest, 2012; Mossey et al., 2018	Berg et al., 2021; David, 2018; König, 2021; Kotamraju & van der Geest, 2012; Mariën & Amon Prodnik, 2014; Park & Humphry, 2019
Establishment-Innovation	de Graaf et al., 2016; Grube, 2013; Ingrams, 2019; Kassen, 2021; Kotamraju & van der Geest, 2012; Miniaoui et al., 2020	Aschhoff & Vogel, 2018; Brown, 2021; Cordella & Bonina, 2012; de Graaf et al., 2016; Kotamraju & van der Geest, 2012; Mariën & Amon Prodnik, 2014	Aschhoff & Vogel, 2018; Bason & Austin, 2022; de Graaf et al., 2016; Grube, 2013; Ingrams, 2019; Kotamraju & van der Geest, 2012; Mossey et al., 2018	Clark, 2021; Kotamraju & van der Geest, 2012; Mariën & Amon Prodnik, 2014
Multistakeholder	Ingrams, 2019; Kassen, 2021; Kotamraju & van der Geest, 2012; Nabatchi, 2012; Sorn-in et al., 2015	Aschhoff & Vogel, 2018; Kotamraju & van der Geest, 2012; Scott et al., 2016	Ingrams, 2019	

Table 12. Codebook.

Main code category	Sub-code category	Sub-code category
User-values conflict sources	Degree of participation	
	Multistakeholder issue	
	Establishment-innovation tension	
	Resource deficit	

	Decision-making dominance	
User-values overlap		
Knowledge society	ICT infrastructure	
	Role of new media	
	Regulatory policy and governance	
	Political vision	
	Human capital development	
	Education	
Facilitating conditions	Funding	
	Government process change	
	Coordination	
	Multichannel delivery of e-government	
	Access limitation	
	Infrastructure	
	Availability of data	
Collaborative governance	Influence	
	Citizen disinterest	
	Networks	
	Deliberation	
	Dialogue	
	Co-design	
Government	E-government	Policy-making
		Challenges, barriers and failures
		E-governance
		Infrastructure
		Success

		Risks
		Benefits
	Multiple Stakeholders	Coordination
		Interaction
		Dispute resolution
	Institutionalized processes	
Design choices	User-centered design	
	Value-infused design choices	
	Proactivity	
	Democracy	
	Inclusiveness	
	Performance	
	Productivity	
	Durability	
	Compliance	
	Engagement	
	Service quality	
	Efficiency	
	Political neutrality	
	Transparency	
	Trust	
	Accountability	Accountability to the public
		Accountability to government
	Cost savings	
	Equality	
	Responsiveness	
	Representation	
	Participation	
	Effectiveness	
	Justice	
	Legitimacy	
	Innovation	
	Equity	
	Confidence	
	Accessibility	
	Reliability	
	Fairness	
	Diversity	
	Flexibility	
	Sustainability	
	Economy / parsimony	
	Privacy	
	Security	

	Proper use of public funds	
	Responsibility	
Citizens	Skills	Informed citizens
		Expected skills
		Awareness of existing system
		Knowledge
		Content availability and literacy
	Needs	Interoperability
		Needs, abilities and expectations
		Usability, functionality and accessibility
		Citizen satisfactions
	Adoption	Ease of use
		Perceived usefulness
		Citizen readiness
		Benefits
		Intention to use
Digital divide		
User-centricity	System personalization	
	User involvement	
	User focus	