Technovation 149 (2026) 103371

Contents lists available at ScienceDirect

Technovation

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

Stimulating data marketplace adoption in manufacturing: The impact of perceived control on willingness to share data

Antragama Ewa Abbas [a,b], Floris Kool [a], Wirawan Agahari [a,c], Mark de Reuver [a,*]

[a] Delft University of Technology, Department Engineering Systems and Services, Section Information and Communication Technology, the Netherlands
[b] Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg, Luxembourg, L-1855, Luxembourg
[c] Department of Information Systems and Operations Management, Tilburg School of Economics and Management, Tilburg University, the Netherlands

ARTICLE INFO

Keywords:
Digital platforms
Control mechanisms
Platform control
B2B platforms
Data sovereignty
Data marketplaces

ABSTRACT

Data marketplaces potentially accelerate digital transformation in the manufacturing industries as they enable businesses to share Internet-of-Things (IoT) data. As data marketplaces are business-to-business (B2B) platforms that mediate between unrelated businesses, managers often fear losing control over shared data (or, in other words, losing data sovereignty). However, despite extensive work in the technical community to create control mechanisms, the impact of enhanced control on data marketplace adoption by data owners remains unclear. This study develops and tests a theoretical model that relates perceived control to willingness to share data in the context of IoT data marketplaces for manufacturing industries. We surveyed 299 managers in manufacturing businesses using a scenario of a data marketplace that allowed data owners to control their data offerings directly through smart contracts that enforce data sharing conditions. We find that perceived control significantly impacts willingness to share data. The effect is partially mediated by lower risk perceptions but not by trust in data buyers. The research shows the importance of perceived control for data sharing intentions, implying that data marketplace operators should provide noticeable control mechanisms to foster adoption. This research contributes to the broader platform control literature by theorising *reflective supply-side control*, an underexplored phenomenon where supply-side control (e.g., data owners) over the demand side (e.g., data buyers) shapes the supply side's own behaviour.

1. Introduction

Business-to-business (B2B) platforms are powerful tools to enable digital transformation in manufacturing (den Hartigh et al., 2023), an industry that accounts for approximately 15 % of global GDP[1] and thus holds substantial economy-wide influence. A specific instance of a B2B platform is data marketplaces, which enable businesses to share data, such as from Internet-of-Things (IoT) devices. For example, Afteriize[2] enables car manufacturers to sell (IoT-based) data on maintenance and repair patterns, which insurance companies can buy to create tailored, personalised insurance packages. Such a data marketplace facilitates advertising data products (by disclosing metadata), negotiation, contracting, payment, and data transfer. Unlocking IoT data sharing in manufacturing alone could deliver substantial benefits, potentially helping to realise revenue generation of $3.3 trillion.[3] In general, data sharing in manufacturing provides opportunities for digital transformation, such as predictive maintenance, supply optimisation, and benchmarking of production processes. However, the adoption of data marketplaces is low (Simon et al., 2021; Spiekermann, 2019), especially in the B2B domain (Azcoitia and Laoutaris, 2022).

The adoption of B2B data marketplaces, in general, depends on several factors and contexts (see Appendix 1 for the overview). For instance, perceived risks hinder the adoption of B2B data marketplaces. Data owners may fear competitive risks (e.g., knowledge spillovers to

This article is part of a special issue entitled: Digital B2B Platforms for Manufacturing published in Technovation.

* Corresponding author. Delft University of Technology Faculty Technology, Policy & Management Department Engineering Systems & Services Section Information and Communication Technology Building 31 Jaffalaan 5, 2628 BX, Delft, the Netherlands.https://www.tudelft.nl/staff/g.a.dereuver
E-mail address: g.a.dereuver@tudelft.nl (M. de Reuver).

[1] https://ourworldindata.org/grapher/manufacturing-value-added-to-gdp, accessed on 11 July 2025.
[2] https://info.dawex.com/afteriize-case-study/, accessed on 14 January 2025.
[3] https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-the-internet-of-things, accessed on 11 July 2025.

https://doi.org/10.1016/j.technovation.2025.103371
Received 22 March 2024; Received in revised form 5 September 2025; Accepted 10 September 2025
Available online 15 September 2025

competitors) and data misuse (e.g., data buyers exploit data in unforeseen ways) (Agahari et al., 2022). At the same time, data buyers face the *Arrow information paradox*, as assessing data products' value and quality is difficult without first accessing and using them (Stahl et al., 2017). It means data marketplace users also struggle to determine the optimal price for data products (Fassnacht et al., 2024). Meanwhile, data marketplace operators face a dilemma: offering additional analytics capabilities benefits less experienced users but may disadvantage more established ones (X. Zhang et al., 2023a).

This study focuses on data control (or data sovereignty) as a key adoption factor in B2B data marketplaces (Abbas et al., 2024; Spiekermann, 2019; von Scherenberg et al., 2024). Control appears to be among the most critical factors, potentially outweighing efficiency motives (e.g., streamlining supply chains) (Dahlberg and Nokkala, 2019) or economic motives (e.g., generating revenue through optimal pricing) (Otto and Jarke, 2019). Generally speaking, maintaining *control over shared data* is even more challenging for data owners in data marketplaces compared to traditional data-sharing settings, such as classical inter-organisational information systems (IOS) (Dahlberg and Nokkala, 2019; Jussen et al., 2023; Kembro et al., 2017).

While such classical settings typically involve data sharing between two parties that have predefined and formalised relationships, data marketplaces are characterised by their open and complex scope (Möller et al., 2024). To illustrate, consider that suppliers can share data products, such as inventory levels or production forecasts, with original equipment manufacturers (OEMs). In a traditional setting, the OEM establishes customised data-sharing connections with each supplier. This involves agreeing on data formats, defining protocols, and setting up technical integrations tailored to each supplier. Managing ten suppliers can thus mean ten separate data sharing configurations. In contrast, data marketplaces enable OEMs to discover, purchase, and access data products from a myriad of suppliers without setting up individual connections. However, the open and complex scope of data marketplaces often leads to ambiguous use cases that cannot be fully anticipated by data owners. Control mechanisms should thus enable data owners to define data-sharing terms, monitor usage, and retract data if necessary, such as in cases of misuse. Without control, managers fear that the shared data could benefit competitors (Agahari et al., 2022). As a result, data owners may be reluctant to adopt B2B data marketplaces.

In response to the need for control, various (technical) mechanisms are emerging to enable such a capability in the context of data marketplaces. For instance, smart contracts can enhance control by technically enforcing compliance with data access policies defined by data owners (Koutsos et al., 2022; Park et al., 2018). These technical mechanisms may reduce the risks of data sharing (e.g., by enforcing compliance with data access policies) or induce trust (e.g., by making data buyer behaviour more predictable), which in turn could increase willingness to share data. Yet, achieving control is technically challenging and complex, requiring marketplace operators to consider if their investments pay off by making data owners more willing to share data. The few studies that examine behavioural impacts mainly focus on mechanisms to control what data is being exposed (e.g. multi-party computation, see Agahari and de Reuver, 2022; Agahari et al., 2025). However, to our knowledge, research focusing specifically on the behavioural impact of mechanisms to control what happens after data is shared (e.g., through smart contracts) remains limited. This is surprising, as smart contracts and blockchain-based systems are widely discussed in the context of data marketplaces (e.g., see a review by Driessen et al., 2022). This highlights the need for exploration and empirical evidence on how control mechanisms, especially those enabled by smart contracts, affect behavioural intentions in data marketplaces.

From a theoretical perspective, control is a major theme in the broader literature on digital platforms (see Appendix 2 for an overview), but our phenomenon of supply-side users exercising control over demand-side users has received little attention. Most scholars assume that platform providers exercise control rather than platform users (e.g., Wareham et al., 2014; Goldbach et al., 2018). The smaller body of literature that considers decentralised control largely focuses on demand-side users that control supply-side users (e.g., Huang et al., 2023; Shi et al., 2023). For instance, when travellers (i.e., demand-side) write reviews about hotel providers (i.e., supply-side), hotel providers may adapt their behaviour (Ananthakrishnan et al., 2023). Only a few studies have begun exploring cases where the supply side enacts control over the demand side (e.g., Cai et al., 2023; Li et al., 2019). For instance, sellers may offer (conditional) rewards for reviews, which can steer buyers to post more honest (positive) feedback (Li et al., 2020). However, these studies focus on the behavioural impacts on the demand side rather than the supply side.

This oversight in the literature can be explained as sellers often lack both the interest and ability to control how buyers use products purchased on a platform. For instance, sellers of tangible products such as clothes have no desire to control how buyers wear them, and both the sellers and the e-commerce platform have no way to enforce ways of wearing clothes. For the emerging category of data products, however, such a desire to control is high due to the risks of misuse. For example, data buyers can manipulate data in such a way that they de-anonymise or reverse engineer trade secrets (Ofe and de Reuver, 2024). Moreover, the ability to control is now afforded through distributed technologies, for instance, blockchain-based, that provide the transparency to exercise direct control over buyers. Hence, we argue that a novel phenomenon becomes relevant: *reflective supply-side control,* which refers to how supply-side control over the demand side influences the supply side's own behaviour.

This paper aims to study if and how perceived control of data sellers over data buyers affects their willingness to share data in the context of data marketplaces, focusing on smart contracts as control mechanisms to ensure perceived control of data owners. We define perceived control as the extent to which data owners feel they can influence and direct data flows to other parties (Abbas et al., 2024). We develop and test hypotheses through a survey using structural equation modelling. As a setting for the study, we study the sharing of IoT data by manufacturing businesses through data marketplaces. This context is suitable as keeping control over what happens to shared data is considered crucial for data marketplace users (Dahlberg and Nokkala, 2019). Losing control over manufacturing data creates massive risks for leaking strategic important information or reverse engineering critical processes (de Prieëlle et al., 2022).

The study contributes to the literature at the intersection of B2B data marketplaces and manufacturing in three ways. First, we provide additional empirical evidence of the importance of perceived control (or sovereignty) as a key adoption factor for data marketplaces. It means we provide insight into the potential of technology-based control mechanisms (i.e., smart contracts) to address the low adoption of industry-oriented data marketplaces (Azcoitia and Laoutaris, 2022), which is relevant for data marketplace operators as well as policymakers who intend to foster data-driven collaboration in manufacturing industries. Second, we explore a justificatory mechanism that explains the relationship between perceived control and willingness to share data. Our findings reveal that trust in data buyers is not a significant mediator, which calls for further theorising on whether trust remains a necessary condition in data-sharing settings equipped with technology-based control mechanisms. This is especially relevant considering the extensive efforts to create trust-based mechanisms (e.g., trust frameworks such as those adopted in industry standards like Gaia-X). Finally, we contribute to the discourse on the role of B2B digital platforms, such as data marketplaces, in transforming the manufacturing industry.[4] For instance, these platforms can facilitate a shift from using data *for*

[4] https://www.sciencedirect.com/special-issue/10GSRFPKD6C,accessed on 16 January 2025.

business to treating data *as* a business, as shown in the Afteriize case. This shift is facilitated by leveraging data marketplaces as (1) a secondary revenue stream for data owners and (2) an external data source to enhance insights for data buyers. We further examine the conditions in data marketplaces that drive manufacturing transformation. These marketplaces are particularly effective when they enhance data control, which, in turn, encourages user adoption.

For the broader stream of literature on platform control, we theorise a novel phenomenon: *reflective supply-side control*, which describes how supply-side control over the demand side shapes the supply side's own behaviour. This extends the mainstream literature on decentralised control in transaction platforms, which predominantly focuses on how control mechanisms of one group affect the behaviour of the other user group on the platform. In addition, during the theorising process, we introduce *the behavioural impact matrix of platform control* (see Table 1), which helps platform control scholars position their contributions more precisely, as demonstrated in this study.

2. Background

In the background section, we begin by discussing data marketplaces (Section 2.1), starting with an overview of data marketplace research in a broader context (Section 2.1.1) and then focusing specifically on the manufacturing industry (Section 2.1.2). In Section 2.2, we present the theoretical perspective on platform control (Section 2.2.1), followed by the behavioural impact matrix of platform control, which helps position our study within this theoretical angle (Section 2.2.2). We then discuss technology-based process control as a key mechanism for ensuring perceived control (Section 2.2.3), and finally justify how smart control can be seen as a form of technology-based process control (Section 2.2.4).

2.1. Data marketplaces

2.1.1. Data marketplace research

We view data marketplaces as inherently possessing platform characteristics, aligning with the recent definition and status of data marketplaces (Simon et al., 2021). Thus, in this study, data marketplaces are special instances of digital platforms, matching businesses that provide and use data (Driessen et al., 2022; Spiekermann, 2019). As indicated in Section 1, one example of a data marketplace in the manufacturing industry is Afteriize, which specialises in the automotive domain. In such a marketplace, for instance, manufacturers may act as data sellers, while insurance companies may act as data buyers. Manufacturers can (responsibly and legally) share (IoT-based) data on maintenance and repair patterns for specific vehicles or brands. Insurance companies can then analyse these data to offer tailored, personalised insurance packages to their end-customers. Marketplace transactions begin with user registration and role selection (seller or buyer). Sellers list metadata to showcase their data products, enabling buyers to identify matches and initiate negotiations. Upon agreement, both parties sign a contract, process payment, and transfer data via application programming interfaces.

Data marketplaces can have a modular architecture, enabling third-party providers to integrate with and enhance the platform's offerings (Spiekermann, 2019). Data marketplaces may be built on standardisation initiatives such as the International Data Spaces Association[5] and GAIA-X.[6] These standards typically offer high-level guidance that serves as building blocks for developing data marketplaces. Such building blocks consist of 1) business and organisational elements (e.g., contractual frameworks) and 2) technical elements (e.g., identity and attestation management).[7] This allows such marketplaces to focus on their unique value propositions, such as implementing data quality checks (cf. Fruhwirth et al., 2020).

Schomm et al. (2013) are among the first scholars to explore diverse types of data marketplaces. After that, the literature covers topics such as data marketplace trends (Stahl et al., 2014), classification frameworks (Stahl et al., 2016), societal implications (Spiekermann and Korunovska, 2017; Virkar et al., 2019; Wu, 2025), pricing functions (Bauer-Hänsel et al., 2024), and business models (Azcoitia and Laoutaris, 2022; Bergman et al., 2022; Fruhwirth et al., 2020). Recent studies explore design options (Driessen et al., 2022), governance structures (Abraham et al., 2023), configuration of socio-technical elements that support the success of data marketplaces (Kernstock et al., 2025), and an artifact to assess data product value (Martin et al., 2025). Having defined data marketplaces, we now focus the discussion specifically on the manufacturing industry.

2.1.2. Data marketplace in manufacturing industries

In manufacturing, the adoption of IoT in supply chains is a major driver of data marketplaces (Ben-Daya et al., 2019), although such marketplaces can also be driven by factory-level IoT and other non-IoT-related supply chain data. Practical examples of manufacturing data marketplaces include IOTA[8] and Dawex.[9] IoT generates vast amounts of data in each supply chain function, such as warehouse logistics (Yan et al., 2014), inventory management (Goyal et al., 2016), and transportation (Lou et al., 2011). Data marketplaces allow manufacturing businesses to capture revenues from their data (Kaiser et al., 2021). For instance, a kitchen appliance manufacturer that integrates machine assembly with wireless technology can share insights with partners to discover efficiency-enhancing use cases (Stahl et al., 2023). Similarly, in the automotive industry, original equipment manufacturers (i.e., companies producing parts for new vehicles) can share data from various car brands with independent service providers (i.e., authorised dealers for repairs without being bound by franchise agreements) (Martens and Mueller-Langer, 2020; Sterk et al., 2024). While sharing IoT data can help businesses to optimise supply chains or monetise unused data products, risks are also present, for instance, as competitors may use shared data to reverse engineer critical manufacturing processes that create a competitive edge (de Prieëlle et al., 2022).

Academic literature on data marketplaces in manufacturing covers various themes. One stream of literature proposes *design solutions*, for instance, prototyping specific marketplace functionalities (Eichler et al., 2022a, 2022b) or developing use case diagrams (Shaabany et al., 2016).

Table 1
The behavioural impact matrix of platform control.

		The controller–controllee relationship	
		Control: Demand-side over supply-side	Control: Supply-side over demand-side
Behaviour studied	**Demand–side**	Q2: Buyer's ability to give feedback increases buyer willingness to pay a price premium (Ba and Paul, 2002).	Q1: Seller's control over data product disclosure affects buyer decisions to purchase (Ray et al., 2020).
	Supply–side	Q3: Feedback from buyers leads to intensive seller communication (Curchod et al., 2020).	Q4: Seller's control over transactions makes them more willing to sell (the present paper)

Notes: The cells provide empirical examples

[5] https://internationaldataspaces.org/, accessed on 12 January 2025.
[6] https://gaia-x.eu/, accessed on 12 January 2025.
[7] https://dssc.eu/space/BVE2/1071252426/Building+Block+Overview, accessed on 07 July 2025.
[8] https://www.iota.org/, accessed on 14 March 2024.
[9] https://www.dawex.com/en/solutions/data-marketplace-data-shop/, accessed on 14 March 2024.

Huang et al. (2021) provide strategic directions for developing data marketplaces according to data specificity (e.g., raw data vs. processed insight) while Nagorny et al. (2018) offer a data marketplace design for smart manufacturing.

Another literature stream focuses on *econometrics,* particularly exploring the pricing mechanisms in data marketplaces that deal with manufacturing data. For instance, Azcoitia et al. (2022) compare pricing strategies and propose a data quotation tool. Azcoitia et al. (2023) investigate how data characteristics affect market prices, finding that manufacturing data command some of the highest prices. M. Zhang et al. (2023b) build a classification system to identify various attributes that influence data pricing. Meanwhile, Mišura and Žagar (2016) develop a pricing model that takes into account the budget constraints of data buyers. Finally, Pei (2022) reviews data pricing approaches from different academic disciplines.

Behavioural studies are remarkably lacking, for example, on how users decide to adopt manufacturing data marketplaces. Data marketplace literature, in general, is primarily technologically oriented in nature (Abbas et al., 2021; Azcoitia and Laoutaris, 2022; Driessen et al., 2022). Examples include research on technological solutions that let buyers acquire data based on its purpose-specific utility (Agarwal et al., 2019) and a federated data marketplace architecture that prioritises sovereignty principles (Jahnke et al., 2024). Yet, the data marketplace literature often overlooks the multi-faceted challenges of human factors and strategic issues, such as the fear of revealing competitive advantages (Fassnacht et al., 2023). These concerns may be alleviated by assuring business users that they still control their data after sharing (von Scherenberg et al., 2024).

The broader literature on data sharing antecedents does show a range of factors for user adoption: benefits (Ramdani et al., 2009), costs (Penttinen et al., 2018; Saprikis and Vlachopoulou, 2012), Security (Fu et al., 2014; Sun et al., 2018), trust (Asare et al., 2016; Pavlou and Gefen, 2004), interoperability, and legal concerns (Eurich et al., 2010). However, most of these sources focus on settings in which well-acquainted businesses intend to share data, such as supply chain partners. Since data marketplaces mediate between a variety of unknown users (Möller et al., 2024), existing insights may not be directly transferable. As data owners realise that their data may be reused, repurposed, and recombined in novel contexts (Aaltonen et al., 2021), concerns over keeping control over data may become even higher. In summary, data marketplaces in manufacturing industries are emerging but face adoption challenges, particularly concerning control over data. However, our understanding of how control influences data owners' willingness to share data remains limited.

2.2. Platform control

Control phenomena have been investigated in numerous disciplines for almost a century (Cram et al., 2016). Building from the fundamental control literature, Cram et al. (2016) broadly define control as "… an attempt to affect the behaviour of another person or group as a means to achieve goals." (p. 218). Likewise, in a digital context, Tiwana and Keil (2009) refer to control as "… the process and rules governing controllee actions implemented by the controller to promote desirable controlee behaviours." (p. 12). This implies the existence of two types of actors: *controllers*, who exert control, and *controllees*, who are subject to control. Early work on control takes a cybernetic view, studying how a system is corrected to align with standardised goals, while contemporary views are either functional (i.e., structuring control to meet organisational goals) or behavioural (i.e., examining the impact of control on controllees) (Saunders et al., 2020).

2.2.1. Control mechanisms in digital platforms and data marketplaces

In the broader digital platform literature, control mechanisms are a central theme. While platforms create value by allowing third-party providers to join and create offerings (Venkatraman and Lee, 2004), some can be low-quality or harmful to other user groups (Wareham et al., 2014). If third-party providers free-ride on the collective reputation of a platform, users can become dissatisfied (Cennamo and Santaló, 2019). Ultimately, reduced user satisfaction may trigger instability and the collapse of the platform ecosystem (Wessel et al., 2017). To prevent undesirable interactions, control mechanisms are essential (Wareham et al., 2014) but have to be carefully offset against other goals of growth and winning the market (Ondrus et al., 2015).

Control mechanisms can be *formal* or *informal* (Tiwana and Keil, 2009). Formal control is defined by "… explicit controller prescriptions, " while informal control tries "… to influence implicit determinants of controlee behaviours." (Wiener et al., 2016, p. 743). Formal control is classified into input control, process control, and output control, while informal control includes self-control and clan control (Ouchi, 1979). *Input control* influences the actions of controllees before they begin an activity. *Process control* targets compliance of controllee processes towards prearranged guidelines and rules. *Output control* ensures that temporary outcomes fulfil predefined goals. Meanwhile, *self-control* focuses on intrinsic motivation at the individual-controllee level by defining and monitoring control objectives (Jaworski, 1988). Finally, *clan control* influences peer group behaviour by motivating them via shared norms, values, and visions (Jaworski, 1988; Kirsch, 1997; Ouchi, 1979).

Appendix B reviews examples of control mechanisms in digital platforms and data marketplaces, as identified in key literature. Regarding input control, most of the literature discusses scenarios where platform providers act as controllers while platform users and third-party providers function as controllees. Examples of such platform input control include membership gatekeeping for both platform users (Thies et al., 2018) and third-party providers (Croitor et al., 2021; Tiwana, 2015). This can be implemented by imposing screening requirements (Croitor and Benlian, 2019) or by requiring actors to submit an official identity certificate from the government (Adam et al., 2023). Additionally, platform providers can demand that users and third-party providers pay an access fee to demonstrate their commitment to joining platforms (Chen et al., 2022). In the context of data marketplaces, a well-known input control mechanism is certification, where data owners and buyers must meet specific requirements, both organisational and technical, before joining marketplaces (Driessen et al., 2022).

Similarly, most platform literature on process control views platform providers as controllers, whereas platform users and third-party providers operate as controllees. For instance, platform providers implement a) application development guidelines (Goldbach et al., 2018), b) software development kits (Staub et al., 2022), c) application programming interfaces (Staub et al., 2022), d) rules for intellectual property rights (Staub et al., 2022) and demand regular project updates (Gleasure et al., 2019; Wu et al., 2024) from third-party providers to ensure that developed complementor solutions align with the platform provider's goals. Platform providers also implement process control to platform users, for instance, by guiding them to increase visibility by encouraging sharing behaviours on social media (Ens et al., 2023). In the data marketplace context, existing literature focuses on technology-based process control (or algorithmic control), where processes are controlled through technology. The key difference between traditional control and technology-based control is that traditional control relies on manual human intervention, whereas technology-based control is automated by algorithms (Cram et al., 2022; Wiener et al., 2023a). Examples include multi-party computations (Agahari et al., 2022), usage controls (Abraham et al., 2023; Scheider et al., 2023a), and smart contracts (Moyano et al., 2021). An interesting aspect of technology-based control is its shift in control dynamics, enabling platform users to partially act as controllers over transaction objects, such as data owners managing their data products. It means process control could prescribe how data is prepared, shared, handled, used, and monitored (see Bastiaansen et al., 2019).

Turning to output control, platform providers oversee third-party

providers through mechanisms such as performance metrics and revenue sharing (Goldbach et al., 2018; Mukhopadhyay et al., 2016). They also enable users to observe each other via feedback systems like complementor ratings (Steur and Seiter, 2021). In the data marketplace context, to the best of our knowledge, we find no specific literature explicitly implementing output control.

In informal control, self-control mechanisms include instruments such as training and tools for self-regulation. These help platform users gain independence in setting their own goals, establishing procedures, and following their processes to achieve them (Goldbach et al., 2018). They also allow users discretion in their actions. For example, project owners can critically evaluate investor suggestions and apply them at their discretion without excessive concern about platform provider intervention (Gleasure et al., 2019). To date, we are not aware of any concrete examples of self-control being implemented in data marketplace settings.

Finally, clan controls include normative pressure and social sanctioning. A concrete example is seller communities in e-commerce, where members establish norms to interpret and refine platform providers' guidelines with added nuances and details (Croitor et al., 2022; Ens et al., 2023). In data marketplaces, a code of conduct (e.g., the IDSA rulebook) serves as an example of clan control, as it establishes a set of shared norms, values, and principles that guide actions and decision-making within an organisation or community (Van Der Burg et al., 2021).

Our review of control mechanisms in digital platforms and data marketplaces reveals three key takeaways. First, most scholars assume that platform providers, rather than platform users, exercise control. As a result, control dynamics are typically studied as a dyadic relationship between platform providers and platform users rather than between platform users themselves. Second, while a few exceptions have started to explore user-to-user control, the behavioural consequences of this relationship remain largely unexamined. Third, platform control research in data marketplaces is not yet mainstream. At the same time, there is growing interest in technology-based process control, which warrants further attention. In the following section, we take a deeper look at the user-to-user control literature stream to strengthen the positioning of this study.

2.2.2. Behavioural impact matrix of platform control

Since data marketplaces are still in an early stage of commercialisation (Abbas et al., 2021), we focus on behavioural aspects rather than outcomes like market capitalisation (Chen et al., 2021). To position our study, we propose *the behavioural impact matrix of platform control* (see Table 1). The matrix consists of two dimensions. The first dimension is the *controller–controllee relationship*, specifying who exerts control and who is subject to it (i.e., who acts as the controller and who as the controlled party). The second dimension specifies *whose behaviour is studied* (i.e., demand or supply side). Considering these dimensions allows us to position our contribution within the platform control literature more precisely.

In the first quadrant (Q1), supply-side users enact control over the demand side, and studies examine the control's impact on the demand-side behaviour. For instance, when data owners enact a control mechanism by selectively disclosing preliminary insights during product demonstrations, buyers may reassess and increase the perceived value of data products they had previously underestimated (Ray et al., 2020). This finding generally aligns with Drakopoulos and Makhdoumi (2023), who demonstrate that control mechanisms allowing data owners to offer free samples and gradually sell data products can, indeed, influence buyer decisions. In the second quadrant (Q2), studies examine how the ability of demand-side users to enact control over supply-side affects their own behaviour. Example studies include buyers on eBay, whose ability to provide feedback (indirectly) increases their willingness to pay a price premium (Ba and Paul, 2002), and Airbnb guests, whose likelihood of submitting reviews increases under incentivised review programs (Fradkin and Holtz, 2023). In the third quadrant (Q3), demand-side users enact control over the supply side, and studies examine the impact on the supply-side behaviour. For example, Curchod et al. (2020) show how reviews provided by buyers influence seller behaviour, prompting sellers to engage in intensive communication to avoid dissatisfaction. In addition, Cabral and Hortaçsu (2010) find that negative feedback from buyers can lead sellers to exit the eBay platform. Finally, studies in the fourth quadrant (Q4) examine how the ability of supply-side users to enact control over demand-side affects their own behaviour. Example studies include Agahari and de Reuver (2022) and Agahari et al. (2025), who examine how multi-party computation, as a mechanism to control what data is being exposed, increases individuals' willingness to share data on personal data marketplaces.

Literature for transaction platforms largely focuses on demand-side control over the supply-side (Q2 and Q3). These studies typically focus on the exchange of tangible products, such as in e-commerce or 'sharing economy' platforms. Studies on supply-side control over the demand-side are less prominent (Q1 and Q4). In settings of e-commerce platforms, for instance, sellers typically (1) have no interest in controlling how buyers use the purchased products and (2) lack the means to enforce usage scenarios. For instance, sellers of consumer electronics generally have no interest in controlling how buyers use these items, besides avoiding liability claims from improper usage. However, for data goods, the consumption of a transacted product can harm the interests of the seller beyond liability. Buyers of data products could extract the underlying data to reverse engineer the processes that led to the data, or to de-anonymise the personal identifiers (Ofe and de Reuver, 2024). Hence, for such goods, sellers do have an interest in controlling how buyers use the products, making Q1 and Q4 relevant.

While some studies (e.g., as shown in Appendix 2) discuss supply-side control over the demand side, they do not necessarily focus on the behavioural impacts. Instead, they adopt a design-oriented approach, exploring design knowledge to develop these mechanisms (e.g., Abraham et al., 2023; Moyano et al., 2021; Scheider et al., 2023b; Scheider et al., 2023a). The few existing studies that do consider behavioural implications typically focus on buyers (i.e., Q1). Most related to Q4 are studies by Agahari and de Reuver (2022) and Agahari et al. (2025), but reduce control to the ability to define which parts of the data are being revealed. Agahari and colleagues' work does not consider other aspects of control, such as the ability to define who gets access, enforce what can (not) be done with the data, and revoking access. Having elaborated on the behavioural impact matrix of platform control, the next section will discuss technology-based process control as a key means to ensure perceived control, justifying its relevance.

2.2.3. Technology-based process control as a key means to ensure perceived control

In this study setting, we focus on developing a scenario in which we embed technology-based process control via smart contracts as a primary means to increase perceived control. According to control theory, Cram et al. (2016) highlight how *control environments* drive these selections. In our study, relevant control environments include a) the characteristic of data as an experience good, b) the stage of the platform's lifecycle, and c) the data sharing process. This leads us to focus on formal control, especially process control.

Data as an experience good: In data marketplaces, the primary shared asset is data goods. Data, being an *experience good,* presents challenges in evaluating its quality and value. Additionally, it is a *non-rivalrous good*, allowing for low-cost duplication and simultaneous use by multiple parties (Koutroumpis et al., 2020). Thus, sharing data products triggers high uncertainty. Wiener et al. (2023b) find that an *authoritative control style*, which correlates to a top-down approach and utilises formal control modes, can be more effective in dealing with uncertainty than an *enabling style* that aims for intensive interactions to enable informal control. An authoritative-control style provides clear guidance and direction, avoiding the confusion of seeking too many

consensuses, which Wiener et al. (2023a) refer to as *too many voices* that worsen uncertain conditions. Therefore, in the context of uncertain data goods, selecting formal control is likely more advantageous than informal control.

The stage of the platform's lifecycle: The data marketplace is still in its infancy, meaning they are in the exploration stage instead of the commercialisation stage. In this early stage, formal control portfolios are generally better regarding speed and efficiency (Beese et al., 2023). At this stage, when resources are limited, formal control modes yield immediate, tangible results. In contrast, informal control modes often take longer to produce observable outcomes. These quick, tangible results from formal controls are crucial for demonstrating the platform's capabilities and attracting potential users. Therefore, in this early lifecycle stage, formal control is more suitable.

Data sharing processes: Data sharing processes typically involve well-defined stages, consisting of preparation (e.g., describing metadata), agreement (e.g., creating a contract), and usage (e.g., monitoring data usage) (see Section 4 for the detailed elaboration of these processes). These generic processes are embedded in reference architectures for data sharing (e.g., Firdausy et al., 2022; Scheider et al., 2023b). Therefore, according to Ouchi (1979), process control mechanisms are particularly suitable when the process activities are well-defined, but the output is less predictable (e.g., due to the nature of data as experience goods). Process control is appropriate because it enables thorough monitoring of each step, operating under the premise that diligent adherence to the process will yield the anticipated outcomes, even when the exact nature of these outcomes remains uncertain. Based on the above elaboration, this study will employ process control as a means to ensure perceived control.

2.2.4. *Smart contracts as a form of technology-based platform control*

Smart contracts are one instance of technology-based platform control. Smart contracts are often viewed as the next generation of usage control (Chiquito et al., 2022; Siddiqui et al., 2022). Smart contracts are "… any self-executing program running in the distributed ledger environment, and it is often meant to implement automated transactions agreed by the parties" (Governatori et al., 2018, p. 378). Smart contracts potentially offer automatic contract execution with greater transparency (Petersen, 2022). Smart contracts help control access to sensitive data, shipments, payments, and automatic tracking, among others (Chang et al., 2019). For instance, smart contracts can enforce the timing of a transaction (Li et al., 2021). Smart contracts help businesses control transactions through better visibility, transparency, and verifiability (De Giovanni, 2020). In this way, smart contracts can be seen as process control because they automate and regulate the steps of contractual negotiation, agreement, and enforcement.

Within our study context of the manufacturing industry, smart contracts are widely considered (Groschopf et al., 2021; Yadlapalli et al., 2022). For instance, smart contracts can automate knowledge work and improve transparency (Grida and Mostafa, 2023) by obtaining more accurate and complete information (Hamledari and Fischer, 2021). There are examples of technical papers that develop smart contracts for supply chains to improve the traceability of transacted goods and ingredients (Terzi et al., 2019; Wang et al., 2019). Also, there is work showing that smart contracts can be used for handling payment processes in supply chains, improving trustworthiness (Raj et al., 2022).

For the specific context of data sharing, smart contracts may dynamically adapt transaction conditions (Xuan et al., 2020). Smart contracts can automatically monitor data compliance usage (Karger et al., 2021; Tuler De Oliveira et al., 2022). Furthermore, data owners can automatically revoke the license if buyers violate the use and access rights (Jagals et al., 2021). For instance, smart contracts may be used to force buyers to use data only in ways agreed upon by withholding a deposit in case of violations (Moyano et al., 2021). In sum, various ways to utilise smart contracts for process control have been suggested in the literature on data sharing and data marketplaces. Thus, we argue that smart contracts naturally enhance the perceived control of data owners.

3. Hypotheses

Trust is a crucial factor in uncertain or interdependent relationships (Mayer et al., 1995; Pavlou and Gefen, 2004). Trust can be understood as the belief that another party will act in accordance with agreed-upon expectations, even in situations of vulnerability (Mayer et al., 1995). Thus, we conceptualise trust as the subjective belief that transactions with data buyers will align with data owner expectations (cf. Pavlou and Gefen, 2004). Achieving (actual) trust requires trust-building processes. Among others, a key process of trust-building is that a party can *predict* the trustworthiness of other parties. For example, a company may trust a supplier based on how long they have had a previous partnership and the frequency with which the company communicates with the supplier (Doney and Cannon, 1997). With the rise of digital technologies, trust prediction is increasingly supported by emerging solutions such as blockchain-based systems (Fan et al., 2024). This is especially helpful for the parties that have never been in a partnership before, so they cannot access the actual trust directly but rather rely on predictive proximity. W. Zhang et al. (2023a), for example, propose a design in which predictions can be evaluated in blockchain-based systems due to the ability to trace what happens to data products, thereby enhancing overall trustworthiness.

On the other hand, we define perceived control as the extent to which data owners feel they can influence and direct data flows to other parties (Abbas et al., 2024), including who can access specific data types for particular purposes (Koutroumpis et al., 2020; Mosterd et al., 2021; Reimsbach-Kounatze, 2021). In the context of data-sharing, perceived control can be a trust-building mechanism, representing the degree to which data owners can decide how their data is used, which enhances confidence in transactions (Lapets et al., 2018). Previous research suggests that contractual safeguards, access controls, and verification mechanisms contribute to trust by reducing fears of opportunistic behaviour (Raj et al., 2022; Terzi et al., 2019).

Trust is essential in manufacturing, where firms collaborate and share data for supply chain optimisation, predictive maintenance, and process innovation (Wang et al., 2019). In this context, firms are reluctant to share data when they fear supply chain partners will behave opportunistically (Dahlberg and Nokkala, 2019; Opriel et al., 2021). Therefore, companies seek assurance that shared data will not be misused (Grida and Mostafa, 2023). Technologies such as smart contracts and distributed ledgers are often introduced to enhance control and transparency, which in turn creates trust among industrial data partners (Hamledari and Fischer, 2021).

In B2B data marketplaces, trust plays a role in facilitating data transactions between firms that may not have prior relationships (Reimsbach-Kounatze, 2021). Technology-oriented work on control in data marketplaces often aims at fostering trust. For instance, smart contracts are believed to reduce opportunistic behaviour (Bottoni et al., 2020), improve transparency (Grida and Mostafa, 2023) and obtain more accurate and complete information (Hamledari and Fischer, 2021). Smart contracts can also contribute to traceability in supply chains (Terzi et al., 2019; Wang et al., 2019) or handle payment processes in trustworthy ways (Raj et al., 2022). In all, smart contracts automate compliance and accountability, reducing uncertainty in transactions (Bottoni et al., 2020). Moreover, privacy-enhancing technologies (PETs) allow businesses to control the data that they share, increasing trust in third-party providers that organise data sharing (Lapets et al., 2018) and supply chain partners (Bogetoft et al., 2009). By restricting data access, defining usage rights, and implementing audit mechanisms, data marketplaces seek to build trust and mitigate concerns about misuse (Agahari et al., 2022). Overall, technologies that allow control over assets are often assumed or shown to enhance antecedents or proxies of trust between supply chain partners, such as transparency, trustworthiness and traceability. Yet, whether higher

perceptions of being in control contribute to trust in data buyers is not empirically shown. To evaluate this, we hypothesise that:

H1. Perceived control increases trust in other data buyers.

Risk perception is a fundamental driver of decision-making in uncertain environments, influencing willingness to share resources (Jaspreet Bhatia et al., 2016a,b; Xu et al., 2011). Perceived control has been linked to risk mitigation because organisations feel more secure when they can define and enforce data access rules (Eurich et al., 2010). Manufacturers face significant risks when sharing operational, customer, and supply chain data, as unintended data leakage can lead to competitive disadvantages and intellectual property theft (Dahlberg and Nokkala, 2019). Control mechanisms, such as role-based access controls, confidential computing, and federated learning, allow firms to share insights without exposing raw data, thereby reducing perceived risks (Opriel et al., 2021). For example, data sovereignty solutions have emerged to allow firms to define clear data-sharing boundaries while preventing unauthorised access (Richter and Slowinski, 2019). In industrial settings, reducing the perceived risks of sharing sensitive data is essential for fostering collaboration and enabling digital transformation.

In B2B data marketplaces, perceived risks are a major barrier to participation, as firms fear that shared data may be misused, resold, or repurposed beyond their intended scope (Agahari et al., 2022). It means that competitors might gain an advantage from shared data (Spiekermann, 2019). Control mechanisms such as data licensing, differential privacy, and smart contracts are designed to reduce perceived risks by enforcing strict data governance policies (Reimsbach-Kounatze, 2021). Fine-grained data access policies and usage tracking further help to alleviate concerns about potential data misuse (Eurich et al., 2010). Although technological solutions for risk reduction through control exist, the psychological effect of perceived control on risk perceptions is not well-documented. In other words, whether perceived control directly translates into lower risk perceptions is yet to be empirically established. Therefore, we hypothesise that:

H2. Perceived control reduced perceived risks of data misuse

Trust is often associated with perceived risks (Hart and Saunders, 1997). Trust can be understood as the belief that another party will act in accordance with agreed-upon expectations, even in situations of vulnerability (Mayer et al., 1995). In contexts such as online marketplaces, trust has been shown to significantly reduce concerns about fraud or misuse (Nicolaou and McKnight, 2006; Pavlou and Gefen, 2004). Trust in online marketplaces can be generated through a large variety of trust-generating mechanisms (Son et al., 2006). By extending this concept to data sharing, it follows that trust in data buyers can reduce the fear that data might be mishandled, leaked, or exploited for competitive advantage.

In the manufacturing industry, risks are especially related to competitive advantages. For instance, manufacturers fear that sharing data on their operational processes allows competitors to reverse-engineer their unique approaches, as seen in, for instance, the agriculture industry (de Prieëlle et al., 2022). Trust between users may reduce the perception of risk as manufacturers gain confidence in the integrity of data buyers, as found in earlier empirical studies of manufacturing (Shih et al., 2013). For example, collaborative data-sharing initiatives like the International Data Spaces rely on trust-building measures such as certifications and adherence to common data-sharing frameworks to reduce perceived risks (von Scherenberg et al., 2024).

In the specific context of B2B data marketplaces, trust is essential for reducing concerns about data misuse. When data buyers are perceived as trustworthy, sellers are more likely to believe that their data will be handled responsibly, even beyond formal control measures (Agahari et al., 2022; Roman and Stefano, 2016). Given this, our hypothesis is:

H3. Trust in other data buyers decreases perceived risk of data misuse

Perceived control is a fundamental determinant of human behaviour, influencing decision-making across various domains, from consumer behaviour to digital interactions. For instance, in the theory of planned behaviour (Ajzen, 1991), it is assumed that when people feel they have control over an action, they are more likely to engage in that behaviour. In the context of data sharing, greater control over one's data can reduce psychological barriers and increase confidence in making data-sharing decisions. Studies on digital privacy and personal data management show that when users perceive control over how their data is used, they are more inclined to participate in data sharing (Smith et al., 2011). The same principle applies to organisations, where decision-makers prefer environments that provide autonomy and governance over shared assets.

In manufacturing, companies are often reluctant to share data due to concerns about competitive advantage, misuse, and loss of proprietary insights. Manufacturers are likely more willing to engage in data-sharing initiatives when they perceive mechanisms that grant them control over access, usage rights, and security. Industry initiatives such as data sovereignty and smart contract-based governance models aim to empower firms with more control over their shared data (von Scherenberg et al., 2024). Usage control is also seen as an integral way to realise data sovereignty (Zrenner et al., 2019). If manufacturers perceive that they can regulate who accesses their data and under what conditions, they are more likely to participate in data-driven collaborations.

Unlike personal data-sharing contexts that focus on privacy (Cichy et al., 2021), B2B data marketplaces require mechanisms to ensure intellectual property protection, fair compensation, and enforceable contracts (Bonnet and Teuteberg, 2023). Control is required to resolve tensions between the interests of the buyers and data owners (Bonnet and Teuteberg, 2023). Decentralised data sharing architectures with smart contracts offer increased control over data transactions, which can enhance trust and willingness to share (Agahari et al., 2022). In these settings, perceived control not only reduces uncertainty and risk perceptions but also serves as a direct signal that organisations can share data without jeopardising their competitive position. Consequently, firms that perceive greater control over their data-sharing interactions are more likely to engage in B2B data sharing. Thus, we hypothesise:

H4. Perceived control increases willingness to share data.

Literature on the relationship between trust and data sharing is abundant, especially within supply chains. Trust has been shown to affect willingness to share data between businesses (Nicolaou et al., 2013; Nicolaou and McKnight, 2006). For instance, a study by Chen et al. (2014) shows that inter-organisational trust is a prerequisite for data sharing among organisations. Mechanisms to enhance trust must be established before initiating data sharing through digital infrastructures (Müller et al., 2018). If data owners trust data buyers, they are more willing to share data (Müller et al., 2020).

In manufacturing supply chains, buyers and sellers face a risk of opportunistic behaviour when interacting, for instance, regarding price negotiations and squeezing. The importance of trust for data sharing in supply chains, including manufacturing, has been demonstrated in expert studies (Müller and Gaudig, 2011). A study in the horticulture industry found trust to be a key antecedent for data sharing (de Prieëlle et al., 2022). In B2B data marketplaces, trust in buyers is likely an important driver of adoption decisions. Regulations such as the Data Governance Act are primarily aimed at creating a basis for trust between actors for data sharing, seeing trust as a 'glue' for realising the data economy (Bernal, 2024). The relevance of trust is highlighted in the emerging literature on data marketplaces (Richter and Slowinski, 2019; Spiekermann, 2019). A key differentiating factor of the data marketplace context is that users lack familiarity, which may create a barrier to data sharing (Christidis et al., 2022). Still, mechanisms in data marketplaces, such as reviews or certification, may boost trust in data buyers. Such mechanisms may generate trust in the data being shared as well as in the transaction partners (Genés-Durán et al., 2022). Therefore, we hypothesise:

H5. Trust in other data buyers increases willingness to share data.

Perceived risk is a well-established barrier to sharing in various contexts (Genés-Durán et al., 2022). Risk perception arises from uncertainties about the recipient's intentions or potential misuse (Xu et al., 2011). For instance, vagueness about the privacy policies in data usage is a core concern for partnering in the digital economy (Jaspreet Bhatia et al., 2016a,b). Lower perceptions of risk positively affect willingness to share data in inter-organisational systems (Nicolaou and McKnight, 2006). Manufacturers face significant risks when sharing proprietary data, including potential competitive disadvantages and loss of intellectual property. IoT-generated data, for example, can reveal operational insights that competitors could exploit (de Prieëlle et al., 2022). Supply chain research shows that data sharing is often undesirable because of opportunistic behaviours by other organisations (Cheng et al., 2013). Consequently, risk-averse manufacturers are hesitant to engage in data-sharing initiatives, even when the potential benefits, such as supply chain optimisation, are substantial.

Businesses are generally concerned about participating in data sharing because they risk sharing their sensitive information with other parties to their disadvantage (Kwon and Suh, 2005; Tsai and Ghoshal, 1998). In the context of data marketplaces, Spiekermann (2019) found that competitors might gain an advantage from the data shared by data owners via such a platform. Therefore, we posit:

H6. Perceived risk of data misuse reduces willingness to share data

4. Method

An online survey was administered through Qualtrics. Approval was obtained from the authors' institutional human research ethics board. Informed consent forms were approved by the ethics board and presented to respondents before starting the survey.

4.1. Sample

Our population comprises business managers in the manufacturing industry who are involved in decisions on adopting a data marketplace. Sampling was done among business managers in the EU, UK and US with the help of Prolific.ac. Prolific is a crowdsourcing platform that is widely used in academic research. The sampling frame consists of 829 potential respondents who are registered in Prolific and who have a managerial role in a manufacturing business. Eligibility was verified through filter questions that asked respondents to describe their industry and role. Only those respondents who indicated the manufacturing industry and selected roles of 'Upper Management', 'Middle Management', 'Junior Management', 'Consultant' and 'Researcher'[10] were retained. Respondents received a small amount of financial compensation (i.e., £2,60 for the 15-min survey).

The survey yielded 299 complete and eligible responses (36 % response rate). Five respondents who filled out the survey too quickly were removed. One respondent was omitted for giving invariable responses to each question. Missing values were scarce and dealt with through imputation using the FIML algorithm in JASP. Respondents are from the UK (43 %), the US (29 %) and the EU (28 %). Most respondents have a managerial role (84 %) and at least three years of working experience (81 %). According to self-reports, our respondents are generally familiar with Industrial IoT (63 %) and data marketplaces (60 %).

[10] In our sample, only 3 % of participants identified as researchers. We assume that these individuals are primarily affiliated with R&D departments within manufacturing firms and thus likely involved in technology strategy and data-related initiatives. Given the novelty of smart contracts and data marketplaces, we considered it likely that such profiles would have relevant insights and influence on decisions about inter-organisational data sharing. Nonetheless, we verified that excluding these cases does not significantly affect our findings. Re-running the analysis on the sample without the nine researchers leads to marginal differences in the regression weights, see Appendix C.

4.2. Scenario

Respondents were presented with a scenario to ensure that they had a similar reference for answering the survey questions (see Appendix D). The scenario specified the conditions of data sharing, the data marketplace, and control mechanisms. In this scenario, the platform provider grants data owners some autonomy in deciding data usage, enabled by technology-based process control via smart contracts. As a result, control over data shifts toward platform participants rather than the platform provider. This suggests that our scenario aligns closely with a decentralised data trading model that relies on decentralised architecture through smart contracts (cf. Fruhwirth et al., 2020).

Respondents were asked to imagine that their machines and manufacturing processes create data that can be shared. Considering that organisational readiness affects data-sharing decisions (Kuan and Chau, 2001), respondents were asked to imagine all their systems to be interoperable, with data being easily accessible and the data marketplace requiring no effort to train personnel. As pricing is another hurdle (Mao et al., 2019) but not affected by perceived control, we told respondents to assume receiving a 'fair price', covering expenses of sharing data and a small profit margin. Considering that trust in data platform providers plays a role (Chang et al., 2020), respondents were asked to assume that the provider would be a small specialised company independent from 'big tech' cloud providers.

Respondents were presented with a description and visualisation of data marketplaces. We simplified an existing description of a data marketplace (Gupta et al., 2021). Respondents were explained that the data marketplace would be operated by various facilitators that store transactions on a public blockchain, which should be understood as a long list of transactions that are open for inspection and non-malleable. Further, respondents were told that regulators could audit and monitor compliance with local privacy laws.

To ensure that respondents would perceive a degree of control, a form of technology-based process control was operationalised into the survey scenario. Participants acting as data owners were explained that requesting parties have to specify the data they wish to access, the purpose and the price. Upon negotiating these terms of use, a smart contract will be initiated to enforce these agreements. The descriptions were pre-tested, after which clarifications were made in content and formatting.

4.3. Measures

Table 2 provides an overview of the measures. To measure perceived control, we adapted items from Xu et al. (2008). The items focus on the control over who can access shared data and in what way. To measure trust, we adapted existing measures from Kehr et al. (2015), tailoring them to our context by specifying the entity to be trusted (i.e., data buyers) and the scope of the activity for which they are to be trusted (i.e., handling data from the data marketplace). In B2B data marketplaces, interactions often occur between parties without prior relationships. As such, actual trust based on past experience is typically unavailable. Instead, trust must be inferred in advance, making expected trustworthiness a suitable proxy. This aligns with Kehr et al. (2015), who build on Doney and Cannon's (1997) view of trust as a belief in the predictability of another's behaviour. For perceived risk, scales were adapted from two sources (Kehr et al., 2015; Xu et al., 2008). Finally, we adapted a scale from Pavlou (2003) to measure data owners' willingness to share data.

The measurement model was tested through confirmatory factor analysis, showing an acceptable model fit (CFI = .915; TLI = .893; NFI = .893, RMSEA = .116). Convergent validity is high, as the variance

Table 2
Measurement model.

Construct	Adapted from	Measure	Std factor load	Avg var extr	Comp Rel
Perceived control	Xu et al. (2008)	I believe I have control over who can get access to my data	.743	.583	.753
		I think I have control over what data is released by the marketplace	.778		
		I believe I have control over how data is used by the other users	.795		
		I believe I can control my data after providing it to the marketplace	.735		
Trust in data buyers	Kehr et al. (2015)	I expect that data buyers would be trustworthy in handling the data they got from this data marketplace	.861	.842	.795
		I expect that data buyers would tell the truth and fulfil promises in handling the data they got from this data marketplace	.932		
		I expect that data buyers would be honest when handling the data they got from this data marketplace	.953		
Perceived risk	Xu et al. (2008) and (Kehr et al., 2015)	It would be risky to share this data in the marketplace	.798	.613	.839
		There would be a high potential of giving away personal information	.778		
		There would be a high potential of giving away a competitive advantage	.860		
		The data could be inappropriately used.	.717		
		Sharing this data could involve many unexpected problems	.756		
Willingness to share data	Pavlou (2003)	Given the chance, I would share my data via this data marketplace	.926	.867	.732
		Given the chance, I predict that I should share my data via this data marketplace in the future	.968		
		It is likely that I will share my data via this data marketplace in the near future	.899		

Notes: Std factor load = Standardised factor loading; Avg var extr = Average variance extracted; Comp Rel = Composite Reliability

extracted exceeds .6 for all constructs, and standardised factors loadings exceed .7. Composite reliability is acceptable as well, exceeding .7 for all constructs.

Discriminant validity is acceptable, as shown by the heterotrait-monotrait (HTMT) ratio (Henseler et al., 2015), with values well below .9 for all combinations of constructs, see Table 3.

Common method bias was assessed through confirmatory factor analysis, comparing the fit of a single-factor to a multi-factor model. A chi-square difference test shows that a single-factor model fits significantly worse on the data compared to a multi-factor model ($\Delta\chi^2$ (6) = 962.452, $p < .001$), whereas the fit indices similarly indicate a low fit of the single-factor model (CFI = .670, TLI = .615).

5. Results

5.1. Structural model

Hypotheses are tested through structural regression using maximum likelihood estimation, using the lavaan package. Overall model fit is acceptable, with χ^2 (8) = 418.078, $p < .001$; CFI = .915; TLI = .894; NFI = .894; RMSEA = .115. All regression weights are significant at the $p < .001$ level (see Fig. 1), except for the path from trust to perceived risk. Hence, all hypotheses are supported except for H3. Explained variance is moderate to high for all constructs. For our dependent variable of willingness to share data, the explained variance equals 65.7 %.

To assess the mediating role of trust and perceived risk, we perform mediation tests in lavaan, using robust standard errors to compute confidence intervals. The proportion of mediation was calculated as the ratio of the indirect effect to the sum of the direct and indirect effects. Our findings indicate that only perceived risk significantly mediates the effect of perceived control on willingness to share data (20.8 % mediation, see Table 4). Although perceived control significantly influences trust (see Fig. 1), trust does not significantly mediate this relationship, as its confidence interval includes zero, indicating that the indirect effect is not statistically different from zero. Thus, we find no evidence that trust in data buyers significantly mediates the effect of perceived control on willingness to share data. Perceived control exhibits a stronger indirect effect via perceived risk than via trust.

5.2. Robustness tests

As controls in our study, we have familiarity with IoT, familiarity with data marketplaces and perceived sensitivity of data. First, we examine whether the control variables have a direct effect on the endogenous variables in the model. These variables were specified as direct predictors of all endogenous constructs in the lavaan syntax (i.e., perceived risk, trust, and willingness to share). The results in Table 5 show that the core paths of our model remain stable and significant, with similar path weights.

Among the control variables, perceived sensitivity of the data had a significant negative effect on willingness to share (std regression weight = −.094, p = .021) and a positive effect on perceived risk (std regression weight = .181, $p < .001$). This suggests that individuals who perceive the data as more sensitive are both more risk-aware and less willing to share it. In contrast, familiarity with IoT and familiarity with data marketplaces had no significant direct effects on risk, trust, or willingness to share.

Table 3
Heterotrait-monotrait ratio.

Construct	Perceived control	Trust in data buyers	Perceived risk	Willingness to share data
Perceived control	1			
Trust in data buyers	.788	1		
Perceived risk	.698	.593	1	
Willingness to share data	.787	.690	.693	1

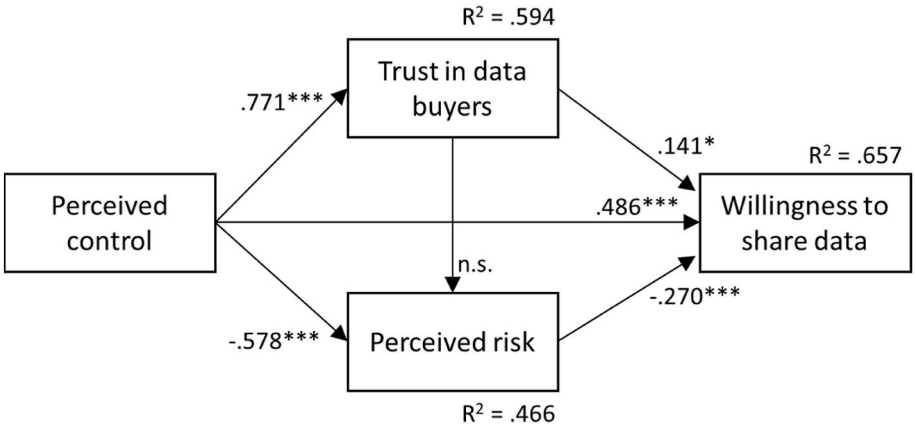

Fig. 1. Structural model (n.s. = non-significant; *p < .05; ***p < .001).

Table 4
Mediation tests.

Indirect effect path	Estimate	Proportion mediated	p-value	95 % confidence interval
Control → Trust → Willingness	.103	13.3 %	.107	−.022, .229
Control →Trust → Risk → Willingness	.029	3.8 %	.223	−.018, .076
Control → Risk → Willingness	.162	20.8 %	.003	.056, .286

Table 5
Robustness check.

	Model 1: With controls	Model 2: With controls
Path	Std regression weight	Std regression weight
Control → Risk	−.578***	−.545***
Trust → Risk	n.s.	n.s.
Control → Trust	.771***	.759***
Control → Willingness	.486***	.479***
Trust → Willingness	.141*	.151*
Risk → Willingness	−.270***	−.249***
IOT Familiarity → Risk	–	n.s.
DMP Familiarity → Risk	–	n.s.
Sensitivity → Risk	–	.181***
IOT Familiarity → Trust	–	n.s.
DMP Familiarity → Trust	–	n.s.
Sensitivity → Trust	–	n.s.
IOT Familiarity → Willingness	–	n.s.
DMP Familiarity → Willingness	–	n.s.
Sensitivity → Willingness	–	−.094*

Next, we run a multigroup analysis in lavaan, after converting the control variables to binary levels. Specifically, overall model fit is compared between models with regression weights constrained to be equal and not (see Table 6). We find that familiarity with IoT and with data marketplaces have no significant moderating effect. However, perceived sensitivity of data has (p = .010) a significant moderating effect.

To examine which specific regression weights are significantly moderated, we release the constrained regression weights one by one, starting with those that have the largest difference in the unconstrained models (see Table 7). We find that releasing the path from control to risk significantly increases the model fit. In the unconstrained model, the regression weight is −.847 (p < .001) for respondents who find the data not sensitive and −.405 (p < .001) for respondents who find the data sensitive. The other regression weights are not significantly different between the groups, as releasing the constraints does not improve model fit.

Although the effect size of control on risk differs between groups, it is significantly negative in both groups. Thus, the direction of the effect supports our hypothesis consistently across perceived sensitivity levels.

Table 6
Moderating tests.

	$\Delta\chi^2$	Δdf	p
Familiarity with IoT	2.563	6	.861
Familiarity with data marketplaces	2.348	6	.885
Perceived sensitivity of data	16.735	6	.010

6. Discussion

In Section 6, we discuss our contributions to the literature (Section 6.1), focusing on three areas: (1) the intersection of B2B data marketplaces and manufacturing literature, (2) platform control literature, and (3) technology-oriented adjacent disciplines. We also address policy implications in this section. In Section 6.2, we discuss the limitations of this study.

6.1. Contributions to literature

Contribution to the intersection of B2B data marketplaces and manufacturing literature: First, our results show that perceived control is an important antecedent of willingness to share data on data marketplaces in manufacturing industries. This means that our findings provide additional empirical evidence of the importance of perceived control (or sovereignty) as a key adoption factor for data marketplaces, which aligns with previous studies that take a more limited understanding of control over data (e.g., Agahari and de Reuver, 2022; Agahari et al., 2025).

Second, we provide a justificatory mechanism that explain the relationship between perceived control and willingness to share data. This contrasts with earlier studies on the behavioural impact of control mechanisms in data marketplaces, which did not examine the nomological networks of such impacts (e.g., Agahari and de Reuver, 2022;

Table 7
Unconstrained model fit.

Unconstrained path	$\Delta\chi^2$	Δdf	p
Control → Risk	8.592	1	.003
Trust → Risk	1.258	1	.262
Control → Trust	.034	1	.855
Control → Willingness	1.027	1	.311
Trust → Willingness	2.265	1	.132
Risk→ Willingness	.124	1	.724

Agahari et al., 2025). In doing so, our discovery about the partial mediation of perceived risks suggests that control mainly affects the negative consequences of data sharing that businesses trade off against benefits. In this way, our findings shed light on the reasons for the low adoption of data marketplaces (Azcoitia and Laoutaris, 2022). We suggest that perceived control should be considered a core antecedent of data sharing in the context of data marketplaces mediating between unfamiliar parties. In addition, our findings also imply that perceived control over data products is a more critical factor for firms adopting data marketplaces than trust in data buyers. While trust has often been considered a key determinant of data-sharing behaviour (Chen et al., 2014; Müller et al., 2018, 2020), our results indicate that its mediating role in the relationship between perceived control and willingness to share data is not statistically significant.

One potential explanation for this result is that perceived control over data products reduces the reliance on trust. When firms feel they can exert control over their data, through mechanisms such as smart contracts, privacy-enhancing technologies, or contractual safeguards, they may not need to place as much trust in data buyers. This aligns with perspectives from the literature on smart contracts (Hawlitschek et al., 2018; Tech et al., 2019) and inter-organisational data sharing (Lumineau et al., 2023), which suggests that technologies enabling control can substitute for interpersonal or inter-organisational trust. Furthermore, in the context of data marketplaces, where transactions often occur between unfamiliar parties, trust may be more challenging to establish, in contrast to settings such as supply chains (Chen et al., 2014; Collier et al., 2022), where trust can be built between well-known partners.

Another potential explanation is that different types of trust influence willingness to share data in data marketplaces. For instance, trust in technology (e.g., confidence in brands or the companies behind it) may still play a mediating role (Ferraro et al., 2023). In data marketplaces that embed smart contracts, trust in technology might outweigh trust in data consumers. Since these technologies are still emerging, questions remain about their functionality. This lack of clarity can create doubt (cf. Agahari et al., 2022). Although omitted variable bias is possible, the high R^2 value in our empirical results suggests that the model explains a substantial portion of the variance in data providers' willingness to share data. Future research, however, could still further examine how different types of trust influence data-sharing behaviour.

It is also possible that perceived control has a cognitive effect: when perceiving to be in control over what happens with data, risks of data misuse are thought to be lower, increasing willingness to share data. Trust in data buyers does not play a significant mediating role. This finding supports the idea that technologies that afford control may replace the need to trust, for instance, in the literature on smart contracts (Hawlitschek et al., 2018; Tech et al., 2019) or inter-organisational data sharing (Lumineau et al., 2023). As such, our findings support the argument that trust in actors like data buyers is expected to be less relevant in the future, and more questions will be asked about trust in underlying technologies (Agahari et al., 2022; Lumineau et al., 2023; Seidel, 2018).

Our findings thus present an alternative theoretical perspective that goes beyond the commonly accepted view of trust as a necessary condition (e.g., Stachon et al., 2023; von Scherenberg et al., 2024). Instead, this perspective suggests that trust in data buyers may be less significant if data owners feel they retain control over their assets. Adopting this view allows us to reflect on and move beyond initiatives focused on building an "ecosystem of trust" among companies participating in a data ecosystem (e.g., Werling et al., 2025). Our findings provide a starting point for future research to rethink and further investigate the prevailing assumption that trust-building initiatives, such as certification and transparency measures, are necessary for data-sharing adoption. This aligns with emerging perspectives in regulatory frameworks such as the Data Act, which emphasises restoring control to data owners rather than relying solely on trust-building. Initiatives such as IDSA and GAIA-X, which focus on building data spaces as environments of trust and well-behaved buyers (Huber et al., 2022), should prioritise experimenting with mechanisms to enable control rather than concentrating on trust-building measures such as certification. Thus, this finding can guide efforts in developing technical solutions for data marketplaces, mainly by initiating discourses on technical research focused on mechanisms like data provenance to ensure control over data (e.g., Scheider et al., 2023a).

Third, bringing the findings back to the manufacturing context, this study aims to address the role of B2B platforms, particularly data marketplaces, in transforming manufacturing sectors such as supply chains. Specifically, we discuss a key condition under which such B2B data marketplaces can thrive: perceived control, which significantly influences the willingness to engage in data sharing. This study extends the existing literature on data marketplaces in manufacturing, which has yet to consider the impact of perceived control despite its importance and relevance. Perceived control can be facilitated by emerging technologies, such as smart contracts, which we explore as enablers of transformation in the manufacturing sector. Ultimately, we contribute to the call for theory development on the next generation of B2B digital platforms, moving beyond the focus on B2C platforms.[11]

Contribution to platform control literature: We contribute to the platform control literature in two ways. First and foremost, we theorise a novel phenomenon: *reflective supply-side control,* which refers to how supply-side control over the demand side influences the supply side's own behaviour. This extends beyond the mainstream platform control literature, which primarily focuses on demand-side (e.g., buyer) control over the supply side (e.g., sellers) (Chen et al., 2021). While a few studies examine supply-side control over the demand side, they focus on how such control affects demand-side behaviour (e.g., Drakopoulos and Makhdoumi, 2023; Ray et al., 2020), not how the ability to enact control influences the supply side's own behaviour. In broader contexts (e.g., decentralised digital platforms), this perspective may help explain why such technologies often struggle to deliver on their promises. One possible reason is that users tasked with enacting control mechanisms themselves may not find the technology useful or usable. As such, this line of research can offer more behavioural explanations for resistance to innovation in decentralised technology beyond well-known narratives such as high infrastructure costs (Iyengar et al., 2023), environmental concerns (Sedlmeir et al., 2020), or complex coordination challenges (Hsieh and Vergne, 2023).

Second, we offer the *behavioural impact matrix of platform control.* This helps platform control scholars to position their contribution more precisely, as we have done in this study. Although this study focuses on the controller–controllee relationship between platform users, the framework can also be applied to other relationships, such as (1) between platform providers and third-party providers (and vice versa), and (2) between platform users and third-party providers (and vice versa). By applying this framework from the perspective of third-party providers exercising control over platform users, for example, we can identify another underexplored area of research. A relevant case may be found in e-commerce platforms, where third-party instalment payment providers act as controllers by enforcing repayment schedules and conducting credit eligibility checks, thus influencing how users transact and manage purchases. This raises a key question: to what extent do such control mechanisms affect the payment providers' own willingness to participate in the platform ecosystem? To our knowledge, this question remains insufficiently addressed in the literature, and this gap can be spotted thanks to our proposed framework.

Secondary contribution to adjacent disciplines: Our work also offers insights for adjacent, technology-oriented fields. Several advanced technologies are being developed that provide control over

[11] https://www.sciencedirect.com/special-issue/10GSRFPKD6C, accessed on 16 January 2025.

data while sharing it with other parties. Examples include smart contracts, as studied in this paper, but also a variety of privacy-enhancing technologies, such as multi-party computation and zero-knowledge proofs (Álvarez et al., 2024). Technologies such as federated learning also offer a potential technical solution, enabling machine learning developers to train models on data at its source (e.g., provided by data owners) without the need to transfer the training data products to a central location owned by data buyers, thus enabling control over data products to data owners. This paper shows that such technologies can foster adoption, assuming that managers indeed perceive higher levels of control. The findings legitimise the search for technologies that provide control over data in settings where organisations do not have prior relationships (Kumar et al., 2020) but also show the importance of addressing decision-makers' perceptions about these technologies. Thus, policymakers can initiate horizontal non-legislative measures, such as fostering research funding in such technology (Wauters European Commission et al., 2018), given their potential to increase control over data products that a) enable digital transformation in the manufacturing industries specifically and b) unlock the potential benefits in data sharing generally.

Policy implications: Regarding the implications of the regulatory framework for data sharing, we can reflect on two recently developed policies: the Data Governance Act (DGA)[12] and the Data Act.[13] For instance, the DGA heavily emphasises trust as a primary goal. An explicit objective of the DGA is to "… provide a framework to enhance *trust* in voluntary data sharing for the benefit of businesses and citizens." However, if achieving trust is too difficult, we suggest focusing instead on control measures. In practice, alongside mandating data intermediaries (e.g., data marketplaces) to provide anonymisation and explicit contractual mechanisms, policymakers could also require the implementation of sovereignty measures as technical requirements.

Additionally, these findings provide evidence supporting the Data Act's goal to restore control to data owners. For instance, the Data Act "… clarifies *who* can use *what* data and under *which* conditions." One of its key benefits is mitigating the abuse of contractual imbalances; for example, it empowers data owners with less negotiating power to have a voice in setting terms for data sharing. All these efforts aim to enhance control over data. If data owners perceive these measures as effective, they are more likely to view data-sharing risks as manageable, ultimately increasing their willingness to share data.

6.2. Limitations

To ensure internal validity, several contextual factors were controlled; these include assumptions related to 1) fair price, 2) data sensitivity, and 3) organisational readiness. To do so, participants were instructed to assume they would receive a fair price for their data (e.g., "You can assume that you will receive a fair price for your shared data. This means that it is enough to cover any expenses that you need to make to share the data and make some profit. Enough to consider sharing the data you're already producing"). They were also told to assume the data was sensitive (e.g., "This data might be sensitive. It could give away an advantage to a competitor or contain personal information"). We also informed participants that their organisation is prepared to share data. For example, we stated: "Imagine the company you work for has spent the past 5–10 years investing into smart manufacturing systems."

Our results, thus, may be generalisable only to settings in which data owners are being offered sufficient monetary compensation for their sensitive data while also possessing enough organisational readiness. Consequently, potential interaction effects exist, which may be explored in future work. For instance, following a privacy calculus logic, benefits may offset risk, implying that the mediating role of perceived risk could be lower in settings where payments for data are perceived to be high. Moreover, price levels appear to be a crucial factor influencing data providers' willingness to share. For example, companies may still be willing to share data even in low-control, low-trust, and high-risk situations if the monetary incentive is sufficiently high. Further, lower levels of organisational readiness could reduce the ability to utilise control mechanisms, which may reduce the importance of perceived control. We, therefore, recommend testing our model in controlled settings with varying levels of payment, data sensitivity, and readiness to share data.

As discussed in Section 3, we rely on proximity to assess actual trust (i.e., trustworthiness), which emerges through specific trust-building mechanisms. In this study, we focus on *predictive* mechanisms, in particular, those that can be supported through blockchain-based technologies such as smart contracts. However, other trust-building mechanisms may also play a role. For instance, *capability-based* mechanisms involve assessing a data consumer's ability to fulfil commitments, often based on brand reputation or perceived power (cf. Doney and Cannon, 1997). This aspect was not included in our current research, but future work could explore how different technological affordances influence specific dimensions of trustworthiness. Nevertheless, our approach remains valid, as smart contracts primarily operationalise *predictive* mechanisms, which aligns with our objective of measuring trust in blockchain-enabled data marketplaces.

While representativeness cannot be demonstrated, our sample contained many people with manager roles in manufacturing companies. Although respondents received a moderate fee for participating, we assume this does not create a large bias, and respondents who were overly quick in answering the questions were removed from the sample. The knowledgeability of respondents on topics of data marketplaces was based on self-reports and was not verified with knowledge questions. We addressed this issue by having a relatively extensive description of a data marketplace and its control mechanism, refined for understandability in qualitative pre-test steps. Finally, our results are transferable to settings with highly granular data (e.g., IoT-generated) with significant risks of reverse engineering or knowledge spillover (e.g., manufacturing industries).

As in any cross-sectional study, causal claims should be made with care, as temporal precedence cannot be established. However, trust and perceived risk are widely used antecedents of willingness to share data. Our findings motivate us to conduct follow-up studies, for instance, involving experimental designs that systematically manipulate levels of perceived control and trust.

Considering the limitation of the design, we assume that technology-based process control (i.e., via smart contracts) is a primary means to ensure increased perceived control. It means that there is a limitation in terms of isolating the effects of this control mechanism. Although generally, such technology-based process control has an impact on perceptions of control (c.f., Agahari and de Reuver, 2022), there are variations in how data owners perceive this. This study shows that such variations, in fact, explain the willingness to participate. We acknowledge this and thus advise future research to adopt an experimental design or compare different forms/levels of control mechanisms to perceived control. Yet, this design is sufficient for our goal to see how perceived control (even if they vary) generally impacts trust, risk, and willingness rather than a cause-and-effect comparison between groups with different types of control.

7. Conclusions and future work

This paper shows that perceived control over data products can increase the willingness to share data on data marketplaces in manufacturing industries, especially as data owners perceive less risk of sharing data. It means that technologies that give control to data owners may be effective in incentivising data marketplace adoption. In contrast,

[12] https://digital-strategy.ec.europa.eu/en/policies/data-governance-act, accessed on 15 January 2025.

[13] https://digital-strategy.ec.europa.eu/en/policies/data-act, accessed on 15 January 2025.

while perceived control influences trust in data buyers, we find no evidence that trust plays an important role in mediating data-sharing decisions in data marketplaces.

Future research directions include incorporating additional data-sharing antecedents that may be affected by perceived control. Further, interactions with contextual variables such as organisational and technical readiness may be examined. Further research could also investigate the design features of control mechanisms that are most influential in promoting data sharing while managing perceived risks, such as contrasting smart contracts with alternative decentralised technologies like multi-party computations and zero-knowledge proofs.

This paper is the first to examine how supply-side control over demand-side users influences the behaviour of supply-side users themselves. Specifically, we investigate how data owners' ability to enact a control mechanism, smart contracts, shapes their perceptions of data sharing. This perspective extends prior studies that examine supply-side control over demand-side users but focus primarily on demand-side behavioural impacts (e.g., how data owners' control over data product disclosure influences buyers' purchase decisions). It also contrasts with the broader platform control literature, which typically studies platform provider control over platform users (e.g., gatekeeping platform membership by imposing upfront criteria).

CRediT authorship contribution statement

Antragama Ewa Abbas: Writing – review & editing, Writing – original draft, Project administration, Conceptualization. **Floris Kool:** Writing – original draft, Methodology, Investigation, Conceptualization. **Wirawan Agahari:** Writing – review & editing, Writing – original draft, Supervision, Methodology, Conceptualization. **Mark de Reuver:** Writing – review & editing, Writing – original draft, Validation, Supervision, Project administration, Methodology, Investigation, Funding acquisition, Formal analysis, Data curation, Conceptualization.

Acknowledgement

The first author's research was funded in part by the Luxembourg National Research Fund (FNR) and PayPal, PEARL grant reference 13342933/Gilbert Fridgen.The research leading to these results has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under Grant Agreement No 825225–Safe Data-Enabled Economic Development (Safe-DEED).

Appendix A. Adoption factors of data marketplaces

Table A1
Key literature on factors influencing the adoption of data marketplaces (listed alphabetically).

Key empirical literature	Domain	Key perspective	Approach	Key relevant construct	Key result
Abbas et al. (2024)	B2B data marketplace	Data owners	Qualitative – Interviews	• Data sovereignty	• Data owners must feel sovereign over their data to engage with data marketplaces, with data control as a key dimension of this sovereignty.
Abraham et al. (2023)	Generic data marketplaces	Multiple perspectives	Taxonomy development	• Data governance decision domains	• To ensure adoption, data marketplace operators should consider five domains of data governance (e.g., data lifecycle).
Agahari et al. (2022)	B2B data marketplaces	Data owners	Qualitative – Interviews	• Control • Trust • Risk	• Multi-party computation increases perceived control of personal data providers, increases trust, and reduces risks.
Agahari and de Reuver (2022)	Personal data marketplaces in the automotive industry	Personal data owners	Experiment	• Perceived control enabled by multi-party computation	• Multi-party computation enables perceived control of personal data owners.
Azcoitia and Laoutaris (2022)	B2B data marketplaces	Multiple perspectives	Review of secondary (empirical) data	• N/A	• Five key challenges for data marketplace adoptions include fragmentation, pricing mechanisms, data valuation, data ownership, and data provenance.
Bauer-Hänsel et al. (2024)	B2B data marketplaces	Data owners	Design science research	• Pricing functions	• Optimizing data trading and welfare is possible using a logarithmic pricing function; this can help data owners to better value their data assets
Bergman et al. (2022)	B2B data marketplaces in the automotive industry	Multiple perspectives	Qualitative - Case studies	• Value creation	• Relying on network effects may not be fully beneficial in data marketplaces, as successful data marketplaces tend to be built on intimate relationships between data owners and buyers.
Dahlberg and Nokkala (2019)	B2B data marketplaces	Data owners and buyers	Qualitative - Interviews	• Factors that increase and decrease willingness to share data	• Control is more important than cost saving (e.g., efficiency for data sharing).
Fassnacht et al. (2023)	B2B data marketplaces	Multiple perspectives	Systematic literature review and interviews	• Strategic, operational, technological, cultural, and regulatory barriers to B2B data sharing	• Organizational data sharing is hindered by multiple factors.
Fassnacht et al. (2024)	B2B data marketplaces	Multiple perspectives	Taxonomy development	• Key dimensions of taxonomy are data, organisation, and network.	• Efficiency and financial motives are the key incentives for adopting data marketplaces.
Jahnke et al. (2024)	B2B data marketplaces	Data owners	Design science research	• Federated architectures	• Data providers feel sovereignty over their data assets.
Jussen et al. (2023)	B2B data marketplaces	Multiple perspectives	Systematic literature review and interviews	• Business models • Organisational • Data sovereignty	• Businesses want to share their data but also need to safeguard it, creating multi-faceted tensions.

(*continued on next page*)

Table A1 (*continued*)

Key empirical literature	Domain	Key perspective	Approach	Key relevant construct	Key result
Kernstock et al. (2025)	Cross-domain data ecosystems, where data marketplaces are conceptualised as an instance of such ecosystems	Data marketplace operators	Fuzzy-set Qualitative Comparative Analysis	• Technical boundary resources • Social boundary resources • Architecture centralisation • Domain specialisation • Number of developing partners	• The success or failure of data ecosystems can be attributed to various configurations.
Otto and Jarke (2019)	B2B data marketplaces	Multiple perspectives	Case studies	• (Internal) regulatory instruments	• Data sovereignty and trust are more important than pricing mechanisms as adoption factors.
Scheider et al. (2023)	Personal data marketplaces	Multiple perspectives	Taxonomy developments	• Design elements	• Personal data marketplaces share common characteristics with B2B marketplaces but have distinct design elements, such as the need for individuals' consent.
Spiekermann and Korunovska (2017)	Personal data marketplaces in social media	Personal data owners	Experiment	• Privacy concern • Data market awareness • Data control	• Awareness of data marketplaces plays a more significant role than privacy concerns. • Sellers are unlikely to share their data unless they feel a strong sense of control over it.
Stahl et al. (2017)	Generic data marketplaces	Data owners	Review of secondary (empirical) data	• N/A	• ARROW's information paradox hinders the adoption of data marketplaces
Virkar et al. (2019)	Personal and B2B data marketplaces	Personal data owners	Systematic literature review and workshops	• Privacy • Trust	• Privacy and trust are the most pressing issues for data marketplace adoption.
X. Zhang et al. (2023)	B2B data marketplaces	Data owners	Econometrics	• Firm characteristics • Data marketplace operator's analytics capability • Firms' competition intensity	• Firms possessing competitive advantages sell less data compared to those with not. • High-value firms reduce the volume of data they sell to data marketplace operators with advanced analytics capabilities, as this intensifies competition.

Appendix B. Control mechanisms in digital platforms and data marketplaces

Table B1
Control Mechanisms in digital platforms, including data marketplaces

Control mode	Control mechanisms	Description	Controller	Controllee	Digital platform types	Sources
Formal: Input	Membership gatekeeping	Established criteria for determining whether a project owner is permitted to join a platform.	Platform providers	Supply-side user: Project owners	Crowd platforms	Thies et al. (2018)
	Application complementor gatekeeping	Filtering which extensions are permitted within a web browser platform.	Platform providers	Third-party providers	Web browsers	(Croitor et al., 2021; Tiwana, 2015)
	Product gatekeeping	Filtering which products can be sold on platforms	Platform providers	Supply-side user: Sellers	E-commerce	Croitor et al. (2022)
	Certification	Submit an official government certificate to confirm the status as a recognised charitable association.	Platform providers	• Supply-side user: Campaigners • Platform users: data owners and consumers	• Crowd platforms • Data marketplaces	(Adam et al., 2023; Driessen et al., 2022)
	Screening requirements	Four criteria used for gatekeeping include financial cost, regulatory compliance requirements, technical specifications, and time investment.	Platform providers	Third-party providers	Mobile application	Croitor and Benlian (2019)
	Access fee	Imposing an access fee for third-party providers to join a platform and utilise its resources, thus filtering out low-quality complements.	Platform providers	Third-party providers	General platforms	Chen et al. (2022)
Formal: Process	Application development guidelines	A well-structured, sequential guide outlining the process of developing and launching apps on digital platforms.	Platform providers	Third-party providers	Mobile application	Goldbach et al. (2018)
	Software development kits	The required use of a specific software development environment, such as Apple's Xcode.	Platform providers	Third-party providers	Mobile application	(Goldbach et al., 2018; Staub et al., 2022)
	Social background prescription	Guide platform users on how to increase visibility by encouraging sharing behaviours	Platform providers	Platform users	Social commerce platform	Ens et al. (2023)
	Regular project updates	Requiring project owners to regularly report their progress toward achieving the goal	Demand-side users: Investors	Supply-side users: Project owners	Crowd platforms	(Gleasure et al., 2019; Wu et al., 2024)

(*continued on next page*)

Table B1 (*continued*)

Control mode	Control mechanisms	Description	Controller	Controllee	Digital platform types	Sources
	Application development interfaces	Technical bridge to allow integration between platforms and complementors	Platform providers	Third-party providers	General platforms	Staub et al. (2022)
	Rules for intellectual property rights	Define rules for third-party providers on permissible and restricted uses of platform resources.	Platform providers	Third-party providers	General platforms	Staub et al. (2022)
	Multi-party computation (MPC)	MPC ensures that data buyers can only access the computation results without viewing the raw data.	Supply-side users: Data owners	Demand-side users: Data buyers	Data marketplaces	Agahari et al. (2022)
	Usage control	Technically enforce contractual agreements of data usage	Supply-side users: Data owners	Demand-side users: Data buyers	Data marketplaces	(Abraham et al., 2023; Scheider et al., 2023)
	Smart contract	Smart contracts embed legal terms and consensus in computer-based languages.	Supply-side users: Data owners	Demand-side users: Data buyers	Data marketplaces	Moyano et al. (2021)
Formal: Output	Output metrics	Metrics for evaluating app development success include time, budget, and functionality.	Platform providers	Third-party providers	Mobile application	Goldbach et al. (2018)
	Feedback mechanisms	Supply- and demand-side users provide feedback based on their interactions on platforms (e.g., ratings)	Platform users	Platform users	General platforms	Steur and Seiter (2021)
Informal: Self-control	Independence	The platform provider allows third-party providers to set their own goals, establish procedures, and follow their own processes to achieve them.	Platform providers	Third-party providers	Mobile application	Goldbach et al. (2018)
	Discretion behaviour	Project owners can critically evaluate investor suggestions and apply them at their discretion.	Platform user: Investors	Platform user: Project owners	Crowd platforms	Gleasure et al. (2019)
Informal: Clan-control	Seller community	A community where shared beliefs, norms, and values among sellers are established.	Platform providers	Supply-side user: Sellers	E-commerce	Croitor et al. (2022)
	Seller community	Forming norms to translate and refine platform providers' guidelines with added nuances and details.	Supply-side user: Sellers	Demand-side user: Sellers	Social commerce platform	Ens et al. (2023)

Note: Italic indicates technology-based control (or algorithmic control)

Appendix C. Robustness check of sampling

In our sample, only 3 % of participants identified as researchers. We assume that these individuals are primarily affiliated with R&D departments within manufacturing firms and thus likely involved in technology strategy and data-related initiatives. Given the novelty of smart contracts and data marketplaces, we considered it likely that such profiles would have relevant insights and influence on decisions about inter-organisational data sharing.

Nonetheless, we verified that excluding these cases does not significantly affect our findings. Re-running the analysis on the sample without the nine researchers leads to marginal differences in the regression weights, as seen in the table below.

Table C1
Robustness check of sampling

Path	Full sample (N = 399)	Sample without researchers (N = 390)
Perceived control → Trust in data buyers	.771	.777
Perceived control → Perceived risk	−.578	−.573
Perceived control → Willingness to share data	.486	.493
Trust in data buyers → Perceived risk	n.s.	n.s.
Trust in data buyers → Willingness to share data	.141	.138
Perceived risk → Willingness to share data	−.270	−.267

Appendix D. Survey design

Fig. C.1 illustrates the survey design, outlining the scenario used to measure our constructs.

Fig. C.1. Survey design.

Demographic information

After the opening statement is read and agreed to, the respondents are asked for some personal information. These serve to describe the demographic, and it will not be possible to identify a person based on this information.

- **Country of residence**
  - ❑ UK
  - ❑ USA
  - ❑ EU
- **Industry role**
  - ❑ Upper management
  - ❑ Middle management
  - ❑ Junior management
  - ❑ Consultant
  - ❑ Researcher
  - ❑ Other
- **Years of experience**
  - ❑ <1
  - ❑ 1–2
  - ❑ 3–5
  - ❑ 6–10
  - ❑ 10+
- **Familiarity with IoT**
  - ❑ Not familiar at all
  - ❑ Slightly familiar
  - ❑ Moderately familiar
  - ❑ Very familiar
  - ❑ Extremely familiar
- **Familiarity with data marketplaces**
  - ❑ Not familiar at all
  - ❑ Slightly familiar
  - ❑ Moderately familiar
  - ❑ Very familiar
  - ❑ Extremely familiar
- **Sector**
  - ❑ Blank
  - ❑ Other
  - ❑ Manufacturing/B2B
  - ❑ Food
  - ❑ Medical
  - ❑ Consumers/Retail
  - ❑ Automotive

Marketplace description

Imagine the company you work for has spent the past 5–10 years investing into smart manufacturing systems. All the applicable machines have sensors that collect data and all the steps in the manufacturing process get tracked and stored. You've also spent a lot of effort in organizing the data, so the systems are interoperable and you can access everything easily. In this hypothetical scenario you can simply log into a server and see the real time status of all your machines and active manufacturing processes, as well as all historical data. Any data you can think of that can be useful to track in a manufacturing process is available. This data might be sensitive. It could give away an advantage to a competitor or contain personal information.

This data may be very valuable to you, but it can also create value for other (unrelated) companies. For example a company that uses a similar machine to create different products might be interested in seeing how you optimized it's processes. Or a company that's proficient in the use of data analytics can use your data to make their business processes more efficient. Because of this value, you could sell your data. This is what a data marketplace is for.

A data marketplace connects buyers (consumers) and sellers (providers). We are interested in what risks you perceive when sharing data in a marketplace and how data marketplaces could be designed so you trust the other party. Pricing might be important, but is not part of this questionnaire. You can assume that you will receive a fair price for your shared data. This means enough to cover any expenses that you need to make to share the data and some profit. Enough to consider sharing the data you're already producing. You can also assume that your company is ready to share the data. All systems are compatible and it takes little to no effort to train personnel to use the marketplace. It's really almost as simple as clicking a "Share data" button.

Architecture description

Before showing how you can share data, we think it's important to get to know the owner of the marketplace and how the marketplace is structured. The party that's facilitating all the data exchange is a new scale-up company. The company is independent from big tech and other companies and is purely interested in facilitating data exchange, making revenue with every transaction on the marketplace. This facilitating company has various geographically distributed locations to reach companies in many areas.

The facilitating company makes sure every transaction between the users gets stored on a blockchain. You can view this as a long list of transactions where every new transaction gets added to the top of the list. Every new addition to the list gets verified through a large network of computers. Once a facilitator has sent the transaction and it's been verified, it's permanently stored on the blockchain. There is no way to hack or change transactions stored on the blockchain.

To ensure no privacy sensitive data is traded regulators have access to this blockchain. These are government bodies in various countries. They audit and monitor if the facilitators are complying to local privacy laws.Fig. C.2

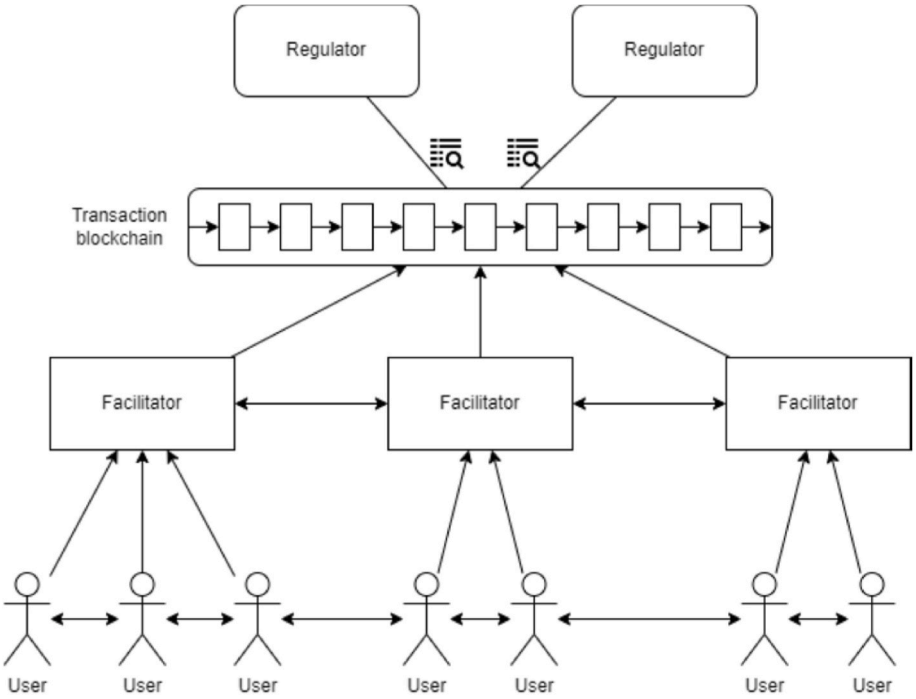

Fig. C.2. Data marketplace architecture. Image and description are adopted and simplified from Gupta et al. (2021).

Data sharing scenario

In this data marketplace users need to go through a verification process. The process verifies the identity of the users and the company they work for. On this marketplace you can be fairly sure that you know who you're selling the data to. The marketplace will allow you to select which data you'd like to share. You will also write down some terms of use, where you state for example for what purpose the data may be used, along with a suggested price. If someone wants to access your data they will have to send a request. In this request they have to state what data they want access to, what they intent to use your data for and what price they are willing to pay. You can negotiate these terms with the potential buyer until you reach an agreement. Once you both agree on the data being sold, the terms of use and the price, a smart contract will be created. This is a self-executing contract. It can for example grant access to your data for a set amount of time or allow for automatic payment every time the user accesses the data.

Key questions

- **How sensitive do you consider the datasets you have left to be?** *(Likert 1–7)*
  - ❑ Not sensitive (1) – Very sensitive (7)
- **Let's say you share your data on this marketplace, how do you feel about this data?** *(Likert 1–7)*
  - ❑ I believe I have control over who can get access to my data
  - ❑ I think I have control over what data is released by the marketplace
  - ❑ I believe I have control over how data is used by the other users
  - ❑ I believe I can control my data after providing it to the marketplace
- **What is your opinion on the potential buyers in this marketplace?** *(Likert 1–7)*
  - ❑ I expect that data buyers would be trustworthy in handling the data they got from this data marketplace
  - ❑ I expect that data buyers would tell the truth and fulfil promises in handling the data they got from this data marketplace
  - ❑ I expect that data buyers would be honest when handling the data they got from this data marketplace.
- **Let's say you share your data on this marketplace, how do you feel about this data?** *(Likert 1–7)*
  - ❑ It would be risky to share this data in the marketplace
  - ❑ There would be a high potential of giving away personal information
  - ❑ There would be a high potential of giving away a competitive advantage
  - ❑ The data could be inappropriately used
  - ❑ Sharing this data could involve many unexpected problems
- **When answering the following questions, you can assume the previously mentioned preconditions are still the same. You have data ready to share, you'll receive a fair price, and you can remove sensitive parts of the data.** *(Likert 1–7)*
  - ❑ Given the chance, I would share my data via this data marketplace.
  - ❑ Given the chance, I predict that I should share my data via this data marketplace in the future.
  - ❑ It is likely that I will share my data via this data marketplace in the near future.

Data availability

Data will be made available on request.

References

Aaltonen, A., Alaimo, C., Kallinikos, J., 2021. The making of data commodities: data analytics as an embedded process. J. Manag. Inf. Syst. 38 (2), 401–429. https://doi.org/10.1080/07421222.2021.1912928.

Abbas, A.E., Agahari, W., van de Ven, M., Zuiderwijk, A., de Reuver, M., 2021. Business data sharing through data marketplaces: a systematic literature review. Journal of Theoretical and Applied Electronic Commerce Research 16 (7), 3321–3339. https://doi.org/10.3390/jtaer16070180.

Abbas, A.E., van Velzen, T., Ofe, H., van de Kaa, G., Zuiderwijk, A., de Reuver, M., 2024. Beyond control over data: conceptualizing data sovereignty from a social contract perspective. Electron. Mark. 34 (20), 1–21. https://doi.org/10.1007/s12525-024-00695-2.

Abraham, R., Schneider, J., vom Brocke, J., 2023. A taxonomy of data governance decision domains in data marketplaces. Electron. Mark. 33 (1), 1–13. https://doi.org/10.1007/s12525-023-00631-w.

Adam, M., Croitor, E., Werner, D., Benlian, A., Wiener, M., 2023. Input control and its signalling effects for complementors' intention to join digital platforms. Inf. Syst. J. 33 (3), 437–466. https://doi.org/10.1111/isj.12408.

Agahari, W., de Reuver, M., 2022. Rethinking consumers' data sharing decisions with the emergence of multi-party computation: an experimental design for evaluation. In: The 30th European Conference on Information Systems, Timişoara, Romania.

Agahari, W., Ofe, H., de Reuver, M., 2022. It is not (only) about privacy: how multi-party computation redefines control, trust, and risk in data sharing. Electron. Mark. 32 (3), 1577–1602. https://doi.org/10.1007/s12525-022-00572-w.

Agahari, W., Dirksen, A., Johns, M., Reuver, M.d., Fiebig, T., 2025. The importance of being earnest: shedding light on johnny's (false) sense of privacy. In: 2025 IEEE Symposium on Security and Privacy (SP), San Francisco, California, the United States.

Agarwal, A., Dahleh, M., Sarkar, T., 2019. A marketplace for data: an algorithmic solution. In: Proceedings of the 2019 ACM Conference on Economics and Computation, Phoenix, Arizona, the United States.

Ajzen, I., 1991. The theory of planned behavior. Organ. Behav. Hum. Decis. Process. 50 (2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T.

Álvarez, I.A., Ehaus, M., Frank, M.-L., Sedlmeir, J., 2024. Privacy-enhancing technologies. In: Fridgen, G., Guggenberger, T., Sedlmeir, J., Urbach, N. (Eds.), Decentralization Technologies: Financial Sector in Change. Springer, Nature Switzerland, pp. 97–119. https://doi.org/10.1007/978-3-031-66047-4_6.

Ananthakrishnan, U., Proserpio, D., Sharma, S., 2023. I hear you: does quality improve with customer voice? Mark. Sci. 42 (6), 1143–1161. https://doi.org/10.1287/mksc.2023.1437.

Asare, A.K., Brashear-Alejandro, T.G., Kang, J., 2016. B2B technology adoption in customer driven supply chains. J. Bus. Ind. Market. 31 (1), 1–12. https://doi.org/10.1108/JBIM-02-2015-0022.

Azcoitia, S.A., Laoutaris, N., 2022. A survey of data marketplaces and their business models. SIGMOD Record 51 (3), 18–29. https://doi.org/10.1145/3572751.3572755.

Azcoitia, S.A., Iordanou, C., Laoutaris, N., 2022. Measuring the price of data in commercial data marketplaces. In: Proceedings of the 1st International Workshop on Data Economy, Rome, Italy.

Azcoitia, S.A., Iordanou, C., Laoutaris, N., 2023. Understanding the price of data in commercial data marketplaces. In: 2023 IEEE 39th International Conference on Data Engineering (ICDE), Anaheim, California, the United States.

Ba, S., Paul, A.P., 2002. Evidence of the effect of trust building technology in electronic markets: price premiums and buyer behavior. MIS Q. 26 (3), 243–268. https://doi.org/10.2307/4132332.

Bastiaansen, H., Dalmolen, S., Kollenstart, M., Punter, M., 2019. Infrastructural sovereignty over agreement and transaction data ('Metadata') in an open network-model for multilateral sharing of sensitive data. In: ICIS 2019 Proceedings, Munich, Germany.

Bauer-Hänsel, I., Liu, Q., Tessone, C.J., Schwabe, G., 2024. Designing a blockchain-based data market and pricing data to optimize data trading and welfare. Int. J. Electron. Commer. 28 (1), 3–30. https://doi.org/10.1080/10864415.2023.2295068.

Beese, J., Haki, K., Schilling, R., Kraus, M., Aier, S., Winter, R., 2023. Strategic alignment of enterprise architecture management – how portfolios of control mechanisms track a decade of enterprise transformation at commerzbank. Eur. J. Inf. Syst. 32 (1), 92–105. https://doi.org/10.1080/0960085X.2022.2085200.

Ben-Daya, M., Hassini, E., Bahroun, Z., 2019. Internet of things and supply chain management: a literature review. Int. J. Prod. Res. 57 (15–16), 4719–4742. https://doi.org/10.1080/00207543.2017.1402140.

Bergman, R., Abbas, A.E., Jung, S., Werker, C., de Reuver, M., 2022. Business model archetypes for data marketplaces in the automotive industry. Electron. Mark. 32 (2), 747–765. https://doi.org/10.1007/s12525-022-00547-x.

Bernal, J., 2024. Private sector trust in data sharing: enablers in the european union. Data & Policy 6, e30. https://doi.org/10.1017/dap.2024.20. Article e30.

Bhatia, J., Breaux, T.D., Friedberg, L., Hibshi, H., Smullen, D., 2016a. Privacy risk in cybersecurity data sharing. In: Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security, Vienna, Austria. https://doi.org/10.1145/2994539.2994541.

Bhatia, J., Breaux, T.D., Reidenberg, J.R., Norton, T.B., 2016b. A theory of vagueness and privacy risk perception. In: 2016 IEEE 24th International Requirements Engineering Conference (RE), Beijing, China.

Bogetoft, P., Christensen, D.L., Damgård, I., Geisler, M., Jakobsen, T., Krøigaard, M., Nielsen, J.D., Nielsen, J.B., Nielsen, K., Pagter, J., Schwartzbach, M., Toft, T., 2009. Secure multiparty computation goes live. Financial Cryptography and Data Security. Berlin, Heidelberg.

Bonnet, S., Teuteberg, F., 2023. Impact of blockchain and distributed ledger technology for the management, protection, enforcement and monetization of intellectual property: a systematic literature review. Inf. Syst. E Bus. Manag. 21 (2), 229–275. https://doi.org/10.1007/s10257-022-00579-y.

Bottoni, P., Gessa, N., Massa, G., Pareschi, R., Selim, H., Arcuri, E., 2020. Intelligent smart contracts for innovative supply chain management. Frontiers in Blockchain 3. https://doi.org/10.3389/fbloc.2020.535787 [Original Research].

Cabral, L., Hortaçsu, A., 2010. The dynamics of seller reputation: evidence from eBay. J. Ind. Econ. 58 (1), 54–78. https://doi.org/10.1111/j.1467-6451.2010.00405.x.

Cai, X., Cebollada, J., Cortiñas, M., 2023. Impact of Seller- and buyer-created content on product sales in the electronic commerce platform: the role of informativeness, readability, multimedia richness, and extreme valence. J. Retailing Consum. Serv. 70, 1–15. https://doi.org/10.1016/j.jretconser.2022.103141.

Cennamo, C., Santaló, J., 2019. Generativity tension and value creation in platform ecosystems. Organ. Sci. 30 (3), 617–641. https://doi.org/10.1287/orsc.2018.1270.

Chang, S.E., Chen, Y.-C., Lu, M.-F., 2019. Supply chain Re-Engineering using blockchain technology: a case of smart contract based tracking process. Technol. Forecast. Soc. Change 144, 1–11. https://doi.org/10.1016/j.techfore.2019.03.015.

Chang, Y.-Y., Lin, S.-C., Yen, D.C., Hung, J.-W., 2020. The trust model of enterprise purchasing for B2B e-marketplaces. Comput. Stand. Interfac. 70, 103422. https://doi.org/10.1016/j.csi.2020.103422.

Chen, Y.-H., Lin, T.-P., Yen, D.C., 2014. How to facilitate inter-organizational knowledge sharing: the impact of trust. Inf. Manag. 51 (5), 568–578. https://doi.org/10.1016/j.im.2014.03.007.

Chen, Y., Richter, J.I., Patel, P.C., 2021. Decentralized governance of digital platforms. Journal of management 47 (5), 1305–1337. https://doi.org/10.1177/0149206320916755.

Chen, L., Tong, T.W., Tang, S., Han, N., 2022. Governance and design of digital platforms: a review and future research directions on a meta-organization. Journal of management 48 (1), 147–184. https://doi.org/10.1177/01492063211045023.

Cheng, J.-H., Chen, S.-W., Chen, F.-Y., 2013. Exploring how inter-organizational relational benefits affect information sharing in supply chains. Inf. Technol. Manag. 14 (4), 283–294. https://doi.org/10.1007/s10799-013-0165-x.

Chiquito, E., Chiquito, A., Bodin, U., Synnes, K., 2022. Automated usage control for secure data sharing based on Ricardian contracts. In: IECON 2022 – 48th Annual Conference of the IEEE Industrial Electronics Society, Brussels, Belgium.

Christidis, J., Karkazis, P.A., Papadopoulos, P., Leligou, H.C., 2022. Decentralized blockchain-based IoT data marketplaces. J. Sens. Actuator Netw. 11 (3), 39. https://www.mdpi.com/2224-2708/11/3/39.

Cichy, P., Salge, T.O., Kohli, R., 2021. Privacy concerns and data sharing in the internet of things: mixed methods evidence from connected cars. MIS Q. 45 (4), 1863–1892. https://doi.org/10.25300/MISQ/2021/14165.

Collier, Z.A., Guin, U., Sarkis, J., Lambert, J.H., 2022. Decision model with quantification of buyer-supplier trust in advanced technology enterprises. Benchmark Int. J. 29 (10), 3033–3056. https://doi.org/10.1108/BIJ-06-2021-0336.

Cram, W.A., Brohman, K., Gallupe, R.B., 2016. Information systems control: a review and framework for emerging information systems processes. J. Assoc. Inf. Syst. Online 17 (4), 216–266. https://doi.org/10.17705/1jais.00427.

Cram, W.A., Wiener, M., Tarafdar, M., Benlian, A., 2022. Examining the impact of algorithmic control on uber drivers' technostress. J. Manag. Inf. Syst. 39 (2), 426–453. https://doi.org/10.1080/07421222.2022.2063556.

Croitor, E., Benlian, A., 2019. Perceived input control on online platforms from the application developer perspective: conceptualisation and scale development. J. Decis. Syst. 28 (1), 19–40. https://doi.org/10.1080/12460125.2019.1616977.

Croitor, E., Adam, M., Benlian, A., 2021. Perceived input control on digital platforms: a mixed-methods investigation of web-browser platforms. J. Decis. Syst. 30 (1), 50–71. https://doi.org/10.1080/12460125.2020.1815440.

Croitor, E., Werner, D., Adam, M., Benlian, A., 2022. Opposing effects of input control and clan control for sellers on e-marketplace platforms. Electron. Mark. 32 (1), 201–216. https://doi.org/10.1007/s12525-021-00465-4.

Curchod, C., Patriotta, G., Cohen, L., Neysen, N., 2020. Working for an algorithm: power asymmetries and agency in online work settings. Adm. Sci. Q. 65 (3), 644–676. https://doi.org/10.1177/0001839219867024.

Dahlberg, T., Nokkala, T., 2019. Willingness to share supply chain data in an ecosystem governed Platform–An interview study. In: BLED 2019 Proceedings. Bled, Slovenia.

De Giovanni, P., 2020. Blockchain and smart contracts in supply chain management: a game theoretic model. Int. J. Prod. Econ. 228, 1–18. https://doi.org/10.1016/j.ijpe.2020.107855.

de Prieëlle, F., de Reuver, M., Rezaei, J., 2022. The role of ecosystem data governance in adoption of data platforms by internet-of-things data providers: case of Dutch horticulture industry. IEEE Trans. Eng. Manag. 69 (4), 940–950. https://doi.org/10.1109/TEM.2020.2966024.

den Hartigh, E., Stolwijk, C.C.M., Ortt, J.R., Punter, L.M., 2023. Configurations of digital platforms for manufacturing: an analysis of seven cases according to platform functions and types. Electron. Mark. 33 (1), 1–17. https://doi.org/10.1007/s12525-023-00653-4.

Doney, P.M., Cannon, J.P., 1997. An examination of the nature of trust in buyer–seller relationships. J. Market. 61 (2), 35–51. https://doi.org/10.1177/002224299706100203.

Drakopoulos, K., Makhdoumi, A., 2023. Providing data samples for free. Manag. Sci. 69 (6), 3536–3560. https://doi.org/10.1287/mnsc.2022.4534.

Driessen, S.W., Monsieur, G., Van Den Heuvel, W., 2022. Data market design: a systematic literature review. IEEE Access 10, 33123–33153. https://doi.org/10.1109/access.2022.3161478.

Eichler, R., Gröger, C., Hoos, E., Schwarz, H., Mitschang, B., 2022a. Data shopping — how an enterprise data marketplace supports data democratization in companies. In: De Weerdt, J., Polyvyanyy, A. (Eds.), Intelligent Information Systems. Springer International Publishing, pp. 19–26.

Eichler, R., Gröger, C., Hoos, E., Schwarz, H., Mitschang, B., 2022b. From data asset to data product – the role of the data provider in the enterprise data marketplace. In: Barzen, J., Leymann, F., Dustdar, S. (Eds.), Service-Oriented Computing. Springer International Publishing, pp. 119–138.

Ens, N., Hukal, P., Blegind Jensen, T., 2023. Dynamics of control on digital platforms. Inf. Syst. J. 33 (4), 890–911. https://doi.org/10.1111/isj.12429.

Eurich, M., Oertel, N., Boutellier, R., 2010. The impact of perceived privacy risks on organizations' willingness to share item-level event data across the supply chain. Electron. Commer. Res. 10 (3), 423–440. https://doi.org/10.1007/s10660-010-9062-0.

Fan, S., Ilk, N., Kumar, A., Xu, R., Zhao, J.L., 2024. Blockchain as a trust machine: from disillusionment to enlightenment in the era of generative AI. Decis. Support Syst. 182, 1–8. https://doi.org/10.1016/j.dss.2024.114251.

Fassnacht, M., Benz, C., Heinz, D., Leimstoll, J., Satzger, G., 2023. Barriers to data sharing among private sector organizations. In: Proceedings of the 56rd Hawaii International Conference on Systems Sciences. the United States, Honolulu, Hawaii.

Fassnacht, M., Leimstoll, J., Benz, C., Heinz, D., Satzger, G., 2024. Data sharing practices: the interplay of data, organizational structures, and network dynamics. Electron. Mark. 34 (1). https://doi.org/10.1007/s12525-024-00732-0.

Ferraro, C., Wheeler, M.A., Pallant, J.I., Wilson, S.G., Oldmeadow, J., 2023. Not So trustless after all: trust in WEB3 technology and opportunities for brands. Bus. Horiz. 66 (5), 667–678. https://doi.org/10.1016/j.bushor.2023.01.007.

Firdausy, D.R., De Alencar Silva, P., Van Sinderen, M., Iacob, M.-E., 2022. *Towards a reference enterprise architecture to enforce digital sovereignty in international data spaces* 2022. In: IEEE 24th Conference on Business Informatics (CBI), Amsterdam, Netherlands.

Fradkin, A., Holtz, D., 2023. Do incentives to review help the market? Evidence from a field experiment on airbnb. Mark. Sci. 42 (5), 853–865. https://doi.org/10.1287/mksc.2023.1439.

Fruhwirth, M., Rachinger, M., Prlja, E., 2020. Discovering business models of data marketplaces. In: Proceedings of the 53rd Hawaii International Conference on System Sciences. the United States, Honolulu, Hawaii.

Fu, H.-P., Chang, T.-H., Ku, C.-Y., Chang, T.-S., Huang, C.-H., 2014. The critical success factors affecting the adoption of inter-organization systems by smes. J. Bus. Ind. Market. 29 (5), 400–416. https://doi.org/10.1108/JBIM-04-2012-0070.

Genés-Durán, R., Esparza, O., Hernández-Serrano, J., Román-García, F., Soriano, M., Zappa, A., Serrano, M., Stahnke, S., Böhm, B., Fries, E., Koniakou, V., Michel, B., Muñoz-Tapia, J.L., 2022. Data marketplaces with a free sampling service. In: 2022 IEEE International Conference on Services Computing (SCC).

Gleasure, R., Conboy, K., Morgan, L., 2019. Talking up a storm: how backers use public discourse to exert control in crowdfunded systems development projects. Inf. Syst. Res. 30 (2), 447–465. https://doi.org/10.1287/isre.2019.0840.

Goldbach, T., Benlian, A., Buxmann, P., 2018. Differential effects of formal and self-control in Mobile platform ecosystems: multi-method findings on third-party developers' continuance intentions and application quality. Inf. Manag. 55 (3), 271–284. https://doi.org/10.1016/j.im.2017.07.003.

Governatori, G., Idelberger, F., Milosevic, Z., Riveret, R., Sartor, G., Xu, X., 2018. On legal contracts, imperative and declarative smart contracts, and blockchain systems. Artif. Intell. Law 26, 377–409. https://doi.org/10.1007/s10506-018-9223-3.

Goyal, S., Hardgrave, B.C., Aloysius, J.A., DeHoratius, N., 2016. The effectiveness of RFID in backroom and sales floor inventory management. Int. J. Logist. Manag. 27 (3), 795–815. https://doi.org/10.1108/IJLM-03-2015-0051.

Grida, M., Mostafa, N.A., 2023. Are smart contracts too smart for supply chain 4.0? A blockchain framework to mitigate challenges. J. Manuf. Technol. Manag. 34 (4), 644–665. https://doi.org/10.1108/JMTM-09-2021-0359.

Groschopf, W., Dobrovnik, M., Herneth, C., 2021. Smart Contracts for Sustainable Supply Chain Management: Conceptual Frameworks for Supply Chain Maturity Evaluation and Smart Contract Sustainability Assessment [Hypothesis and Theory]. Frontiers in Blockchain 4, 1–22. https://doi.org/10.3389/fbloc.2021.506436.

Gupta, P., Dedeoglu, V., Kanhere, S.S., Jurdak, R., 2021. Towards a blockchain powered iot data marketplace. In: 2021 International Conference on Communication Systems & Networks (COMSNETS), Bangalore, India.

Hamledari, H., Fischer, M., 2021. Measuring the impact of blockchain and smart contracts on construction supply chain visibility. Adv. Eng. Inform. 50, 1–14. https://doi.org/10.1016/j.aei.2021.101444.

Hart, P., Saunders, C., 1997. Power and trust: critical factors in the adoption and use of electronic data interchange. Organ. Sci. 8 (1), 23–42. https://doi.org/10.1287/orsc.8.1.23.

Hawlitschek, F., Notheisen, B., Teubner, T., 2018. The limits of trust-free systems: a literature review on blockchain technology and trust in the sharing economy. Electron. Commer. Res. Appl. 29, 50–63. https://doi.org/10.1016/j.elerap.2018.03.005.

Henseler, J., Ringle, C.M., Sarstedt, M., 2015. A new criterion for assessing discriminant validity in variance-based structural equation modeling. J. Acad. Market. Sci. 43 (1), 115–135. https://doi.org/10.1007/s11747-014-0403-8.

Hsieh, Y.-Y., Vergne, J.-P., 2023. The future of the web? The coordination and early-stage growth of decentralized platforms. Strateg. Manag. J. 44 (3), 829–857. https://doi.org/10.1002/smj.3455.

Huang, L., Dou, Y., Liu, Y., Wang, J., Chen, G., Zhang, X., Wang, R., 2021. Toward a research framework to conceptualize data as a factor of production: the data marketplace perspective. Fundamental Research 1 (5), 586–594. https://doi.org/10.1016/j.fmre.2021.08.006.

Huang, H., Sunar, N., Swaminathan, J.M., Roy, R., 2023. Do noisy customer reviews discourage platform sellers? Empirical analysis of an online solar marketplace. Manuf. Serv. Oper. Manag. 25 (6), 2195–2215. https://doi.org/10.1287/msom.2021.0104.

Huber, M., Wessel, S., Brost, G., Menz, N., 2022. Building trust in data spaces. In: Otto, B., ten Hompel, M., Wrobel, S. (Eds.), Designing Data Spaces : the Ecosystem Approach to Competitive Advantage. Springer International Publishing, pp. 147–164. https://doi.org/10.1007/978-3-030-93975-5_9.

Iyengar, G., Saleh, F., Sethuraman, J., Wang, W., 2023. Economics of permissioned blockchain adoption. Manag. Sci. 69 (6), 3415–3436. https://doi.org/10.1287/mnsc.2022.4532.

Jagals, M., Karger, E., Ahlemann, F., Brée, T., 2021. Enhancing inter-organizational data governance via blockchain-shaping scopes and research avenues. In: Forty-Second International Conference on Information Systems, Austin, Texas, the United States.

Jahnke, N., Jussen, I., Schoormann, T., Möller, F., 2024. Designing federated data marketplaces in industrial production: findings from a prototypical implementation. Wirtschaftsinformatik 2024 Proceedings. Würzburg, Germany.

Jaworski, B.J., 1988. Toward a theory of marketing control: environmental context, control types, and consequences. J. Market. 52 (3), 23–39. https://doi.org/10.1177/002224298805200303.

Jussen, I., Schweihoff, J., Möller, F., 2023. Tensions in inter-organizational data sharing: findings from literature and practice. In: 2023 IEEE 25th Conference on Business Informatics (CBI), Prague, Czech Republic.

Kaiser, C., Stocker, A., Viscusi, G., Fellmann, M., Richter, A., 2021. Conceptualising value creation in data-driven services: the case of vehicle data. Int. J. Inf. Manag. 59, 1–15. https://doi.org/10.1016/j.ijinfomgt.2021.102335.

Karger, E., Jagals, M., Ahlemann, F., 2021. Blockchain for AI data–state of the art and open research. In: Forty-Second International Conference on Information Systems, Texas, Texas, the United States.

Kehr, F., Kowatsch, T., Wentzel, D., Fleisch, E., 2015. Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. Inf. Syst. J. 25 (6), 607–635. https://doi.org/10.1111/isj.12062.

Kembro, J., Näslund, D., Olhager, J., 2017. Information sharing across multiple supply chain tiers: a Delphi study on antecedents. Int. J. Prod. Econ. 193, 77–86. https://doi.org/10.1016/j.ijpe.2017.06.032.

Kernstock, P., Altenkamp, P., Böttcher, T., Hein, A., Krcmar, H., 2025. A configurational approach to understanding data ecosystems. In: Proceedings of the 58th Hawaii International Conference on System Sciences, Waikoloa Village, Hawaii, the United States.

Kirsch, L.S., 1997. Portfolios of control modes and IS project management. Inf. Syst. Res. 8 (3), 215–239. https://doi.org/10.1287/isre.8.3.215.

Koutroumpis, P., Leiponen, A., Thomas, L.D.W., 2020. Markets for data. Ind. Corp. Change 29 (3), 645–660. https://doi.org/10.1093/icc/dtaa002.

Koutsos, V., Papadopoulos, D., Chatzopoulos, D., Tarkoma, S., Hui, P., 2022. Agora: a privacy-aware data marketplace. IEEE Trans. Dependable Secure Comput. 19 (6), 3728–3740. https://doi.org/10.1109/TDSC.2021.3105099.

Kuan, K.K.Y., Chau, P.Y.K., 2001. A perception-based model for EDI adoption in small businesses using a technology–organization–environment framework. Inf. Manag. 38 (8), 507–521. https://doi.org/10.1016/S0378-7206(01)00073-8.

Kumar, A., Liu, R., Shan, Z., 2020. Is blockchain a silver bullet for supply chain management? Technical challenges and research opportunities. Decis. Sci. J. 51 (1), 8–37. https://doi.org/10.1111/deci.12396.

Kwon, I.W.G., Suh, T., 2005. Trust, commitment and relationships in supply chain management: a path analysis. Supply Chain Manag.: Int. J. 10 (1), 26–33. https://doi.org/10.1108/13598540510578351.

Lapets, A., Jansen, F., Albab, K.D., Issa, R., Qin, L., Varia, M., Bestavros, A., 2018. Accessible privacy-preserving web-based data analysis for assessing and addressing economic inequalities. In: Proceedings of the 1st ACM SIGCAS Conference on Computing and Sustainable Societies. the United States, Menlo Park and San Jose, California.

Li, M., Li, H., Fang, Y., Wang, Y., Ming, Q., 2019. Pricing-oriented web technologies and product returns in the E-marketplace: the moderating role of seller reputation. In: 2019 International Conference on Information Systems, Munich, Germany.

Li, L., Tadelis, S., Zhou, X., 2020. Buying reputation as a signal of quality: evidence from an online marketplace. Rand J. Econ. 51 (4), 965–988. https://doi.org/10.1111/1756-2171.12346.

Li, T., Ren, W., Xiang, Y., Zheng, X., Zhu, T., Choo, K.-K.R., Srivastava, G., 2021. FAPS: a fair, autonomous and privacy-preserving scheme for big data exchange based on oblivious transfer, ether cheque and smart contracts. Inf. Sci. 544, 469–484. https://doi.org/10.1016/j.ins.2020.08.116.

Lou, P., Liu, Q., Zhou, Z., Wang, H., 2011. Agile supply chain management over the internet of things. In: 2011 International Conference on Management and Service Science, Wuhan, China.

Lumineau, F., Schilke, O., Wang, W., 2023. Organizational trust in the age of the fourth industrial revolution: shifts in the form, production, and targets of trust. J. Manag. Inq. 32 (1), 21–34. https://doi.org/10.1177/10564926221127852.

Mao, W., Zheng, Z., Wu, F., 2019. Pricing for revenue maximization in IoT data markets: an information design perspective. In: IEEE INFOCOM 2019 - IEEE Conference on Computer Communications, Paris, France.

Martens, B., Mueller-Langer, F., 2020. Access to digital car data and competition in aftermarket maintenance services. J. Compet. Law Econ. 16 (1), 116–141. https://doi.org/10.1093/joclec/nhaa005.
Martin, D., Heinz, D., Glauner, M., Kühl, N., 2025. Selecting data assets in data marketplaces. Business & Information Systems Engineering. https://doi.org/10.1007/s12599-025-00940-8.
Mayer, R.C., Davis, J.H., Schoorman, F.D., 1995. An integrative model of organizational trust. Acad. Manag. Rev. 20 (3), 709–734. https://doi.org/10.2307/258792.
Mišura, K., Žagar, M., 2016. Data marketplace for internet of things. In: 2016 International Conference on Smart Systems and Technologies (SST), Osijek, Croatia.
Möller, F., Jussen, I., Springer, V., Gieß, A., Schweihoff, J.C., Gelhaar, J., Guggenberger, T., Otto, B., 2024. Industrial data ecosystems and data spaces. Electron. Mark. 34 (1), 41. https://doi.org/10.1007/s12525-024-00724-0.
Mosterd, L., Sobota, V.C.M., Van De Kaa, G., Ding, A.Y., De Reuver, M., 2021. Context dependent trade-offs around platform-to-platform openness: the case of the internet of things. Technovation 108 (1), 1–15. https://doi.org/10.1016/j.technovation.2021.102331.
Moyano, J.P., Avital, M., Bühler, M., Schmedders, K., 2021. Fostering peer-to-peer blockchain-based data markets. In: The 25th Pacific Asia Conference on Information Systems, Dubai, the United Arab Emirates.
Mukhopadhyay, S., De Reuver, M., Bouwman, H., 2016. Effectiveness of control mechanisms in Mobile platform ecosystem. Telematics Inf. 33 (3), 848–859. https://doi.org/10.1016/j.tele.2015.12.008.
Müller, M., Gaudig, S., 2011. An empirical investigation of antecedents to information exchange in supply chains. Int. J. Prod. Res. 49 (6), 1531–1555. https://doi.org/10.1080/00207540903567317.
Müller, J.M., Buliga, O., Voigt, K.-I., 2018. Fortune favors the prepared: how smes approach business model innovations in industry 4.0. Technol. Forecast. Soc. Change 132, 2–17. https://doi.org/10.1016/j.techfore.2017.12.019.
Müller, J.M., Veile, J.W., Voigt, K.-I., 2020. Prerequisites and incentives for digital information sharing in industry 4.0 – an international comparison across data types. Comput. Ind. Eng. 148, 1–14. https://doi.org/10.1016/j.cie.2020.106733.
Nagorny, K., Scholze, S., Ruhl, M., Colombo, A.W., 2018. Semantical support for a CPD data marketplace to prepare big data analytics in smart manufacturing environments. In: 2018 IEEE Industrial Cyber-Physical Systems (ICPS), St. Petersburg, Russia.
Nicolaou, A.I., McKnight, D.H., 2006. Perceived information quality in data exchanges: effects on risk, trust, and intention to use. Inf. Syst. Res. 17 (4), 332–351. https://doi.org/10.1287/isre.1060.0103.
Nicolaou, A.I., Ibrahim, M., van Heck, E., 2013. Information quality, trust, and risk perceptions in electronic data exchanges. Decis. Support Syst. 54 (2), 986–996. https://doi.org/10.1016/j.dss.2012.10.024.
Ofe, H., de Reuver, M., 2024. Rethinking openness in data platforms: the impact of data artifact characteristics on platform openness. Business & Information Systems Engineering. https://doi.org/10.1007/s12599-024-00887-2.
Ondrus, J., Gannamaneni, A., Lyytinen, K., 2015. The impact of openness on the market potential of multi-sided platforms: a case study of Mobile payment platforms. J. Inf. Technol. 30 (3), 260–275. https://doi.org/10.1057/jit.2015.7.
Opriel, S., Skubowius, E., Lamberjohann, M., 2021. How usage control fosters willingness to share sensitive data in inter-organizational processes of supply chain. In: International Scientific Symposium on Logistics 2021, Bremen, Germany.
Otto, B., Jarke, M., 2019. Designing a multi-sided data platform: findings from the international data spaces case. Electron. Mark. 29 (4), 561–580. https://doi.org/10.1007/s12525-019-00362-x.
Ouchi, W.G., 1979. A conceptual framework for the design of organizational control mechanisms. Manag. Sci. 25 (9), 833–848. https://doi.org/10.1287/mnsc.25.9.833.
Park, J.-S., Youn, T.-Y., Kim, H.-B., Rhee, K.-H., Shin, S.-U., 2018. Smart contract-based review system for an IoT data marketplace. Sensors 18 (1–16). https://doi.org/10.3390/s18103577.
Pavlou, P.A., 2003. Consumer acceptance of electronic commerce: integrating trust and risk with the technology acceptance model. Int. J. Electron. Commer. 7 (3), 101–134. https://doi.org/10.1080/10864415.2003.11044275.
Pavlou, P.A., Gefen, D., 2004. Building effective online marketplaces with institution-based trust. Inf. Syst. Res. 15 (1), 37–59. https://doi.org/10.1287/isre.1040.0015.
Pei, J., 2022. A survey on data pricing: from economics to data science. IEEE Trans. Knowl. Data Eng. 34 (10), 4586–4608. https://doi.org/10.1109/tkde.2020.3045927.
Penttinen, E., Halme, M., Lyytinen, K., Myllynen, N., 2018. What influences choice of business-to-business connectivity platforms? Int. J. Electron. Commer. 22 (4), 479–509. https://doi.org/10.1080/10864415.2018.1485083.
Petersen, D., 2022. Automating governance: blockchain delivered governance for business networks. Ind. Mark. Manag. 102 (1), 177–189. https://doi.org/10.1016/j.indmarman.2022.01.017.
Raj, P.V.R.P., Jauhar, S.K., Ramkumar, M., Pratap, S., 2022. Procurement, traceability and advance cash credit payment transactions in supply chain using blockchain smart contracts. Comput. Ind. Eng. 167. https://doi.org/10.1016/j.cie.2022.108038.
Ramdani, B., Kawalek, P., Lorenzo, O., 2009. Predicting SMEs' adoption of enterprise systems. J. Enterprise Inf. Manag. 22 (1/2), 10–24. https://doi.org/10.1108/17410390910922796.
Ray, J., Menon, S., Mookerjee, V., 2020. Bargaining over data: when does making the buyer more informed help? Inf. Syst. Res. 31 (1), 1–15. https://doi.org/10.1287/isre.2019.0872.
Reimsbach-Kounatze, C., 2021. Enhancing access to and sharing of data: striking the balance between openness and control over data. In: Data Access, Consumer Interests and Public Welfare. Nomos Verlagsgesellschaft mbH & Co. KG, pp. 25–68. https://doi.org/10.5771/9783748924999-25.
Richter, H., Slowinski, P.R., 2019. The data sharing economy: on the emergence of new intermediaries. IIC - International Review of Intellectual Property and Competition Law 50 (1), 4–29. https://doi.org/10.1007/s40319-018-00777-7.
Roman, D., Stefano, G., 2016. Towards a reference architecture for trusted data marketplaces: the credit scoring perspective. In: 2016 2nd International Conference on Open and Big Data (OBD), Vienna, Austria.
Saprikis, V., Vlachopoulou, M., 2012. Determinants of suppliers' level of use of B2B e-marketplaces. Ind. Manag. Data Syst. 112 (4), 619–643. https://doi.org/10.1108/02635571211225512.
Saunders, C., Benlian, A., Henfridsson, O., Wiener, M., 2020. MIS quarterly research curation: IS control & governance. MIS Q.
Scheider, S., Lauf, F., Geller, S., Möller, F., Otto, B., 2023a. Exploring design elements of personal data markets. Electron. Mark. 33 (28), 1–16. https://doi.org/10.1007/s12525-023-00646-3.
Scheider, S., Lauf, F., Möller, F., Otto, B., 2023b. A reference system architecture with data sovereignty for human-centric data ecosystems. Business & Information Systems Engineering 65 (1), 577–595. https://doi.org/10.1007/s12599-023-00816-9.
Schomm, F., Stahl, F., Vossen, G., 2013. Marketplaces for data: an initial survey. ACM SIGMOD Record 42 (1), 15–26. https://doi.org/10.1145/2481528.2481532.
Sedlmeir, J., Buhl, H.U., Fridgen, G., Keller, R., 2020. The energy consumption of blockchain technology: beyond myth. Business & Information Systems Engineering 62 (6), 599–608. https://doi.org/10.1007/s12599-020-00656-x.
Seidel, M.-D.L., 2018. Questioning centralized organizations in a time of distributed trust. J. Manag. Inq. 27 (1), 40–44. https://doi.org/10.1177/1056492617734942.
Shaabany, G., Grimm, M., Anderl, R., 2016. Secure information model for data marketplaces enabling global distributed manufacturing. Proced. CIRP 50, 360–365. https://doi.org/10.1016/j.procir.2016.05.003.
Shi, Z., Srinivasan, K., Zhang, K., 2023. Design of platform reputation systems: optimal information disclosure. Mark. Sci. 42 (3), 500–520. https://doi.org/10.1287/mksc.2022.1392.
Shih, Y.-W., Lin, S.-C., Ke, Y.-L., 2013. Influence of transaction trust in B2B E-marketplaces: an investigation of tan and thoen's views. International Journal of Innovation, Management and Technology 4 (4), 397.
Siddiqui, M.S., Syed, T.A., Nadeem, A., Nawaz, W., Alkhodre, A., 2022. Permission and usage control for virtual tourism using blockchain-based smart contracts. Int. J. Adv. Comput. Sci. Appl. 13 (11), 231–240. https://doi.org/10.14569/IJACSA.2022.0131126.
Simon, N., Markopoulos, I., Gindl, S., Utermark, B., Kaltenböck, M., Abbas, A.E., Ofe, H., van de Ven, M., Bergman, R., Zuiderwijk, A., de Reuver, M., Gras, N., Kuster, A., Jakuzzi, J., Emons, S., Rosam, G., Fribus, M., Brockob, A., 2021. D2. 1 'definition and analysis of the EU and worldwide data market trends and industrial needs for growth. https://www.trusts-data.eu/wp-content/uploads/2021/07/D2.1-Definition-and-analysis-of-the-EU-and-worldwide-data-market-trends-....pdf.
Smith, H.J., Dinev, T., Xu, H., 2011. Information privacy research: an interdisciplinary review. MIS Q. 35 (4), 989–1015. https://doi.org/10.2307/41409970.
Son, J.-Y., Tu, L., Benbasat, I., 2006. A descriptive content analysis of trust-building measures in B2B electronic marketplaces. Commun. Assoc. Inf. Syst. 18 (1), 99–128. https://doi.org/10.17705/1CAIS.01806.
Spiekermann, M., 2019. Data marketplaces: trends and monetisation of data goods. Intereconomics 54 (4), 208–216. https://doi.org/10.1007/s10272-019-0826-z.
Spiekermann, S., Korunovska, J., 2017. Towards a value theory for personal data. J. Inf. Technol. 32 (1), 62–84. https://doi.org/10.1057/jit.2016.4.
Stachon, M., Möller, F., Guggenberger, T., Tomczyk, M., Henning, J.-L., 2023. Understanding data trusts. ECIS 2023 Research-in-Progress Papers, Kristiansand, Norway.
Stahl, F., Schomm, F., Vossen, G., 2014. Data Marketplaces: an Emerging Species. IOS Press.
Stahl, F., Schomm, F., Vossen, G., Vomfell, L., 2016. A classification framework for data marketplaces. Vietnam Journal of Computer Science 3 (3), 137–143. https://doi.org/10.1007/s40595-016-0064-2.
Stahl, F., Schomm, F., Vomfell, L., Vossen, G., 2017. Marketplaces for digital data: quo vadis? Comput. Inf. Sci. 10 (4), 22. https://doi.org/10.5539/cis.v10n4p22.
Stahl, B., Häckel, B., Leuthe, D., Ritter, C., 2023. Data or business first?—manufacturers' transformation toward data-driven business models. Schmalenbach Journal of Business Research 75 (3), 303–343. https://doi.org/10.1007/s41471-023-00154-2.
Staub, N., Haki, K., Aier, S., Winter, R., 2022. Governance mechanisms in digital platform ecosystems: addressing the generativity-control tension. Commun. Assoc. Inf. Syst. 51 (1), 906–939. https://doi.org/10.17705/1CAIS.05137.
Sterk, F., Stocker, A., Heinz, D., Weinhardt, C., 2024. Unlocking the value from car data: a taxonomy and archetypes of connected car business models. Electron. Mark. 34 (1), 13. https://doi.org/10.1007/s12525-024-00692-5.
Steur, A.J., Seiter, M., 2021. Properties of feedback mechanisms on digital platforms: an exploratory study. J. Bus. Econ. 91 (4), 479–526. https://doi.org/10.1007/s11573-020-01009-6.
Sun, S., Cegielski, C.G., Jia, L., Hall, D.J., 2018. Understanding the factors affecting the organizational adoption of big data. J. Comput. Inf. Syst. 58 (3), 193–203. https://doi.org/10.1080/08874417.2016.1222891.
Tech, R.P.G., Kahlert, J., Schmeiss, J., 2019. Blockchain-enabled open business models: new means to shared value capturing? In: Redlich, T., Moritz, M., Wulfsberg, J.P. (Eds.), Co-creation: Reshaping Business and Society in the Era of Bottom-up Economics. Springer International Publishing, pp. 63–76. https://doi.org/10.1007/978-3-319-97788-1_6.
Terzi, S., Zacharaki, A., Nizamis, A., Votis, K., Ioannidis, D., Tzovaras, D., Stamelos, I., 2019. Transforming the supply-chain management and industry logistics with

blockchain smart contracts. In: Proceedings of the 23rd Pan-Hellenic Conference on Informatics, Nicosia, Cyprus.
Thies, F., Wessel, M., Benlian, A., 2018. Network effects on crowdfunding platforms: exploring the implications of relaxing input control. Inf. Syst. J. 28 (6), 1239–1262. https://doi.org/10.1111/isj.12194.
Tiwana, A., 2015. Evolutionary competition in platform ecosystems. Inf. Syst. Res. 26 (2), 266–281. https://doi.org/10.1287/isre.2015.0573.
Tiwana, A., Keil, M., 2009. Control in internal and outsourced software projects. J. Manag. Inf. Syst. 26 (3), 9–44. https://doi.org/10.2753/mis0742-1222260301.
Tsai, W., Ghoshal, S., 1998. Social capital and value creation: the role of intrafirm networks. Acad. Manag. J. 41 (4), 464–476. https://doi.org/10.2307/257085.
Tuler De Oliveira, M., Reis, L.H.A., Verginadis, Y., Mattos, D.M.F., Olabarriaga, S.D., 2022. SmartAccess: attribute-based access control system for medical records based on smart contracts. IEEE Access 10 (1), 117836–117854. https://doi.org/10.1109/access.2022.3217201.
Van Der Burg, S., Wiseman, L., Krkeljas, J., 2021. Trust in farm data sharing: reflections on the EU code of conduct for agricultural data sharing. Ethics Inf. Technol. 23 (3), 185–198. https://doi.org/10.1007/s10676-020-09543-1.
Venkatraman, N., Lee, C.-H., 2004. Preferential linkage and network evolution: a conceptual model and empirical test in the U.S. video game sector. Acad. Manag. J. 47 (6), 876–892. https://doi.org/10.5465/20159628.
Virkar, S., Viale Pereira, G., Vignoli, M., 2019. Investigating the social, political, economic and cultural implications of data trading. In: Lindgren, I., et al. (Eds.), Electronic Government. EGOV 2019. Lecture Notes in Computer Science. Springer, Cham, pp. 215–229. https://doi.org/10.1007/978-3-030-27325-5_17.
von Scherenberg, F., Hellmeier, M., Otto, B., 2024. Data sovereignty in information systems. Electron. Mark. 34 (1), 1–15. https://doi.org/10.1007/s12525-024-00693-4.
Wang, S., Li, D., Zhang, Y., Chen, J., 2019. Smart contract-based product traceability system in the supply chain scenario. IEEE Access 7, 115122–115133. https://doi.org/10.1109/ACCESS.2019.2935873.
Wareham, J., Fox, P.B., Cano Giner, J.L., 2014. Technology ecosystem governance. Organ. Sci. 25 (4), 1195–1215. https://doi.org/10.1287/orsc.2014.0895.
European Commission, Wauters, P., Siede, A., Cocoru, D., Linz, F., Barbero, M., Osimo, D., Hillebrand, A., Graux, H., 2018. Study on emerging issues of data ownership, interoperability, (Re-)Usability and access to data, and liability – final report. https://op.europa.eu/en/publication-detail/-/publication/74cca30c-4833-11e8-be1d-01aa75ed71a1/language-en.
Werling, M., Werth, D., Lasi, H., 2025. Towards a framework for building trust and transparency in collaborative data-driven use cases - learnings from a mobility case study. In: Proceedings of the 58th Hawaii International Conference on System Sciences, Waikoloa Village, Hawaii, the United States.
Wessel, M., Thies, F., Benlian, A., 2017. Opening the floodgates: the implications of increasing platform openness in crowdfunding. J. Inf. Technol. 32 (4), 344–360. https://doi.org/10.1057/s41265-017-0040-z.
Wiener, M., Mähring, M., Remus, U., Saunders, C., 2016. Control configuration and control enactment in information systems projects: review and expanded theoretical framework. MIS Q. 40 (3), 741–774.
Wiener, M., Cram, W.A., Benlian, A., 2023a. Algorithmic control and gig workers: a legitimacy perspective of uber drivers. Eur. J. Inf. Syst. 32 (3), 485–507. https://doi.org/10.1080/0960085x.2021.1977729.
Wiener, M., Cram, W.A., Remus, U., Mähring, M., 2023b. Control-style choices and performance impacts: how should senior is managers enact control over uncertain is projects? Decis. Support Syst. 167 (1), 1–12. https://doi.org/10.1016/j.dss.2022.113915.
Wu, J., 2025. Secondary market monetization and willingness to share personal data. Management Science, pp. 1–20. https://doi.org/10.1287/mnsc.2022.03423. *Articles in Advance*.
Wu, Y., Ye, H., Jensen, M.L., Liu, L., 2024. Impact of project updates and their social endorsement in online medical crowdfunding. J. Manag. Inf. Syst. 41 (1), 73–110. https://doi.org/10.1080/07421222.2023.2301173.
Xu, H., Dinev, T., Smith, H.J., Hart, P.J., 2008. Examining the formation of individual's privacy concerns: toward an integrative view. In: ICIS 2008 Proceedings, Paris, France.
Xu, H., Dinev, T., Smith, J., Hart, P., 2011. Information privacy concerns: linking individual perceptions with institutional privacy assurances. J. Assoc. Inf. Syst. Online 12 (12), 798–824. https://doi.org/10.17705/1jais.00281.
Xuan, S., Zheng, L., Chung, I., Wang, W., Man, D., Du, X., Yang, W., Guizani, M., 2020. An incentive mechanism for data sharing based on blockchain with smart contracts. Comput. Electr. Eng. 83, 1–12. https://doi.org/10.1016/j.compeleceng.2020.106587.
Yadlapalli, A., Rahman, S., Gopal, P., 2022. Blockchain technology implementation challenges in supply chains – evidence from the case studies of multi-stakeholders. Int. J. Logist. Manag. 33 (5), 278–305. https://doi.org/10.1108/ijlm-02-2021-0086.
Yan, J., Xin, S., Liu, Q., Xu, W., Yang, L., Fan, L., Chen, B., Wang, Q., 2014. Intelligent supply chain integration and management based on cloud of things. Int. J. Distributed Sens. Netw. 10 (3), 1–15. https://doi.org/10.1155/2014/624839.
Zhang, M., Beltrán, F., Liu, J., 2023. A survey of data pricing for data marketplaces. IEEE Transactions on Big Data 9 (4), 1038–1056. https://doi.org/10.1109/TBDATA.2023.3254152.
Zhang, W., Xu, R., Zhao, J.L., Jiang, Q., 2023a. A blockchain-centric data sharing framework for building trust in healthcare insurance. In: Lu, C., Tanniru, M. (Eds.), Blockchain in Healthcare: Analysis, Design and Implementation. Springer International Publishing, pp. 101–118. https://doi.org/10.1007/978-3-031-45339-7_5.
Zhang, X., Yue, W.T., Yu, Y., Zhang, X., 2023b. How to monetize data: an economic analysis of data monetization strategies under competition. Decis. Support Syst. 173, 1–12. https://doi.org/10.1016/j.dss.2023.114012.
Zrenner, J., Möller, F.O., Jung, C., Eitel, A., Otto, B., 2019. Usage control architecture options for data sovereignty in business ecosystems. J. Enterprise Inf. Manag. 32 (3), 477–495. https://doi.org/10.1108/jeim-03-2018-0058.