Harmonizing sensitive data exchange and double-spending prevention through blockchain and digital wallets: The case of e-prescription management

VINCENT SCHLATT and JOHANNES SEDLMEIR, FIM Research Center, University of Bayreuth, Germany
JANINA TRAUE, University of Bayreuth, Germany
FABIANE VÖLTER, Branch Business & Information Systems Engineering of the Fraunhofer FIT, Germany

The digital transformation of the medical sector requires solutions that are convenient and efficient for all stakeholders while protecting patients' sensitive data. One example that has already attracted design-oriented research are medical prescriptions. However, current implementations of electronic prescription management systems typically create centralized data silos, leaving user data vulnerable to cybersecurity incidents and impeding interoperability. Research has also proposed decentralized solutions based on blockchain technology, but privacy-related challenges have often been ignored. We conduct design science research to develop and implement a system for the exchange of electronic prescriptions that builds on two blockchains and a digital wallet app. Our solution combines the bilateral, verifiable, and privacy-focused exchange of information between doctors, patients, and pharmacies through verifiable credentials with a token-based, anonymized double-spending check. Our qualitative and quantitative evaluations as well as a security analysis suggest that this architecture can improve existing approaches to electronic prescription management by offering patients control over their data by design, a high level of security, sufficient performance and scalability, and interoperability with emerging digital identity management solutions for users, businesses, and institutions. We also derive principles on how to design decentralized, privacy-oriented information systems that require both the exchange of sensitive information and double-usage protection.

CCS Concepts: • **Security and privacy** → *Privacy-preserving protocols*; **Privacy protections**; • **Information systems** → *Mobile information processing systems*; E-commerce infrastructure.

Additional Key Words and Phrases: Distributed ledger, healthcare, token, privacy, self-sovereign identity

Authors' addresses: Vincent Schlatt, vincent.schlatt@fim-rc.de; Johannes Sedlmeir, johannes.sedlmeir@fim-rc.de, FIM Research Center, University of Bayreuth, Germany; Janina Traue, janina.traue@uni-bayreuth.de, University of Bayreuth, Germany; Fabiane Völter, fabiane.voelter@fit.fraunhofer.de, Branch Business & Information Systems Engineering of the Fraunhofer FIT, Germany.

2769-6472/2022/12-ART $15.00
https://doi.org/10.1145/3571509

1 INTRODUCTION

The ongoing digital transformation of the healthcare sector affects its stakeholders in various ways. Healthcare providers, public institutions, and patients alike face a constant pressure to develop and use digital tools in the healthcare sector. As recent developments caused by the Covid-19 pandemic indicate, this pressure is often exacerbated by the need to balance privacy requirements and adequate digital healthcare provisioning [36]. However, this apparent dichotomy appeared before the pandemic, too, for example in the context of digital health records or electronic medical prescriptions [68, 111]. Medical prescriptions refer to authorizations issued by qualified healthcare practitioners that allow patients to obtain medication and services for medical treatment. These authorizations typically manifest as physical, paper-based documents signed or sealed by a qualified physician, which patients present to pharmacies or health service providers. However, such paper-based medical prescriptions suffer from various drawbacks. For example, due to their format, they proved to be slow to process [92] and susceptible to manipulation, unauthorized reproduction, and errors [71]. Moreover, physical prescriptions can hardly integrate with telemedicine, which has increased by a factor of up to 78 during the Covid-19 pandemic and has stabilized at a level that is 38 times higher than pre-Covid [8]. Paper-based prescriptions also impede automatic checks for cross-reactions of pharmaceuticals [1] and seamlessly claiming reimbursement from health insurances. Consequently, several attempts to introduce medical prescriptions in an electronic format have emerged. These digital references or documents allow for automatic validity checks and are typically stored in databases run by parties that are regarded as trustworthy to prevent fraud and the abuse of sensitive data [1]. Thus, existing approaches to electronic prescriptions (e-prescriptions) rely on highly centralized infrastructures and data silos, such as current efforts in Germany illustrate [69]. While this design is relatively simple, avoids the double-usage of e-prescriptions, and addresses confidentiality requirements through access control enforced by the trusted third party, the corresponding data silos are attractive targets for attackers aiming to capture sensitive health information on a large scale [59, 63]. Moreover, they pose the socio-economic threat of creating monopolies or oligopolies [116] and ethical issues associated with privacy concerns [1]. Also, centralized implementations of e-prescriptions are often not interoperable as they create lock-in effects. In consequence, patients, healthcare practitioners, or pharmacies need to purchase proprietary and expensive software [10].

To eliminate these drawbacks of centralized approaches, researchers recently proposed alternative solutions based on decentralized infrastructures [101, 102]. These approaches rely on distributed data storage and aim to provide higher security, privacy, and interoperability than centralized approaches [107]. As such, decentralized solutions address several issues of both paper-based and centralized electronic approaches to medical prescriptions. Extant literature often uses a blockchain as the underlying decentralized infrastructure. Its function as a synchronized single source of truth allows for the avoidance of, e.g., manipulations or the double-spending of e-prescriptions [119]. Nonetheless, several issues remain, and new problems emerge in blockchain-based approaches. In particular, privacy concerns are exacerbated due to replicated data storage as well as the immutability of blockchains that renders deletion practically impossible [41, 107]. This affects not only patients' confidentiality requirements but also compliance with associated regulatory requirements, such as the EU's general data protection regulation (GDPR), the California consumer privacy act (CCPA) or the US health insurance portability and accountability act (HIPAA). Furthermore, interoperability often remains a problem, as the suggested implementations are not built on common standards, and sensitive data is typically exchanged using third-party infrastructures. Besides, the existing suggestions often impose the management of cryptographic keys directly on the users or rely on yet another smartphone app (or even device) that users need to carry and use specifically for e-prescriptions.

In the last years, an alternative approach for exchanging verifiable data in a decentralized way has emerged through portable digital identities managed in so-called "digital wallets" [96, 114]. This paradigm is often termed self-sovereign identity (SSI) [20, 96]. SSI offers standards and protocols for end-to-end encrypted bilateral

communication and practices for selective and verifiable information disclosure based on digital certificates [26, 105]. However, preventing the double-spending of e-prescriptions that are purely based on digital certificates is not possible solely through bilateral communication, as one pharmacy cannot know whether an e-prescription has already been presented and redeemed at another pharmacy. We hence propose that the combination of blockchain technology for double-spending prevention and SSI digital wallets for the verifiable exchange of sensitive e-prescription data and key management potentially offers properties solving current solutions' shortcomings regarding interoperability, performance, scalability, and security to e-prescription management. Summarizing, paper-based prescriptions are susceptible to forgery, inefficiency, and do not integrate with digital services. Digitizing prescriptions through centralized technical infrastructures poses socio-economic, interoperability, and security issues. Decentralizing e-prescriptions through blockchain technology has proven to be susceptible to privacy-related issues and did not specify a suitable user interface. Digital wallets based on the principles of SSI have been suggested in fields with similar requirements, such as event ticketing [27], and they may be suitable to also solve this issue [84]. Thus, we pose the following research question: *How to design and implement a decentralized system for e-prescription management using blockchain technology and digital wallets?* To answer this research question, we follow the design science research paradigm. Our evaluation finds that our solution overcomes the shortcomings of existing approaches regarding interoperability, performance, scalability, and provides a sufficient level of security.

2 THEORETICAL BACKGROUND

2.1 E-Prescriptions

In the UK alone, nearly 1.5 million medical prescriptions are processed on a daily basis [1]. Similarly, 11.6 prescriptions were filled in US-pharmacies per capita in the year 2019 [50]. The value of prescription pharmaceuticals prescribed per year globally accounts for approximately $1 trillion [66]. To account for limitations of existing approaches to handling the increasing number and value of medical prescriptions, researchers and practitioners alike aim to optimize the process of prescribing and dispensing pharmaceuticals. Accordingly, e-prescription systems have been introduced, which can help to increase both the accuracy and the efficiency of provisioning medication to ensure patients' safety while streamlining processes [1, 34, 112]. Submitting and exchanging prescription information digitally is considered to reduce medication errors, minimize overhead due to paperwork and, thus, time resources needed for administrative tasks, additional to increasing patients' convenience [1, 34]. Accordingly, e-prescription management systems enable the creation of prescriptions, their transmission to a pharmacy, and their validation and usage at a pharmacy in a solely digital manner.

However, e-prescription systems come with several challenges. While paper-based prescriptions can be physically invalidated upon redemption, e-prescriptions must have a sophisticated mechanism for preventing double-spending [54], as copying electronic documents has close to zero marginal costs. This requires some degree of transparency about whether an e-prescription has been already redeemed, particularly when the ecosystems involves several different stakeholders such as many independent pharmacies and doctors among which the patient can choose. These transparency requirements, however, are to be balanced with the protection of sensitive information, for example, patients' data according to the GDPR within the EU. This includes aspects like the right to erasure ("Right to be forgotten"), meaning that users can request their data to be deleted at any point in time (Article 17 GDPR) [25]. Besides, the data specified in an e-prescription must also be secure against manipulation by unauthorized parties. A further challenge for e-prescription systems is posed by the need for standardization, as data processing and exchange between many stakeholders requires interoperable systems [54].

Countries such as the USA, Australia, the UK, Spain, and Denmark have already introduced e-prescription systems at scale [1, 10]. The respective systems are usually not standalone products but embedded in more

comprehensive e-health systems including, e. g., patients' electronic health records. A comparative study conducted by Aldughayfiq and Sampalli [1] found that most implementations build on designs employing a central database for storing e-prescriptions. This design choice can effectively enforce access control and compliance with business logic (such as double-spending prevention) and provide fine-grained access management rules to address confidentiality requirements. However, there are also considerable risks. First, a centralized approach represents a single point of failure, meaning that the system is more vulnerable to attacks [116]. This is also illustrated by a considerable number of privacy breaches in centralized systems in the past [74]. Second, patients cannot be sure that the operator of a centralized system or database does not sell sensitive data to third parties. Sensitive data is available for any participant integrated in the infrastructure with the necessary access permissions [1], and the patient needs to rely on the effectiveness of regulation and audits to enforce data protection. Third, centralized solutions challenge the interoperability of systems. For example, Bruthans [10] found that the authentication mechanisms used for e-prescription systems in Europe are often incompatible. Fourth, network effects carry the risk of centralizing control over data and operations and, thus, can cause monopolies, which hinders productive collaboration in the long run [43].

Decentralized systems aim to address some of these problems. For example, Surescripts, an e-prescription management system in the USA, allows entities such as caregivers to access patient information from patients' pharmacies and health insurance companies through the system [1]. However, such approaches impose significant responsibility regarding IT security and access management on pharmacies and health insurances, which may be particularly problematic for small organizations. Furthermore, in Surescripts, patients have to choose a specific dispensing pharmacy when their e-prescription is created, which decreases users' flexibility and convenience. Consequently, researchers have continued searching for better solutions, and in recent years, they have considered blockchain technology [116].

2.2 Blockchain

Since the emergence of Bitcoin [72], an increasing number of researchers, companies, and government agencies have pointed out the technology's potential beyond financial applications to provide decentralized digital infrastructures and improve cross-organizational processes [29, 47]. This has also led to the emergence of a large number of architectural proposals and implementations at varying stages of maturity, especially in the healthcare sector [67]. At its core, blockchain technology provides a distributed and replicated append-only database that groups transactions in blocks on each node of a peer-to-peer network [12]. Aiming to obliterate the need for a central trusted authority [72], the nodes of the peer-to-peer network repeatedly agree on the state of the system by following a consensus protocol [16, 30]. Each block in a blockchain is linked to the previous block through a cryptographic hash pointer. The blocks, therefore, form a chain, creating a tamper-resistant historical data record [12]. Thus, blockchains create a single point of truth between all participants in the distributed ledger [82]. As such, blockchain technology can create neutral platforms [4, 45, 94, 113] that naturally improve the interoperability between individual organizational solutions. Previous research has already analyzed the benefits of blockchain for interoperability in the health sector [19, 31]. Furthermore they provide a solution to the double-spending problem in decentralized systems [72]. Due to their technical structure, blockchain systems provide several important properties. Resulting from the resistance against crashes or the malicious behavior of a small number of nodes, blockchain systems are highly available and decentralized digital infrastructures [3]. To participate in consensus or to interact with the peer-to-peer network and authorize transactions, users of a blockchain system must authenticate using public-key cryptography. As a result, blockchain systems also offer an integrated public key infrastructure.

To account for the requirements of different use cases, various concepts of blockchain technology have emerged. A prominent conceptualization by Peters and Panayi [76] distinguishes blockchains along two dimensions. First,

transactions in public blockchains are publicly visible, while transactions in private blockchains are only visible to the parties that run the network's nodes. Second, permissionless blockchain systems allow anyone to participate in consensus by proposing new blocks, while this right is retained to authorized parties only in permissioned blockchain systems. As the technology has gained increasing prominence, developers introduced smart contracts, which can be defined as scripts that are executed redundantly on the nodes' virtual machines [11, 62]. Smart contracts enable a large variety of transactions that go well beyond the transfer of cryptocurrencies [7]. One specific application area of smart contracts is the exchange of a broad variety of digital assets. These so-called *tokens* are value containers that represent digital or non-digital, scarce objects and that can be transferred among the participants in a blockchain system [73, 77]. The opportunities related to the "tokenization" of physical and digital objects are considered an essential trend for the economy [108]. Tokens' inherent value can also help coordinate processes among mutually distrusting parties or in fluid organizations[60, 89].

Nonetheless, several tradeoffs and challenges remain when using blockchain systems [51]. While energy consumption is only problematic for a specific consensus mechanism, namely proof of work [93], blockchains in general exhibit challenges regarding scalability and data visibility due to the inherent replicated storage and execution of transactions [51, 57]. Specifically excessive information exposure implies significant challenges both from the perspective of natural persons' data protection as well as organizations' sensitive business data. This issue is aggravated by blockchains' immutability guarantees that inhibit the retrospective deletion of sensitive information accidentally stored on a blockchain [88]. Blockchains' inherent pseudonymization through addresses representing public keys does not considerably mitigate this problem, as the aggregation of information from different domains can provide sufficient means for de-anonymization [81]. While permissioned blockchains partially address this problem through restricting access to selected organizations running the network's nodes, still all of these participants can see each other's transactions by design. Thus, from the perspective of an attacker that intends to retrieve sensitive information, a permissioned blockchain is a centralized system with yet more attack vectors [78]. "Private transactions" that contain only hashed or encrypted information have been implemented in permissioned blockchains to address enterprises' requirements (e. g., in Hyperledger Fabric and Quorum); however, this approach also restricts the functionality of smart contracts, as these typically cannot run on obfuscated data. Trusted execution environments and advanced cryptographic tools such as zero-knowledge proofs (ZKPs), multiparty computation, and (fully) homomorphic encryption can be used to bring some of this functionality back, but can come at significant complexity and often have their own performance issues [97, 119]. Consequently, the use of blockchains should be well-considered when it comes to the processing of sensitive information.

2.3 Self-Sovereign Identity and Digital Wallets

SSI aims to facilitate verifiable digital identities for organizations, end users, and networked machines that are not tied to a certain place or organization and that can be used across domains with the identity owners' consent [2]. SSI involves three distinct types of entities [70]: the issuer of an identity document, the holder of the respective document, and the verifier of properties described in the document. An analogy from the physical world serves as an illustration of the basic interactions [96]: An SSI system builds upon digital representations of tamper-resistant physical documents like ID cards or driver's licenses [5]. Appropriate organizations, such as government authorities, issue the respective documents to their holders, who subsequently store them in a physical infrastructure of their choice, such as a wallet [114]. Such documents typically follow specific schemas, such as watermarks and attribute names, which have been made public by their issuer. As a result, the integrity of such documents can be verified by third parties in bilateral interactions with their holders. In this system, the issuer's trustworthiness is important from the verifier's perspective.

The building blocks and principles of an SSI system can be derived from this analogy. Tamper-resistant physical documents relate to verifiable credentials (VCs), which are cryptographically signed digital objects containing claims about their holder's identity and authorizations [20, 79, 105]. Holders store these VCs in an (for end users typically mobile) application called "digital wallet" [84]. To prove properties, or claims, described in their VCs to a verifier, holders generate verifiable presentations (VPs). These VPs are tamper-proof attestations derived from one or multiple VCs to address the requirements posed by a verifier [39, 79, 105]. This can either be achieved by presenting the signed credentials themselves, e. g., a JSON Web Token, or by creating a cryptographic ZKP, for example from an anonymous credential [15, 40]. The latter method allows data minimization in the form of selective disclosure, where only a subset of the attributes contained in a VC can be revealed.

Entities within an SSI system often use so-called decentralized identifiers (DIDs) as identifiers, which are unique and follow a standardized schema [106]. They also serve to create a standardized end-to-end encryption between two parties. DIDs corresponding to public institutions can be made publicly discoverable as an alternative to certificate authority (CA)-based binding of public keys, domain names, and IP addresses. To avoid unnecessary causes of correlation, it is recommendable for natural persons to use a new, private ("peer") DID in each interaction [91]. While these building blocks provide a solid foundation for an SSI system, a neutral infrastructure is necessary: information about issuers of VCs, such as their current signing keys, and revocation-related information must be publicly available to verify the correctness of VPs. By proving knowledge of the issuer's digital signature and non-inclusion of their VC in a public but privacy-protecting revocation registry (in the form of a cryptographic accumulator), holders can convince a verifier that their VC has not been revoked without having to contact the credential issuer [91]. Furthermore, schemas of VCs must be publicly available to verify the integrity of VPs. Due to its properties as a decentralized and highly available data structure, blockchain technology is often used for this purpose [26, 70]. Lately, the concept of SSI and digital wallets has been applied in a variety of endeavours [27, 58, 91]. For example, the current efforts of the European Union to improve the legislation as well as the realization of electronic Identification, Authentication and Trust Services (eIDAS) feature many parallels to SSIs-based systems [23] . One of the proposed use cases to be developed in the context of eIDAS 2.0 specifically represents e-prescriptions [21].

3 METHOD

3.1 Design Science Research Approach

We answer our research question by employing a design science research (DSR) approach. The goal of DSR is to design, develop, and evaluate IT artifacts as solutions to practical challenges, thus aiming to solve real-world problems [44, 65]. DSR faces the dichotomy of proposing a feasible solution to practice, whilst providing a valid contribution to theory at the same time [6]. We aim to solve this issue by designing, implementing, and evaluating a system for e-prescriptions based on blockchain technology and digital wallets. The resulting IT artifacts build on foundations from previous research. To infer a contribution to theory, we subsequently derive design principles (DPs) to offer more generalizable knowledge on the implications of designing and developing IT artifacts with similar requirements [32] such as privacy protection and double-spending prevention. We adhere to the DSR model proposed by Peffers et al. [75] to guide our research, which consists of six partly overlapping as well as iteratively conducted steps. The initial step starts the process by defining a research problem of practical relevance. As laid out in section 2, current solutions for e-prescriptions are prone to security incidents, lack interoperability, provide socio-economic risks, and offer opportunities for fraud. Thus, the design of systems for e-prescriptions solving these issues is a problem of practical relevance. In the second step, we derive requirements for our solution by reviewing existing proposals for implementing e-prescriptions identified in a structured literature review. We define 8 design objectives for our proposed solution, which we present in section 4.2. Adhering to these design objectives, we develop a system architecture and instantiate it by implementing a

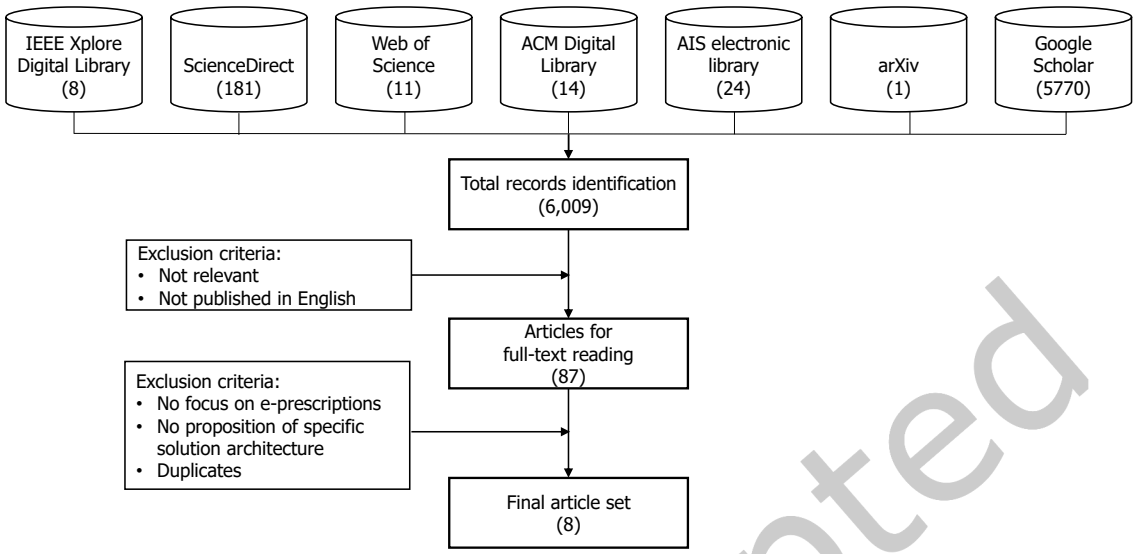

Fig. 1. Systematic literature review for the search string "blockchain AND prescription AND health".

prototype based on blockchain technology and digital wallets[1]. We thus contribute both an architectural design as well as a prototype as IT artifacts. To evaluate the fulfilment of our design objectives and to highlight advantages as well as remaining shortcomings, we evaluate the developed IT artifacts quantitatively as well as qualitatively along the criteria defined by the design objectives [103]. In a sixth step, we present our artifact in this publication.

3.2 Literature Review

We conducted a structured literature review to identify relevant work investigating the potential of decentralized approaches for e-prescriptions management systems following the guidelines proposed by Kitchenham and Charters [56]. Accordingly, we derived our search string on the basis of our research question [56]: "blockchain AND prescription AND health". We decided against using synonyms for blockchain technology as it is regarded as the most prominent concept associated with decentralization and often serves as a solution for implementing e-prescriptions in a decentralized way [41, 110, 112]. We screened the databases ACM Digital Library, AISeL, arXiv, IEEE Xplore, Google Scholar, ScienceDirect and Web of Science as they represent the prevailing databases in the computer science and information systems research domain. The initial search yielded 6,009 results in total (see figure 1).

We included research in English language only. During title screening, we excluded papers that did not mention blockchain and health (or synonyms) in their titles to ensure the relevance of our article set. As Google Scholar yielded 5770 results, we screened the titles of all results until no papers related to our research question could be identified for 50 results in a row, sorted by relevance. Subsequently, we screened the contents of the remaining papers. First, we excluded papers that did not focus on solutions for e-prescriptions. Second, following the goal of our literature review to identify existing propositions for e-prescriptions, we also excluded papers that do not cover a specific solution architecture or that give guidance on architecture design. Last, we excluded duplicates

[1]Our implementation is available at https://github.com/JSedlmeir92/e-Prescriptions.

from our article set. We found that although blockchain is often mentioned as a viable technology for the health care sector in general [22, 52, 98], the literature dismissed challenges related to the privacy of medical data [101], mainly neglecting privacy-by-design in blockchain-based health systems [102]. Moreover, extant literature only rarely explicitly proposes architectures for the management of e-prescriptions. In contrast, the current literature body places its focus on blockchain-enabled medical supply chains [48, 66, 83], electronic health records [17, 118], and the management of medication histories [55, 80]. Furthermore, while some authors address e-prescriptions explicitly, they focus on implementations and requirements in a specific country, hindering the generalization of their findings [64].

4 RELATED WORK AND DESIGN OBJECTIVES

4.1 Related Work

Through our literature review, we identified seven papers in total that explicitly propose or survey blockchain-based solutions for e-prescription processes. After we had identified the final article set, we extracted information about the requirements mentioned by the authors, the proposed solution architecture, as well as related advantages and challenges. To ensure intercoder reliability, every paper was coded by at least two authors. In the following, we will analyze these papers depicted in table 1 in detail.

Many publications exploring the advantages of blockchain technology for e-prescriptions do not address the privacy-related challenges of blockchain technology in their suggested solutions. For example, Thatcher and Acharya [111] as well as [112] propose an e-prescription management system that integrates a blockchain-based "immutable database of prescriptions". While the proposed design ensures tamper-resistance and accountability for processing e-prescriptions, the authors acknowledge that it dismisses patients' privacy [111], thereby highlighting an essential requirement for e-prescriptions. He et al. [41] also acknowledge privacy-related issues in current approaches to decentralized e-prescription systems and suggest a permissioned blockchain for the management of e-prescriptions. However, their proposed architecture still stores sensitive patient data on-chain and hence leaves them more vulnerable to cyber-attacks than they would be in a centralized database, as we discussed in section 2.2. Similarly, Cadoret et al. [13] suggest storing prescription data in private, permissioned blockchains. They also propose using ZKPs for addressing privacy challenges if a public blockchain was used, but do not

Authors	Year	Title	Ref.
Cadoret et al.	2020	Proposed Implementation of Blockchain in British Columbia's Health Care DataManagement	[13]
Gropper	2016	Powering the Physician-Patient Relationship with HIE of One Blockchain Health IT	[33]
He et al.	2019	BlockMeds: A Blockchain-Based Online Prescription System with Privacy Protection	[41]
Li et al.	2019	DMMS: A Decentralized Blockchain Ledger for the Management of Medication Histories	[61]
Meena et al.	2019	Preserving Patient's Privacy using Proxy Re-Encryption in Permissioned Blockchain	[68]
Thatcher and Acharya	2018	Pharmaceutical Uses of Blockchain Technology	[111]
Thatcher and Acharya	2020	Towards the Design of a Distributed Immutable Electronic Prescription System	[112]
Ying et al.	2019	A Secure Blockchain-based Prescription Drug Supply in Health-Care Systems	[117]

Table 1. Results of the structured literature review (conducted in January 2021).

provide details how the associated access management would work or on which layer the sensitive data could be exchanged. In both solutions, patients do not have control over which data is shared. This problem is addressed by Li et al. [61] and Meena et al. [68], who suggest systems which allows patients to decrypt data that is saved on the ledger upon request by pharmacies. As a result, stakeholders other than the patient are unable to make sense of the encrypted data. Yet, as the decrypted data is shared bilaterally between the patient and the pharmacy, the purpose of blockchain is limited to facilitating data integrity checks. Simpler means to achieve data integrity, such as digital signatures, are not considered. Moreover, the permanent storage of encrypted data on a blockchain may become an attack vector in the future due to the increase of computing power over time and the potential availability of sufficiently powerful quantum computers within the next decades [88]. This concern is manifested by ongoing controversial debates in the EU whether or not encrypted data should be classified as personally identifiable [28]. Both publications do not suggest how users' cryptographic keys get managed and how patients are enabled to interact with various involved stakeholders. Finally, Ying et al. [117] propose an architecture that ensures privacy throughout the process of dispensing drugs, but they omit the integration of central stakeholders such as the users in their considerations and, thus, cannot give users control over which data is being shared between doctors and pharmacies.

Our structured literature review includes two publications whose concepts build upon SSI in the digital healthcare context. While Cadoret et al. [13] briefly outline SSI as an authentication mechanism for users of blockchain-based medical services, Gropper [33] propose a more extensive SSI-based system for overcoming the current challenges of electronic medical records. However, the latter authors do not provide details on how multiple usages of e-prescriptions can be prevented. If there is only one pharmacy where the e-prescription can be spent, a serial number in the VC that needs to be revealed can be used to prevent repeated redemptions. In the case of multiple pharmacies, one would either need to synchronize the serial numbers of redeemed VC among all pharmacies or require interactions between pharmacies and doctors, where the pharmacy redeeming the prescription asks the doctor to revoke the credential. This approach would, however, introduce significant additional complexity.

4.2 Design Objectives

From the structured literature review, we derive a set of design objectives for a decentralized e-prescription management system. Both existing paper-based and e-prescription processes demonstrate certain requirements that must be fulfilled. For example, the current redemption process of paper-based prescriptions ensures that each prescription may be redeemed only once. Furthermore, the strengths and weaknesses of decentralized approaches proposed in related work allowed us to derive additional requirements.

Table 2 summarizes the design objectives that we found in our literature review. The derived requirements serve as a basis for the remainder of this paper and inform and guide the design and implementation of our proposed system architecture. They also represent the objectives along which we evaluate our artifact in section 6.

Nr.	Requirement	Context	References
R.1	Disclosure control	As personal health data is highly sensitive, users' privacy must be ensured. Users can choose with whom to share what parts of their e-prescription.	[13], [33], [41], [61], [68], [111], [112] , [117]
R.2	Decentralization	To prevent the abuse of patient data through operators of centralized solutions and large-scale data breaches, no centralized data silos containing patient data must exist. A decentralized solution can also ensure high availability guarantees, which is important for the functionality of a critical system.	[13], [33], [41], [61], [68], [111]
R.3	Pharmacy independence	To ensure competition and a free choice of pharmacy for patients, the user must not be bound to a specific pharmacy for redeeming the prescription.	[33], [41]
R.4	Key management	The developed system must be convenient to use and should not create unnecessary overhead owing to cryptographic key management for users.	[61], [68], [111]
R.5	Interoperability	Current implementations for e-prescriptions differ significantly, hindering interoperability and thereby adoption as a result. Interoperability could furthermore extend the application areas of e-prescription systems.	[13], [33], [61], [112]
R.6	Scalability and performance	The e-prescription management system must be able to quickly handle a sufficient number of prescriptions redeemed on a large scale, even at peak times.	[13], [33], [41]
R.7	Double-spending prevention	To prevent fraud, prescriptions must not be redeemed twice, or not more frequently than the number of times intended in the case of periodic prescriptions.	[112]
R.8	Verifiability	Pharmacies need to fully automatically verify the integrity and authenticity of e-prescriptions to ensure the correctness of prescription information, the doctor's authenticity as well as the patients' eligibility to receive medicals.	[13], [33], [41] [61], [68], [111], [112]

Table 2. Design objectives for an e-prescription management system.

5 ARCHITECTURE AND IMPLEMENTATION

5.1 Conceptual Architecture

Following the DSR research paradigm [44, 75], we iteratively developed an architecture for the management of e-prescriptions that addresses the previously derived design objectives. We built on the two major paradigms for decentralized digital interactions discussed in section 2: On the one hand, we leverage digital wallets for the bilateral and verifiable exchange of sensitive information. On the other hand, we employ blockchain technology to prevent the double-spending of e-prescriptions.

We split the design process in two cycles: First, we designed the architecture involving the stakeholders *doctor*, *patient*, and *pharmacy* for issuing and redeeming e-prescriptions. Doctors and pharmacies are each running an institutional agent [91] to issue VCs and verify VPs, respectively. The patient is carrying a digital wallet on their smartphone and interacts bilaterally with the doctors and pharmacies of their choice. No direct communication between doctors and pharmacies is necessary, as the authenticity of VPs derived from VCs can be verified through the issuer's signature on the VC and revocation registries' accumulator states published on a blockchain or another public data registry. The patient first visits their doctor, who issues an e-prescription that includes information such as the patient's and doctor's name, a specification of the prescribed pharmaceutical, and its quantity to the patient's smartphone wallet through a bilateral, end-to-end (E2E) encrypted communication channel. Subsequently, the patient can present the e-prescription VC to a pharmacy, which checks its validity

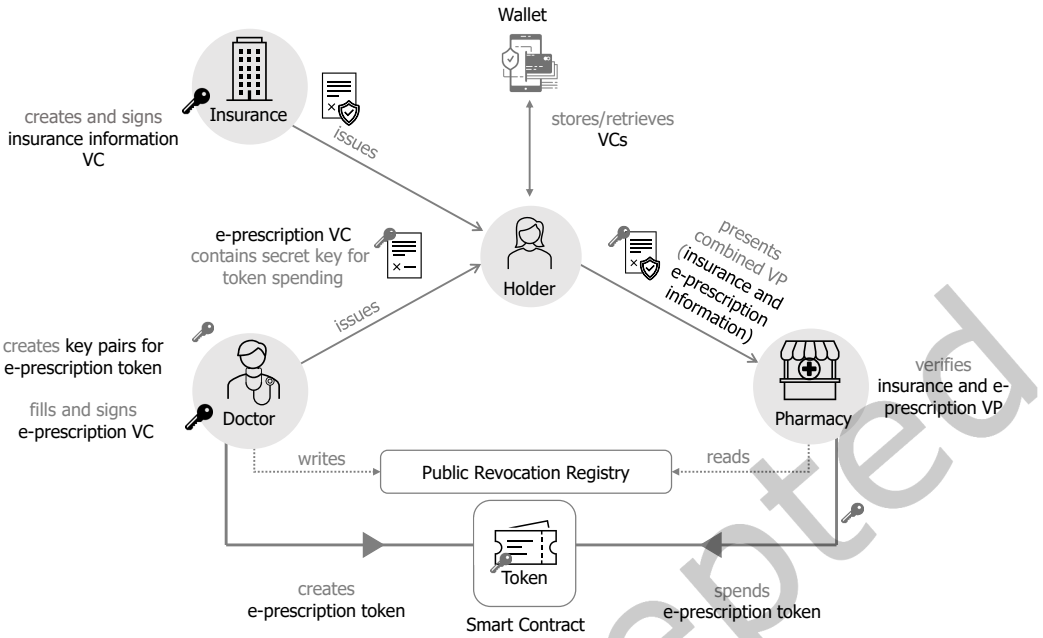

Fig. 2. E-prescriptions based on verifiable credentials with anonymized blockchain-based tokens for double-spending checks.

based on the list of doctors and their associated public keys that they trust and retrieves the information to release the right medical.

As we received feedback on the integration of our e-prescription solution, we extended our architecture to embed it within the healthcare ecosystem. As a result, patients initially receive a VC that attests their identity and health insurance information, such as name, address, and insurance policy number. When connecting with their doctor in a branch or remotely, patients can give a presentation of their health insurance VC, which the doctor can use to verify the patients' identity and, thus, to be sure that they issue the e-prescription VC to the right wallet. Similarly, after having received their e-prescription, patients can then connect with their pharmacy, again either remotely or through visiting a branch, and give a combined VP of the e-prescription VC as well as information associated with the health insurance VC that they can use to streamline the billing process. To add the respective e-prescription to the patient's health record, a receipt could be given to the patient as a VC, which they can then present to their insurance maintaining the respective health records. Alternatively, this could be done directly by the pharmacy in a bilateral interaction with information obtained through the e-prescription VC. We highlight that it is necessary for patients to use a one-time DID for communicating with a pharmacy (and a doctor), as otherwise privacy-compromising data analysis could be performed.

To prevent the double-spending of e-prescriptions, we link a blockchain-based token that does not carry sensitive information to the e-prescription VC. To provide an efficiently and conveniently usable key management associated with the token, the e-prescription VC includes the private key that can be used to control the token: As the patient trusts the doctor and the pharmacy concerning the prescription that they want to spend, it is not necessary that the patient has exclusive control over the token at any point in time – the patient can simply carry information that is necessary to retrieve and invalidate the token for double-spend protection *in*

the e-prescription VC. Doctors and pharmacies hence both run a blockchain client, and upon onboarding, a doctor creates a (long-term) key pair (sk_{doctor}, pk_{doctor}) and deploys a smart contract granting the doctor the right to create new tokens. When the doctor wants to issue an e-prescription, they generate a new keypair (sk_{presc}, pk_{presc}) that is only used for this one specific prescription. Next, the doctor creates a new token that can only be spent by the controller of pk_{presc}, i.e., by anyone who knows sk_{presc}, in the smart contract by signing an associated transaction with sk_{doctor}. The doctor then includes the smart contract's address and sk_{presc} in the e-prescription VC. Consequently, any party that receives a VP of an e-prescription VC that reveals sk_{presc} can potentially invalidate, i.e., spend, the associated token if they can send it to an entity with write access on the blockchain. Thus, the patient should not reveal this attribute on the e-prescription VC to a party that they do not trust. Notably, selective disclosure still allows to use the e-prescription VC for VPs towards entities the patient does not trust regarding the control of the token.

We employ two separate blockchains for the purpose of storing SSI-related information on a specialized infrastructure and implement token-management functions on the other. The rationale behind this design choice is that Hyperledger Indy provides a mature decentralized framework specialized in providing identity management, while Quorum offers wide token management functionalities. Theoretically, the functionalities offered by the Hyperledger Indy blockchain could be implemented on the Quorum blockchain as well. This may even be desirable for managing complexity, albeit initially, several new implementations would be required. Thus, our solution is conceptually reproducible with only one blockchain. Nonetheless, Indy provides a widely accepted standard in other identity ecosystems, such as Germany's IDunion or Canada's Verifiable Organizations Network, which makes integration of the digital wallet in other settings easier. Moreover, as the blockchains manage strictly independent tasks, we consider the complexity due to relying on two blockchain implementations as reasonable for now. Nevertheless, adapting our solution with regards to this aspect could be a long-term improvement goal as soon as the respective tools and frameworks are available within one infrastructure.

Spending the e-prescription involves minimal effort, as all necessary information is contained in the VCs: Upon the verification of a combined VP from the e-prescription VC and health insurance VC, the pharmacy can use their blockchain client to invalidate the respective token, as they can control it using sk_{presc}, which they learned from the VP. As the transactions in a blockchain are ordered, double-spending is prevented. Even in case the patient tries to spend the e-prescription at many pharmacies in parallel, all token-related transactions of pharmacies will be ordered. Thus, only the first transaction will succeed in retrieving the token; all the others will return an error message indicating that the token has already been spent and, thus, the e-prescription cannot be redeemed any more. After spending the e-prescription, the pharmacy can use the billing information also obtained from the VP to enable the automation of their billing processes; which a similar technique that builds on combining a VC and a token to avoid that patients can get reimbursement for the same bill multiple times. For all these functionalities, a user does not need a dedicated app, but can use their digital wallet that is familiar from other identification and authentication processes.

5.2 Implementation

We illustrate the components of our implementation of an e-prescription system based on our proposed architecture in figure 3. We tested this prototype in an isolated environment, without interactions with legacy systems or stakeholders. Our implementation requires smart contracts to create tokens that prevent the double-spending of e-prescriptions. Consequently, we chose an Ethereum-based blockchain because the Ethereum virtual machine and Solidity represent a sufficiently mature technology stack for smart contract implementation. Furthermore, we aimed for a scalable e-prescription system that provides the necessary level of throughput to operate e-prescriptions for several countries across the European Union while keeping transaction costs negligible. Thus, we decided to use the private Ethereum-based blockchain Quorum. It has been designed for enterprise applications

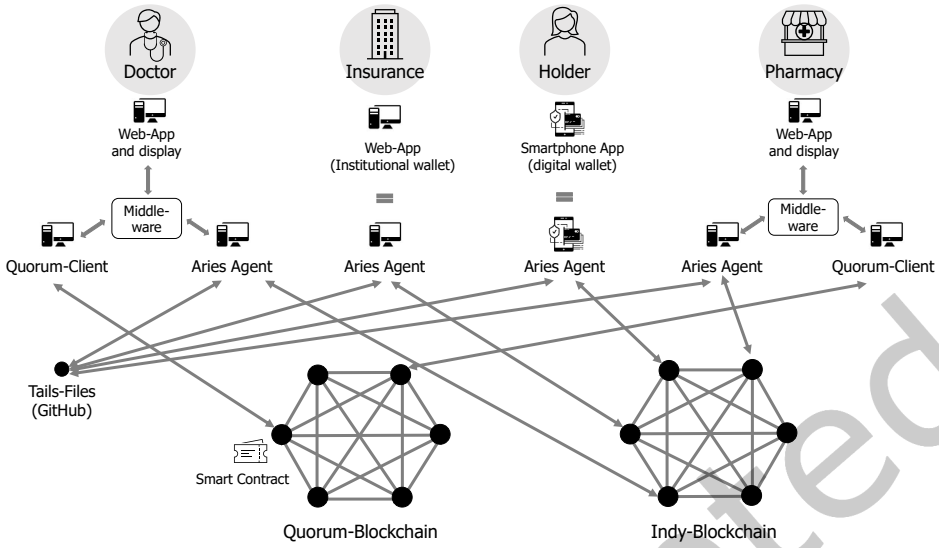

Fig. 3. Technical components of the proposed e-prescription management architecture.

and provides the lowest latency and highest throughput in recent benchmarks [51, 95]. Moreover, due to the use of Istanbul byzantine fault tolerant (IBFT), it provides a highly secure Byzantine Fault tolerant consensus mechanism, whereas many other private Ethereum implementations only provide crash fault tolerance (e.g., Clique consensus of Geth, Aura consensus of Parity).

We decided for the permissioned option due to its high throughput, low latency, low energy consumption, and low transaction costs. Doctors and pharmacies consequently run Quorum clients for token creation and spending. The smart contract that serves to prevent double-spends specifies that a Prescription token must have two attributes, namely its issuer (the doctor's public key) and an indicator of how often it can be spent at most. On instantiation, the contract creates a registry for such prescriptions, i.e., a mapping of public keys (pk_{presc}) to prescription tokens, and specifies that only the creator of the contract (the *admin*, i.e., the doctor) can create new prescription tokens. The smart contract furthermore ensures that only someone who can prove control over a public key associated with a token can spend it, and only as often as initially specified by the doctor in *count*. The smart contract code is provided in figure 6 in the appendix. We also deployed Node.js-based Quorum-clients for doctors and pharmacies, which invoke transactions for creating resp. spending tokens, given the contract address and pk_{presc} resp. the contract address and sk_{presc}.

We set up a four-node Hyperledger Indy blockchain network that provides the functionality to store a schema defining the attributes of e-prescriptions and health insurance VCs ("template"), doctor and insurance-specific credential definitions (specifying a doctor's and insurance's signing keys) and revocation registries based on cryptographic accumulators that allow the patient to create ZKPs of non-revocation in their VP. In addition, we deployed an instance of the Hyperledger Aries Cloud Agent in Python, which acts as an Indy-client and a RESTful API for bilateral communication, issuance of VCs and the verification of VPs, for doctors, health insurance, and pharmacies. In theory, the proposal could also be implemented with one blockchain alone as long as both the functionalities required for smart contracts as well as identity management are given. However, we chose two different blockchains mainly because they are specifically suitable for the two main tasks that we require: On the one hand, we require token management functionalities, which are currently represented by the Quorum

Fig. 4. Screenshots from the user's wallet: Overview of the user's VCs (here: only one e-prescription for simplicity), visual check of requested attributes in a VP, and overview of active connections as well as shared data in the esatus wallet.

blockchain as outlined above. On the other hand, Hyperledger Indy provides a mature decentralized identity management framework. To the best of our knowledge, there is no alternative implementation as mature as Hyperledger Indy specifically when it comes to compatible digital identity provisioning. Furthermore, we aimed to use an implementation framework for SSIs that offers users a high level of usability [84]. Regarding the Aries Cloud Agents, there currently are several different digital wallets are available, which are compatible with the backend (e.g., Trinsic, Lissi, esatus, and ID Wallet). Additionally, the proposed solution should fulfill a high degree of privacy. The DIDComm protocol used in Hyperledger Indy and Aries relies on ZKPs for selective disclosure and set-membership proofs to convince a verifier that an e-prescription is not revoked without revealing a correlatable e-prescription identifier [91]. We also implemented a web-application (frontend) with the Django framework in Python. This web-application can be used for the doctor's onboarding process (deploying the smart contract) as well as connecting to patients, issuing VCs to them, and requesting a VP. For demonstration purposes of the required functionality for the patient, we employed a smartphone digital wallet app based on the .NET implementation of the Hyperledger Aries protocol. The wallet has been developed by the IT company esatus AG and is available for free in the Google Playstore for Android and the App Store for iOS. It is not built for a specific use case like e-prescriptions but for the generic exchange of verifiable information (such as ID cards, credit cards or diploma) based on standards that are related to the W3C DID and VC standards [105, 106]. Beyond the basic capabilities such as ZKP-based selective disclosure and proofs of non-revocation, it additionally supports custom Hyperledger Indy networks, provides backup functionalities, and recently, it was demonstrated that the content of the esatus wallet (including cryptographic keys and VCs) can be exported to and imported from another wallet implemented by Trinsic [104]. Similar wallets are also offered by Evernym (Connect.me wallet) and the German IDunion consortium (Lissi wallet).

Mobile wallets can connect with a cloud agent through scanning a QR-code. Alternatively, existing communication channels, such as an e-mail, can be used for the initial exchange of information, e. g., in the form of a link, on how to establish a connection. The QR-code contains the cloud agent's uniform resource locator (URL) endpoint as well as further meta-information. It can be static or personalized, and it must be accessible to the patient, e.g. when checking in at the doctor, or on a health insurance's or pharmacy's website. At first, the health insurance issues an insurance VC to the patient. Upon a doctor visit, the patient establishes a connection with the doctor's cloud agent and is subsequently asked for a presentation of their insurance VC to map the connection to master data like the patient's name and insurance number. Next, the doctor can fill out the contents of the e-prescription on a simple web interface or further automated programs, as they would do for any electronic and machine-readable prescription. By selecting the connection to the patient, a doctor can trigger the issuance of the e-prescription VC to the patient and the creation of the associated token in the doctor's smart contract. At the pharmacy's branch or website, the patient only needs to scan a static QR-code, which the wallet can again use to establish an E2E encrypted connection to the pharmacy. It is important to understand that this connection can be unique and non-correlative for each pharmacy visit, thus allowing for privacy by avoiding metadata analysis. This action automatically triggers a proof request from the pharmacy. Consecutively, the patient must select the e-prescription they want to spend and the respective insurance information. Upon confirmation, the patient can then share the requested attributes. During all these processes, the patient has full control over which of their personal data is shared, which connections they have established yet, and also an overview of the data that they have shared. We present screenshots from the wallet during and after the process in figure 4.

6 EVALUATION

Our proposed solution aims to address the design objectives that we determined in section 4. Thus, we aim at solving the issues implied by paper-based prescriptions and centralized as well as exclusively blockchain-based e-prescriptions. In the following section, we evaluate our design and implementation along these design objectives.

We address multiple requirements of digital e-prescription management systems by building on the SSI paradigm. We rely on SSI for the interactions of the involved stakeholders, enabling bilateral and hence decentralized data exchange. First, this approach allows users to exercise **disclosure control**, as the standardized VCs containing prescription-related information and the spending key of the associated token is transferred to patients and stored only in their digital wallet of choice. Accordingly, the physical prescription is digitized through a VC that is stored only on the patient's device and in particular not on a centralized or decentralized ledger that would allow to track patients' interactions with doctors and pharmacies. Our design based on bilateral communication between stakeholders is, therefore, more privacy preserving than alternative solutions such as private channels in a Hyperledger Fabric permissioned blockchains. This also allows to avoid the corresponding scalability challenges of partially replicated storage of the private data's hashes on-chain [38]. The data minimization capabilities offered by existing implementations of digital wallets and especially the opportunity to leverage selective disclosure gives patients additional **privacy** and considerably more **control** over which data they share than they would have with a physical prescription.

Furthermore, the SSI paradigm allows patients to interact bilaterally with their doctors and pharmacies. As the authenticity of VPs derived from VCs can be verified through the issuer's signature, no direct communication between doctors and pharmacies is necessary to verify the correctness of information included in the e-prescription. This allows for **pharmacy independence** as well as **verifiability** independent of doctors. The e-prescription's integrity can be checked purely cryptographically, and the issuing doctor's identity and authorizations can be verified through a lookup on the public permissioned Hyperledger Indy blockchain. In contrast to centralized architectures, our solution does not rely on one **central control point aggregating patients' data**

and, therefore, also avoids a single point of failure, a requirement that authors have emphasized in the past [116]. As we rely on bilateral interactions and a highly resilient blockchain infrastructure for information that needs to be publicly accessible, we also achieve *decentralization* and high *availability* guarantees. All additional data required for processing e-prescriptions is stored on the patient's device. Storing the tokens' spending key in the VCs also implies that keys do not have to be transferred to the user through an additional technical component. Accordingly, token-related **key management** does not involve patients directly, which decreases complexity for them throughout the prescribing and redeeming process. Instead, our architecture requires patients to use one digital wallet that they may already use in other contexts. This also addresses interoperability concerns, which are currently often solved by reliance on central authorities offering web interfaces. Because our system provides confidentiality through bilateral interactions and disclosure control, integrity through the verifiability of the information referenced in e-prescriptions, and availability, we also adhere to the general principles of information security [115].

Our demonstration uses a digital wallet and institutional agents that follow common standards for DIDs and VCs; in general, we do not require dedicated e-prescription-related functionalities in the digital wallet. Consequently, the exchange of information between patients and other stakeholders follow common standards for digital identity management and can be used also when SSI-standards develop further in the future. Furthermore, the JSON-based structure of VCs allows to follow international standards regarding the semantics of e-prescription systems such as directed by the European Union. The respective schema can be published and made available for all participating actors on the Hyperledger Indy blockchain. Thus, we argue that our architecture ensures **interoperability**. However, we also identify potential for future research with regards to this aspect. As large-scale health systems often embed e-prescriptions, integration with existing systems like, e.g., electronic health records, should be tested for. Nevertheless, by avoiding lock-in effects induced by data silos and using generic components like standardized digital wallets, we argue that our architecture will likely integrate into other systems without major design changes.

Apart from leveraging digital wallets with the SSI paradigm to satisfy requirements of decentralized e-prescription systems, we rely on blockchain technology to address additional requirements, ensuring **double-spending prevention** through the use of blockchain tokens. In our proposed solution, each e-prescription VC issued involves the creation of a corresponding blockchain token. In analogy to paper-based prescriptions, the doctor can specify the number of times the e-prescription can be redeemed at the time of issuing the e-prescription token, which is of particular importance for long-term medication plans. This is due to the reason that the pharmacy redeeming the prescription will only dispense a pharmaceutical if the associated token has not already been spent. We employ separate blockchain implementations for storing SSI-related public information and managing the tokens due to their respective properties enabling optimized service provision for the required operations. In theory, however, one blockchain implementation would be sufficient for all operations related to our design.

Furthermore, our approach achieves interoperability both on a technical as well as domain-specific level: Since only interfaces for token creation and spending are required, our approach can be adapted to other blockchains. By using openly available and tested building blocks from blockchain technology and digital identities, we avoid the need for implementing complex new functionalities. Thus, we argue that safeguarding costs arising from complexity remains a feasible objective.

Regarding the latter, we facilitate the implementation of multiple standards for e-prescriptions. Thus, we adopt a flexible and, therefore, standard-agnostic approach to representing e-prescriptions via JSON files [9]. International document-oriented standards for health documents, such as Health Level 7 Clinical Document Architecture (HL7 CDA) [42], typically aim to facilitate the fully digital exchange and unambiguous interpretation of machine-readable documents, such as prescriptions. JSON offers these functionalities. However, JSON lacks some of the functionalities of alternatives like XML, which is used in HL7 CDA: Integrity checks are an essential

part of unambiguous and reliable interpretation. We cover this aspect in our approach through the restrictions posed by the verification of a VP: As described in section 2, the restrictions in the pharmacy's proof request ensure that a e-prescription is created according to a schema that has previously been published and hence ensures integrity. Nevertheless, an XML-based implementation of VCs is conceptually possible. Consequently, while our approach does not implement any specific existing standard, we can address all requirements underlying common standards. Our research does not target a specific geography or regulation, but mainly aims to demonstrate the potential of decentralized technologies for providing high levels of privacy and convenience in e-prescriptions.

To ensure the practicability of our system, aspects regarding **scalability and performance** must be considered, including throughput, latency, and costs. Besides, we also assess performance metrics like the end-to-end duration of the e-prescription creation and spending process for our prototype. Regarding costs, several observations of the system can be made. If the smart contract described in figure 6 was deployed on the public Ethereum blockchain, creating the token would currently cost around 60 USD, and the redemption of an e-prescription around 8 USD[2]. Moreover, the throughput would currently be limited to around 10 tx/s, and the latency for creating and sending the token would be in the order of a minute and highly volatile. For this reason, we decided to use a permissioned blockchain in our implementation. In the near future, sharding and second layer solutions such as optimistic and zk-rollups [35, 86] could enable implementing this architecture also on public permissionless blockchains with acceptable costs.

To estimate whether the throughput of existing permissioned blockchains is sufficient for a hypothetical large-scale deployment of our e-prescription management system, we conducted a performance analysis with the distributed ledger performance scan (DLPS) [95]. The respective testing framework is available open source[3]. To simulate a cross-European e-prescription system, we deployed a Quorum network in AWS, with 8 nodes each in data centers in Frankfurt, Dublin, Milan and Stockholm. As mentioned above, we chose IBFT as consensus mechanism because it is more fault-tolerant (and, thus, has a reduced performance compared to RAFT). This makes our network comparable to the design currently deployed by European blockchain service infrastructure (EBSI), where every member state of the European Union is supposed to run a private Ethereum node[4]. For these 32 nodes, we used instances from the AWS EC2 m5.2xlarge series that have 8 vCPUs and 16 GB RAM. This specification is on the lower bound of what EBSI lists as requirements for running a node. With the code of the e-prescription implementation, we also publish a configuration file that fully describes the settings that we used for the benchmarking process. This configuration file can be used to reproduce our results.

We concentrated our benchmarking efforts on the *createPrescription* method, as the gas costs indicate that *spendPrescription* is less computationally expensive. Using the DLPS, we found a maximum sustainable throughput of around 630 tx/s with a latency of 2.0 ± 0.3 s in the described setting (see figure 5).

4.5 billion prescriptions a year get filled inside the U.S. [66] and 1.5 million prescriptions per day in the UK [1]. The maximum of these approximations amounts to 14 prescriptions per citizen and year on average. In the European Union (EU), this would therefore hypothetically amount to approximately 6.1 billion prescriptions per year, so an average throughput of 200 tx/s for each creating and spending e-prescription token is required.

[2]The Gas costs for creating a prescription in the public Ethereum network are approximately 85,000 Gas. 1 Gas currently costs around 10^{11} Wei. One Ether corresponds to 10^{18} Wei, i.e., 1 Gas corresponds to 10^{-7} Ether. One Ether currently costs more than 4,000 USD, so

$$c_{\text{create}} \approx \frac{4,000\,\text{USD} \times 1.5 \cdot 10^5}{10^7} \approx 60\,\text{USD}.$$

Gas for spending a prescription again depends on the amount to around 14,000 Gas, i.e., around 10 USD – cheaper, but still way too expensive for our use case.

[3]Available from: https://www.github.com/DLPS-Framework/

[4]Although EBSI does not run Quorum nodes but Hyperledger BESU instead, Quorum and BESU are at the core both based on very similar protocols [18]. Also, regarding their consensus mechanisms, they have similarities: BESU runs IBFT2, an upgrade of the IBFT consensus mechanism in our Quorum network.

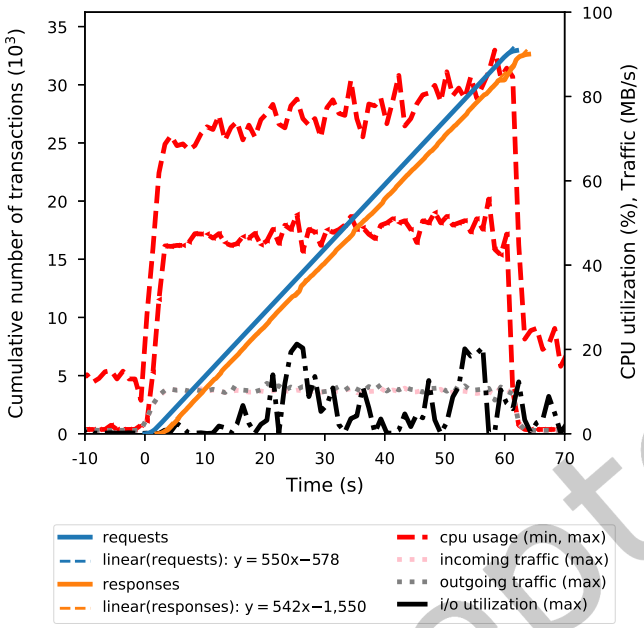

Fig. 5. Benchmark of creating e-prescription tokens on a 32-node cross-European Quorum network on Amazon web services (AWS) m5.2xlarge instances (8 vCPUs, 16 GB RAM) network with IBFT consensus at a request rate of 550 tx/s. Max respectively min means the maximum measured over all nodes; for CPU usage, additionally max respectively min is taken over all of a node's cores first.

We assume that prescriptions will be created and spent mainly on working days between 08:00 and 17:00 and there also will be fluctuations. Thus, a multiplier of at least 3, more likely 5–10, should be taken into account, which means that around 2,000 tx/s are required. Note that a larger throughput than 550 tx/s can be achieved with smaller network sizes, better hardware, or using RAFT instead of IBFT. Thus, we conclude that a large-scale implementation of our proposed solution can be considered realistic with existing technology. We also expect performance improvements caused by optimizations, improvements in hardware, and the opportunity to set up two or three separate blockchain networks for token management if performance is not sufficient by the time that all prescriptions in Europe have been digitized. Concerning costs, even running 10 of the the described Quorum blockchains would cost only around 1,000,000 USD per year for server provision on AWS [99], which amounts to less than 10^{-3} USD per e-prescription.

The latency for the *createToken* and *spendToken* methods that the doctor respectively the pharmacy need to invoke during issuing respectively verifying an e-prescription in our implementation each take around 2.5 s at low throughput when the block-time of IBFT is configured to 1 second. Our measurements also yield that at higher throughput, latency does not increase considerably.

The steps involved in an SSI-based interaction (establishing a connection, issuing a VC or verifying a VP) as described do not provide a significant challenge regarding scalability as the interactions are conducted bilaterally: We found that a single cloud agent that the doctor and the pharmacy run can issue and verify at least two VCs per second, which should be sufficient even for a medical office with several doctors. Moreover, these clients can be scaled horizontally if necessary. The processes conducted on the Hyperledger Indy network do not negatively

affect scalability: Doctors can update their revocation registries in batches, e. g., once a day; and revocation is likely to happen only rarely anyway. The creation of credential schemas or credential definitions only has to be conducted during onboarding processes of doctors and, thus, does not require high throughput. Finally, a single Indy node can serve several hundred read operations per second[5], so a medium-sized Indy network with a two-digit number of nodes can handle sufficiently many read requests per second. Note that if no proof of revocation is necessary and a pharmacy stores the DIDs and public keys (credential definitions) of the doctors in their vicinity and only updates this local copy occasionally, a VP would not even need a single write or read operation on the Indy blockchain. We conclude that our e-prescription management system provides sufficient scalability and performance for hundreds of millions of users.

Regarding the patient-side processes, it takes a total of around 15 seconds for the patient to open their wallet, establish a connection with the doctor, and accept that the e-prescription is issued to and stored in the patient's smartphone wallet (this involves two user-side confirmations). A similar amount of time is needed from the patient opening their wallet, scanning the QR code for the redemption process, until the pharmacy has verified the VP and that the token has not been spent yet. We consider this a reasonable time for the end-to-end automation of the paper-based process, although practical trials would ultimately need to confirm patient's satisfaction with the process' speed.

Privacy and security become increasingly important in networked systems and related threats to blockchain-based systems are well-known [90]. To formally assess the security and privacy implications of the developed system, we performed a thorough security analysis following the STRIDE framework [46]. This framework assesses the security of a system by evaluating threats grouped in six categories. These categories comprise spoofing, tampering, repudiation, information disclosure, denial of service, as well as escalation of privileges. Thus, it covers several security properties including authorization, confidentiality, integrity, and availability [53], which are also reflected in our requirements. The respective evaluation can be performed both component-based as well as interaction-based to provide a granular analysis of the system [100]. We assume that the open-source components that we build on were already analyzed for their security properties. Consequently, we opt for an interaction-based analysis to assess the interplay of the different components making up our system and, thus, our contribution. We consider two main interactions relevant in our use case: *(I1)* the doctor issues a prescription to the patient and *(I2)* the patient redeems a prescription in a pharmacy. To make our considerations visible, we first documented the interactions through detailed sequence diagrams (see Figures 8 and 9). Table 3 features our analysis' results regarding their respective susceptibility to STRIDE threats.

Interaction	S	T	R	I	D	E
I1	x	o	o	x	o	x
I2	x	o	o	?	o	o

Table 3. Results of the STRIDE threat analysis.

We identified four major threats (indicated through x and ?) to security and privacy in our proposed system, which we briefly elaborate on. First, we identified that man-in-the-middle attacks related to spoofing are potentially possible in the current system design. In practice, setting up interactions between parties involves the patient scanning a QR-code. By replacing the correct QR code, which is used to start a connection with the doctor or,

[5]We measured this on our own with the same method as applied for the Quorum benchmark above.

respectively, the pharmacy, an attacker could pretend to be the intended recipient and subsequently engage in an interaction with the patient. In this context, the attacker could, for example, retrieve information contained in the patient's VCs. Thus, this attack represents a spoofing threat. Because the attack can be conducted in the same manner in both interaction scenarios, we count both instances as one. However, there are several means to identify the relying party. For example, the process may require an authenticated out-of-band channel for transmitting the QR-code to initiate the e-prescription issuance, and regular audits of the QR-codes displayed in pharmacies. Furthermore, we can achieve this through a lookup in a DLT-based trust registry. Alternatively, the verification of established SSL or **QWAQ!** (**QWAQ!**) certificates is possible. The implementation of these approaches is currently in progress, for instance, in the Lissi SSI-wallet. Second, the current setup discloses information about the number of prescriptions issued by each individual doctor to all Quorum nodes. While this makes already much less information visible on-chain than the related work that we presented in section 3.2, it is a shortcoming that future work should address, e.g., through ZKPs. We discuss this in more detail in the conclusion (section 8. Corresponding confidentiality issues could also be mitigated through the suitable restriction of participating nodes; the extreme solution being a centralized solution for double-spending prevention that does not harm the protection of sensitive data by design. Third, we found that doctors may prescribe arbitrary prescriptions in the current design, resulting in an elevation of privileges. This shortcoming can be addressed by adapting the proposed e-prescriptions smart contracts. In specific, regulatory bodies creating the smart contracts for the doctor's public key can include public information about which medicals the doctor may or may not prescribe. A more privacy-oriented alternative would be to issue e-prescriptions as chained credentials, i.e., doctors issue e-prescriptions together with a digital certificate that a regulatory body issued to them. Consequently, pharmacies could check that the doctor that issued the e-prescription was him-/herself entitled to do so by the doctor's certification. While this additional mechanism is feasible, it lies outside the scope of the purpose of our prototype. Fourth, as self-sovereign identities represent a novel concept, it is still contested whether information can be deduced from revocation registries using cryptographic accumulator. However, an intermediate assessment from large-scale pilots in Germany suggests that relying on revocation registries using cryptographic accumulators is indeed compliant with the GDPR.

We discuss some of these important guidelines and the corresponding opportunities for further research in more detail in the following two chapters. Nonetheless, we can summarize that we can address of the remaining potential security threats and, therefore, claim that our approach is secure.

7 DISCUSSION

The following section offers a discussion of four important implications related to the contribution of our design. First, the role and necessity of applying blockchain in the context of SSI systems remain debatable. In our design, we deliberately chose to use a blockchain for several distinct purposes. As a transparent, highly available, and tamper-resistant decentralized infrastructure, one blockchain implementation serves as a permanent ledger storing information of public interest in the context of SSI: profiles of issuing doctors, privacy-preserving revocation registries for e-prescriptions, and schemas thereof. These functionalities are relevant in the context of any SSI system, which is why we deem it reasonable to include a blockchain for these purposes in the respective designs. Nevertheless, these functionalities are also achievable using centralized infrastructures, however giving up some of the advantages coming with a blockchain such as independence from CAs (in the context of e-prescriptions) and availability. While in many SSI applications the re-use of VCs is desired, such as for national ID VCs, for e-prescriptions avoiding possibilities for double-spending is of utmost importance regarding e-prescriptions. As a result, we incorporated a second blockchain implementation managing unique tokens corresponding to each e-prescription VC. In principle, a centralized system could also be used for this from a pure privacy perspective, as the data required for the double-spending check is no more confidential in our construction. We suggest a

design that separates the double-spending check from the layer of exchange of confidential data for any SSI use case requiring a restricted number of usages in VCs. Separating the restriction regarding double-spending (token) from invalidation (revocation) also allows to prevent multiple redemptions but at the same time reusing the VC for information exchange, e. g., to check for cross-reactions of medicals, without a limit.

Second, it is important to note that SSI and blockchain technologies are characterized by open-source software philosophies and are often freely available. Moreover, the respective technologies do not include a centralized, controlling party by design. Therefore, the stakeholders need to establish adequate governance structures to ensure the creation of a functioning ecosystem, including secure processes outside of the technical system proposed [91]. In the context of prescriptions, the central entities in the respective communities could take up important roles in this regard. For example, stakeholders must agree on mechanisms for certifying doctors or the attributes including their data types specified in e-prescription VCs. In this paper, we focus on the technical design, since there is valuable related work on governance, both in the realm of blockchain technology [7] and SSI [49].

Third, prior research indicates that the acceptance and usefulness of e-prescriptions increases when the required functionalities are embedded in a larger ecosystem [109]. This could, for example, include generic systems for managing and exchanging patient health data. To this end, the generic nature of the components used in SSI systems can provide several promising opportunities [37]. Network effects can occur through the interplay of a VC-based e-prescription with other VCs such as digital insurance cards, ID cards, or vaccination credentials. Thereby, the mutual utility of such VC can be improved, making the e-prescription framework even more versatile, e. g. for a proof of identity in telemedicine, communicating with an insurance company, or digitizing the reimbursement process for prescriptions.

Fourth, by combining SSI and blockchain, we suppose that our solution addresses several regulatory requirements, especially those imposed by the strict EU GDPR. These include principles for processing personal data such as data minimization, integrity, and confidentiality, as well as lawfulness, fairness, and transparency (Article 5 GDPR) [25]. We address data minimization and confidentially by relying on ZKP through using selective disclosure and releasing only the data requested by the pharmacy. No third parties have access to this data. This is complemented by the use of unique DIDs for each connection as well as E2E encrypted connections to provide a private connection between the parties involved and to minimize the risk of unintended correlation [91]. Nevertheless, ZKPs have been rarely used for signature schemas in practice so far and are thus still uncharted territory from a regulatory perspective. We respect the rights of data subjects, such as the right to erasure ("right to be forgotten") (Article 17 GDPR), as no patient-related data or metadata is stored on the ledger. Rather, by relying on the SSI paradigm, we give the user the responsibility for their own data such that the right to erasure and the right to rectification are also adhered to (Article 16 GDPR). This design choice also addresses the right to data portability (Article 20 GDPR) as we use components oriented at the DID and VC standards and interoperable wallets for implementing the paradigm.

Yet, owing to the scope of our prototype, several domain-specific requirements remain to be implemented through evaluation of our system in practice. For instance, the current prototype allows any doctor to prescribe any medicine in theory. As remedies for each of these shortcomings exist, we propose future research to address those.

Our system relates to and addresses shortcomings of related research. Compared to existing work identified in our literature review (Section 3), we facilitate data privacy in blockchain-based e-prescription management systems by avoiding storage of personal information on-chain, which has been identified as a limitation in prior research [111]. Furthermore, we allow for bilateral exchange of cryptographically verifiable e-prescriptions rather than simply allowing for data integrity checks through blockchain, like Li et al. [61] and Meena et al. [68]'s solution. In addition, we extend SSI-based solutions by offering a double-spending prevention through

blockchain-based token. Existing work by Cadoret et al. [13] as well as Gropper [33] exhibit these shortcomings. Thus, we combine and extend prior research through our system for e-prescription management.

The design process and evaluation of our solution allowed us to derive design principles for decentralized information systems that involve the exchange of sensitive data and a control on the number of usages. These design principles elevate our research contribution for theoretical discussion, and the additional level of abstraction allows practitioners and researchers to apply our observation in scenarios with similar challenges [32, 44]. As our evaluation suggests, SSI can avoid data silos, provide a standardized interface for the exchange of verifiable information whereas blockchains can solve the challenge of transferring value in a decentralized system. In contrast, blockchains cannot be used for the exchange of verifiable, sensitive information due to their inherent replication and immutability; yet, they allow for control on the number of usages of VCs across different bilateral interactions. Consequently, we formulate the corresponding design principles as follows:

1. Use verifiable credentials stored in a digital wallet to provide sensitive and verifiable user information to services.
2. Implement vouchers through creating a token and including its spending secret to the digital certificate. This benefits usability and ease of implementation because users do not require a mobile app beyond their digital wallet.

Furthermore, several practitioners noted our approach's potential of increasing efficiency and reducing costs. This is specifically so when different stakeholders can refer to the same software (like issuing and verifying components) and credential ecosystems (consensus on the list of trusted issuers and the semantic interpretation of attributes referenced in VCs). For example, adding the health insurance card allows for the fast onboarding of a patient at a doctor or the issuance of a receipt at the pharmacy. Patients can directly present the latter to their health insurance for reimbursement in combination with their health insurance VC. Thus, we formulate this in a third design principle:

3. Create additional value by building an ecosystem in which VCs can be combined and used repeatedly in different contexts.

8 CONCLUSION

To solve the challenges of harmonizing sensitive data exchange and double-spending prevention, we study the case of e-prescriptions and design and implement a decentralized e-prescription management system using blockchain technology and SSI digital wallets. We evaluate the proposed system along requirements derived from a literature review. Thus, we contribute a generic design as well as an illustrative implementation of an e-prescription management system. The findings deduced from our evaluation offer insights into the opportunities and remaining challenges regarding the development of decentralized systems dealing with sensitive data and business-logic that involves multiple stakeholders. Our design and implementation also aid practitioners in developing systems beyond the health sector with similar requirements. We conclude the paper by identifying our work's limitations as well as highlighting opportunities for future applications and research.

During implementation, we experienced technical limitations, which allow us to derive several promising avenues for future research. First, to date credential delegation mechanisms that allows a patient to forward their e-prescription VC (including the spending key) to another user as proposed by Camenisch et al. [14] are not integrated in common SSI frameworks. This feature is desirable as proxies are of particular importance in the healthcare sector, e.g., in the case of old age or severe illness. The missing functionality of credential delegation also implies that certificate chains are currently not supported in our prototype. On the one hand, credential chains would allow to limit the type of medicines that a doctor may prescribe and thus solve on of the possible threats to our system (see thread E - elevation of privileges). As such, regulatory bodies could issue a VC to doctors authorizing the issuance of certain medicine. In turn, doctors could then issue the e-prescription VC

accompanied by a delegated version of their VC, thus proving their authority to prescribe the corresponding medical. On the other hand, credential delegation would simplify the delegation of tasks in a surgery or to fetch a medical on a pharmacy on behalf of the recipient. For instance, if a doctor wanted to delegate the issuance of e-prescription VCs to their employees, these would currently need their own public DID and credential definition to be individually recognized by pharmacies as trusted issuers of e-prescriptions, and their own prescription smart contract. The support of certificate chains and delegation in SSI could make such a system substantially easier to implement, govern, and scale. Furthermore, complexity may be reduced by reproducing the proposed concept with only one blockchain as soon as the respective tools and frameworks are available.

Second, as our security analysis showed, further investigations are required on whether the revocation registry can be stored on a blockchain from a regulatory perspective or whether it should be held in central databases. While we aimed to comply with the current GDPR policies through the cryptographic accumulator-based design of revocation registries, we suggest a more thorough evaluation with legal experts and extending the regulations under considerations to CCPA or HIPAA.

Third, while patients' privacy was of utmost priority for the architectural design, we identified potential for improvement with regards to the tracking of doctors' activities through our threat analysis (see thread I - information disclosure). In specific, the implementation currently relies on the use of long-term key pairs by doctors for deploying smart contracts. Thus, as we highlighted in our security analysis, blockchain nodes can see how many prescriptions a doctor has issued in our current implementation. This shortcoming could be addressed through the usage of ZKP in future work, which are used by, e.g., cryptocurrencies such as Z-Cash [85]. Thus, we propose introducing a single pool for creating and spending e-prescription tokens and replacing the currently used anonymized valid and redeemed e-prescription tokens by cryptographic commitments and nullifiers to prevent the tracking of doctors' activities and, thus, minimize remaining risks regarding information disclosure. In addition, the architecture could be extended to add the respective e-prescription to the patient's health record, or to make it accessible to other domain-specific applications that, e.g., check whether there are potentially interactions between different medicals. For this purpose, a receipt could be given to the patient as a VC, which they can then present to their insurance or application maintaining the respective health records. Alternatively, this could be done directly by the doctor or pharmacy in a bilateral interaction, where the doctor or pharmacy forwards the information contained in the e-prescription VC they issued, respectively the VP they received.To reduce the spoofing risks identified in our threat analysis (see thread S - spoofing, several approaches are currently being implemented, such as identifying the party to which a connection is established through their on-chain identifier and public key, through an initial VP in which they reveal a digital certificate that they received from a certifying body (e.g., an SSL certificate or a **QWAQ!** established in the European eIDAS framework) [87].

Fourth, we have not yet tested our prototype in practice. As the system's potential users and legacy systems are highly heterogeneous, a field test and subsequent evaluation with end users remains a significant limitation and will be one of the next steps in our research. As such, also the costs for implementing our system as proposed cannot be quantified at this stage of our research and remains a promising avenue for further research. However, when we presented our prototype to practitioners with expertise on blockchain and SSI, their feedback gave us confidence that the proposed architecture can experience acceptance by different stakeholders. Yet, an extensive application in practice potentially offers more insights on integration with common legacy systems and other aspects, which can hardly be simulated in research settings.

The health sector is currently undergoing rapid changes due to the constantly advancing digitalization of society. Health data is highly sensitive and therefore requires the application of secure and privacy-preserving technologies. Owing to their respective properties in those regards, the combination of blockchain technology and SSI offers promising opportunities for the digital transformation not only of the health care sector. The need for a high degree of user control on confidential data is also present in many other scenarios, such as interactions of citizens with their government, or business-to-business interactions. We recommend to implement

and evaluate similar designs in other use cases in practice requiring both privacy as well as double-spending protection. Due to the novelty of the applied technologies in our proposed system, studies about the interactions of users with respective systems are still rare. Thus, we encourage researchers and practitioners alike to take up our work and further study the respective interactions and resulting implications as well as improvements for the implementation of our design.

ACKNOWLEDGMENTS

We gratefully acknowledge the Bavarian Ministry of Economic Affairs, Regional Development and Energy for their funding of the project "Fraunhofer Blockchain Center (20-3066-2-6-14)" that made this paper possible. We also want to express our special thanks to Matthias Babel for his support with the e-prescription smart contract, to Jana Glöckler for her groundwork on connecting the Hyperledger Aries Cloud Agent in Python with the Django framework, and to Jonathan Lautenschlager and Felix Paetzold for their valuable feedback and suggestions for improvement. Finally, we want to thank the editor and the anonymous reviewers for their valuable guidance and recommendations for improvement during peer review.

REFERENCES

[1] Bader Aldughayfiq and Srinivas Sampalli. 2020. Digital Health in Physicians' and Pharmacists' Office: A Comparative Study of e-Prescription Systems' Architecture and Digital Security in Eight Countries. *OMICS: A Journal of Integrative Biology* (2020), 1–21.

[2] Christopher Allen. 2016. The Path to Self-Sovereign Identity. http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

[3] Julia Amend, Gilbert Fridgen, Alexander Rieger, Tamara Roth, and Alexander Stohr. 2021. The Evolution of an Architectural Paradigm – Using Blockchain to Build a Cross-Organizational Enterprise Service Bus. In *54th Hawaii International Conference on System Sciences*. 4301–4310.

[4] Julia Amend, Julian Kaiser, Lucas Uhlig, Nils Urbach, and Fabiane Völter. 2021. What Do We Really Need? A Systematic Literature Review of the Requirements for Blockchain-based E-Government Services. In *Wirtschaftsinformatik 2021 Proceedings*. Springer, 398–412. https://doi.org/10.1007/978-3-030-86790-4_27

[5] Oscar Avellaneda, Alan Bachmann, Abbie Barbir, Joni Brenan, Pamela Dingle, Kim Hamilton Duffy, Eve Maler, Drummond Reed, and Manu Sporny. 2019. Decentralized Identity: Where Did it Come From and Where is it Going? *IEEE Communications Standards Magazine* 3, 4 (2019), 10–13.

[6] Richard Baskerville, Abayomi Baiyere, Shirley Gregor, Alan Hevner, and Matti Rossi. 2018. Design science research contributions: Finding a balance between artifact and theory. *Journal of the Association for Information Systems* 19, 5 (2018), 3.

[7] Roman Beck, Christoph Müller-Bloch, and John Leslie King. 2018. Governance in the Blockchain Economy: A Framework and Research Agenda. *Journal of the Association for Information Systems* 19, 10 (2018), 1020–1034.

[8] Oleg Bestsennyy, Greg Gilbert, Alex Harris, and Jennifer Rost. 2021. Telehealth: A Quarter-Trillion-Dollar post-COVID-19 Reality? https://www.mckinsey.com/industries/healthcare-systems-and-services/our-insights/telehealth-a-quarter-trillion-dollar-post-covid-19-reality

[9] Tim Bray. 2022. The JavaScript Object Notation (JSON) Data Interchange Format. https://datatracker.ietf.org/doc/rfc8259/

[10] Jan Bruthans. 2020. The State of National Electronic Prescription Systems in the EU in 2018 with Special Consideration given to Interoperability Issues. *International Journal of Medical Informatics* (2020), 1–6.

[11] Vitalik Buterin et al. 2014. A Next-Generation Smart Contract and Decentralized Application Platform. https://www.the-blockchain.com/docs/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf

[12] Bert-Jan Butijn, Damian A. Tamburri, and Willem-Jan van den Heuvel. 2020. Blockchains: A Systematic Multivocal Literature Review. *Comput. Surveys* 53, 3 (2020), 1–37.

[13] Danielle Cadoret, Tamara Kailas, Pedro Velmovitsky, Plinio Morita, and Okechukwu Igboeli. 2020. Proposed Implementation of Blockchain in British Columbia's Health Care Data Management. *Journal of Medical Internet Research* 22, 10 (2020), 1–15.

[14] Jan Camenisch, Manu Drijvers, and Maria Dubovitskaya. 2017. Practical UC-Secure Delegatable Credentials with Attributes and their Application to Blockchain. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*. 683–699.

[15] Jan Camenisch and Anna Lysyanskaya. 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, 93–118.

[16] Mathieu Chanson, Andreas Bogner, Dominik Bilgeri, Elgar Fleisch, and Felix Wortmann. 2019. Blockchain for the IoT: Privacy-preserving Protection of Sensor Data. *Journal of the Association for Information Systems* 20, 9 (2019), 1274–1309.

[17] Shekha Chenthara, Khandakar Ahmed, Hua Wang, Frank Whittaker, and Zhenxiang Chen. 2020. Healthchain: A Novel Framework on Privacy Preservation of Electronic Health Records Using Blockchain Technology. *Plos one* 15, 12 (2020), 1–35.

[18] European Comission. 2020. EBSI Architecture. https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/Architecture

[19] Gaby G Dagher, Jordan Mohler, Matea Milojkovic, and Praneeth Babu Marella. 2018. Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustainable Cities and Society* 39 (2018), 283–297.

[20] Tobias Ehrlich, Daniel Richter, Michael Meisel, and Jürgen Anke. 2021. Self-Sovereign Identity als Grundlage für universell einsetzbare digitale Identitäten. *HMD Praxis der Wirtschaftsinformatik* 58, 2 (2021), 247–270.

[21] eIDAS Expert Group. 2022. European Digital Identity Architecture and Reference Framework – Outline. https://cloud.eid.as/index.php/s/DQ5aRjyzJDNKXpW

[22] Mark A. Engelhardt. 2017. Hitching Healthcare to the Chain: An Introduction to Blockchain Technology in the Healthcare Sector. *Technology Innovation Management Review* 7, 10 (2017), 22–34.

[23] European Commission. 2022. Evaluation study of the Regulation no.910/2014 (eIDAS Regulation). https://digital-strategy.ec.europa.eu/en/library/evaluation-study-regulation-no9102014-eidas-regulation

[24] European Union. 2014. Guidelines on ePrescriptions Dataset for Electronic Exchange Under Cross-Border Directive 2011/24/EU. https://ec.europa.eu/health/system/files/2016-11/eprescription_guidelines_en_0.pdf

[25] European Union. 2016. General Data Protection Regulation (GDPR). https://gdpr.eu/tag/gdpr/

[26] Md Sadek Ferdous, Farida Chowdhury, and Madini Obad Alassafi. 2019. In Search of Self-sovereign Identity Leveraging Blockchain Technology. *IEEE Access* 7 (2019), 103059–103079.

[27] Simon Feulner, Johannes Sedlmeir, Vincent Schlatt, and Nils Urbach. 2022. Exploring the use of self-sovereign identity for event ticketing systems. *Electronic Markets* (2022).
[28] Michèle Finck. 2018. Blockchains and Data Protection in the European Union. *European Data Protection Law Review* 4 (2018), 17–35.
[29] Gilbert Fridgen, Sven Radszuwill, Nils Urbach, and Lena Utz. 2018. Cross-organizational workflow management using blockchain technology – towards applicability, auditability, and automation. In *Proceedings of the 51st Hawaii International Conference on System Sciences*. 51st Hawaii International Conference on System Sciences, 3507–3517.
[30] Florian Glaser. 2017. Pervasive Decentralisation of Digital Infrastructures: A Framework for Blockchain enabled System and Use Case Analysis. In *50th Hawaii International Conference on System Sciences*. 1543–1552.
[31] William J Gordon and Christian Catalini. 2018. Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability. *Computational and Structural Biotechnology Journal* 16 (2018), 224–230.
[32] Shirley Gregor and Alan R Hevner. 2013. Positioning and Presenting Design Science Research for Maximum Impact. *MIS Quarterly* (2013), 337–355.
[33] Adrian Gropper. 2016. Powering the Physician-Patient Relationship with HIE of One Blockchain Health IT. In *ONC/NIST Use of Blockchain for Healthcare and Research Workshop*. 1–11.
[34] Joy M. Grossman, Dori A. Cross, Ellyn R. Boukus, and Genna R. Cohen. 2012. Transmitting and Processing Electronic Prescriptions: Experiences of Physician Practices and Pharmacies. *Journal of the American Medical Informatics Association* 19, 3 (2012), 353–359.
[35] Lewis Gudgeon, Pedro Moreno-Sanchez, Stefanie Roos, Patrick McCorry, and Arthur Gervais. 2019. SoK: Off The Chain Transactions. https://eprint.iacr.org/2019/360.pdf
[36] Tobias Guggenberger, Jannik Lockl, Maximilian Röglinger, Vincent Schlatt, Johannes Sedlmeir, Jens-Christian Stoetzer, Nils Urbach, and Fabiane Völter. 2021. Emerging Digital Technologies to Combat Future Crises : Learnings From COVID-19 to be Prepared for the Future. *International Journal of Innovation and Technology Management* (2021).
[37] Tobias Guggenberger, Lena Neubauer, Jan Stramm, Fabiane Völter, and Till Zwede. 2022. Accept Me as I Am or See Me Go: A Qualitative Analysis of User Acceptance of Self-Sovereign Identity Applications. In *56th Hawaii International Conference on System Sciences (forthcoming)*.
[38] Tobias Guggenberger, Johannes Sedlmeir, Gilbert Fridgen, and André Luckow. 2021. An In-Depth Investigation of the Performance Characteristics of Hyperledger Fabric. *Computers and Industrial Engineering* (2021). https://doi.org/10.1016/j.cie.2022.108716
[39] Daniel Hardman. 2019. A Gentle Introduction to Verifiable Credentials. https://www.evernym.com/blog/gentle-introduction-verifiable-credentials/
[40] Daniel Hardman. 2020. No Paradox Here: ZKPs Deliver Savvy Trust. https://www.evernym.com/blog/no-paradox-here-zkps-deliver-savvy-trust/
[41] Minhua He, Xu Han, Frank Jiang, Rongbai Zhang, Xingzi Liu, and Xiao Liu. 2019. BlockMeds: A Blockchain-Based Online Prescription System with Privacy Protection. In *International Conference on Service-Oriented Computing*. 299–303.
[42] Health Information and Quality Authority. 2015. ePrescription dataset and clinical document architecture standard. https://www.hiqa.ie/sites/default/files/2017-01/ePrescribing-Dataset_and_CDA_Specification.pdf
[43] Andreas Hein, Maximilian Schreieck, Tobias Riasanow, David Soto Setzke, Manuel Wiesche, Markus Böhm, and Helmut Krcmar. 2019. Digital platform ecosystems. *Electronic Markets* (2019), 1–12.
[44] Alan Hevner, Salvatore T March, Jinsoo Park, Sudha Ram, et al. 2004. Design Science Research in Information Systems. *MIS Quarterly* 28, 1 (2004), 75–105.
[45] Alexandra Hoess, Vincent Schlatt, Alexander Rieger, and Gilbert Fridgen. 2021. The Blockchain Effect: From Inter-ecosystem to Intra-Ecosystem Competition. In *Proceedings of the 29th Conference on Information Systems*. AIS.
[46] Michael Howard and Steve Lipner. 2006. *The security development lifecycle*. Vol. 8. Microsoft Press Redmond.
[47] Laurie Hughes, Yogesh K. Dwivedi, Santosh K. Misra, Nripendra P. Rana, Vishnupriya Raghavan, and Viswanadh Akella. 2019. Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda. *International Journal of Information Management* 49 (2019), 114–129.
[48] Faisal Jamil, Lei Hang, KyuHyung Kim, and DoHyeun Kim. 2019. A Novel Medical Blockchain Model for Drug Supply Chain Integrity Management in a Smart Hospital. *Electronics* 8, 5 (2019), 1–32.
[49] Rieks Joosten, Sterre den Breeijen, and Drummond Reed. 2021. Decentralized SSI Governance, the Missing Link in Automating Business Decisions. https://www.researchgate.net/publication/348325716_Decentralized_SSI_Governance_the_missing_link_in_automating_business_decisions
[50] Kaiser Family Foundation. 2021. Retail Prescription Drugs Filled at Pharmacies per Capita. https://www.kff.org/health-costs/state-indicator/retail-rx-drugs-per-capita/
[51] Niclas Kannengießer, Sebastian Lins, Tobias Dehling, and Ali Sunyaev. 2020. Trade-offs between Distributed Ledger Technology Characteristics. *Comput. Surveys* 53, 2 (2020), 1–37.
[52] Gajendra J. Katuwal, Sandip Pandey, Mark Hennessey, and Bishal Lamichhane. 2018. Applications of Blockchain in Healthcare: Current Landscape & Challenges. https://arxiv.org/pdf/1812.02776

[53] Rafiullah Khan, Kieran McLaughlin, David Laverty, and Sakir Sezer. 2017. STRIDE-based threat modeling for cyber-physical systems. In *2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*. IEEE, 1–6.
[54] Patrick Kierkegaard. 2013. E-Prescription across Europe. *Health and Technology* 3, 3 (2013), 205–219.
[55] Ji Woong Kim, Ah Ra Lee, Min Gyu Kim, Il Kon Kim, and Eun Joo Lee. 2019. Patient-centric Medication History Recording System using Blockchain. In *IEEE International Conference on Bioinformatics and Biomedicine*. 1513–1517.
[56] Barbara Ann Kitchenham and Stuart Charters. 2007. Guidelines for performing Systematic Literature Reviews in Software Engineering. In *EBSE Technical Report EBSE-2007-01*.
[57] John Kolb, Moustafa AbdelBaky, Randy H. Katz, and David E. Culler. 2020. Core Concepts, Challenges, and Future Directions in Blockchain: A Centralized Tutorial. *Comput. Surveys* 53, 1 (2020), 1–39.
[58] Michael Kuperberg. 2020. Blockchain-based Identity Management: A Survey from the Enterprise and Ecosystem Perspective. *IEEE Transactions on Engineering Management* 67, 4 (2020), 1008–1027. https://ieeexplore.ieee.org/document/8792372/
[59] Aurore Le Bris and Walid El Asri. 2016. State of Cybersecurity & Cyber Threats in Healthcare Organizations. https://blogs.harvard.edu/cybersecurity/files/2017/01/risks-and-threats-healthcare-strategic-report.pdf
[60] Keon Myung Lee and Ilkyeun Ra. 2020. Data Privacy-preserving Distributed Knowledge Discovery Based on the Blockchain. *Information Technology and Management* 21, 4 (2020), 191–204.
[61] Patrick Li, Scott D. Nelson, Bradley A. Malin, and You Chen. 2019. DMMS: A Decentralized Blockchain Ledger for the Management of Medication Histories. *Blockchain in Healthcare Today* 2 (2019), 1–22.
[62] Jannik Lockl, Vincent Schlatt, André Schweizer, Nils Urbach, and Natascha Harth. 2020. Toward Trust in Internet of Things Ecosystems: Design Principles for Blockchain-Based IoT Applications. *IEEE Transactions on Engineering Management* (2020), 1–9.
[63] Nate Lord. 2020. Top 10 Biggest Healthcare Data Breaches of All Time. https://digitalguardian.com/blog/top-10-biggest-healthcare-data-breaches-all-time
[64] Jitendra Mahatpure, Mahesh Motwani, and Piyush Kumar Shukla. 2019. An Electronic Prescription System Powered by Speech Recognition, Natural Language Processing and Blockchain Technology. *International Journal of Scientific & Technology Research* 8, 8 (2019), 1454–1462.
[65] Salvatore T March and Gerald F Smith. 1995. Design and natural science research on information technology. *Decision Support Systems* 15, 4 (1995), 251–266.
[66] Jens Mattke, Christian Maier, and Axel Hund. 2019. How an Enterprise Blockchain Application in the U.S. Pharmaceuticals Supply Chain is Saving Lives. *MIS Quarterly Executive* 18, 4 (2019), 245–261.
[67] Thomas McGhin, Kim-Kwang Raymond Choo, Charles Zhechao Liu, and Debiao He. 2019. Blockchain in Healthcare Applications: Research Challenges and Opportunities. *Journal of Network and Computer Applications* 135 (2019), 62–75.
[68] Devendra K. Meena, Ras Dwivedi, and Sandeep Shukla. 2019. Preserving Patient's Privacy using Proxy Re-Encryption in Permissioned Blockchain. In *IEEE Sixth International Conference on Internet of Things: Systems, Management and Security*. 450–457.
[69] Hilke Messal, Thomas Müller, Laura Richter, and Tobias Silberzahn. 2022. Germany's e-health transformation makes uneven progress. hhttps://www.mckinsey.com/industries/life-sciences/our-insights/germanys-ehealth-transformation-makes-good-but-uneven-progress
[70] Alexander Mühle, Andreas Grüner, Tatiana Gayvoronskaya, and Christoph Meinel. 2018. A Survey on Essential Components of a Self-sovereign Identity. *Computer Science Review* 30 (2018), 80–86.
[71] Darren Mundy and David W. Chadwick. 2002. A System for Secure Electronic Prescription Handling. In *Proceedings of The Hospital of the Future, Second International Conference On The Management Of Healthcare And Medical Technology*.
[72] Satoshi Nakamoto. 2008. Bitcoin: A Peer-to-peer Electronic Cash System. http://bitcoin.org/bitcoin.pdf
[73] Luis Oliveira, Liudmila Zavolokina, Ingrid Bauer, and Gerhard Schwabe. 2018. To Token or not to Token: Tools for Understanding Blockchain Tokens. In *Proceedings of the 39th International Conference on Information Systems*. 1–17.
[74] Alexander Papageorgiou, Antonis Mygiakis, Konstantinos Loupos, and Thomas Krousarlis. 2020. DPKI: A Blockchain-Based Decentralized Public Key Infrastructure System. In *2020 Global Internet of Things Summit (GIoTS)*. 1–5.
[75] Ken Peffers, Tuure Tuunanen, Marcus A Rothenberger, and Samir Chatterjee. 2007. A design science research methodology for information systems research. *Journal of Management Information Systems* 24, 3 (2007), 45–77.
[76] Gareth W. Peters and Efstathios Panayi. 2016. Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money. In *Banking Beyond Banks and Money*. Springer, Heidelberg, GER, 239–278.
[77] Marc Pilkington. 2016. Blockchain Technology: Principles and Applications. In *Research Handbook on Digital Transformations*. Edward Elgar Publishing, Cheltenham, UK.
[78] Moritz Platt, Ruwan J. Bandara, Andreea-Elena Drăgnoiu, and Sreelakshmi Krishnamoorthy. 2021. *Information Privacy in Decentralized Applications*. Springer.
[79] Alex Preukschat and Drummond Reed. 2021. *Self-Sovereign Identity: Decentralized Digital Identity and Verifiable Credentials*. Manning, Shelter Island, NY.

[80] Meda Raghavendra. 2019. Can Blockchain Technologies Help Tackle the Opioid Epidemic: A Narrative Review. *Pain Medicine* 20, 10 (2019), 1884–1889.
[81] Fergal Reid and Martin Harrigan. 2013. An Analysis of Anonymity in the Bitcoin System. In *Security and Privacy in Social Networks*. Springer, 197–223.
[82] Matti Rossi, Christoph Mueller-Bloch, Jason Bennett Thatcher, and Roman Beck. 2019. Blockchain Research in Information Systems: Current Trends and an Inclusive Future Research Agenda. *Journal of the Association for Information Systems* 20, 9 (2019), 1388–1403.
[83] K. Ruby Benita, S. Ganesh Kumar, B. Murugamantham, and A. Murugan. 2020. Authentic Drug Usage and Tracking with Blockchain Using Mobile Apps. *International Journal of Interactive Mobile Technologies* 14, 17 (2020), 20–31.
[84] Sebastian Sartor, Johannes Sedlmeir, Alexander Rieger, and Tamara Roth. 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.
[85] Eli Ben Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza. 2014. Zerocash: Decentralized anonymous payments from bitcoin. In *Symposium on Security and Privacy*. IEEE, 459–474.
[86] Tobias Schaffner. 2021. *Scaling Public Blockchains*. Master's thesis. https://wwz.unibas.ch/fileadmin/user_upload/wwz/00_Professuren/Schaer_DLTFintech/Lehre/Tobias_Schaffner_Masterthesis.pdf
[87] Benjamin Schellinger, Johannes Sedlmeir, Lukas Willburger, Jens Strüker, and Nils Urbach. 2022. Mythbusting Self-Sovereign Identity (SSI): Diskussionspapier zu selbstbestimmten digitalen Identitäten. https://eref.uni-bayreuth.de/68552
[88] Benjamin Schellinger, Fabiane Völter, Nils Urbach, and Johannes Sedlmeir. 2022. Yes, I Do: Marrying Blockchain Applications with GDPR. In *55th Hawaii International Conference on System Sciences*.
[89] Nina-Birte Schirrmacher, Johannes Rude Jensen, and Michel Avital. 2021. Token-Centric Work Practices in Fluid Organizations: The Cases of Yearn and MakerDAO. In *42nd International Conference on Information Systems*.
[90] Vincent Schlatt, Tobias Guggenberger, Jonathan Schmid, and Nils Urbach. 2022. Attacking the Trust Machine: Developing an Information Systems Research Agenda for Blockchain Cybersecurity. *International Journal of Information Management* (2022), 102470.
[91] Vincent Schlatt, Johannes Sedlmeir, Simon Feulner, and Nils Urbach. 2021. Designing a Framework for Digital KYC Processes Built on Blockchain-Based Self-Sovereign Identity. *Information & Management* (2021).
[92] Ryan W Seaberg, Tyler R Seaberg, and David C Seaberg. 2021. Use of Blockchain Technology for Electronic Prescriptions. *Blockchain in Healthcare Today* (2021). https://doi.org/10.30953/bhty.v4.183
[93] Johannes Sedlmeir, Hans Ulrich Buhl, Gilbert Fridgen, and Robert Keller. 2020. The Energy Consumption of Blockchain Technology: Beyond Myth. *Business & Information Systems Engineering* 62, 6 (2020), 599–608.
[94] Johannes Sedlmeir, Jonathan Lautenschlager, Gilbert Fridgen, and Nils Urbach. 2022. The Transparency Challenge of Blockchain in Organizations. *Electronic Markets* (2022).
[95] Johannes Sedlmeir, Philipp Ross, André Luckow, Jannik Lockl, Daniel Miehle, and Gilbert Fridgen. 2021. The DLPS: A Framework for Benchmarking Blockchains. In *Proceedings of the 54th Hawaii International Conference on System Sciences*. 6855–6864.
[96] Johannes Sedlmeir, Reilly Smethurst, Alexander Rieger, and Gilbert Fridgen. 2021. Digital Identities and Verifiable Credentials. *Business & Information Systems Engineering* 63, 5 (2021), 603–613.
[97] Johannes Sedlmeir, Fabiane Völter, and Jens Strüker. 2022. The Next Stage of Green Electricity Labeling: Using Zero-Knowledge Proofs for Blockchain-Based Certificates of Origin and Use. *SIGENERGY Energy Informatics Review* 1, 1 (2022), 20–31. https://doi.org/10.1145/3508467.3508470
[98] Juergen Seitz and Nilmini Wickramasinghe. 2020. Opportunities for Using Blockchain Technology in E-Health: E-Prescribing in Germany. In *Delivering Superior Health and Wellness Management with IoT and Analytics*. Springer, Heidelberg, GER, 299–316.
[99] Amazon Web Services. 2021. Amazon EC2 On-Demand Pricing. https://aws.amazon.com/ec2/pricing/on-demand/?nc1=h_ls
[100] Adam Shostack. 2014. *Threat modeling: Designing for security*. John Wiley & Sons.
[101] Alexandre Siqueira, Arlindo Flávio da Conceição, and Vladimir Rocha. 2021. Blockchains and Self-Sovereign Identities Applied to Healthcare Solutions: A Systematic Review. *CoRR* abs/2104.12298 (2021). https://arxiv.org/abs/2104.12298
[102] Rahul Ganpatrao Sonkamble, Shraddha P. Phansalkar, Vidyasagar M. Potdar, and Anupkumar M. Bongale. 2021. Survey of Interoperability in Electronic Health Records Management and Proposed Blockchain Based Framework: MyBlockEHR. *IEEE Access* 9 (2021), 158367–158401. https://doi.org/10.1109/ACCESS.2021.3129284
[103] Christian Sonnenberg and Jan Vom Brocke. 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, 381–397.
[104] Sovrin. 2020. Interoperability Series: Sovrin Stewards Achieve Breakthrough in Wallet Portability. https://sovrin.org/sovrin-stewards-wallet-portability/
[105] Manu Sporny, Dave Longley, and David Chadwick. 2019. Verifiable Credentials Data Model 1.0. https://www.w3.org/TR/vc-data-model/
[106] Manu Sporny, Dave Longley, Markus Sabadello, Drummond Reed, Orie Steele, and Christopher Allen. 2021. Decentralized Identifiers (DIDs) v1.0. https://w3c.github.io/did-core/
[107] Thomas F. Stafford and Horst Treiblmaier. 2020. Characteristics of a Blockchain Ecosystem for Secure and Sharable Electronic Medical Records. *IEEE Transactions on Engineering Management* 67, 4 (2020), 1340–1362.

[108] Ali Sunyaev, Niclas Kannengießer, Roman Beck, Horst Treiblmaier, Mary Lacity, Johann Kranz, Gilbert Fridgen, Ulli Spankowski, and André Luckow. 2021. Token Economy. *Business & Information Systems Engineering* (2021), 1–22.
[109] Robyn Tamblyn, Allen Huang, Yuko Kawasumi, Gillian Bartlett, Roland Grad, André Jacques, Martin Dawes, Michal Abrahamowicz, Robert Perreault, Laurel Taylor, et al. 2006. The Development and Evaluation of an Integrated Electronic Prescribing and Drug Management System for Primary Care. *Journal of the American Medical Informatics Association* 13, 2 (2006), 148–159.
[110] Sudeep Tanwar, Karan Parekh, and Richard Evans. 2020. Blockchain-based Electronic Healthcare Record System for Healthcare 4.0 Applications. *Journal of Information Security and Applications* 50 (2020), 2214–2126.
[111] Camden Thatcher and Subrata Acharya. 2018. Pharmaceutical Uses of Blockchain Technology. In *IEEE International Conference on Advanced Networks and Telecommunications Systems*. 1–6.
[112] Camden Thatcher and Subrata Acharya. 2020. RxBlock: Towards the Design of a Distributed Immutable Electronic Prescription System. *Network Modeling Analysis in Health Informatics and Bioinformatics* 9, 1 (2020), 1–11.
[113] Fabiane Völter, Nils Urbach, and Julian Padget. 2021. Trusting the Trust Machine: Evaluating Trust Signals of Blockchain Applications. *International Journal of Information Management* (2021), 12 pages. https://doi.org/10.1016/j.ijinfomgt.2021.102429
[114] Linda Weigl, Tom Barbereau, Alexander Rieger, and Gilbert Fridgen. 2021. The Social Construction of Self-Sovereign Identity: An Extended Model of Interpretive Flexibility. In *55th Hawaii International Conference on System Sciences*. 2543–2552.
[115] Michael Whitman and Herbert Mattord. 2011. *Principles of Information Security*. Cengage Learning, Boston, MA.
[116] Hsin-Te Wu and Chun-Wei Tsai. 2018. Toward Blockchains for Health-care Systems: Applying the Bilinear Pairing Technology to Ensure Privacy Protection and Accuracy in Data Sharing. *IEEE Consumer Electronics Magazine* 7, 4 (2018), 65–71.
[117] Bidi Ying, Wen Sun, Nada Radwan Mohsen, and Amiya Nayak. 2019. A Secure Blockchain-based Prescription Drug Supply in Health-Care Systems. In *IEEE International Conference on Smart Applications, Communications and Networking*. 1–6.
[118] Peng Zhang, Douglas C Schmidt, Jules White, and Gunther Lenz. 2018. Blockchain Technology Use Cases in Healthcare. In *Advances in Computers*. Vol. 111. Elsevier, Amsterdam, NL, 1–41.
[119] Rui Zhang, Rui Xue, and Ling Liu. 2019. Security and Privacy on Blockchain. *Comput. Surveys* 52, 3 (2019), 1–34.

APPENDIX

```
pragma solidity ^0.5.16;

contract PrescriptionContract {
    address admin;

    struct Prescription {
        address issuer; //the doctor's public key
        uint remainingRedemptions; //number of times that the prescription can still be spent
    }

    constructor() public {
        admin = msg.sender;
    }

    modifier onlyAdmin() {
        require (msg.sender == admin, "Sender is not the admin of the contract");
        _;
    }

    // a prescription token registry, associating public keys with prescriptions
    mapping (address => Prescription) public prescriptions;

    function create(address patient, uint number) public onlyAdmin() {
        prescriptions[patient] = Prescription({issuer: msg.sender, remainingRedemptions:
            number});
    }

    function spend() public {
        require (prescriptions[msg.sender].remainingRedemptions >= 1,
            "Already spent");
        prescriptions[msg.sender].remainingRedemptions--;
    }
}
```

Fig. 6. The e-prescription smart contract implementation in Solidity that each doctor deploys for the token management of the e-prescriptions that they issue.

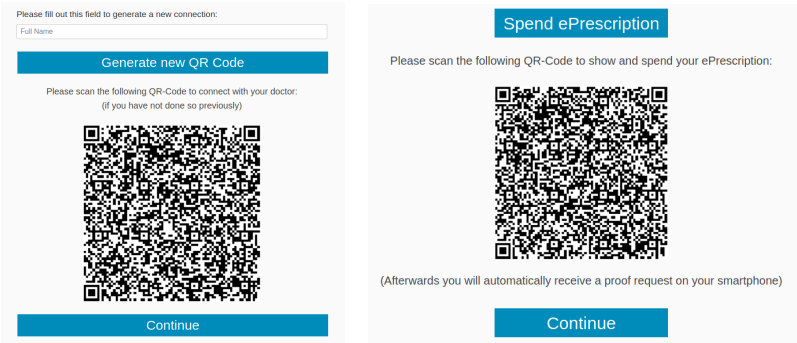

Fig. 7. Frontend for establishing a connection between the user's smartphone and the doctor resp. the pharmacy.

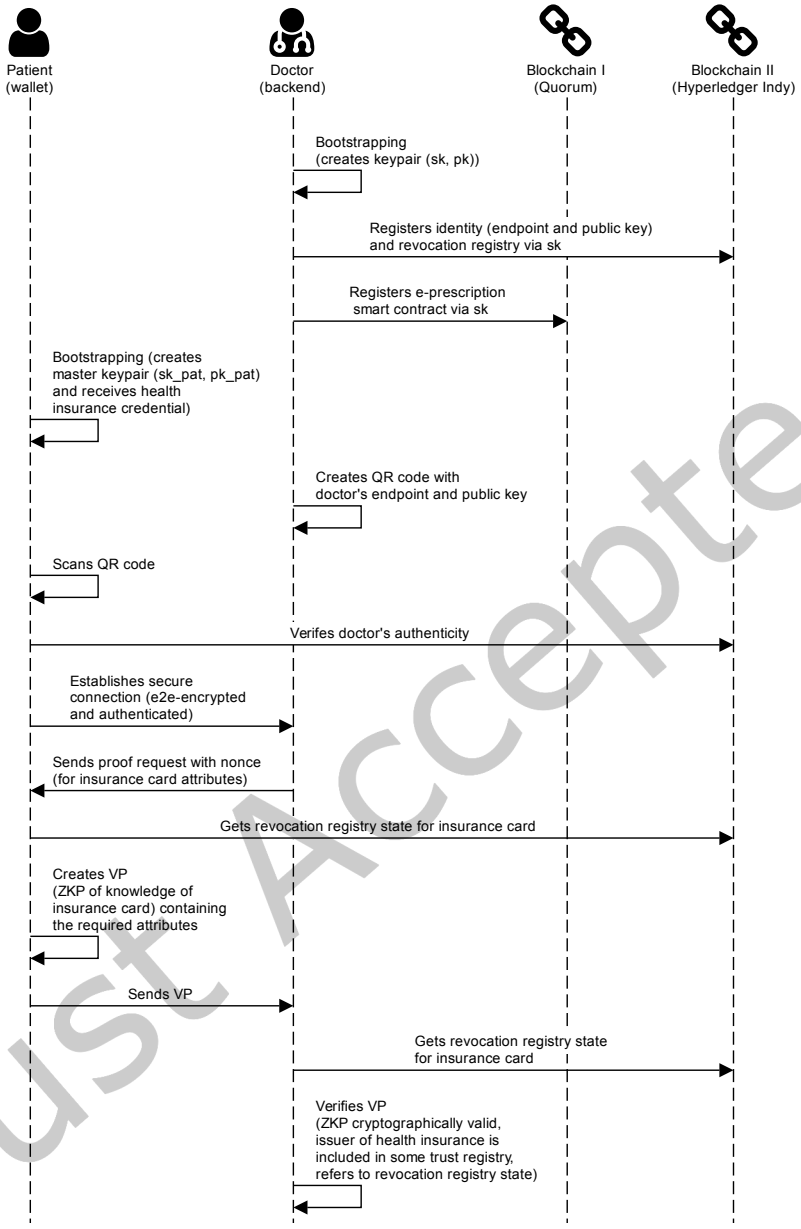

Fig. 8. e-prescription issuance.

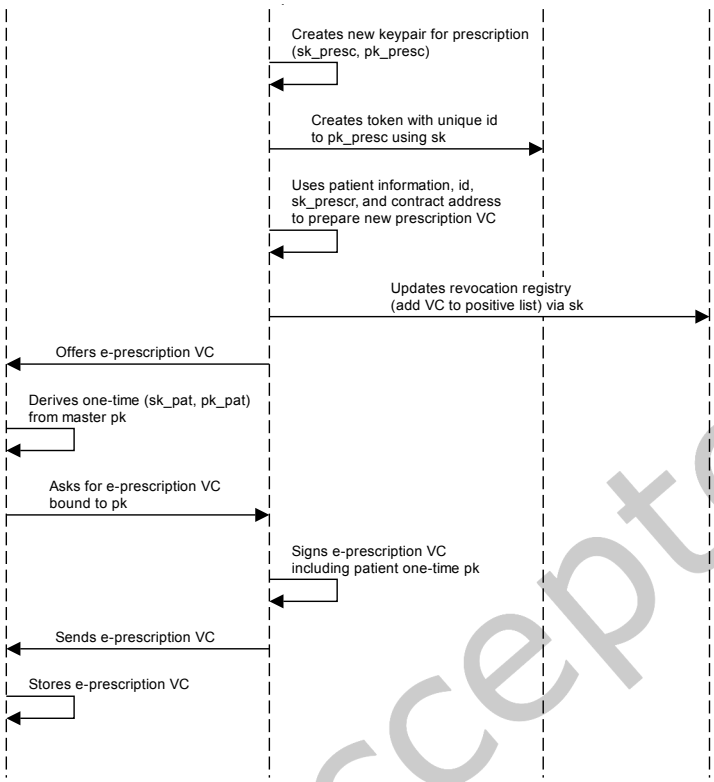

Fig. 8. e-prescription issuance (cont.)

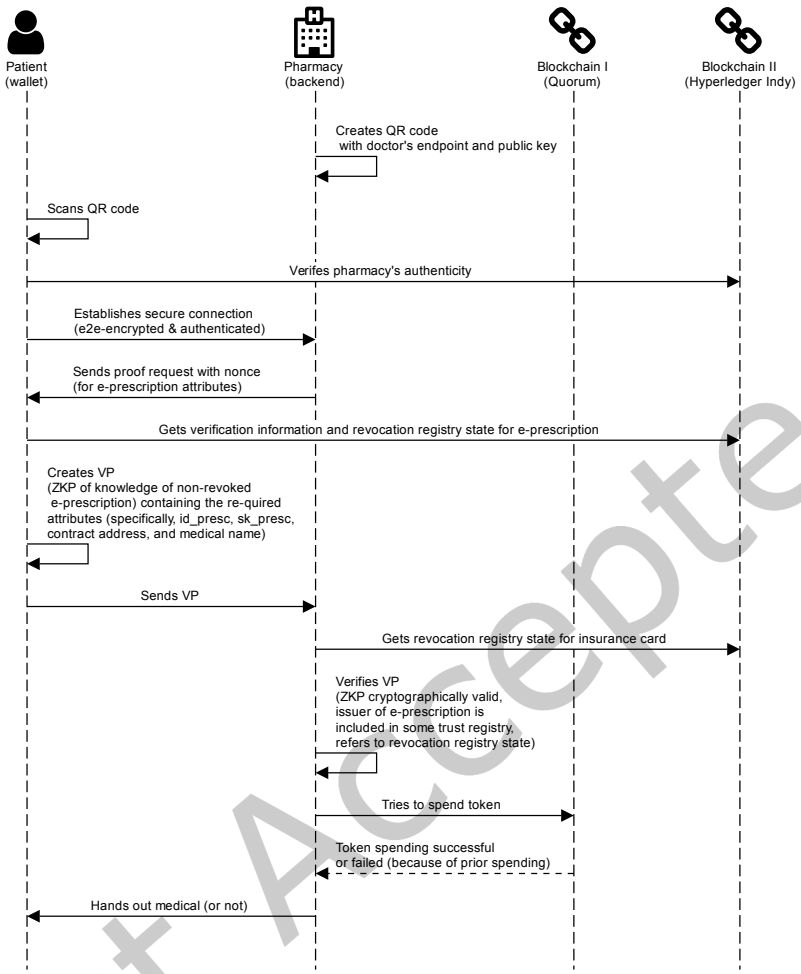

Fig. 9. e-prescription redemption.