# *Designing and Managing Decentralized Systems: Coping with Adoption Dynamics for Practical Diffusion*

**Dissertation**

zur Erlangung des Grades eines Doktors der Wirtschaftswissenschaft

der Rechts- und Wirtschaftswissenschaftlichen Fakultät

der Universität Bayreuth

Vorgelegt

von

*Jonathan Lautenschlager*

aus

*Frankfurt am Main*

| | |
|---|---|
| Dekan: | Prof. Dr. Claas Christian Germelmann |
| Erstberichterstatter: | Prof. Dr. Nils Urbach |
| Zweitberichterstatter: | Prof. Dr. Jens Strüker |
| Tag der mündlichen Prüfung: | 03.07.2025 |

## Abstract

Emerging decentralized information systems challenge conventional assumptions about data control, trust, and governance. Rooted in technologies such as blockchain and self-sovereign identity (SSI), they promise increased autonomy, privacy, and interoperability, but also face significant adoption hurdles. This cumulative dissertation investigates how organizations can design and manage such decentralized information systems to cope with adoption dynamics and facilitate their practical diffusion. It comprises seven essays, structured around three overarching research goals. In Essays 1–2, I explore the foundational tensions of transparency and control in decentralized systems (RG1), outlining how blockchain-based infrastructures and digital identity wallets confront data governance, privacy, and institutional legitimacy. Essays 3–4 address the challenges of implementing and designing decentralized architectures in multi-stakeholder ecosystems (RG2), focusing on digital identity in mobility, supply chain management, and public services. These essays identify design principles and governance mechanisms to navigate coopetition, enable interoperability, and manage sensitive data. Finally, Essays 5–7 investigate the conditions under which emerging decentralized technologies—specifically SSI and Central Bank Digital Currencies (CBDCs)—can deliver value to public and private actors (RG3), highlighting organizational affordances, experimental innovation processes and ecosystem-level value propositions.

The dissertation is structured in two main parts. In the first part, I introduce the relevance of decentralized systems, outline conceptual and technological foundations, derive research gaps and questions, explain the applied research methods, synthesize the core findings of the seven essays, and discuss their theoretical, practical and artefactual contributions, limitations, and implications for future research. The second part comprises the seven individual essays. Collectively, this dissertation contributes to information systems research by offering a nuanced socio-technical understanding of decentralization and by providing actionable guidance for designing and managing decentralized information systems in practice.

Keywords: Decentralized systems, blockchain, self-sovereign identity, digital identity, supply chain management, public sector, decentralization, practical adoption.

## Acknowledgments

Completing my PhD has been much more than the process of conducting research and writing a dissertation. It has been an essential chapter in my life — shaped by the people who have supported, challenged, and inspired me along the way. Since 2017, I have had the privilege of being part of the FIM Research Center — a place characterized by mutual support, high standards, and a shared ambition to make a difference. I am thankful for having taken my first academic and professional steps in an environment shaped by colleagues and friends whose dedication, support, and spirit have profoundly influenced my journey over the years. This journey would definitely not have been the same without you. Your collaboration, advice, and friendship enriched both everyday work and special moments. Whether through challenging questions or shared laughter — your support and advice have been truly meaningful to me.

I am particularly grateful to my doctoral advisor, Prof. Dr. Nils Urbach, for his trust, consistent support, and thoughtful guidance throughout the process. His ability to provide direction while allowing me to follow my own ideas created the space in which my work could grow, while also giving me the opportunity to develop myself — both as a researcher and as a person. I also sincerely thank my second supervisor, Prof. Dr. Jens Strüker, for his openness and encouragement in developing my research interests.

To my friends, who provided encouragement, fresh perspectives, and much-needed distraction when it was most welcome. To my parents, who guided me through school and beyond with unwavering support, never with pressure, but always with the belief that doing one's personal best is enough to succeed. To my two older brothers, who have known and supported me since day one — no matter what. And to my fiancée, Celine — your presence has been the foundation beneath this entire journey. You have stood by me unconditionally, in moments of progress and in moments of doubt. You reminded me of my strengths when I couldn't see them myself and gave me calm when I needed clarity. Your support, patience, and encouragement have been an essential part of this journey. I am deeply thankful to have you by my side.

*Frankfurt am Main, May 2025*

Jonathan Lautenschlager

## Abbreviations and initializations

| | |
|---|---|
| A-E-A | Affordance-Experimentation-Actualization |
| AML | Anti-Money-Laundering |
| DeFi | Decentralized Finance |
| DLT | Distributed Ledger Technology |
| DOI | Diffusion of Innovations |
| DSR | Design Science Research |
| EUDIW | European Digital Identity Wallet |
| ERP | Enterprise Resource Planning |
| FinTech | Financial Technology |
| GDPR | General Data Protection Regulation |
| JSON | JavaScript Object Notation |
| KYC | Know-Yor-Customer |
| PoW | Proof of Work |
| PoS | Proof of Stake |
| RG(s) | research goal(s) |
| SSI | Self-Sovereign Identity |
| TAM | Technology Acceptance Model |
| VCs | verifiable credentials |
| VPs | verifiable presentations |
| ZKP(s) | zero-knowledge proof(s) |

# Table of contents

# Introduction to Designing and Managing Decentralized Systems: Coping with Adoption Dynamics for Practical Diffusion


## Abstract

This cumulative dissertation investigates how organizations can design and manage emerging decentralized information systems to cope with adoption dynamics and facilitate their practical diffusion. It comprises seven essays, structured around three primary research goals: identifying and understanding the potentials and challenges of decentralized systems for implementing decentralized systems in organizational contexts (RG1), developing and designing solution approaches for the adoption of decentralized systems in practice (RG2), and investigating and exploiting potentials of decentralized solutions in practice. (RG3). The introduction of this dissertation is organized as follows: Section 1 advocates the relevance of researching decentralized information systems and the importance of addressing adoption dynamics to enable their diffusion into practice; Section 2 outlines the conceptual and technological foundations, including blockchain technology and SSI as exemplary units of analysis; Section 3 identifies key research gaps and determines the overarching research questions and goals; Section 4 presents the applied research designs and methodological approach; Section 5 synthesizes the findings of the seven essays with respect to the three research goals; and Section 6 concludes with a discussion of the theoretical and practical contributions, limitations, and implications for future research. By virtue of its findings, this dissertation contributes to information systems research by illuminating the sociotechnical complexities of decentralization and providing actionable guidance for addressing adoption dynamics in order to support the practical diffusion of decentralized systems.


Keywords: Adoption dynamics, decentralized systems, blockchain, self-sovereign identity, practical diffusion.

# Table of contents – Introduction

# 1 Motivation

The continuous advancement and interconnection of digital infrastructures are reshaping the way organizations and societies coordinate, govern, and exchange information (Constantinides et al., 2018). In this regard, digitalization has led to increasingly complex socio-technical systems which integrate technological and organizational dimensions (Bostrom & Heinen, 1977; Carroll, 2016). As these systems evolve into broader networks, questions regarding their governance, trust mechanisms, and the provisioning of interoperability become ever more pressing in order to facilitate their adoption and widespread implementation in practice (Addo & Senyo, 2021; Engert et al., 2025; Tiwana, 2014). Historically, traditional models of digital coordination have relied on centralized governance structures (Wareham et al., 2014), which provide efficiency and control but often struggle to accommodate the distributed and multi-stakeholder nature of modern digital networks (Heines et al., 2021; Zwitter & Hazenberg, 2020). Such dependencies on a centralized intermediary have fueled discussions around alternative infrastructures, such as blockchain-based systems, to mitigate dependencies and enhance resilience in a multi-stakeholder network (Heines et al., 2021; Nofer et al., 2017). As a result, research has increasingly been concerned with exploring decentralized system architectures with the goal of reconfiguring digital coordination mechanisms, thereby challenging established governance paradigms and raising concerns over data sovereignty, transparency, and security in practice (Queiroz & Fosso Wamba, 2019).

During the past decade, scholarly interest has shifted towards the potentials of those decentralized systems, particularly blockchain technology (Alt, 2020; Beck et al., 2017). While much of the early research has focused on the financial sector (e.g., cryptocurrencies within financial technologies (FinTech) or decentralized finance (DeFi)) (Oliveira et al., 2018; Zetzsche et al., 2020), applications have increasingly extended to other domains beyond finance, including supply chain management or public services (Beck et al., 2018; Jensen et al., 2019; Rieger et al., 2019). Furthermore, upcoming paradigms such as SSI have emerged as an alternative decentralized approach to identity management with the aim of enhancing user control while providing data sovereignty across borders (Hoess et al., 2024; Hoess et al., 2022; Schlatt et al., 2021). Despite, however, the growing academic interest and significant theoretical potential of decentralized systems initially predicted by scholars, widespread adoption and large

scale integration have not yet been achieved (Lautenschlager et al., 2023; Sternberg et al., 2020; Toufaily et al., 2021).

Upon closer examination, pertinent research has identified compelling advantages offered by decentralized architectures, such as reduced dependencies on intermediaries and enhanced information transparency for automation purposes. However, significant challenges persist in translating these benefits into practical, scalable implementations (Feulner et al., 2022; Lautenschlager et al., 2023; Schlatt et al., 2021). Issues related to adoption dynamics - such as executing suitable governance models, the provisioning of interoperability measures with existing infrastructures, and establishing regulatory alignment - remain largely unresolved, raising concerns about their feasibility beyond isolated pilot projects (Sedlmeir, Lautenschlager, et al., 2022). One significant key barrier to widespread adoption in practice is the tension between decentralization, market environments, and regulatory compliance (Savoldelli et al., 2014). Decentralized architectures aim to reduce reliance on intermediaries, yet market-specific and regulatory requirements, such as those within the user's identity management and related obligatory data protection, often assume centralized oversight mechanisms (Glöckler et al., 2023; Heines et al., 2021). This misalignment creates operational uncertainties and practical difficulties in integrating decentralized solutions into existing regulatory supervised markets. Moreover, the long-term implications of decentralized systems within broader domains and networks, including their socio-economic and institutional effects, have yet to be comprehensively examined. These observations highlight a persistent disconnect between the conceptual potential of decentralized information systems and their practical realization across institutional settings (Beck et al., 2017). To bridge this gap, it is essential to develop a deeper understanding of the mechanisms, design, and management of these decentralized systems that shape their adoption and integration. Accordingly, this dissertation investigates the following research question:

*How can emerging decentralized information systems be designed and managed to cope with adoption dynamics in practice?*

To address this question, this dissertation synthesizes insights from seven individual essays, each contributing to a comprehensive understanding of decentralized information systems focusing on blockchain technology and SSI across multiple application domains, such as the public-, mobility-, or construction sector. This research illustrates

how the essays collectively address three overarching research goals: first, to enhance the understanding of the potentials and challenges associated with the adoption dynamics of decentralized systems (RG1); second, to explore the design and development of solution approaches that cope with adoption dynamics (RG2); and third, to investigate and exploit potentials of decentralized solutions in practice (RG3). By analyzing their interrelations, this dissertation demonstrates how the individual contributions complement one another in advancing both theoretical and practical insights into the design, adoption, and governance of decentralized systems.

The remainder of the introduction of this dissertation is organized as follows: Section 2 outlines the conceptual and technical foundations of emerging decentralized information systems and their current potentials, challenges, and tensions for practical diffusion. Section 3 identifies research gaps and introduces the key questions addressed across the seven essays. Section 4 details the rationale behind the chosen research methods, while Section 5 summarizes the findings of the seven essays. The dissertation concludes with a discussion of its theoretical and practical contributions, limitations, and potential directions for future research.

# 2 Background

## 2.1 Foundations of centralized versus decentralized technologies

Centralized systems are currently the dominant structural approach in digital infrastructures, relying on hierarchical control structures in which a single entity or a small group of entities governs data and access control (Hanseth & Lyytinen, 2010; Tiwana et al., 2010). This model has traditionally been favored for its efficiency and the structured governance mechanisms which also aid compliance with regulatory requirements in various contexts. By consolidating decision-making within a central entity, these systems facilitate streamlined operations and a high degree of control over security and data management. Prominent examples include organizational Enterprise Resource Planning (ERP) systems, in which a single provider simultaneously manages updates, access control, and data storage for multiple client organizations, thereby ensuring standardized security protocols and operational consistency. However, particularly in the context of multi-stakeholder environments, these benefits come at the cost of increased vulnerability to systemic failures, heightened risks of monopolization and market concentration, and limited adaptability (Hanseth & Lyytinen, 2010; van Dijck et al., 2018).

In contrast, decentralized technologies aim to distribute control and data management across multiple stakeholders, reducing dependency on a central authority while fostering a more resilient and adaptive infrastructure (Zysman & Kenney, 2018). These approaches have gained increasing attention as digital networks expand in complexity, requiring governance models that can better accommodate transparency and trust minimization among stakeholders (Beck et al., 2017). At their core, decentralized systems strive to enhance efficiency and autonomy by eliminating or reducing the involvement of intermediaries in digital interactions. Decentralized architectures use cryptography, consensus protocols, and distributed ledgers to enable secure, integrity-preserving peer-to-peer interactions without a central authority (Zwitter & Boisse-Despiaux, 2018). Peer-to-peer networks facilitate direct communication and resource sharing among participants without centralized coordination, enhancing fault tolerance and censorship resistance (Nofer et al., 2017). Similarly, distributed databases replicate data across multiple nodes to prevent single points of failure, ensuring higher resilience and data availability. Yet while these decentralized models offer compelling

advantages in terms of robustness and transparency, they also introduce challenges related to governance, scalability, and regulatory oversight, which require novel frameworks to balance decentralization with practical operational control (Butijn et al., 2020).

Blockchain and SSI, as aforementioned in Section 1, exemplify decentralized approaches by enabling transparent and tamper-proof transactions and identity management without dependence on traditional intermediaries. Blockchain technology provides an immutable, tamper-resistant infrastructure for value exchange, while SSI as a concept fosters the shift of identity management procedures from centralized identity providers to user-controlled digital credentials (Babel et al., 2025; Nakamoto, 2008). The growing interest in decentralized technologies stems from their potential to address issues related to digital data sovereignty and platform monopolization, making them increasingly relevant for digital economies and information systems research. Particularly in a multistakeholder context, such as digital identity or supply chain applications, decentralized models offer innovative solutions to longstanding challenges of interoperability or data security (Sedlmeir, Lautenschlager, et al., 2022).

In the context of this dissertation, the focus lies on the analysis of the architectural and governance models driving the adoption of decentralized technologies into practice. Two key architectural paradigms will be explored in detail: (1) blockchain technology, often used as a synonym for distributed ledgers (DLT), and (2) SSI as one of the predominant decentralized identity management concepts. These paradigms serve as primary examples of decentralized solutions that illustrate both the potential benefits and the challenges of transitioning from traditional centralized infrastructures to more distributed models. The following sections will provide a more detailed examination of blockchain technology and SSI while exploring their technical foundations and real-world adoption dynamics.

## 2.2 Fundamentals of blockchain technology

Blockchain technology represents a paradigm shift in how data is recorded, verified, and secured in distributed environments. Initially conceptualized as the underlying technology for Bitcoin (Nakamoto, 2008), blockchain has evolved into a broader class of DLTs that enable tamper-resistant, transparent, and decentralized record-keeping without dependence on a central authority. At its core, blockchain consists of a

sequential chain of data blocks, each cryptographically linked to its predecessor by virtue of cryptographical hash-pointer. This structural design prevents unauthorized modifications, since any attempt to alter past records requires the alteration of all subsequent blocks (Butijn et al., 2020; Nofer et al., 2017). Unlike traditional databases, which rely on a central party to maintain and verify records, blockchain technology levers cryptographic mechanisms and distributed consensus protocols to ensure trust among participants without necessitating a trusted intermediary. A defining characteristic of blockchain technology is its decentralization, which enhances fault tolerance and censorship resistance by distributing control across multiple nodes within a peer-to-peer-network (Beck et al., 2017). Transparency is another fundamental property, since transactions recorded on a blockchain are typically publicly verifiable. This openness contributes to trustworthiness but also introduces challenges with regard to organizational or individual data privacy and confidentiality. To address these concerns, privacy-enhancing technologies such as zero-knowledge proofs (ZKPs) (a cryptographic method which allows one party to prove the validity of a statement without revealing the underlying data) and confidential transactions have been developed to enable selective disclosure of information whilst preserving the integrity of the underlying data (Bossler et al., 2024; Sedlmeir, Lautenschlager, et al., 2022).

The security and functionality of blockchain largely depend on its consensus mechanism, which ensures agreement on the current state of the ledger across a distributed network. Different consensus mechanisms have been developed to balance security, scalability, and energy efficiency. *Proof of Work*, which requires participants to solve complex cryptographic puzzles, is highly secure (assuming sufficiently aligned incentive structures), but has been criticized for its high energy consumption and limited transaction throughput (Abellán Álvarez et al., 2024). In contrast, *Proof of Stake* selects validators based on the number of tokens they hold and are willing to stake as collateral significantly reducing energy consumption while maintaining security (Yang Xiao et al., 2020). *Practical Byzantine Fault Tolerance*, commonly used in permissioned blockchain networks, ensures rapid consensus through predefined validator nodes, making it particularly suitable for enterprise applications (Guggenberger et al., 2022). The choice of consensus mechanism determines the efficiency, security, and degree of decentralization in each blockchain system, often involving trade-offs that impact its practical applicability.

The different types of blockchain networks further influence their design and use cases. Public blockchains, such as Bitcoin and Ethereum, operate in a permissionless environment, allowing any participant to join and validate transactions (Buterin, 2013). While these networks offer the highest level of decentralization and security, they face scalability challenges and often struggle with regulatory compliance (Bamakan et al., 2020). In contrast, private blockchains restrict participation to a single organization or a tightly controlled group of authorized entities, thus prioritizing transaction confidentiality and operational efficiency, but significantly limiting decentralization and transparency. Consortium blockchains, by comparison, are jointly managed by multiple preselected organizations, striking a balance between transparency and control by enabling shared governance while still restricting access to a defined set of participants. Each of these models serves distinct purposes with public blockchains often facilitating open financial ecosystems and decentralized applications and private and consortium blockchains being more commonly adopted in enterprise settings where regulatory compliance and operational control are paramount (Guggenberger et al., 2022).

Despite its advantages, blockchain technology faces significant challenges that hinder its widespread adoption. Interoperability remains a critical issue since most blockchains operate in isolation thus limiting seamless data exchange across networks. Without standardized protocols the integration between different blockchain platforms and traditional IT infrastructures remains complex (Toufaily et al., 2021). Additionally, governance and regulatory uncertainties pose barriers to institutional adoption, particularly in highly regulated industries such as finance or supply chain management. The governance of blockchain networks varies significantly depending on their level of decentralization, whilst private and consortium models implement structured decision-making processes. The lack of clear regulatory frameworks further complicates adoption, since legal and compliance concerns vary across organizations (Wüst & Gervais, 2018). The future development of blockchain technology focuses on overcoming these limitations through advancements in scalability, interoperability, and governance models. Layer-2 scaling solutions, such as rollups and state channels, aim to enhance transaction throughput while maintaining security. Cross-chain interoperability frameworks seek to facilitate seamless interaction between different blockchain networks, enabling a more interconnected decentralized ecosystem (Zhang et al., 2019). Additionally, the integration of ZKPs with blockchain technology is emerging as

a promising approach to reduction of the computational load of consensus mechanisms, enablement of rule-based automation in governance processes (e.g., voting or compliance checks), and the protection of sensitive input data during smart contract execution by ensuring that transactions can be validated without revealing underlying information (Sedlmeir, Lautenschlager, et al., 2022).

## 2.3 Fundamentals of Self-Sovereign Identity

SSI introduces a novel approach to digital identity management with the goal of shifting control over personal credentials from third-party centralized providers to individuals and organizations (Ehrlich et al., 2021; Soltani et al., 2021). Unlike conventional identity systems, where third-party providers issue and validate credentials, SSI enables users to manage their own identity attributes in a secure and privacy-preserving manner. This paradigm is closely tied to advancements in cryptographic verification and decentralized architectures allowing identity holders to interact with verifiers without exposing unnecessary personal data. By minimizing dependencies on intermediaries, SSI enhances autonomy, mitigates risks associated with data breaches, and reduces the need for repeated identity verification across different services (Babel et al., 2025). In this context, Figure 1 illustrates the SSI-specific *Triangle of Trust*, which condenses the core building blocks of SSI and defines the fundamental relationships within a decentralized identity ecosystem.

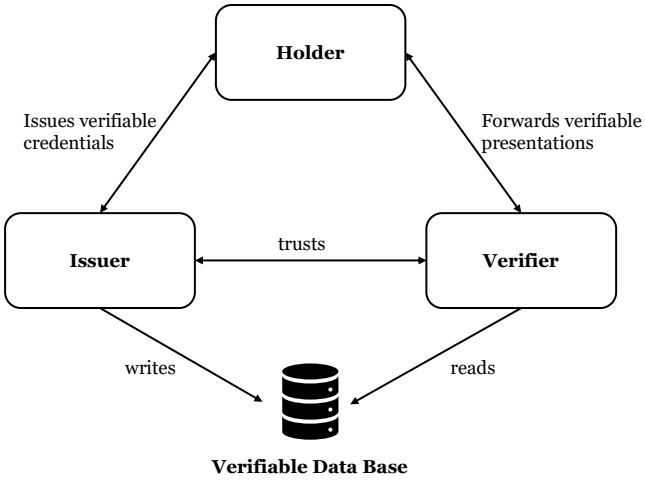


Figure 1 SSI Triangle of Trust: Own illustration based on Babel et al. (2025)

This model consists of three key roles: issuers, holders, and verifiers. Issuers are trusted entities, such as governments, universities, or financial institutions creating

digital verifiable credentials (VCs) (Babel et al., 2025). Holders, typically individuals or organizations, receive these VCs and store them securely in digital wallets. Verifiers, such as employers, service providers, or government agencies, request proof of identity from holders and validate the credentials against the issuer's cryptographic signature (Ehrlich et al., 2021; Sedlmeir et al., 2021). Together, these roles constitute the core of the SSI ecosystem by enabling the sovereign exchange of identity data, thereby establishing trust through cryptographically verifiable interactions. Another complementary component of SSI is the concept of Decentralized Identifiers (DIDs). As defined by the W3C DID 1.0 specification, a DID is a globally unique identifier that is resolvable to a DID document, and which is grounded on a JSON-based data structure which describes the DID subject, including associated public keys, authentication mechanisms, and service endpoints (Reed et al., 2020). Unlike traditional identifiers which depend on central issuing authorities, DIDs are designed to be created and managed by their subjects, typically leveraging decentralized technologies. This architecture facilitates cryptographic verifiability, data minimization, and user control, thereby supporting privacy-preserving and interoperable identity ecosystems. This foundational shift in identity architecture, enabled by components such as DIDs and VCs, distinguishes SSI from traditional identity management models (Rieger et al., 2024).

Furthermore, regulatory frameworks play a crucial role in shaping the adoption and implementation of SSI solutions. The European Union's eIDAS 2.0 regulation, which aims to establish a unified digital identity framework across member states, represents a significant step toward institutional recognition of decentralized identity models (European Commission, 2024). However, legal uncertainties regarding the enforceability and liability of self-sovereign credentials remain, particularly in areas requiring strict compliance with Anti-Money Laundering (AML) and Know-Your-Customer (KYC) regulations (Schlatt et al., 2021). Additionally, the General Data Protection Regulation (GDPR) introduces complex requirements with regard to data minimization and user consent, which must be carefully balanced against the principles of SSI (Goddard, 2017; Schwalm et al., 2022). The governance of decentralized identity ecosystems remains a subject to ongoing discussion, with key questions surrounding the establishment of trust anchors and accountability frameworks for credential issuers and verifiers (Schmeiss et al., 2019; Sule et al., 2021). Despite these challenges, SSI is increasingly recognized as a transformative solution for digital identity management across various sectors. Financial services, the mobility sector, and public administration are

among the domains exploring SSI to enhance security, streamline authentication processes, and reduce dependence on centralized identity providers (Hoess et al., 2024; Schlatt et al., 2021; Sourabh, 2019). The growing interest in VCs, particularly in the context of cross-border identity verification and digital wallets, highlights the potential of SSI to create a more user-centric and privacy-preserving digital identity landscape. However, addressing technical limitations, regulatory complexities, and governance models with the potential to overcome adoption dynamics will be critical to ensuring widespread adoption and interoperability of SSI-based solutions in practice (Nassr Eddine et al., 2023; Schwalm et al., 2022).

SSI thus marks a fundamental shift from traditional identity management approaches by prioritizing user control, cryptographic security, and decentralized trust. By making use of DIDs, VCs and privacy-preserving authentication methods, SSI offers an alternative to existing identity models which often compromise user autonomy and data privacy. While significant progress has been made in developing standards and pilot implementations, further advancements in interoperability, usability, and regulatory alignment are needed to fully realize the potential of SSI in real-world applications.

## 2.4 Adoption dynamics of decentralized systems in practice

Understanding the dynamics of technology adoption is essential for evaluating how innovative systems diffuse into organizational and societal practice. Prior research has extensively investigated the adoption of digital technologies through models such as the Technology Acceptance Model (TAM) and the Diffusion of Innovations (DOI) framework, each emphasizing distinct but overlapping factors such as perceived usefulness, social influence, and innovation attributes (Davis, 1989; Karnowski & Kümpel, 2015). More recent studies in information systems have extended these perspectives to examine socio-technical adoption processes, highlighting the role of institutional settings, stakeholder interactions, and governance structures (Constantinides et al., 2018; Tilson et al., 2010). In contexts involving decentralized technologies, such as blockchain or SSI, these dynamics become particularly essential, since adoption entails not only technological implementation but also alignment across organizational, regulatory, and infrastructural domains (Beck et al., 2018). Accordingly, this section reviews the adoption dynamics associated with decentralized systems, situating them within the broader literature on technology diffusion and socio-technical systems change.

The adoption dynamics of decentralized systems present a complex interplay of technological, organizational, and regulatory factors in various domains which influence their practical viability (Toufaily et al., 2021). While decentralized architectures offer advantages in terms of security, transparency, and autonomy, their successful implementation requires structured governance frameworks, mechanisms for stakeholder coordination, and strategic regulatory alignment. Many real-world applications, particularly in enterprise settings, adopt hybrid governance models which balance decentralization with operational oversight, for example by proposing hybrid Decentralized Autonomous Organizations (DAOs) (Shah, 2024). At the same time, economic dynamics, for example, shape incentives for adoption, particularly in ecosystems characterized by coopetition (an inherent tension between simultaneous cooperation and competition endeavors), where market participants must navigate between collaboration and competition (Lautenschlager et al., 2023; Queiroz & Fosso Wamba, 2019). Against this backdrop, this dissertation examines adoption dynamics through three interrelated but analytically distinct lenses: governance structures, coopetition-based economic incentives, and regulatory alignment.

Governance remains one of the most critical aspects influencing the adoption of decentralized systems, particularly in hybrid models which integrate both centralized and decentralized components (Zwitter & Hazenberg, 2020). Unlike purely decentralized networks, which operate autonomously based on consensus mechanisms, hybrid governance structures introduce off-chain coordination through predefined roles and decision-making processes. Consortium blockchains, for instance, rely on governance committees to establish participation rules, validate transactions, and enforce compliance measures. In digital identity ecosystems, federated governance approaches are often necessary to ensure interoperability and regulatory recognition while maintaining the sovereignty of individual users (Rieger et al., 2024). A major challenge lies in designing governance mechanisms which ensure both accountability and adaptability, since decentralized networks need to accommodate evolving regulatory requirements and technological advancements, whilst at the same time avoiding excessive centralization that would undermine their core principles (Esener, 2023; Rikken et al., 2019).

Beyond governance structures, the competitive dynamics surrounding decentralized technologies play a crucial role in their adoption (Fernandez & Chiambaretto, 2016). Many decentralized ecosystems exist within markets characterized by coopetition,

where firms must simultaneously cooperate to develop shared infrastructure while competing on value-added services (Gleiss et al., 2023). This is particularly evident in supply chain networks or digital identity frameworks where decentralized technologies facilitate cross-organizational collaboration while enabling differentiation through proprietary services and business models (Lautenschlager et al., 2023; Queiroz & Fosso Wamba, 2019). Blockchain-based supply chain solutions, for example, require cooperation among industry participants to establish transparent data-sharing mechanisms, yet firms remain cautious about exposing competitive intelligence. Similarly, in digital identity ecosystems, whilst decentralized identity solutions enable interoperability across platforms, competing stakeholders may seek to maintain control over identity verification processes in order to preserve their market influence. These tensions necessitate governance mechanisms that incentivize fair participation while preventing monopolization by dominant players (Rieger et al., 2024).

Regulatory challenges represent another significant barrier to the adoption of decentralized systems, since legal frameworks often lag behind technological innovation. Whilst decentralization offers advantages such as enhanced privacy and reduced reliance on intermediaries, it also raises concerns about liability, compliance, and fraud prevention. In digital identity ecosystems, for instance, ensuring legal recognition of VCs remains a challenge, particularly in jurisdictions where traditional, government-issued identity documents are mandated for official processes. Recent regulation, such as the European Union's eIDAS 2.0 framework (European Commission, 2021), seeks to provide legal clarity for decentralized identity solutions, but inconsistencies across global regulatory environments continue to create uncertainties for adopters. To achieve large-scale adoption, decentralized systems must develop governance frameworks that align with existing regulatory expectations while leveraging policy adaptations that accommodate the unique attributes of decentralized architectures (Atzori, 2017).

In sum, the adoption of decentralized systems requires a multifaceted approach incorporating considerations of technological feasibility, economic incentives, and regulatory alignment. Hybrid governance models offer a pragmatic balance between decentralization and institutional oversight, enabling broader adoption in enterprise and public-sector applications. Competitive tensions in decentralized ecosystems necessitate mechanisms that encourage cooperation without undermining competitive

differentiation. Regulatory frameworks must evolve to accommodate decentralized architectures while ensuring compliance with legal and security requirements. Addressing these factors will be essential in determining the long-term viability and impact of decentralized technologies across industries.

While these dynamics are conceptually separable, they frequently occur in intertwined ways in real-world settings, such as in decentralized identity ecosystems, supply chain networks, and public sector innovation projects. Accordingly, this dissertation engages with these adoption dynamics across various empirical and conceptual constellations, thereby contributing differentiated yet complementary insights into their interplay. Given the breadth and systemic character of adoption-related challenges, a holistic analysis of all possible dynamics remains elusive. Instead, this dissertation focuses on selected research areas which are analytically tractable and aligned with the overarching research goals. By doing so, it provides an in-depth understanding of adoption processes in situations where technological, economic, and regulatory forces collide and offers design-oriented implications for fostering the practical diffusion of decentralized information systems.

# 3 Derivation of research goals, gaps, and questions

This dissertation elaborates on *how to design and manage emerging decentralized systems to cope with adoption dynamics, thereby facilitating practical diffusion.* Building upon the overarching research question, this study seeks to achieve three distinct research goals:

***RG1:*** *Identify and understand potentials and challenges for implementing decentralized systems in organizations.*

***RG2:*** *Develop and design decentralized systems for practical adoption.*

***RG3:*** *Investigate and facilitate exploitation potentials of decentralized solutions in practice.*

To accomplish these research goals, this dissertation identifies existing gaps in the literature on decentralized technologies and formulates corresponding research questions. These questions are examined across seven individual essays, each contributing to a comprehensive understanding of the fundamentals, design, and management of decentralized information systems. The following section outlines the specific research gaps, and the research questions addressed in each essay. Table 1 provides an overview of all essays discussed in the subsequent sections, highlighting their thematic focus and contribution to the overarching research goals.

Table 1 Overview of the seven research essays, which address the identified RGs

| Title | Publication outlet | VHB JQ4 ranking | Publication status |
|---|---|---|---|
| **RG1: Identify and understand potentials and challenges for implementing decentralized systems in organizations.** | | | |
| **Essay 1:** The transparency challenge of blockchain in organizations | Electronic Markets | B | Published |
| **Essay 2:** Self-sovereign identity and digital wallets | Electronic Markets | B | Published |
| **RG2: Develop and design decentralized systems for practical adoption.** | | | |
| **Essay 3:** Toward seamless mobility-as-a-service: Providing multimodal mobility through digital wallets | Business & Information Systems Engineering | B | Published |

| Title | Publication outlet | VHB JQ4 ranking | Publication status |
|---|---|---|---|
| **Essay 4:** Striking a balance: Designing a blockchain-based solution to navigate coopetition dynamics in supply chain management | Electronic Markets | B | Under Review (Minor Revision) |
| **Based on:** Overcoming the data transparency trade-off: Designing a blockchain-based delivery invoice system for the construction industry | Wirtschaftsinformatik 2023 Proceedings | B | Published |
| **RG3: Investigate and facilitate exploitation potentials of decentralized solutions in practice.** | | | |
| **Essay 5:** Interoperability dynamics in digital identity ecosystems | Journal of the Association for Information Systems | A | Under review |
| **Essay 6:** Self-sovereign identity in the public sector: Affordances, experimentation, and actualization | Government Information Quarterly | B | Under review (Minor Revision) |
| **Essay 7:** A multivocal literature review on capturing value propositions for private organizations in a CBDC ecosystem | Communications of the Association for Information Systems | B | Under review (Major Revision) |

## 3.1 RG1: Identify and understand potentials and challenges for implementing decentralized systems in organizations

In recent years, decentralized technologies such as blockchain have attracted growing scholarly and practical interest as enablers of new forms of inter-organizational coordination, autonomy, and trust (Beck et al., 2017). However, despite their theoretical promise, the diffusion of such systems within organizational contexts has remained surprisingly limited. Much of the existing discourse emphasizes barriers such as technical scalability, regulatory ambiguity, or economic uncertainty (Bossler et al., 2024; Rieger et al., 2019; Schellinger et al., 2021). Yet beyond these frequently cited issues, adoption is often hindered by a misalignment between the infrastructural characteristics of blockchain systems and the socio-organizational logics of enterprises.

A critical, nevertheless, unexplored friction point lies in the design assumption that transparency is inherently beneficial for trust and accountability. While this assumption may hold true for public or peer-to-peer systems, it can pose considerable risks for organizational environments where confidentiality, compliance, and selective disclosure are not optional but foundational (Bossler et al., 2024; Kannengießer et al., 2020).

Especially in highly regulated industries, the tension between structural transparency and data governance emerges as a systemic adoption barrier yet to be fully conceptualized by current research.

Despite widespread discussions of technical and regulatory barriers, implicit assumptions in blockchain infrastructures remain largely unexplored. One such assumption is that transparency inherently fosters trust and accountability. However, in enterprise settings, transparency can become a double-edged sword, particularly when sensitive data is involved. Organizations operating under strict confidentiality requirements and compliance regimes frequently find that a blockchain's structural openness conflicts with established data governance practices (Kannengießer et al., 2020). Among the various adoption hurdles, the challenge of excessive transparency in data sharing represents a particularly critical yet insufficiently examined barrier and reveals a conspicuous research gap concerning its implications for organizational blockchain adoption and the strategies required to address it (Platt et al., 2021). Although concerns around privacy and data protection have been recognized in the literature, existing research often remains focused on individual rights and personal data, while neglecting the broader architectural implications for organizational blockchain adoption (Schellinger et al., 2021). However, this addressing this privacy-preserving perspective fails to take into account the practical challenges organizations face when attempting to scale blockchain solutions beyond isolated prototypes.

Thus, current research lacks a comprehensive understanding of transparency as a cross-cutting, systemic challenge shaping both the technical and organizational dimensions of blockchain adoption (Ben-Sasson et al., 2019). In particular, little is known about how transparency concerns evolve during the design process, how they affect stakeholder alignment and governance decisions, and how they influence the viability of decentralized architectures in sensitive application domains. In order to fill this research gap, we[1] strive to reach the research objective *to investigate the challenges of organizational blockchain adoption and, in particular, why we consider excessive transparency to be one of the key reasons for the observable lack of blockchain adoption (Essay 1).*

[1] Since all essays in this dissertation emerged from collaborative research and were co-authored, the plural "*we*" is used when referring to the respective study results.

Beyond the transparency-related challenges associated with blockchain adoption, decentralized identity systems represent another foundational element in the broader landscape of decentralized information infrastructures. In particular, the emerging concept of SSI introduces a fundamentally different approach to identity management by shifting control over digital identities from centralized entities to individual users (Ehrlich et al., 2021; Sedlmeir et al., 2021). This paradigm challenges established architectural models and introduces new questions around governance, usability, and interoperability. As SSI technology matures, understanding its conceptual and architectural foundations becomes crucial for analyzing the prerequisites for decentralized system adoption in organizational contexts.

Despite its potential, SSI remains technically fragmented, with key mechanisms like VCs, digital wallets, and decentralized identifiers still under development. This technological complexity, coupled with the absence of standardized governance frameworks, leaves organizations uncertain about effective SSI implementation. Further, the integration of SSI with existing IT infrastructures and the ability to ensure trust and interoperability across different identity ecosystems remain significant challenges (Hoess et al., 2023; Sedlmeir et al., 2021). Whilst much of the current debate around SSI centers on user empowerment and privacy, its broader organizational implications, especially in terms of system design, stakeholder coordination, and institutional acceptance, are still insufficiently understood. In particular, there is a lack of clarity regarding the foundational principles of SSI architectures and how these principles translate into viable and scalable identity solutions in practice.

To fill this research gap, we strive to reach the research objective *to examine the conceptual foundations of SSI and to derive a structured understanding of the technological, organizational, and governance-related value propositions that arise when implementing decentralized identity systems (Essay 2).*

## 3.2 RG2: Develop and design decentralized systems for practical adoption

Since decentralized systems face technical, organizational, and institutional adoption barriers (Rossi et al., 2019), it becomes essential not only to understand these fundamentals and potential challenges (see RG1), but also to develop actionable design knowledge which addresses them in specific application domains. This includes

clarifying how decentralized infrastructures can be configured to account for sector-specific coordination needs, regulatory constraints, and the strategic interests of involved stakeholders. In practical terms, this means investigating not only the enabling technologies and concepts themselves, such as blockchain or SSI, but also the architectural principles, governance models, and trust mechanisms that shape their implementation. For instance, one tangible domain known as Mobility-as-a-Service (MaaS), faces substantial challenges in achieving collaboration among actors while preserving strategic autonomy.

Current MaaS platforms, often based on centralized architectures, have so far failed to attract a critical mass of mobility service providers (MSPs) prepared to integrate these solutions into their operational business strategy (Hoffmann et al., 2021). One central barrier is the inability of these platforms to adequately manage coopetition among MSPs (Köhler & Pizzol, 2020; Zhang et al., 2019). Specifically, providers are reluctant to integrate their services into platforms operated by competitors since this integration would require transferring control over customer interfaces and exposing strategic business or customer data to third parties (Hoess et al., 2021; Schulz et al., 2021). Centralized systems thus foster the risk of market concentration and lock-in effects, which fundamentally undermine the willingness of MSPs to participate and collaborate in such a network.

Decentralized solution approaches, particularly blockchain-based architectures promising neutral market access and transparent coordination, have recently been proposed as an alternative in order to break up the monopolism structures of such centralized platforms (Hoffmann et al., 2021; Jensen et al., 2019). These solutions, however, face their own limitations, especially in terms of scalability, data privacy, and the complexity of on-chain governance mechanisms (see Section 3.1). The replicated processing of transactions and the lack of granular data control conflict with regulatory requirements and providers' strategic interests. These shortcomings hinder the practical realization of decentralized MaaS ecosystems capable of balancing the need for interoperability with confidentiality and strategic autonomy (Goulding & Kamargianni, 2018).

In response to these challenges, digital wallets and SSI have increasingly gained attention as promising approaches for enabling decentralized identity and access management within MaaS ecosystems (Hoffmann et al., 2021). By allowing travelers to store and selectively share VCs such as digital tickets or driver's licenses, digital wallets

facilitate privacy-preserving interactions with MSPs (Lacity & Carmel, 2022). In contrast to blockchain-based coordination, the use of wallets and VCs may support a bilateral and modular system architecture that mitigates the need for sensitive data replication while maintaining a high degree of user control and provider independence (Kersic et al., 2023; Lacity & Carmel, 2022). Despite the growing interest in SSI for mobility contexts, research has yet to provide actionable design guidance on how such architectures should be conceptualized and implemented. In particular, little is known about the technical and organizational requirements of wallet-based MaaS systems, the design trade-offs between decentralization and manageability, and the integration of such systems into existing mobility infrastructures.

To fill this research gap, further investigation is needed to examine how decentralized identity and coordination mechanisms can support the development of interoperable, privacy-preserving, and provider-inclusive MaaS ecosystems as part of the second research goal. Building on the identified challenges of data sovereignty, stakeholder alignment, and the lack of neutral infrastructure, the analysis focuses on digital wallets and VCs as enablers of a decentralized system architecture. Thus, we ask:

*RQ 1: "What are the requirements for an IT architecture to support seamless MaaS provisioning (Essay 3)?"*

Understanding these requirements, however, is only the first step. To enable practical implementation and develop a corresponding system design, it is further necessary to explore how such requirements can be translated into concrete technical architecture. Therefore, we ask in addition:

*RQ 2: "How can these requirements be addressed through an IT architecture based on digital wallets (Essay 3)?"*

While digital wallets and SSI offer a promising foundation for decentralized identity and access management in user-centric contexts such as mobility services, the organizational adoption of decentralized architectures in competitive inter-organizational environments remains highly complex. A particularly challenging domain is supply chain management, where actors are expected both to cooperate on operational levels and compete strategically in the same markets (Ketchen et al., 2004). Supply chains are characterized by a complex interplay of cooperation and competition: while organizations must share operational data to enable coordination, they simultaneously seek

to retain control over strategically sensitive information (Brandao et al., 2025; Katsaliaki et al., 2024). This tension is particularly observable in industries such as construction, where project-based collaboration and fragmented stakeholder constellations require temporary, trust-intensive data exchange.

While blockchain technologies have been proposed to support transparency and traceability in such settings, their adoption remains limited. Particularly in data-rich processes like digital invoice exchanges, the transparent and immutable nature of blockchain often conflicts with the need to protect confidential business information—raising concerns around data exposure, compliance, and governance complexity (Fridgen et al., 2018; Sternberg et al., 2020; Treiblmaier & Beck, 2019). These limitations underline the need for more flexible, privacy-preserving architectures capable of balancing interoperability with strategic autonomy.

In light of these challenges, further research is needed to investigate how blockchain-based information systems can be designed to support coopetition in supply networks (Bengtsson & Kock, 1999; Nalebuff & Brandenburger, 1997). Thus, to fill this research gap, we ask: *"How to design a blockchain-based information system to facilitate coopetition in supply networks by fostering cooperative interactions while ensuring data confidentiality (Essay 4)?"*

## 3.3 RG3: Investigate and facilitate exploitation potentials of decentralized solutions in practice

While RG1 focused on identifying fundamentals and challenges of decentralized systems and RG2 focused on designing viable decentralized system solutions in specific domains, the third research goal shifts the perspective toward the systemic realization and exploitation of decentralized solutions on a broader scale. As decentralized technologies mature, their ability to generate sustainable impact increasingly depends on interoperability across technical layers, organizational structures, and regulatory regimes. This is particularly relevant in cross-sectoral and cross-border settings, where siloed implementations risk undermining the integrative potential of decentralized identity infrastructures.

As digital identity systems gain relevance across public and private sectors, numerous digital identity networks are emerging to meet growing demands for secure, user-centric identification solutions (Lacity & Carmel, 2022). However, their real-world

exploitation and scalability critically hinge on achieving robust interoperability across technical, organizational, and legal boundaries. Without such interoperability, the envisioned benefits of cross-sectoral and cross-border identity usage remain largely aspirational (Hodapp & Hanelt, 2022).

This challenge is particularly pressing with respect to large-scale public investments, such as the EU's European Digital Identity Wallet (EUDIW) initiative and national showcase programs, such as "Secure Digital Identities", which aim to establish interoperable SSI ecosystems as foundational infrastructures for future digital services (Federal Ministry for Economic Affairs & Energy, 2021). Whilst these efforts reflect high strategic priority, the ability to integrate diverse technological components, governance models, and stakeholder interests into functioning identity ecosystems remains a persistent barrier. Existing research often focuses on individual components, such as digital wallets or VCs (Jørgensen & Beck, 2022; Lacity & Carmel, 2022), but fails to capture the systemic, multi-level interactions that ultimately determine interoperability.

To address this complexity, research requires enhanced knowledge that can conceptualize digital identity ecosystems, particularly by examining how their various components interact within broader socio-technical systems. Understanding these interactions is crucial for identifying the underlying structures and processes that enable or hinder interoperability across multiple platforms, sectors, and jurisdictions. Moreover, a comprehensive framework is needed to analyze how governance models, legal regulations, and stakeholder dynamics influence the functioning and scalability of these ecosystems. By mapping these interdependencies, researchers can develop more effective strategies for overcoming technical, organizational, and regulatory barriers, ultimately ensuring that decentralized identity systems achieve their full potential in fostering privacy, security, and user autonomy across diverse environments (Engert et al., 2025). To fill this research gap, we follow the framework of P. Wang (2021), which conceptualizes digital infrastructures as holarchies, namely nested systems of interacting units ("holons") that function as both parts and wholes, to guide our exploration of digital identity ecosystems. Based on this approach, we ask: *"How do holon activities*

*and interactions stabilize or destabilize interoperability equilibria in digital identity ecosystems (Essay 5)?"*

Beyond structural considerations such as interoperability, the successful exploitation of decentralized identity infrastructures also hinges on the ability of implementing organizations to identify, experiment with and actualize the opportunities these systems afford (Markus & Silver, 2008). Particularly in the public sector, where institutional complexity and legacy structures often constrain innovation, the process of engaging with novel technologies requires more than mere technical readiness or regulatory alignment (Rikken et al., 2019). Successfully implementing those technologies involves a deeper organizational capacity to understand and integrate emerging system capabilities into existing services and strategic objectives. Empirical insights into how public sector organizations approach this challenge, however, remain scarce. The literature offers limited guidance on the internal mechanisms and conditions that enable organizations to move from experimentation to actualization when adopting decentralized identity solutions.

In this context, upcoming research needs to address this gap by drawing on the concept of technological affordances, which refer to the action potentials offered by technology to a particular actor in a specific context (Gibson, 1979; Leonardi, 2013) to investigate the realization of SSI in the public sector (Du et al., 2019). Understanding how these affordances are perceived, interpreted, and actualized provides valuable insight into the socio-technical dynamics of innovation processes. Based on a qualitative case study of a multi-stakeholder SSI initiative involving various German public sector actors, we identify key factors influencing how affordances are discovered and translated into organizational practice. To fill this research gap, we ask:

*RQ 1: "Which affordances does SSI offer within an organizational setting (Essay 6)?"*

Identifying these affordances is a necessary first step. However, to support meaningful organizational innovation, it is equally important to understand how public sector entities can move beyond initial recognition toward practical experimentation and the

actualization of such affordances within their institutional and operational contexts. Thus, we additionally ask:

*RQ 2: "How can the public sector experiment with and actualize the SSI affordances (Essay 6)?"*

Building on the preceding analysis of public sector engagement with decentralized infrastructures, this dissertation concludes the third research goal by shifting perspective to the role of private organizations in emerging monetary ecosystems. In particular, it examines how companies can actively shape and contribute to the development of CBDC ecosystems an area thus far dominated by central banks, regulators, and macroeconomic discourse. Whilst CBDCs are commonly framed as public infrastructures aimed at strengthening monetary sovereignty (Atlantic Council, 2024; Auer et al., 2020), ensuring financial inclusion, or addressing risks of privately issued stablecoins, their effective implementation also depends on contributions from the private sector. These contributions are not limited to distribution or wallet provision but span a wide range of potential services and infrastructures which complement and enhance the core functionalities of a CBDC system.

Driven by pilot implementations and strategic initiatives by central banks worldwide, the role of private-sector actors in CBDC ecosystems—such as banks, wallet providers, and infrastructure operators—is gaining strategic relevance (BIS, 2021; European Central Bank, 2022; World Bank, 2022). Most existing studies focus on the implications of CBDCs for banks or payment providers (Sethaput & Innet, 2023; Y.-R. Wang et al., 2022), often framing them as passive adopters or potential competitors (Chen et al., 2024). However, a growing body of literature and emerging academic work suggests that companies can actively develop complementary value propositions to make CBDC ecosystems more robust, accessible, and innovative (Bank of England, 2020; Gupta et al., 2023; Leinonen, 2023). These include services related to identity and compliance management, privacy-preserving analytics, programmable payment solutions, end-user interface design, and infrastructure interoperability (Kiff et al., 2020).

To systematically investigate the role of private-sector engagement in CBDC ecosystems, further research is needed to synthesize insights from both academic literature

and practical sources in order to develop a comprehensive understanding of the topic. To fill this research gap, we ask:

*"What value propositions can companies offer in the context of a CBDC ecosystem and which needs do they fulfill (Essay 7)?"*

# 4 Research designs

This section outlines the methodological frameworks employed across the seven essays, highlighting their alignment with the overarching research objectives and guiding research questions. Additionally, it provides a detailed account of the specific research methodologies, data collection procedures, and analytical techniques utilized, thereby ensuring the rigor and validity of the research findings. Table 2 provides a summary of the selected research designs.

Table 2 Overview of research designs

| Title | Research design | Core contribution |
|---|---|---|
| **Essay 1:** The transparency challenge of blockchain in organizations | Conceptual analysis | Identifies excessive transparency risks of blockchain systems highlighting trade-offs between efficiency and confidentiality |
| **Essay 2:** Self-sovereign identities and digital wallets | Conceptual analysis and structured literature review | Establishes a conceptual fundamental for wallet-based SSI identity models for individuals and organizations |
| **Essay 3:** Toward seamless mobility-as-a-service: Providing multimodal mobility through digital wallets | Design Science Research | Develops a wallet-based decentralized IT architecture enabling seamless and privacy-preserving MaaS provisioning |
| **Essay 4:** Striking a balance: Designing a blockchain-based solution to navigate coopetition dynamics in supply chain management | Design Science Research | Designs a blockchain-based solution architecture for managing coopetition and safeguarding sensitive business data within the construction industry |
| **Essay 5:** Interoperability in digital identity ecosystems | Embedded single-case study | Develops a multilevel, holarchic framework for understanding and managing interoperability dynamics in decentralized digital identity ecosystems by identifying the sociotechnical mechanisms that stabilize or destabilize interoperability equilibria over time. |
| **Essay 6:** Self-sovereign identity in the public sector: Affordances, experimentation, and actualization | Embedded single-case study | Identifies public sector-specific SSI affordances and provides an innovation framework for public institutions |
| **Essay 7:** Capturing value propositions for private organizations in CBDC ecosystems | Multivocal literature review | Synthesizes value propositions for private actors in emerging CBDC ecosystems and their role in ecosystem formation |

## 4.1 Research designs within RG1

Within RG1, **Essay 1** explores the challenges of excessive transparency in organizational blockchain applications through a conceptual research approach. Given the limited empirical diffusion of blockchain systems in practice and the emerging but fragmented academic discourse, we chose to structure our investigation as a position paper. This format allows for a literature-based exploration of the topic while aiming to synthesize dispersed insights and provide guidance for both scholars and practitioners (Electronic Markets, 2025; Hertzmann, 2023).

We began by conducting a literature review across major information systems and computer science databases to identify prevailing assumptions and underexplored risks associated with transparency in blockchain systems (Kannengießer et al., 2020). In particular, we analyzed technological features such as replicated transaction processing and the immutability of data storage, which are often seen as enablers of trust but which may, in practice, inadvertently expose sensitive information within various sectors such as healthcare, supply chain, energy or the public sector. Building on this literature foundation, we developed a pattern-based analytical framework to categorize types of blockchain applications according to their data exposure characteristics. We integrated findings from sixteen literature-based blockchain implementation projects in sectors such as mobility, energy, and public administration (Andoni et al., 2019; Jensen et al., 2019; Mattke et al., 2019; Rieger et al., 2019). Drawing on this experiential base, we identified recurring concerns voiced by stakeholders regarding data protection, privacy, and strategic information control. To enrich our conceptual analysis, we reviewed relevant legal and regulatory frameworks, particularly the GDPR, and technological approaches such as permissioned blockchains, SSI and privacy-enhancing technologies (e.g., ZKPs). These components were analyzed as potential mitigators of transparency-related challenges. The essay thus serves as a theoretical foundation for further empirical and design-oriented research on balancing challenges of transparency and confidentiality in decentralized systems for practical diffusion.

In **Essay 2**, we adopted a conceptual research approach to explore SSI as a fundamental paradigm for wallet-based identity management. Given the fragmented and often technologically driven discourse surrounding SSI, this essay aims to provide a structured theoretical grounding by synthesizing current literature, institutional developments, and architectural considerations systematically. To this end, we conducted a

systematic literature review following Webster and Watson (2002) spanning the domains of identity management, cryptography, and decentralized information systems. Using the search string ("self-sovereign identity" OR "self-sovereign identities" OR ("wallet" AND "identity") OR ("wallet" AND "identities") OR "verifiable credential" OR "verifiable credentials" OR "decentralized identity" OR "decentralized identities"), we queried three academic databases (AISeL, Web of Science and ScienceDirect) for the period until January 2025. The initial search yielded 1,269 articles which were reduced to 1,173 – following the removal of duplicates. As a next step, we conducted a screening based on title (271), abstract (108), and full text. We complemented the sample with forward and backward searches and manual additions, resulting in a final corpus of 62 articles. On the basis of literature, we derived the core value propositions of self-sovereign identity within the issuer–holder–verifier trust triangle.

Our review included academic contributions and partially relevant regulatory and policy documents, such as the European Union's eIDAS 2.0 regulation and the proposed EUDIW. By mapping the evolution from siloed and federated identity systems toward decentralized, user-centric architectures, as also described by Rieger et al. (2024), we established a clear conceptual basis for understanding the unique characteristics and transformative potential of SSI. We analyzed how technological components such as VCs, digital wallets, and verifiable data registries enable secure, interoperable, and privacy-preserving identity interactions. Particular emphasis was placed on mechanisms such as selective disclosure and ZKPs which support data minimization and user sovereignty (Abraham et al., 2021). Following our analysis, we identified and categorized the value propositions offered by SSI to its key stakeholders. By doing so, we demonstrated how SSI can contribute to trust, efficiency, and data control in both business-to-consumer (B2C) and business-to-business (B2B) contexts.

## 4.2 Research designs within RG2

In relation to RG2, Essays 3 and 4 adopt a design science research (DSR) methodology following Peffers et al. (2007) for the development of emerging decentralized systems. This methodological lens is particularly appropriate for tackling complex challenges in the information systems research domain by means of iterative cycles of artifact construction and evaluation (Baskerville et al., 2018; vom Brocke et al., 2020). The resulting artifacts, which may take the form of conceptual constructs, design models,

procedural methods or technological implementations, are intended to contribute to both theoretical understanding and practical application (March & Storey, 2008).

In ***Essay 3***, we followed the DSR methodology as proposed by Peffers et al. (2007) to develop and evaluate a wallet-based IT architecture for enabling seamless MaaS provisioning. This approach supports the systematic development of relevant IT artifacts through iterative build-and-evaluate cycles, addressing the complex socio-technical challenges of decentralized service ecosystems (vom Brocke et al., 2020).

We initiated our research by identifying core problems in the current MaaS landscape, particularly the lack of interoperability, the risk of market power concentration, and the absence of trust-preserving mechanisms for handling sensitive data between competing MSPs. To derive design objectives and requirements, we conducted an SLR following Webster and Watson (2002) across seven major academic databases. Our initial search yielded 2,165 results, from which we screened 2,051 articles after removing duplicates. Applying a four-stage filtering process, we identified 14 relevant publications to inform our conceptual foundation. Recognizing limitations in the literature, particularly the lack of business and implementation perspectives, we complemented the SLR with 17 ex-ante expert interviews, each lasting an average of 51 minutes, totaling approximately 867 minutes of recorded material (Myers & Newman, 2007). We analyzed the transcripts using open and axial coding to derive four design objectives and nine detailed requirements for seamless, privacy-preserving, and cooperative MaaS architectures (Corbin & Strauss, 2015; Saldana, 2021). Based on these insights, we iteratively designed and instantiated an SSI-based IT architecture following the structure of Kruchten (1995), including a prototype wallet application for ticket issuance and verification. We then conducted a criteria-based qualitative evaluation involving seven ex-post expert interviews with practitioners from OEMs, IT providers, and mobility operators, totaling approximately 406 minutes of interview time (average of approximately 58 minutes per interview) (Venable et al., 2016). The evaluation combined a live prototype demonstration with structured discussions to assess the artifact's feasibility, utility, and alignment with the identified requirements. To analyze the data, we applied a two-cycle coding process: first, provisional coding aligned with the predefined requirements, followed by axial coding to surface underlying design mechanisms (Saldana, 2021). These evaluations informed refinements to the artifact and supported the derivation of three nascent design principles for SSI-based MaaS systems. These

principles highlight the need for hybrid architectures combining centralized and decentralized elements to balance cooperation and competition among MSPs. By combining rigorous literature synthesis, in-depth expert input, and artifact evaluation, this essay contributes actionable design knowledge and architectural guidance for the development of privacy-aware, interoperable MaaS solutions using digital wallets.

In ***Essay 4,*** we also employed the DSR methodology as outlined by Peffers et al. (2007) to develop and evaluate a blockchain-based IT architecture to support coopetition dynamics in supply chain management. The DSR process enabled us to iteratively construct and refine a decentralized solution to address the trade-off between cooperation benefits and the need to protect sensitive business information, particularly in the construction industry, which is characterized by project-based supply chains and strong competitive interdependencies.

We began by identifying the core problem of centralized platform dominance and the associated risk of strategic data disclosure, which hinders collaboration among direct competitors. To establish a robust conceptual foundation, we conducted an SLR following Webster and Watson (2002) across seven academic databases using a defined search string. The initial search yielded 677 articles, which we filtered through title, abstract, and full-text screening, as well as forward and backward searches, ultimately resulting in a final set of 23 peer-reviewed publications relevant to blockchain-enabled coopetition in supply chain contexts. From this literature base, we applied a three-phase coding process including open, axial, and selective coding following Corbin and Strauss (2015) and Saldana (2021) to derive eight overarching design objectives. These comprise data protection, accountability, decentralization, performance, interoperability, traceability, transparency, and automation. These objectives guided the design of our decentralized delivery invoice system architecture, conceptualized through the 4+1 architectural view model, which structures system architecture through multiple interrelated perspectives and supporting use-case scenarios (Kruchten, 1995), with a specific focus on the process and physical views.

To evaluate our design artifact, we conducted nine ex-post expert interviews with professionals from the blockchain and construction domains. Each interview was semi-structured and accompanied by a live demonstration of the prototype, resulting in a total of 469 recorded minutes (average of 52 minutes per interview). The evaluation followed the Framework for Evaluation in Design Science (FEDs) proposed by Venable

et al. (2016), applying both formative and summative elements. We assessed the artifact's feasibility, utility, and alignment with the derived design objectives. Data from the interviews were analyzed through a two-cycle coding approach, including provisional coding based on the predefined design objectives and axial coding to identify architectural design mechanisms. Based on these analyses, we derived three implementation guidelines which outline when to adopt decentralized systems, how to protect inter-organizational data exchanges through private channels and data collections, and how to enhance confidentiality via privacy-preserving technologies such as ZKPs. By integrating theoretical insights, stakeholder input, and architectural design in a coopetitive supply chain setting, this essay contributes prescriptive knowledge concerning the way in which decentralized information systems can be configured to manage sensitive data while enabling collaboration among competitors.

## 4.3 Research designs within RG3

The third research goal addresses the practical realization of decentralized information systems by exploring how such systems can be successfully structured and governed in complex multi-actor environments. Whilst earlier essays focused on technological adoption mechanisms and design, this part of the dissertation shifts the analytical lens towards the conditions under which decentralized systems, particularly those concerned with digital identity, can be effectively orchestrated across organizational and ecosystem boundaries.

In **Essay 5**, we adopted a theory-building, embedded single-case study approach following Yin (2018) to explore the interoperability dynamics in digital identity ecosystems. Drawing on the information ecology theory of digital innovation ecosystems (P. Wang, 2021), we investigated how multi-layered interactions between ecosystem actors affect the stabilization or destabilization of interoperability as a key requirement for the sustainable development of decentralized identity solutions. This methodological approach is particularly well-suited for capturing the complex and evolving nature of digital identity ecosystems by enabling an in-depth analysis of interactions across individual, organizational, and systemic levels (Eisenhardt, 1989; Meredith, 1998).

Our case study centers on Germany's *Secure Digital Identities* showcase program, one of the most prominent national initiatives to establish a digital identity infrastructure aligned with eIDAS 2.0. We collected and triangulated data from six qualitative

sources, including public documents (226 pages), internal documentation (123 pages and 138 slides), social media data (610 tweets and 319 LinkedIn posts), audiovisual materials (18 hours and 11 minutes), and 16 documents of field notes. The primary data source consisted of 24 semi-structured expert interviews conducted between June 2021 and March 2024, totaling 16 hours and 40 minutes of interview recordings and more than 920,000 transcribed characters.

Our analytical process followed a structured four-phase coding approach (Saldana, 2021). In Phase 1, we performed open coding to derive part-whole relationships, leading to a preliminary holarchy of the showcase program. In subsequent phases, we iteratively developed second-order themes based on innovation tasks, such as negotiating, integrating, or standardizing interactions (Gioia et al., 2013). To ensure analytical rigor and internal validity, we conducted peer debriefings, triangulated across multiple data types, and applied theory-driven categorization in alignment with the P. Wang (2021) holarchy model. In this regard, we conceptualized the ecosystem as composed of "holons", which embody self-contained subsystems that also function as parts of broader structures. Our embedded units of analysis included four showcase projects (IDunion, ID-Ideal, ONCE, SDIKA), associated work packages, organizations, and use cases (Federal Ministry for Economic Affairs & Energy, 2021). The resulting holarchy model enabled us to analyze systematically how ecosystem-wide decisions about interoperability emerge through iterative negotiation, harmonization, and standardization across ecosystem levels. Our contribution is a theory-informed framework that conceptualizes interoperability as a dynamic outcome of recursive multi-level interactions. By mapping innovation tasks and stakeholder roles across holonic layers, we offer theoretical and practical guidance for designing decentralized identity ecosystems and inform future research and policy.

In **Essay 6**, we adopted a single-case study methodology informed by the Affordance-Experimentation-Actualization (A-E-A) (Du et al., 2019) to explore how public sector organizations engage with SSI as an emerging digital identity paradigm (Eisenhardt, 1989; Yin, 2018). This approach enabled us to investigate the socio-technical dynamics of innovation in a real-world public administration context, with particular attention given to the iterative nature of experimentation and organizational learning.

The case study focused on a tax authority's applied research project aiming to prototype an SSI-based identity and tax registration process for online marketplaces. Over

a six-month period, we gathered qualitative data from five different sources, comprising semi-structured expert interviews, project documentation, archival records, direct observations, and technical artifacts. Our primary data consisted of 10 in-depth expert interviews conducted with stakeholders from public administration, IT service providers, and research institutions. The interviews were conducted at the end of the project and supplemented with follow-up communications. In total, we recorded approximately 590 minutes of interview material. We triangulated this data with over 300 pages of internal documentation, project presentations, technical implementation records, and observations from 20 formal and informal meetings.

For data analysis, we followed a structured three-phase coding procedure inspired by Corbin and Strauss (2015) and Saldana (2021) consisting of open, axial, and selective coding. In the first phase, two researchers independently coded the data to identify activities related to affordance discovery, experimentation, and actualization. During axial coding, first-order codes were grouped into second-order themes. A series of coding workshops ensured inter-coder reliability and theoretical alignment. In the final stage, we mapped relationships between themes and phases of the A-E-A framework to trace how affordances emerged and were actualized following Gioia et al. (2013). Furthermore, we documented six distinct experimentation activities, including conceptual exploration of identity processes, adaptation of technical frameworks to legal constraints, and mitigation of technical and organizational barriers. These experimentation phases improved the organization's technical, political, and cultural readiness for SSI adoption. By capturing the interplay between emerging digital identity technologies and institutional constraints, the essay contributes an affordance-based innovation framework tailored to public sector contexts. This framework elucidates how public agencies can discover and realize the value of SSI through structured experimentation, stakeholder alignment, and iterative learning processes.

Finally, in **Essay 7**, we conducted a multivocal literature review (MLR) following the methodological guidance of Garousi et al. (2019) to investigate the value propositions that private companies can offer within emerging CBDC ecosystem rollouts. This approach was particularly suited to our research goal, as it enabled us to systematically synthesize insights from both academic (white) and practitioner (grey) literature, thereby capturing a more holistic view of an emergent and rapidly evolving topic situated at the intersection of finance, technology, and policy.

We began by formulating a comprehensive search string based on an initial scoping review and keyword extraction, which we applied across four major academic databases (AIS eLibrary, ScienceDirect, Scopus, and Web of Science) and supplemented with a structured Google Scholar search for grey literature. Our database search returned 1,134 records, from which we removed 326 duplicates. The remaining 808 items were screened in four phases including title, abstract, full-text, and a forward/backward citation search which resulted in a final dataset of 52 publications: 39 white literature and 13 grey literature items. To ensure rigor, we applied inclusion and exclusion criteria, screened all grey literature using a 17-point quality assessment, and applied a literature saturation criterion during grey literature collection. Notably, grey literature from institutions such as the BIS Innovation Hub and various central banks added depth to the evolving discourse on CBDCs. Each publication was analyzed through qualitative coding and categorized into two non-exclusive groups: (1) value propositions explicitly mentioned in 22 sources and (2) value propositions derived from unmet needs identified in 43 sources.

The final set of value propositions was structured into four overarching categories: (1) accessibility and usability, (2) financial infrastructure, (3) regulatory compliance and onboarding, and (4) operations and support services. These were matched against corresponding ecosystem needs, which we extracted and organized in parallel to the coded propositions. Where gaps were identified between existing needs and documented propositions, we derived additional conceptual value propositions, such as cybersecurity solutions, audit and reporting mechanisms, and end-user incentivization strategies. By adopting a multivocal and inductive approach, this essay contributes a comprehensive synthesis of how private organizations can create value in a CBDC ecosystem rollout. The results not only systematize existing knowledge but also serve as a foundation for developing business models and guiding further empirical research into the evolving CBDC landscape.

# 5 Summary of the results

The following section synthesizes insights from the seven essays, which investigate how persistent adoption challenges can be overcome, how emerging decentralized systems can be effectively designed and managed, and, ultimately and above all, how to cope with adoption dynamics as challenge to be overcome to facilitate the successful diffusion into practice.

## 5.1 Essay 1: The transparency challenge of blockchain in organizations

In Essay 1, we investigated at a conceptual level how excessive transparency in blockchain-based organizational systems can hinder adoption and diffusion in practice. Our analysis was grounded in the assumption that technological features such as immutable data storage and replicated transaction processing, while commonly framed as sources of trust, can create unintended risks when sensitive data becomes broadly visible across organizational boundaries (Kannengießer et al., 2020).

To understand the practical implications of this tension, we synthesize insights from more than sixteen real-world blockchain implementation projects across sectors including energy, mobility, and public administration (Andoni et al., 2019; Mattke et al., 2019; Rieger et al., 2019; Shi et al., 2020; Warkentin & Orgeron, 2020). Drawing from this empirical base, we identify recurring stakeholder concerns regarding data protection, strategic control, and compliance with regulatory frameworks (Sternberg et al., 2020). These concerns are particularly relevant in inter-organizational contexts where transaction visibility may lead to competitive disadvantages or legal vulnerabilities (Kannengießer et al., 2020; Platt et al., 2021)

As a result, we categorize blockchain application types according to their respective data exposure profiles. Our analysis reveals that across various use cases considering token transfers, process automation, and verifiable data exchange, a persistent trade-off exists between the benefits of transparency and the need for data confidentiality. Even in permissioned blockchain systems, where access is restricted to a defined set of actors, data replication and process automation often reintroduce exposure risks (Toufaily et al., 2021). In response, we explore three categories of solution approaches: First, permissioned blockchains can help limit access and control consensus participation as they require robust governance and may hinder interoperability (Sedlmeir,

Wagner, et al., 2022). Second, SSI systems offer mechanisms for bilateral and verifiable data exchange that minimize on-chain data exposure (Sedlmeir et al., 2021). Third, privacy-preserving technologies such as ZKPs enable validation without disclosure while, however, technical and organizational barriers remain (Ben-Sasson et al., 2019; Bootle et al., 2020).

Through this synthesis, we contribute a nuanced understanding of transparency as a context-sensitive design challenge rather than a universally desirable property. By positioning excessive data transparency as a central barrier to the diffusion of blockchain systems in practice, the essay offers conceptual foundations and design considerations for both scholars and practitioners aiming to develop privacy-aware decentralized information systems.

## 5.2 Essay 2: Self-Sovereign Identity and digital wallets

In Essay 2, we investigate the foundational value propositions of SSI systems and their role in shaping future digital identity ecosystems. Against the backdrop of fragmented identity management solutions and increasing demands for privacy, portability, and user-centricity (Franz & Benlian, 2022; Pfitzmann & Hansen, 2010), we synthesize fragmented insights into a coherent theoretical foundation. The essay contributes to the understanding of SSI not merely as a technical innovation but as a paradigm shift in digital identity management (Sedlmeir et al., 2021).

We conduct a systematic literature review following Webster and Watson (2002) to identify key limitations of current identity models and derive core SSI components—VCs, wallets, and registries—analyzed through the trust triangle of issuers, holders, and verifiers (Čučko et al., 2022; Sedlmeir et al., 2021). In particular, we analyze how SSI enables selective disclosure, privacy-preserving verification, and cryptographically assured data integrity (Babel & Sedlmeir, 2023; Ben-Sasson et al., 2019). Drawing on recent research and implementation projects such as the EUDIW (Schwalm et al., 2022), we articulate distinct value propositions for each actor group: efficiency and risk reduction for issuers, data control and usability for holders, and verifiability, cost reduction, and (regulatory) compliance for verifiers.

Our contributions position SSI as an enabler of trusted, decentralized digital identity interactions, while acknowledging the socio-technical and organizational challenges

that hinder widespread adoption. These include the need for standardization, governance mechanisms and balanced incentive structures across the ecosystem. By systematically mapping the potentials and limitations of SSI, this essay provides a theoretical basis for future empirical studies and design-oriented research on identity systems in electronic markets.

## 5.3 Essay 3: Toward seamless mobility-as-a-service: Providing multimodal mobility through digital wallets

In Essay 3, we adopt a rigorous DSR approach in order to develop and evaluate an SSI-based IT architecture that enables seamless provisioning of MaaS through digital wallets (Peffers et al., 2007). The research objective of this architecture is to reconcile the coopetitive tensions between MSPs by facilitating decentralized and privacy-preserving interactions without requiring the disclosure of sensitive strategic business data or customer interfaces to centralized intermediaries (Ritala, 2022; Smichowski Carballa, 2018). By instantiating a functional prototype, conducting an SLR (Webster & Watson, 2002), and expert interviews (Myers & Newman, 2007), we demonstrate how digital wallets can serve as a foundational enabler for modular, interoperable, and user-centric MaaS ecosystems. In this context, we make three main contributions to the existing knowledge base:

First, we design a decentralized MaaS architecture as the design science core contribution to empower travelers to seamlessly discover, book, and verify multimodal mobility services via their digital wallet within a decentralized system. The conceptual architecture enables bilateral credential exchange between travelers and MSPs and introduces a modular routing service which can be implemented by any MSP. This approach fosters open competition while avoiding platform lock-in and maintaining data sovereignty for all stakeholders (Hoffmann et al., 2021).

Second, and based on our design, we derive three design principles to inform the development of decentralized and wallet-based identity management infrastructures in coopetitive service markets: (1) separate coordination and exchange of general service information from the exchange of personal or sensitive business data, (2) coordinate general service information through multiple competing service aggregator applications, and (3) use digital wallets for the secure and efficient exchange of verifiable personal data (Hoess et al., 2024). These principles reflect a hybrid design paradigm that

integrating centralized and decentralized components to enable scalable, trustworthy, and interoperable seamless mobility services.

Third, we demonstrate how identity management via digital wallets can address the limitations of blockchain-based MaaS infrastructures (Jørgensen & Beck, 2022; Lacity & Carmel, 2022). In particular, our findings illustrate that SSI enables verifiable yet disintermediated service provisioning, allowing MSPs to remain independent while still contributing to integrated traveler experiences. By decoupling credential issuance and verification from booking logic, our architecture mitigates coordination problems and reduces the risk of market power concentration. At the same time, travelers benefit from improved onboarding, selective identity disclosure, and consistent user experience across multiple services.

Taken together, these contributions advance the discourse on decentralized identity management and service orchestration in the mobility domain. By demonstrating a privacy-preserving, modular, and technically feasible approach to seamless MaaS provisioning, this research offers actionable design knowledge for both academia and practice. The proposed architecture not only resolves key tensions between cooperation and competition but also lays a robust foundation for future MaaS infrastructures prioritizing interoperability, user empowerment, and equitable market participation.

## 5.4 Essay 4: Striking a balance: Designing a blockchain-based solution to navigate coopetition dynamics in supply chain management

In Essay 4, we also apply a rigorous DSR approach to develop and evaluate a blockchain-based information system that enables secure, decentralized processing of digital delivery invoices in the construction industry (Peffers et al., 2007). The proposed system addresses the coopetitive tension between data transparency and confidentiality by facilitating collaboration through verifiable automation while safeguarding sensitive business information from competitive exploitation (Lautenschlager et al., 2023). To that end, we synthesize insights from a systematic literature review, derive design objectives, and instantiate a functional prototype evaluated through expert interviews. Thus, we contribute to the existing knowledge base in three significant ways:

First, we derive eight design objectives for coopetition-aware information systems in supply chains: data protection, accountability, decentralization, performance, interoperability, traceability, transparency, and automation. These objectives collectively

ground our solution approach which advocates the integration principle of coopetition theory and inform the development of digital infrastructures necessary to balance competitive and cooperative concerns (Bengtsson & Kock, 2000; Fernandez & Chiambaretto, 2016). Our artifact demonstrates how these objectives can be instantiated through technical features, such as identity management, privacy-preserving invoice routing and blockchain-based process governance.

Second, we design a decentralized blockchain architecture tailored to the dynamics of construction supply chains, which supports secure and automated invoice processing without central intermediaries (Bagni et al., 2024). The architecture leverages permissioned blockchain features such as private channels, data collections, and role-based access control within Hyperledger Fabric to ensure traceability and accountability while maintaining granular data privacy (Zhong et al., 2020). Through its modular backend and frontend components, the solution accommodates diverse organizational requirements, thereby enabling interoperability and process customization for stakeholders of different sizes and technological maturity (Guggenberger et al., 2022).

Third, we synthesize our design and evaluation findings into three implementation guidelines for practitioners. These guidelines recommend (1) opting for a decentralized solution when the benefits of leveraging network effects in a coopetitive market surpass the complexities and challenges of its implementation, (2) utilizing private data collections and private channels to protect inter-organizational data exchanges from unauthorized third-party access, and (3) enhancing private data collections and channels with additional privacy-preserving technologies to ensure complete data confidentiality. In doing so, we respond to persistent barriers to blockchain adoption—particularly data disclosure concerns—and propose actionable pathways to foster trust, compliance, and efficiency in digital supply chain ecosystems (Platt et al., 2021; Troncoso et al., 2017).

Together, these contributions advance the design and implementation of blockchain-based systems for supply chain automation by integrating coopetition theory with privacy-enhancing system design. Our research provides theoretically grounded and practically relevant design knowledge which supports decentralized collaboration whilst at the same time mitigating the risks of information asymmetry, market monopolization, and legal non-compliance.

## 5.5 Essay 5: Interoperability in digital identity ecosystems

In Essay 5, we examine the dynamics of interoperability in digital identity ecosystems by applying the information ecology theory to a large-scale public sector initiative in Germany. Conceptualizing digital identity ecosystems as holarchically structured systems (Engert et al., 2025; P. Wang, 2021), we investigate how part-whole relationships, interactions among actors, and temporal dynamics contribute to the stabilization or destabilization of interoperability over time (Hanseth & Lyytinen, 2010). Our empirical findings reveal that interoperability is not a static, technically determined feature but a continuously negotiated outcome of socio-technical interactions between diverse stakeholders across ecosystem levels. Using an embedded single-case study (Yin, 2018), we identify a range of mechanisms, such as harmonization, negotiation, integration, and adaptation shaping the conditions under which interoperability emerges and evolves in practice.

This essay advances the information ecology theory by adapting it to the specific characteristics of digital identity ecosystems. We demonstrate that these ecosystems are inherently polycentric, lacking a central coordinating entity, and thus require decentralized governance structures and bottom-up coordination to achieve sustained interoperability. We contribute to the theoretical discourse by introducing a multi-level framework which conceptualizes digital identity ecosystems, according Rieger et al. (2024), and interoperability within those ecosystems as a dynamic socio-technical equilibrium shaped by ongoing holon activities and interactions. Furthermore, we extend existing research on ecosystem governance (Hanseth & Lyytinen, 2010), by illustrating how interoperability equilibria depend not only on technical standardization but also on the alignment of regulatory, organizational, and strategic logics. By embedding interoperability within the broader theoretical constructs of holarchies and part-whole interactions, we offer a novel lens for analyzing decentralized innovation ecosystems beyond the context of digital identities (Gasser, 2015).

In practical terms, the study provides actionable guidance for policymakers, ecosystem designers, and practitioners involved in the development and orchestration of digital identity infrastructures. We show that interoperability can be supported through multi-stakeholder coordination practices, cross-ecosystem knowledge exchange, and the alignment of governance mechanisms. Our findings underscore the need to actively manage the tensions between both decentralization and harmonization, innovation

and standardization, and to foster scalable and resilient digital identity ecosystems. By revealing how interoperability is enacted in practice through iterative interaction and co-development, this essay contributes to the design and governance of ecosystem architectures which are both adaptable and inclusive. In sum, we offer both theoretical and empirical foundations for understanding interoperability as a dynamic and situated phenomenon in complex socio-technical systems.

## 5.6 Essay 6: Self-Sovereign Identity in the public sector: Affordances, experimentation, and actualization

Essay 6 investigates how public sector organizations can successfully innovate with SSI by examining a real-world implementation project in the context of tax registration processes. Grounded in the A-E-A theory (Du et al., 2019), the study provides an in-depth review of how organizational actors engage with emerging digital identity technologies through iterative experimentation and contextual adaptation. The case reveals four organizational-level affordances of SSI: (1) Organizations can issue signed identity documents using a decentralized PKI, (2) the identity holder can verifiably present identity independent from the identity provider, (3) the identity holder can selectively combine properties from certificates issued by different issuers, and (4) verifiers can prove that they received a verifiable presentation.

The study extends the A-E-A framework by detailing how experimentation activities, including conceptual exploration, adaptation to legal frameworks, and constraint mitigation, increase an organization's technical, political, and cultural readiness to actualize the potential of SSI (Hong et al., 2022; Kankanhalli et al., 2017). This procedural understanding advances affordance theory in the context of emerging technologies and demonstrates its relevance for public sector innovation. Furthermore, the study contributes to the SSI literature by highlighting not only technical capabilities but also the socio-organizational shifts required for successful adoption, including changes in perceptions of data sovereignty, trust, and responsibility. Importantly, it uncovers an underexplored capability of SSI in public sector contexts which is crucial in audit-heavy domains such as tax administration (Goh & Arenas, 2020).

In practical terms, the essay provides actionable insights for public managers and system designers seeking to implement SSI in government services. It demonstrates that successful implementation depends on aligning emerging technologies with legal

requirements and addressing organizational and cultural barriers through structured experimentation. The developed enterprise agents and the adaptation of verification flows illustrate the necessity of tailoring SSI infrastructures to the operational realities of public institutions. Moreover, the study emphasizes the importance of interoperability and standards to ensure that SSI systems can scale and function across administrative and jurisdictional boundaries (Meijer, 2015). In summary, Essay 6 offers both conceptual clarity and empirical grounding for understanding how decentralized digital identity solutions can be effectively developed and managed in public sector contexts.

## 5.7 Essay 7: A multivocal literature review on capturing value propositions for private organizations in a CBDC ecosystem

Essay 7 explores the value propositions private organizations can offer within CBDC ecosystems by conducting an MLR (Garousi et al., 2019). We thus integrate insights from both academic (white) and industry (grey) literature to develop a holistic understanding of private sector VPs. In this context, we explore the emergence of CBDCs as a transformative development in the financial system which can integrate elements of traditional banking with innovations from DeFi and FinTech. By examining both explicit value propositions from literature and those derived from unmet ecosystem needs, the study contributes to the evolving discourse on the ability of private organizations to facilitate the implementation and adoption of CBDCs.

Essay 7 extends the current literature on digital currencies, FinTech, and decentralized finance by proposing a structured framework of four overarching categories of value propositions: accessibility and usability, financial infrastructure, regulatory compliance and onboarding, and operations and support services (Gramlich et al., 2023). This categorization serves as a conceptual scaffold to promote an understanding of how companies can align their offerings with key ecosystem needs. The study also identifies previously underexplored areas such as cybersecurity, auditability, and incentivization strategies, thereby broadening the scope of CBDC-related value creation beyond commonly discussed topics. Furthermore, by integrating value propositions derived from general CBDC ecosystem needs, the essay extends the business model ontology of Osterwalder and Pigneur (2010) and emphasizes the foundational role of value propositions in designing viable business models for CBDC adoption.

The essay provides practical, actionable insights for both policymakers and private actors. It identifies specific opportunities for organizations to deliver technological solutions, such as CBDC wallets, identity-linked infrastructure, privacy-enhancing technologies, and AML/CFT compliance systems. Additionally, it highlights support services such as user education, consultancy, and customer onboarding which can ease the transition toward CBDC use. These insights are critical for fostering collaboration between central banks and private firms, ensuring that CBDC systems are not only technically viable but also socially and economically embedded. By surfacing and synthesizing concrete service areas and business opportunities, the essay supports the development of sustainable and innovative business models in an emerging digital monetary ecosystem.

# 6 Discussion and conclusion

To conclude the introduction of my dissertation, I will now summarize the outlined contents, reflect on the contributions to theory and the implications for practice, identify the limitations of my research, and propose avenues for further research.

## 6.1 Summary

In this dissertation, I contribute to the investigation of how emerging decentralized information systems can be designed and managed to cope with adoption dynamics in practice. To address this overarching question, I define three research goals: RG1 focuses on identifying and understanding potentials and challenges for implementing decentralized systems in organizations. RG2 aims to develop and design solution approaches that support the adoption of decentralized systems in practical contexts. RG3 seeks to investigate and successfully exploit decentralized solutions in real-world ecosystems.

To explore these goals, the dissertation builds on a series of seven individual research essays, applying a range of research methods including conceptual analysis, systematic literature reviews, design science research, and embedded single-case studies. These methods enable a multi-faceted examination of the design, implementation, and governance of decentralized information systems. Addressing RG 1, Essay 1 explores how excessive transparency in blockchain systems can undermine adoption by exposing sensitive organizational data and proposes design implications for balancing transparency and confidentiality. Essay 2 develops a conceptual foundation for SSI by outlining stakeholder-specific value propositions in SSI-based digital identity ecosystems. Moreover, Essays 3 and 4 contribute to RG2 by applying a DSR approach to develop and evaluate decentralized architectures in mobility and supply chain domains. Essay 3 presents a wallet-based architecture for privacy-preserving seamless MaaS while Essay 4 introduces a blockchain-based solution to enable secure and selective data exchange in coopetitive supply networks in the context of the exchange of delivery invoices within the construction industry. Finally, Essays 5, 6, and 7 contribute to RG3. Essay 5 conceptualizes interoperability stabilized or destabilized interactions in digital identity ecosystems as a dynamic, multi-level process shaped by stakeholder alignment and institutional coordination. Essay 6 investigates how public sector organizations engage

with SSI through affordance-based experimentation and actualization processes. Essay 7 synthesizes the value propositions that private organizations can offer in emerging CBDC ecosystems and highlights their strategic roles in ecosystem formation.

## 6.2 Theoretical, empirical, and artefactual contributions

In the seven essays comprising this cumulative dissertation, I explore how emerging decentralized information systems can be designed and managed to cope with adoption dynamics in practice. By investigating the interplay of socio-technical, organizational, and institutional factors, I answer my initially outlined research question by providing contributions across three interconnected dimensions, as conceptualized by Agerfalk and Karlsson (2020): theoretical, empirical, and artefactual.

### *Theoretical contributions*

This dissertation contributes to the theoretical understanding of how emerging decentralized information systems can be designed and managed to cope with adoption dynamics in practice. Grounded in a socio-technical perspective, the theoretical contributions span foundational conceptual insights, domain-specific theory development, and theory-informed design knowledge, responding thereby to the three overarching research goals (RG1 - RG3) structuring this work.

In addressing RG1, this dissertation emphasizes dedicated adoption dynamics that are context-specific and extend beyond general technical considerations. While prior research has often centered on scalability (Sternberg et al., 2020), energy consumption (Sedlmeir et al., 2020), or security challenges (Warkentin & Orgeron, 2020), our focus within RG1 lies specifically on data protection and privacy aspects as one of the central determinants of decentralized system adoption (Platt et al., 2021). Essay 1 challenges the assumption that transparency is inherently beneficial in decentralized systems by conceptualizing it as a double-edged sword which may hinder adoption and diffusion in practice (Bossler et al., 2024). It develops a typology of excessive information disclosure to explain adoption barriers in inter-organizational blockchain use cases and highlights the need for privacy-preserving design strategies in data-sensitive domains (Lautenschlager et al., 2023; Schlatt et al., 2021). To address these challenges, the essay discusses architectural mitigation options such as ZKPs and SSI frameworks, enabling selective disclosure while maintaining institutional trust and compliance.

Through this lens, Essay 1 demonstrates how transparency-related design tensions must be actively managed in order to support adoption (Sedlmeir, Lautenschlager, et al., 2022). Building on this foundation, Essay 2 expands RG1 by examining SSI as a distinct form of decentralization which prioritizes user control, interoperability, and trust in fragmented ecosystems (Rieger et al., 2024). It provides a theoretical synthesis of SSI's core components—VCs, wallets, and registries—and analyzes their interaction through the trust triangle of issuers, holders, and verifiers (Soltani et al., 2021). By outlining stakeholder-specific value propositions and governance implications, the essay offers conceptual clarity and highlights how SSI systems can address adoption challenges in identity-centric, compliance-sensitive contexts. Together, the two essays contribute directly to RG1 by advancing the understanding of key adoption dynamics influencing the uptake of decentralized systems in practice.

With regard to RG2, which concerns the design of decentralized information systems for adoption in practice, this dissertation contributes design knowledge which builds on and extends existing theoretical frameworks in information systems design science (Gregor & Hevner, 2013). Essay 3 develops a design theory for decentralized, wallet-based MaaS systems that addresses coordination challenges among competing mobility providers (Hoess et al., 2024). It identifies design tensions between service integration and platform control and derives principles—such as selective disclosure and hybrid architectures—which inform the design of privacy-preserving, interoperable infrastructures in multi-actor settings. Essay 4 complements this perspective by using a DSR approach to design a blockchain-based solution for data exchange in coopetitive supply networks. It introduces coopetitive transparency as a design lens and provides modular components for balancing collaboration and competition, showing how technical architectures can resolve strategic tensions without relying solely on institutional governance (Lautenschlager et al., 2023). Together, these two essays contribute directly to RG2 by developing and designing concrete solution approaches that facilitate the adoption of decentralized systems in practice.

In relation to RG3, which focuses on managing decentralized information systems in practice, this dissertation contributes to a process-oriented theoretical understanding of how decentralized systems are implemented, governed, and leveraged to exploit value in complex ecosystems. Essay 5 conceptualizes interoperability in digital identity ecosystems as a dynamic, multi-level equilibrium shaped by socio-technical

interactions (P. Wang, 2021). It identifies mechanisms such as harmonization and negotiation which stabilize or destabilize interoperability and provides guidance for managing decentralized infrastructures beyond static standardization. Essay 6 extends this view by analyzing how public sector organizations engage with SSI through iterative experimentation. Using the A-E-A framework (Du et al., 2019), it demonstrates how aligning political, technical, and cultural dimensions enables innovation despite institutional constraints. Essay 7 shifts the focus to financial ecosystems and explores how private actors contribute to the formation and governance of CBDC infrastructures. It systematizes their roles and value propositions and embeds them in public–private partnership theory to address institutional asymmetries. Together, these three essays contribute directly to RG3 by advancing a theoretical understanding of how decentralized systems can be managed in practice through dynamic implementation, governance, and value realization processes.

### *Empirical contributions*

Beyond theoretical contributions, the dissertation offers rich empirical insights into how decentralized information systems are implemented, adapted, and institutionalized in organizational and ecosystem contexts. Drawing on case studies, expert interviews, and structured literature reviews, these findings enhance IS research on adoption barriers, stakeholder alignment, and institutional readiness, particularly for technologies which currently remain emergent and contested, such as blockchain and SSI.

In line with RG1, the dissertation surfaces sociotechnical frictions related to transparency, trust, and regulatory alignment. Essay 1 consolidates findings from sixteen blockchain pilot projects, revealing recurring concerns around uncontrolled data exposure, legal incompatibilities, and strategic resistance. These empirical observations contextualize the conceptual argument that transparency can act as an adoption barrier, especially in inter-organizational settings. Similarly, Essay 2 draws on a systematic literature review to map how SSI is framed across academic and institutional discourses. The analysis identifies critical gaps between design ambitions and ecosystem realities—particularly with regard to control delegation and interoperability—thereby enriching empirical understanding of SSI's institutional complexity.

In the context of RG2, the dissertation draws on deep stakeholder engagement to explore the design of practically adoptable decentralized systems. Essay 3 analyzes an SSI-based MaaS prototype through pre- and post-evaluation interviews with

practitioners (ex-ante and ex-post interviews). The study reveals concrete adoption tensions - such as market concentration risks, governance ambiguity, and selective disclosure feasibility - which inform broader IS debates on user-centered and regulator-compatible system design. Essay 4 evaluates a blockchain solution for digital invoice handling by providing a structured literature review in order to derive nascent design objectives and ex-post expert interviews for evaluation. The evaluation highlights how coopetitive dynamics, data sovereignty concerns, and legacy system integration can constrain even technically viable solutions in practice. Rather than assuming rational platform uptake, the essay reveals how organizational asymmetries and strategic positioning shape actual adoption trajectories.

Regarding RG3, the dissertation provides rare empirical access to public-sector innovation processes. Essay 5 offers a detailed look into Germany's national SSI initiative (Federal Ministry for Economic Affairs & Energy, 2021), demonstrating how interoperability emerges not from technical specifications alone but also from iterative alignment across governance, funding, and stakeholder expectations. Essay 6 deepens this perspective by examining a digital tax project through the lens of the A-E-A framework. The study illustrates how public actors gradually enact technical affordances through organizational experimentation, adjusting to legal uncertainty and cultural inertia. By capturing these iterative shifts, the essay contributes a processual view of institutional learning in the public sector. Lastly, Essay 7 conducts an MLR to structure the evolving roles of private actors in CBDC ecosystems (Garousi et al., 2019). It identifies actionable participation models and maps tensions between central bank mandates and commercial innovation agendas—offering grounded insights into how decentralized finance infrastructures are co-shaped by public and private interdependencies.

### *Artefactual contributions*

Complementing the theoretical and empirical contributions, this dissertation advances artefactual knowledge by designing and evaluating novel IT artefacts tailored to address the adoption challenges of decentralized information systems. Across Essay 3 and 4, these artefacts materialize as architectural blueprints, structured design frameworks and prototype instantiations, each grounded in domain-specific requirements and iteratively refined through stakeholder engagement. The developed artefacts include a privacy-preserving SSI wallet architecture for MaaS ecosystems and a blockchain-based invoice management system that operationalizes coopetitive design logic.

Rather than positioning artefacts as isolated technical outcomes, the dissertation embeds them within their sociotechnical context, ensuring that each design reflects the structural constraints, governance demands, and stakeholder needs relevant to its application domain. These contributions enrich the design knowledge base in IS research by offering actionable patterns and system-level structures for navigating decentralization in complex organizational and institutional environments.

## 6.3 Limitations

Exploring the ways in which emerging decentralized information systems can be designed and managed to cope with adoption dynamics in practice involves a high degree of complexity. This complexity results not only from the technical challenges and conceptual novelty of decentralized technologies and concepts (Lacity, 2018; Sternberg et al., 2020), such as blockchain technology and SSI, but also from their embedding in heterogeneous organizational, regulatory, and institutional environments. Considering this complexity, several overarching limitations of this cumulative dissertation must be acknowledged. While the individual essays reflect their own methodological or empirical boundaries, the following section focuses on limitations applicability to this overarching dissertation as a whole.

An initial limitation concerns the methodological emphasis on qualitative and design-oriented approaches, such as conceptual analyses, case studies, and expert-based DSR (Gioia et al., 2013; Peffers et al., 2007; Webster & Watson, 2002; Yin, 2018). These methods were deliberately chosen because they allow for rich and context-sensitive engagement with the practical challenges of emerging technologies. They are particularly well suited for uncovering design tensions, stakeholder frictions, and institutional constraints. However, these methods limit the generalizability of the results since their context-specific nature and reliance on qualitative data make it difficult to derive universally applicable findings. The insights gained are often tied to particular cases, technologies, or stakeholder constellations, which may not readily translate to other settings without further empirical validation or quantitative support. This observation also applies to several design artifacts developed in the course of this research, which were evaluated in structured expert settings but not implemented in operational environments. As a result, long-term organizational effects, integration challenges, and emergent use practices could not be assessed. Operational implementation would not

only allow for longitudinal observation but could also enable more systematic, quantitative evaluation and validation. The dissertation does not include the quantitative, statistical analysis or large-scale empirical validation that would be needed to quantify relationships or test hypotheses across broader populations (Kaplan & Duchon, 1988). Future research could complement the present work with quantitative studies that measure, for example, user acceptance patterns, trust formation, or economic performance indicators in different usage settings (V. Venkatesh et al., 2013).

Second, the technological and institutional conditions under which the research was conducted reflect the state of development of decentralized systems in the early 2020s. Technological progress in areas such as decentralized identity, cryptographic protocols, or interoperability standards continues to evolve rapidly. Likewise, regulatory frameworks and public sector strategies both in Europe and globally remain in flux. Although the dissertation aims to derive design principles and conceptual models with a degree of abstraction, some of the conclusions may require future adjustment in response to new developments and regulations.

Third, the empirical scope of the dissertation is shaped by access to specific ecosystems and institutional actors. The research draws on projects conducted in German and European contexts, including collaborations with public sector organizations and actors in regulated industries (particularly Essays 5 and 6). Whilst these settings offer rare and valuable insights, they reflect specific institutional arrangements, cultural expectations, and regulatory constraints. Findings may therefore not be directly transferable to other jurisdictions, sectors, or organizational structures. Future research could use comparative case studies to analyze how adoption dynamics vary across national or industry contexts.

Finally, while this dissertation emphasizes inter-organizational and institutional adoption dynamics, it only addresses individual user perspectives to a limited extent. Although aspects such as user control, privacy preferences, and trust in digital wallets are considered, the research does not systematically investigate user behavior or experience. Further research could explore how users interact with decentralized systems in

practice, how value is perceived from a citizen or customer perspective, and how usability and accessibility influence adoption outcomes.

## 6.4 Potential avenues for future research

Given that this dissertation contributes theoretical insights, empirical findings, and design artifacts across different domains, including digital identity, mobility, and public sector innovation, the limitations discussed above provide a valuable basis for identifying promising avenues for future research. These directions extend the scope of the work presented and aim to deepen, validate, and broaden its findings.

First, future research should focus on validating the proposed solution frameworks and design artifacts in operational environments. While the prototypes developed in this dissertation were evaluated through expert feedback and structured discussions, full-scale implementations are needed to assess their long-term viability, user interaction patterns, and integration with existing infrastructures. In particular, large-scale pilots surrounding the EUDIW initiative (European Commission, 2023), emerging SSI-based platforms (Schweizerische Eidgenossenschaft, 2025), or decentralized infrastructure rollouts in regulated industries offer unique opportunities for an empirical examination of the real-world performance, interoperability, and institutional anchoring of decentralized architectures.

Second, ongoing advancements in cryptographic methods and decentralized architectures offer fertile ground for further technical investigation. Technologies such as ZKPs (Liu et al., 2025), decentralized identifiers (Vereecken, 2025), VCs, and decentralized governance models are evolving rapidly (Shah, 2024). While this dissertation has already explored the conceptual potential of privacy-preserving technologies and advocates ZKP-based mechanisms, future research should evaluate their scalability, computational performance, and regulatory alignment more systematically by way of implementation in a practical environment. Particular attention should be paid to the extent to which such technologies can resolve the inherent tensions between transparency, control, and confidentiality in multi-actor systems.

Third, future research should expand the methodological lens through which decentralized systems are studied. Whilst this dissertation predominantly employs qualitative and design-oriented methods, further research could benefit from methodological

triangulation. Quantitative approaches, including controlled experiments or large-scale surveys, could offer structured insights into user behaviour, trust formation, or cost–benefit perceptions in decentralized versus centralized system settings (Kaplan & Duchon, 1988). Established theoretical models from information systems adoption research – such as the DOI (Karnowski & Kümpel, 2015) – could be applied to better understand how individual users and organizations perceive and interact with decentralized technologies.

Fourth, longitudinal and comparative research is needed to examine how decentralized systems evolve over time and across institutional contexts (A. Venkatesh & Vitalari, 1991). The findings of this dissertation are embedded in a specific technological and regulatory landscape shaped by European digital policy and German public sector practices. Future research could explore how similar systems develop under different legal, cultural, or economic conditions, or how ecosystems stabilize, fragment, or transform over longer periods. Such comparative perspectives would contribute to a more robust and generalizable body of knowledge on decentralized information infrastructures.

Finally, more attention should be paid to the human and societal dimension of decentralization. Whilst this dissertation focuses primarily on organizational and inter-organizational levels, future research could explore the extent to which different user groups experience autonomy, trust, and responsibility in decentralized systems. Issues such as digital literacy, inclusiveness, and the distribution of control across actors deserve more focused investigation. Understanding how individuals navigate new forms of digital identity, ownership, and accountability will be essential for building systems that are not only technically sound but also socially embedded.

# References

Abellán Álvarez, I., Gramlich, V., & Sedlmeir, J. (2024). Unsealing the secrets of blockchain consensus: A systematic comparison of the formal security of proof-of-work and proof-of-stake. In *SAC '24, Proceedings of the 39th ACM/SIGAPP Symposium on Applied Computing* (pp. 278–287). ACM. https://doi.org/10.1145/3605098.3635970

Abraham, A., Koch, K., More, S., Ramacher, S., & Stopar, M. (2021). Privacy-Preserving eID Derivation to Self-Sovereign Identity Systems with Offline Revocation. In *IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications*.

Addo, A., & Senyo, P. K. (2021). Advancing E-Governance for Development: Digital Identification and Its Link to Socioeconomic Inclusion. *Government Information Quarterly*, *38*(2). https://doi.org/10.1016/j.giq.2021.101568

Agerfalk, P. J., & Karlsson, F. (2020). Artefactual and Empirical Contributions in Information Systems Research. *European Journal of Information Systems*, *29*(2), 109–113. https://doi.org/10.1080/0960085X.2020.1743051

Alt, R. (2020). Electronic Markets on blockchain markets. *Electronic Markets*, *30*(2), 181–188.

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

Atlantic Council. (2024). *Central Bank Digital Currency Tracker*. https://www.atlanticcouncil.org/cbdctracker/

Atzori, M. (2017). Blockchain technology and decentralized governance: Is the state still necessary? *Journal of Governance and Regulation*, *6*(1), 45–62. https://doi.org/10.22495/jgr_v6_i1_p5

Auer, R., Cornelli, G., & Frost, J. (2020). *Rise of the central bank digital currencies: drivers, approaches and technologies*. Bank for International Settlements. https://www.bis.org/publ/work880.pdf

Babel, M., & Sedlmeir, J. (2023). *Bringing data minimization to digital wallets at scale with general-purpose zero-knowledge proofs*.

Babel, M., Willburger, L., Lautenschlager, J., Völter, F., Guggenberger, T., Körner, M.-F., Sedlmeir, J., Strüker, J., & Urbach, N. (2025). Self-sovereign identity and digital wallets. *Electronic Markets*, *35*(1). https://doi.org/10.1007/s12525-025-00772-0

Bagni, G., Godinho Filho, M., Finne, M., & Thürer, M. (2024). Design science research in operations management: is there a single type? *Production Planning & Control*, 1–19. https://doi.org/10.1080/09537287.2024.2310230

Bamakan, S. M. H., Motavali, A., & Babaei Bondarti, A. (2020). A survey of blockchain consensus algorithms performance evaluation criteria. *Expert Systems with Applications*, *154*, 113385. https://doi.org/10.1016/j.eswa.2020.113385

Bank of England. (2020). *Central Bank Digital Currency: Opportunities, challenges and design*. https://www.bankofengland.co.uk/-/media/boe/files/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design.pdf?la=en&hash=DFAD18646A77C00772AF1C5B18E63E71F68E4593

Baskerville, R., Baiyere, A., Gergor, S., Hevner, A., & Rossi, M. (2018). Design Science Research Contributions: Finding a Balance between Artifact and Theory. *Journal of the Association for Information Systems*, *19*(5), 358–376. https://doi.org/10.17705/1jais.00495

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

Beck, R., Müller-Bloch, C., & King John Leslie (2018). Governance in the Blockchain Economy: A Framework and Research Agenda. *Journal of the Association for Information Systems*, 1020–1034. https://doi.org/10.17705/1jais.00518

Bengtsson, M., & Kock, S. (1999). Cooperation and competition in relationships between competitors in business networks. *Journal of Business & Industrial Marketing*, *14*(3), 178–194.

Bengtsson, M., & Kock, S. (2000). "Coopetition" in business Networks—to cooperate and compete simultaneously. *Industrial Marketing Management*, *29*(5), 411–426.

Ben-Sasson, E., Bentov, I., Horesh, Y., & Riabzev, M. (2019). Scalable zero knowledge with no trusted setup. In *Annual International Cryptology Conference*. Symposium conducted at the meeting of Springer.

BIS. (2021). *Central bank digital currencies: system design and interoperability*. https://www.bis.org/publ/othp42_system_design.pdf

Bootle, J., Chiesa, A., & Liu, S. (2020). *Zero-Knowledge Succinct Arguments with a Linear-Time Prover*. https://eprint.iacr.org/2020/1527.pdf

Bossler, L. F., Buchwald, A., & Spohrer, K. (2024). And No One Gets the Short End of the Stick: A Blockchain-Based Approach to Solving the Two-Sided Opportunism Problem in Interorganizational Information Sharing. *Information Systems Research*. Advance online publication. https://doi.org/10.1287/isre.2022.0065

Bostrom, R. P., & Heinen, J. S. (1977). MIS Problems and Failures: A Socio-Technical Perspective. Part I: The Causes. *MIS Quarterly*, *1*(3), 17. https://doi.org/10.2307/248710

Brandao, M. S., Godinho Filho, M., Ganga, G. M. D., & Verschoore, J. R. (2025). Coopetition in supply chain management: Patterns, typology and propositions. *J. Bus. Ind. Mark.*

Buterin, V. (2013). *A Next-Generation Smart Contract and Decentralized Application Platform*. https://ethereum.org/en/whitepaper/

Butijn, B.-J., Tamburri, D. A., & van den Heuvel, W.-J. (2020). Blockchains. *ACM Computing Surveys Related Work Blockchain Uber Case*, *53*(3).

Carroll, N. (2016). So that's what the impact of IT innovation looks like? Examining the socio-technical dynamics of public service innovation. *Journal of Enterprise Information Management*, *29*(5), 677–705. https://doi.org/10.1108/JEIM-07-2014-0072

Chen, S., Liu, Z., Xu, X., Gao, H., Lei, H., Liu, C., Zhang, Y [Yonghong], Qi, L., Liu, Q., Yin, G., & Liu, X. (2024). Blockchain-Based Central Bank Digital Currencies: A Comprehensive Survey. *Proceedings of the 13th International Conference on Computer Engineering and Networks*, *1127*, 456–466. https://doi.org/10.1007/978-981-99-9247-8_45

Constantinides, P., Henfridsson, O., & G. Parker, G. (2018). Introduction - Platforms and Infrastructures in the Digital Age. *Information Systems Research*, *29*(2), 381–400.

Corbin, J. M., & Strauss, A. L. (2015). *Basics of qualitative research: Techniques and procedures for developing grounded theory* (4. ed.). Sage.

Čučko, Š., Bećirović, Š., Kamišalić, A., Mrdović, S., & Turkanović, M. (2022). Towards the classification of Self-Sovereign Identity properties. *IEEE Access*, *10*, 88306–88329. https://doi.org/10.1109/ACCESS.2022.3199414

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, *13*(3), 319. https://doi.org/10.2307/249008

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

Ehrlich, T., Richter, D., Meisel, M., & Anke, J. (2021). Self-Sovereign Identity als Grundlage für universell einsetzbare digitale Identitäten. *HMD Praxis Der Wirtschaftsinformatik*, *58*(2), 247–270. https://doi.org/10.1365/s40702-021-00711-5

Eisenhardt, K. M. (1989). Building Theories from Case Study Research. *The Academy of Management Review*, *14*(4), 532. https://doi.org/10.2307/258557

Electronic Markets. (2025). *Call for Position Papers*. https://electronicmarkets.org/call-for-papers/ccfp/call-for-position-papers

Engert, M., Hein, A., Maruping, L. M., Thatcher, J. B., & Krcmar, H. (2025). Self-Organization and Governance in Digital Platform Ecosystems: An Information Ecology Approach. *MIS Quarterly*, *49*(1), 91–122. https://doi.org/10.25300/MISQ/2024/18413

Esener, E. (2023). Adaptive Governance for Blockchain Networks. *SSRN Electronic Journal*. Advance online publication. https://doi.org/10.2139/ssrn.4500961

European Central Bank. (2022). *Wholesale-CBDC: Gegenwart und Zukunft des digitalen Zentralbankgelds für Geschäftsbanken*. https://www.ecb.europa.eu/press/key/date/2022/html/ecb.sp220926 5f9b85685a.de.html

European Commission. (2021). *Commission proposes a trusted and secure Digital Identity for all Europeans*. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2663

European Commission. (2023). *Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity: Consolidated text - compromise amendments*.

European Commission. (2024). *A digital ID and personal digital wallet for EU citizens, residents and businesses*. https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/EU+Digital+Identity+Wallet+Home

Federal Ministry for Economic Affairs, & Energy. (2021). *Showcase Program "Secure Digital Identities"*. https://www.digitale-technologien.de/DT/Navigation/EN/ProgrammeProjekte/AktuelleTechnologieprogramme/Sichere_Digitale_Identitaeten/sichere_digitale_ident.html

Fernandez, A.-S., & Chiambaretto, P. (2016). Managing tensions related to information in coopetition. *Industrial Marketing Management*, *53*, 66–76. https://doi.org/10.1016/j.indmarman.2015.11.010

Feulner, S., Sedlmeir, J., Schlatt, V., & Urbach, N. (2022). Exploring the use of self-sovereign identity for event ticketing systems. *Electronic Markets*, *32*(3), 1759–1777.

Franz, A., & Benlian, A. (2022). Exploring interdependent privacy - Empirical insights into users' protection of others' privacy on online platforms. *Electronic Markets*, *32*, 2293–-2309. https://doi.org/10.1007/s12525-022-00566-8

Fridgen, G., Radszuwill, S., Urbach, N., & Utz, L. (2018). Cross-Organizational Workflow Management Using Blockchain Technology - Towards Applicability, Auditability, and Automation. In *Proceedings of the 51st Annual Hawaii International Conference on System Sciences* (pp. 3507–3517). Hawaii International Conference on System Sciences.

Garousi, V., Felderer, M., & Mäntylä, M. V. (2019). Guidelines for including grey literature and conducting multivocal literature reviews in software engineering. *Information and Software Technology*, *106*, 101–121. https://doi.org/10.1016/j.infsof.2018.09.006

Gasser, U. (2015). Interoperability in the Digital Ecosystem. *SSRN Electronic Journal*. Advance online publication. https://doi.org/10.2139/ssrn.2639210

Gibson, J. J. (1979). *The ecological approach to visual perception* (Classic ed.). *Psychology Press Classic Editions*. Psychology Press. https://doi.org/10.4324/9781315740218

Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2013). Seeking Qualitative Rigor in Inductive Research. *Organizational Research Methods*, *16*(1), 15–31. https://doi.org/10.1177/1094428112452151

Gleiss, A., Degen, K., & Pousttchi, K. (2023). Identifying the patterns: Towards a systematic approach to digital platform regulation. *Journal of Information Technology*, *38*(2), 180–201. https://doi.org/10.1177/02683962221146803

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

Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. *International Journal of Market Research*, *59*(6), 703–705.

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

Goulding, R., & Kamargianni, M. (2018). The Mobility as a Service Maturity Index: Preparing the Cities for the Mobility as a Service Era. Advance online publication. https://doi.org/10.5281/ZENODO.1485002

Gramlich, V., Guggenberger, T., Principato, M., Schellinger, B., & Urbach, N. (2023). A multivocal literature review of decentralized finance: Current knowledge and future research avenues. *Electronic Markets*, *33*(1), 11. https://doi.org/10.1007/s12525-023-00637-4

Gregor, S., & Hevner, A. R. (2013). Positioning and Presenting Design Science Research for Maximum Impact. *MIS Quarterly*, *37*(2), 337–355. https://doi.org/10.25300/MISQ/2013/37.2.01

Guggenberger, T., Sedlmeir, J., Fridgen, G., & Luckow, A. (2022). An in-depth investigation of the performance characteristics of Hyperledger Fabric. *Computers & Industrial Engineering*, *173*, 108716.

Gupta, S., Pandey, D. K., El Ammari, A., & Sahu, G. P. (2023). Do perceived risks and benefits impact trust and willingness to adopt CBDCs? *Research in International Business and Finance*, *66*, 101993. https://doi.org/10.1016/j.ribaf.2023.101993

Hanseth, O., & Lyytinen, K. (2010). Design Theory for Dynamic Complexity in Information Infrastructures: The Case of Building Internet. *Journal of Information Technology*, *25*(1), 1–19. https://doi.org/10.1057/jit.2009.19

Heines, R., Kannengießer, N., Sturm, B., Jung, R., & Sunyaev, A. (2021). Need for change: Business functions affected by the use of decentralized information systems. In *Proceedings of the 42nd International Conference on Information Systems*. Symposium conducted at the meeting of AIS.

Hertzmann, A. (2023). *Computer Science Venues Should Publish Position Papers*. https://aaronhertzmann.com/2023/06/30/meta-papers.html

Hodapp, D., & Hanelt, A. (2022). Interoperability in the Era of Digital Innovation: An Information Systems Research Agenda. *Journal of Information Technology*, *37*(4), 407–427. https://doi.org/10.1177/02683962211064304

Hoess, A., Lautenschlager, J., Sedlmeir, J., Fridgen, G., Schlatt, V., & Urbach, N. (2024). Toward Seamless Mobility-as-a-Service: Providing Multimodal Mobility Through Digital Wallets. *Business & Information Systems Engineering*. Advance online publication. https://doi.org/10.1007/s12599-024-00856-9

Hoess, A., Rieger, A., Roth, T., Fridgen, G., & Young, A. G. (2023). Managing Fashionable Organizing Visions: Evidence from the European Blockchain Services Infrastructure. *Proceedings of the 31st European Conference on Information Systems*.

Hoess, A., Roth, T., Sedlmeir, J., Fridgen, G., & Rieger, A. (2022). With or Without Blockchain? Towards a Decentralized, SSI-based eRoaming Architecture. In *Proceedings of the 55th Hawaii International Conference on System Sciences*.

Hoess, A., Schlatt, V., Rieger, A., & Fridgen, G. (2021). The blockchain effect: From inter-ecosystem to intra-ecosystem competition. In *Twenty-Ninth European Conference on Information Systems (ECIS)*. Symposium conducted at the meeting of Association for Information Systems.

Hoffmann, I., Jensen, N., & Cristescu, A. (2021). Decentralized Governance for Digital Platforms - Architecture Proposal for the Mobility Market to enhance Data Privacy and Market Diversity. In *2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC)* (pp. 1–6). IEEE. https://doi.org/10.1109/ccnc49032.2021.9369659

Hong, S., Kim, S. H., & Kwon, M. (2022). Determinants of digital innovation in the public sector. *Government Information Quarterly*, *39*(4), 101723. https://doi.org/10.1016/j.giq.2022.101723

Jensen, T., Hedman, J., & Henningsson, S. (2019). How TradeLens Delivers Business Value With Blockchain Technology. *MIS Quarterly Executive*, *18*(4), 221–243.

Jørgensen, K. P., & Beck, R. (2022). Universal Wallets. *Business & Information Systems Engineering*, *64*(1), 115–125.

Kankanhalli, A., Zuiderwijk, A., & Tayi, G. K. (2017). Open innovation in the public sector: A research agenda. *Government Information Quarterly*, *34*(1), 84–89. https://doi.org/10.1016/j.giq.2016.12.002

Kannengießer, N., Lins, S., Dehling, T., & Sunyaev, A. (2020). Trade-offs between Distributed Ledger Technology Characteristics. *ACM Computing Surveys*, *53*(2).

Kaplan, B., & Duchon, D. (1988). Combining qualitative and quantitative methods in information systems research: a case study. *MIS Quarterly*, 571–586.

Karnowski, V., & Kümpel, A. S. (2015). Diffusion of Innovations. In *Schlüsselwerke der Medienwirkungsforschung* (pp. 97–107). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-09923-7_9

Katsaliaki, K., Kumar, S., & Loulos, V. (2024). Supply chain coopetition: A review of structures, mechanisms and dynamics. *Int. J. Prod. Econ.*, *267*(109057), 109057.

Kersic, V., Vidovic, U., Vrecko, A., Domajnko, M., & Turkanovic, M. (2023). Orchestrating Digital Wallets for On- and Off-Chain Decentralized Identity Management. *IEEE Access*, *11*, 78135–78151. https://doi.org/10.1109/ACCESS.2023.3299047

Ketchen, D. J., Snow, C. C., & Hoover, V. L. (2004). Research on Competitive Dynamics: Recent Accomplishments and Future Challenges. *Journal of Management*, *30*(6), 779–804. https://doi.org/10.1016/j.jm.2004.06.002

Kiff, J., Alwazir, J., Davidovic, S., & Farias, A. (2020). *A Survey of Research on Retail Central Bank Digital Currency*. International Monetary Fund.

Köhler, S., & Pizzol, M. (2020). Technology assessment of blockchain-based technologies in the food supply chain. *Journal of Cleaner Production*, *269*.

Kruchten, P. (1995). The 4+1 View Model of architecture. *IEEE Software*, *12*(6), 42–50.

Lacity, M. (2018). Addressing Key Challenges to Making Enterprise Blockchain Applications a Reality. *MIS Quarterly Executive*, *17*(3), 202–222.

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

Lautenschlager, J., Stramm, J., Guggenberger, T., Rösch, A., & Schweizer, A. (2023). Overcoming the Data Transparency Trade-Off: Designing a Blockchain-Based Delivery Invoice System for the Construction Industry. In *Wirtschaftsinformatik 2023 Proceedings*.

Leinonen, H. (2023). Wholesale central bank digital currency vs traditional real-time gross settlement: Benefits beyond a new acronym? *Journal of Payments Strategy & Systems*, *17*(1).

Leonardi, P. M. (2013). When Does Technology Use Enable Network Change in Organizations? A Comparative Study of Feature Use and Shared Affordances. *MIS Quarterly*. Advance online publication. https://doi.org/10.25300/MISQ/2013/37.3.04

Liu, T., Zhang, Z., Zhang, Y [Yuncong], Hu, W., & Zhang, Y [Ye] (2025). Ceno: Non-uniform, segment and parallel zero-knowledge virtual machine. *Journal of Cryptology*, *38*(2), 17.

March, S. T., & Storey, V. C. (2008). Design science in the information systems discipline: an introduction to the special issue on design science research. *MIS Quarterly*, *32*(4), 725–730.

Markus, M. L., & Silver, M. (2008). A Foundation for the Study of IT Effects: A New Look at DeSanctis and Poole's Concepts of Structural Features and Spirit. *Journal of the Association for Information Systems*, *9*(10), 609–632. https://doi.org/10.17705/1jais.00176

Mattke, J., Maier, C., Hund, A., & Weitzel, T. (2019). How an Enterprise Blockchain Application in the U.S. Pharmaceuticals Supply Chain is Saving Lives. *MIS Quarterly Excecutive*, *18*(4), 245–261. https://doi.org/10.17705/2msqe.00019

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

Meredith, J. (1998). Building Operations Management Theory Through Case and Field Research. *Journal of Operations Management*, *16*(4), 441–454. https://doi.org/10.1016/S0272-6963(98)00023-0

Myers, M. D., & Newman, M. (2007). The qualitative interview in IS research: Examining the craft. *Information and Organization*, *17*(1), 2–26.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.* https://bitcoin.org/en/bitcoin-paper

Nalebuff, B. J., & Brandenburger, A. M. (1997). Co-opetition: Competitive and cooperative business strategies for the digital economy. *Strategy & Leadership*, *25*(6), 28–33.

Nassr Eddine, B., Ouaddah, A., & Mezrioui, A. (2023). Blockchain-Based Self Sovereign Identity Systems: High-Level Processing and a Challenges-Based Comparative Analysis. In *International Conference on Advanced Intelligent Systems for Sustainable Development* (pp. 489–500). Springer, Cham. https://doi.org/10.1007/978-3-031-26384-2_

Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. *Business & Information Systems Engineering*, *59*(3), 183–187. https://doi.org/10.1007/s12599-017-0467-3

Oliveira, L., Zavolokina, L., Bauer, I., & Schwabe, G. (2018). To Token or not to Token: Tools for Understanding Blockchain Tokens. Advance online publication. https://doi.org/10.5167/UZH-157908

Osterwalder, A., & Pigneur, Y. (2010). *Business model generation: a handbook for visionaries, game changers, and challengers*. Wiley.

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, *24*(3), 45–77. https://doi.org/10.2753/MIS0742-1222240302

Pfitzmann, A., & Hansen, M. (2010). *A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management*. Dresden, Germany. http://www.maroki.de/pub/dphistory/2010_Anon_Terminology_v0.34.pdf

Platt, M., Bandara, R. J., Dragnoiu, A.-E., & Krishnamoorthy, S. (2021). Information privacy in decentralized applications. In Muhammad Habib ur Rehman, Davor Svetinovic, Khaled Salah, & Ernesto Damiani (Eds.), *Trust Models for Next-Generation Blockchain Ecosystems* (pp. 85–104). Springer.

Queiroz, M. M., & Fosso Wamba, S. (2019). Blockchain adoption challenges in supply chain: An empirical investigation of the main drivers in India and the USA. *International Journal of Information Management*, *46*, 70–82. https://doi.org/10.1016/j.ijinfomgt.2018.11.021

Reed, D., Sporny, M., Longley, D., Allen, C., Grant, R., Sabadello, M., & Holt, J. (2020). Decentralized identifiers (DIDs) v1. 0: Core architecture, data model, and representations. *W3C Working Draft*.

Rieger, A., Guggenmos, F., Lockl Jannik, Fridgen, G., & Urbach, N. (2019). Building a blockchain application that complies with the EU general data protection regulation. *MIS Quarterly Executive*, *18*(4), 263–279.

Rieger, A., Roth, T., Sedlmeir, J., Fridgen, G., & Young, A. (2024). Organizational Identity Management Policies. *Journal of the Association for Information Systems*, *25*(3), 522–527.

Rikken, O., Janssen, M., & Kwee, Z. (2019). Governance challenges of blockchain and decentralized autonomous organizations. *Information Polity*, *24*(4), 397–417. https://doi.org/10.3233/IP-190154

Ritala, P. (2022). Coopetition strategy - When is it successful? Empirical evidence on innovation and market performance. *British Journal of Management*, 307–324.

Rossi, M., Mueller-Bloch, C., Thatcher, J. B., & Beck, R. (2019). Blockchain Research in Information Systems: Current Trends and an Inclusive Future Research Agenda. *Journal of the Association for Information Systems*, 1388–1403. https://doi.org/10.17705/1jais.00571

Saldana, J. (2021). *The coding manual for qualitative researchers* (4th ed.). SAGE Publications.

Savoldelli, A., Codagnone, C., & Misuraca, G. (2014). Understanding the e-government paradox: Learning from literature and practice on barriers to adoption. *Government Information Quarterly*, *31*, S63-S71. https://doi.org/10.1016/j.giq.2014.01.008

Schellinger, B., Völter, F., Sedlmeir, J., & Urbach, N. (2021). Yes, I Do: Marrying Blockchain Applications with GDPR. In *Proceedings of the 55th Hawaii International Conference on System Sciences*.

Schlatt, V., Sedlmeir, J., Feulner, S., & Urbach, N. (2021). Designing a Framework for Digital KYC Processes Built on Blockchain-Based Self-Sovereign Identity. *Information & Management*, 103553. https://doi.org/10.1016/j.im.2021.103553

Schmeiss, J., Hoelzle, K., & Tech, R. P. G. (2019). Designing Governance Mechanisms in Platform Ecosystems: Addressing the Paradox of Openness through Blockchain Technology. *California Management Review*, *62*(1), 121–143. https://doi.org/10.1177/0008125619883618

Schulz, T., Zimmermann, S., Böhm, M., Gewald, H., & Krcmar, H. (2021). Value co-creation and co-destruction in service ecosystems: The case of the Reach Now app. *Technological Forecasting and Social Change*, *170*.

Schwalm, S., Albrecht, D., & Alamillo, I. (2022). eIDAS 2.0: Challenges, Perspectives and Proposals to Avoid Contradictions between eIDAS 2.0 and SSI. In *Open Identity Summit 2022* (pp. 63–74). Gesellschaft für Informatik eV.

Schweizerische Eidgenossenschaft. (2025). *Elektronische Identität e-ID*. https://www.eid.admin.ch/de

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

Sedlmeir, J., Lautenschlager, J., Fridgen, G., & Urbach, N. (2022). The transparency challenge of blockchain in organizations. *Electronic Markets*, *32*, 1779–1794.

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

Sedlmeir, J., Wagner, T., Djerekarov, E., Green, R., Klepsch, J., & Rao, S. (2022). A Serverless Distributed Ledger for Enterprises. In *Proceedings of the 55th Hawaii International Conference on System Sciences, pages=7382 - 7391*.

Sethaput, V., & Innet, S. (2023). Blockchain application for central bank digital currencies (CBDC). *Cluster Computing*, *26*(4), 2183–2197. https://doi.org/10.1007/s10586-022-03962-z

Shah, N. (2024). *Hybrid-DAOs: Enhancing Governance, Scalability, and Compliance in Decentralized Systems*. https://doi.org/10.48550/arXiv.2410.21593

Shi, S., He, D., Li, L., Kumar, N., & Raymond Choo, K.-K. (2020). Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. *Computers & Security*, *97*. https://doi.org/10.1016/j.cose.2020.101966

Smichowski Carballa, B. (2018). Determinants of coopetition through data sharing in MaaS. *Management & Data Science*, *2*(3).

Soltani, R., Nguyen, U. T., An, A., & Galdi, C. (2021). A Survey of Self-Sovereign Identity Ecosystem. *Security and Communication Networks*, *2021*, 1–26. https://doi.org/10.1155/2021/8873429

Sourabh, W. (2019). Decentralized digital identity management using blockchain and its implication on public sector. *UR - Https://www.Semanticscholar.Org/paper/Decentralized-Digital-Identity-Management-Using-and-Wadhwa/9b6e9bd362dfa6182e833358c34b2ec60cf170cd*.

Sternberg, H., Hofmann, E., & Roeck, D. (2020). The Struggle is Real: Insights from a Supply Chain Blockchain Case. *Journal of Business Logistics*, *42*(1), 71–87.

Sule, M.-J., Zennaro, M., & Thomas, G. (2021). Cybersecurity through the Lens of Digital Identity and Data Protection: Issues and Trends. *Technology in Society*, *67*, 101734. https://doi.org/10.1016/j.techsoc.2021.101734

Tilson, D., Lyytinen, K., & Sørensen, C. (2010). Research Commentary—Digital Infrastructures: The Missing IS Research Agenda. *Information Systems Research*, *21*(4), 748–759. https://doi.org/10.1287/isre.1100.0318

Tiwana, A. (2014). *Platform Ecosystems: Aligning architecture, governance, and strategy*. Elsevier.

Tiwana, A., Konsynski, B., & Bush, A. A. (2010). Research Commentary —Platform Evolution: Coevolution of Platform Architecture, Governance, and Environmental Dynamics. *Information Systems Research*, *21*(4), 675–687. https://doi.org/10.1287/isre.1100.0323

Toufaily, E., Zalan, T., & Dhaou, S. B. (2021). A framework of blockchain technology adoption: An investigation of challenges and expected value. *Information & Management*, *58*(3), 103444.

Treiblmaier, H., & Beck, R. (Eds.). (2019). *Business Transformation through Blockchain*. Springer International Publishing. https://doi.org/10.1007/978-3-319-98911-2

Troncoso, C., Isaakidis, M., Danezis, G., & Halpin, H. (2017). Systematizing Decentralization and Privacy: Lessons from 15 Years of Research and Deployments. *Proceedings on Privacy Enhancing Technologies*, *2017*(4), 404–426. https://doi.org/10.1515/popets-2017-0056

van Dijck, J., Poell, T., & Waal, M. de. (2018). *The Platform Society* (Vol. 1). Oxford University Press. https://doi.org/10.1093/oso/9780190889760.001.0001

Venable, J., Pries-Heje, J., & Baskerville, R. (2016). FEDS: a Framework for Evaluation in Design Science Research. *European Journal of Information Systems*, *25*(1), 77–89.

Venkatesh, A., & Vitalari, N. P. (1991). Longitudinal surveys in information systems research: An examination of issues, methods, and applications. *The Information Systems Challenge: Survey Research Methods*, 115–144.

Venkatesh, V., Brown, S. A., & Bala, H. (2013). Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems. *MIS Quarterly*, 21–54.

Vereecken, J. (2025). *Are DIDs a DUD?* https://janvereecken.com/posts/are-dids-a-dud/

vom Brocke, J., Winter, R., Hevner, A., & Maedche, A. (2020). Special Issue Editorial - Accumulation and Evolution of Design Knowledge in Design Science Research: A Journey Through Time and Space. *Journal of the Association for Information Systems*, *21*(3), 520–544.

Wang, P. (2021). Connecting the Parts with the Whole: Toward an Information Ecology Theory of Digital Innovation Ecosystems. *MIS Quarterly*, *45*(1), 397–422. https://doi.org/10.25300/MISQ/2021/15864

Wang, Y.-R., Ma, C.-Q., & Ren, Y.-S. (2022). A model for CBDC audits based on blockchain technology: Learning from the DCEP. *Research in International Business and Finance*, *63*, 101781. https://doi.org/10.1016/j.ribaf.2022.101781

Wareham, J., Fox, P. B., & Cano Giner, J. L. (2014). Technology Ecosystem Governance. *Organization Science*, *25*(4), 1195–1215. https://doi.org/10.1287/orsc.2014.0895

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

Webster, J., & Watson, R. T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MIS Quarterly*, *26*(2), xiii–xxiii.

World Bank. (2022). *Financial Inclusion: Financial inclusion is a key enabler to reducing poverty and boosting prosperity*. *World Bank*. https://www.worldbank.org/en/topic/financialinclusion/overview

Wüst, K., & Gervais, A. (2018). Do you Need a Blockchain? In *IEEE Crypto Valley Conference on Blockchain Technology*. IEEE. https://doi.org/10.1109/cvcbt.2018.00011

Yang Xiao, Ning Zhang, Wenjing Lou, & Y. Thomas Hou (2020). A Survey of Distributed Consensus Protocols for Blockchain Networks. *IEEE Communications Surveys & Tutorials*, *22*(2), 1432–1465. https://doi.org/10.1109/comst.2020.2969706

Yin, R. K. (2018). *Case Study Research and Applications: Design and Methods* (6th ed.). Sage.

Zetzsche, D. A., Arner, D. W., & Buckley, R. P. (2020). Decentralized Finance. *Journal of Financial Regulation*, *6*(2), 172–203. https://doi.org/10.1093/jfr/fjaa010

Zhang, R., Xue, R., & Liu, L. (2019). Security and Privacy on Blockchain. *ACM Computing Surveys*, *52*(3).

Zhong, B., Wu, H., Ding, L., Luo, H., Luo, Y., & Pan, X. (2020). Hyperledger Fabric-based consortium blockchain for construction quality information management. *Frontiers of Engineering Management*, *7*(4), 512–527. https://doi.org/10.1007/s42524-020-0128-y

Zwitter, A., & Boisse-Despiaux, M. (2018). Blockchain for humanitarian action and development aid. *Journal of International Humanitarian Action*, *3*(1). https://doi.org/10.1186/s41018-018-0044-5

Zwitter, A., & Hazenberg, J. (2020). Decentralized Network Governance: Blockchain Technology and the Future of Regulation. *Frontiers in Blockchain*, *3*. https://doi.org/10.3389/fbloc.2020.00012

Zysman, J., & Kenney, M. (2018). The next phase in the digital revolution. *Communications of the ACM*, *61*(2), 54–63. https://doi.org/10.1145/3173550

# Appendices

## Appendix A: Declarations of co-authorship and individual contributions

The contributions of the co-authors to the essays are provided below:

### Essay 1: The transparency challenge of blockchain in organizations

This research paper was co-authored by Johannes Sedlmeir, Jonathan Lautenschlager, Gilbert Fridgen, and Nils Urbach. The co-authors contributed as follows:

**Johannes Sedlmeir (co-author)**

Johannes Sedlmeir supervised the research project and provided scientific mentorship. He engaged in literature work, contributed significantly to the textual elaboration of the paper, and was involved in revising the manuscript during the peer-review process. Thus, Johannes's co-authorship is reflected equally across all phases of the research project.

**Jonathan Lautenschlager (co-author)**

Jonathan Lautenschlager contributed to the research project by conducting the literature work and significantly contributing to textual elaboration. He also participated actively in revising the manuscript during the peer-review process. Thus, Jonathan's co-authorship is reflected equally across all phases of the research project.

**Gilbert Fridgen (co-author)**

Gilbert Fridgen provided the initial inspiration and idea for the research project. He supervised the project and offered scientific mentorship. Additionally, he contributed experience and feedback to support the manuscript development. His contribution is considered secondary.

**Nils Urbach (co-author)**

Nils Urbach provided the initial inspiration and idea for the research project. He supervised the project and offered scientific mentorship. Furthermore, he contributed his scientific experience and feedback to support the manuscript development. His contribution is considered secondary.

### Essay 2: Self-Sovereign Identity and digital wallets

This research paper was co-authored by Matthias Babel, Lukas Willburger, Jonathan Lautenschlager, Fabiane Völter, Tobias Guggenberger, Marc-Fabian Körner, Johannes Sedlmeir, Jens Strüker, and Nils Urbach. The co-authors contributed as follows:

#### Matthias Babel (co-author)

Matthias Babel co-developed the research project. He participated in the conceptualization and textual elaboration of the paper. Further, he engaged in the revision process during peer review. Thus, Matthias's co-authorship is reflected equally across all phases of the research project.

#### Lukas Willburger (co-author)

Lukas Willburger co-developed the research project. He contributed to the development of the paper's content, structure, and textual elaboration. Furthermore, he participated in the revision process during peer review. Thus, Lukas's co-authorship is reflected equally across all phases of the research project.

#### Jonathan Lautenschlager (co-author)

Jonathan Lautenschlager contributed to the research project by supporting the textual elaboration and the revision of the paper. Furthermore, he participated in the revision process during peer review. Additionally, he was involved in the data collection process. His contribution is considered secondary.

#### Fabiane Völter (co-author)

Fabiane Völter contributed to the research project by supporting the textual elaboration and the revision of the paper. Additionally, she was involved in the data collection process. Her contribution is considered secondary.

#### Tobias Guggenberger (co-author)

Tobias Guggenberger provided supervision and scientific mentorship throughout the development of the research project. Furthermore, he contributed his scientific experience and feedback to support the manuscript development. His contributions are considered secondary.

#### Marc-Fabian Körner (co-author)

Marc-Fabian Körner provided supervision and scientific mentorship throughout the

development of the research project. Furthermore, he contributed his scientific experience and feedback to support the manuscript development. His contributions are considered secondary.

**Johannes Sedlmeir (co-author)**

Johannes Sedlmeir provided supervision and scientific mentorship throughout the development of the research project. Furthermore, he contributed his scientific experience and feedback to support the manuscript development. His contributions are considered secondary.

**Jens Strüker (co-author)**

Jens Strüker provided supervision and scientific mentorship throughout the development of the research project. Furthermore, he contributed his scientific experience and feedback to support the manuscript development. His contributions are considered secondary.

**Nils Urbach (co-author)**

Nils Urbach provided supervision and scientific mentorship throughout the development of the research project. Furthermore, he contributed his scientific experience and feedback to support the manuscript development. His contributions are considered secondary.

## Essay 3: Toward seamless mobility-as-a-service: Providing multimodal mobility through digital wallets

This research paper was co-authored by Alexandra Hoess, Jonathan Lautenschlager, Johannes Sedlmeir, Gilbert Fridgen, Vincent Schlatt and Nils Urbach. The co-authors contributed as follows:

### Alexandra Hoess (co-author)

Alexandra Hoess co-developed the research project. She was responsible for conceptualization, formal analysis, investigation, method development, and visualization. Additionally, she engaged in the original drafting of the manuscript and contributed to the review and editing process. Thus, Alexandra's co-authorship is reflected equally across all phases of the research project.

### Jonathan Lautenschlager (co-author)

Jonathan Lautenschlager initiated and co-developed the research project and managed its administration as corresponding author. He contributed to the conceptualization, formal analysis, investigation, method development, and software implementation. Moreover, he participated in visualization, original drafting, and review and editing of the manuscript. Thus, Jonathan's co-authorship is reflected across all phases of the research project.

### Johannes Sedlmeir (co-author)

Johannes Sedlmeir supervised the project and offered scientific mentorship simultaneously supporting the research project through conceptualization, supervision, software contributions, and investigation. He was also involved in the review and editing of the manuscript. His contribution is considered secondary.

### Gilbert Fridgen (co-author)

Gilbert Fridgen provided the initial inspiration and idea for the research project. He supervised the project and offered scientific mentorship. Additionally, he contributed experience and feedback to support the manuscript development. His contribution is considered secondary.

### Vincent Schlatt (co-author)

Vincent Schlatt contributed to the research project by conducting investigation and validation. He was also involved in the review and editing of the manuscript. His contribution is considered secondary.

**Nils Urbach (co-author)**

Nils Urbach supervised the research project and provided scientific mentorship. He contributed to research discussions, offered feedback on the paper's content and structure, and supported the textual elaboration. Consequently, Nils's co-authorship is considered secondary.

### Essay 4: Striking a balance: Designing a blockchain-based solution to navigate coopetition dynamics in supply chain management

This research paper was co-authored by Jonathan Lautenschlager, Jan Stramm, Tobias Guggenberger, and Nils Urbach. The co-authors contributed as follows:

**Jonathan Lautenschlager (leading-author)**
Jonathan Lautenschlager initiated and conceptualized the research project. He conducted literature work, developed artifacts, constructs, models, and methodologies and carried out the evaluation through interviews. He also contributed significantly to the textual elaboration of the paper and participated actively in the revision process during peer review. Thus, Jonathan's co-authorship is reflected as lead author across all phases of the research project.

**Jan Stramm (subordinate-author)**
Jan Stramm contributed to the research project through literature work, the development of artifacts, constructs, models, methodologies and textual elaboration. He also participated in the revision process during peer review. His contribution is considered secondary.

**Tobias Guggenberger (subordinate-author)**
Tobias Guggenberger supervised the research project and provided scientific mentorship. He contributed to the development of artifacts, constructs, models, and methodologies and offered feedback and support during manuscript preparation. His contribution is considered secondary.

**Nils Urbach (subordinate-author)**
Nils Urbach supervised the research project and provided scientific mentorship. He contributed to the development of artifacts, methodologies, and offered feedback and support during manuscript preparation. His contribution is considered secondary.

### Essay 5: Interoperability in digital identity ecosystems

This research paper was co-authored by Martin Brennecke, Tobias Guggenberger, Jonathan Lautenschlager, and Nils Urbach. The co-authors contributed as follows:

#### Martin Brennecke (co-author)

Martin Brennecke co-developed the research project. He contributed significantly to the conceptualization, theoretical development, data collection, analysis and textual elaboration of the paper. Furthermore, he actively participated in revising the manuscript during the peer-review process. Thus, Martin's co-authorship is reflected equally across all phases of the research project.

#### Tobias Guggenberger (co-author)

Tobias Guggenberger co-developed the research project. He contributed significantly to the conceptualization, theoretical development, data collection, analysis and textual elaboration of the paper. Furthermore, he actively participated in revising the manuscript during the peer-review process. Thus, Tobias's co-authorship is reflected equally across all phases of the research project.

#### Jonathan Lautenschlager (co-author)

Jonathan Lautenschlager co-developed the research project. He contributed significantly to the conceptualization, theoretical development, data collection, analysis and textual elaboration of the paper. Furthermore, he actively participated in revising the manuscript during the peer-review process. Thus, Jonathan's co-authorship is reflected equally across all phases of the research project.

#### Nils Urbach (co-author)

Nils Urbach supervised the research project and provided scientific mentorship. He participated in research discussions, offered feedback on the paper's structure and content, and supported the manuscript development. His contribution is considered secondary.

### Essay 6: Self-Sovereign Identity in the public sector: Affordances, experimentation, and actualization

This research paper was co-authored by Simon Feulner, Tobias Guggenberger, Jonathan Lautenschlager, Nils Urbach, and Fabiane Völter. The authors contributed as follows:

**Simon Feulner (co-author)**

Simon Feulner co-developed the research project. He participated in regular discussion rounds and helped develop the paper's theoretical foundations, content, and structure. Further, he engaged in textual elaboration, particularly in the introduction, theoretical background, methodology, results, discussion, and conclusion sections. He also engaged in revision of the paper and in formulating its theoretical contributions. Thus, his co-authorship is reflected in the entire research project.

**Tobias Guggenberger (co-author)**

Tobias Guggenberger initiated and co-developed the research project. He participated in regular discussion rounds and helped develop the paper's theoretical foundations, content, and structure. Further, he engaged in textual elaboration, particularly in the introduction, theoretical background, methodology, results, discussion, and conclusion sections. He also participated in research discussions and co-shaped the paper's content and structure. Thus, his co-authorship is reflected in the entire research project.

**Jonathan Lautenschlager (co-author)**

Jonathan Lautenschlager co-developed the research project. He participated in regular discussion rounds and helped develop the paper's theoretical foundations, content, and structure. He also engaged in textual elaboration, particularly in the introduction, theoretical background, methodology, results, discussion, and conclusion sections. He engaged in revision of the paper and in formulating its theoretical contributions. Thus, his co-authorship is reflected in the entire research project.

**Nils Urbach (co-author)**

Nils Urbach supervised the research project and provided scientific mentorship. He participated in research discussions, provided feedback on the paper's content and structure, and engaged in textual elaboration. Thus, his co-authorship is reflected in the entire research project.

**Fabiane Völter (co-author)**

Fabiane Völter initiated and co-developed the research project. She participated in research discussions and helped develop the paper's theoretical foundations, content, structure and engaged in textual elaboration. She also participated in research discussions and co-shaped the paper's content and structure. Thus, her co-authorship is reflected in the entire research project.

### Essay 7: A multivocal literature review on capturing value propositions for private organizations in a CBDC ecosystem

This research paper was co-authored by Vincent Schaaf, Jonathan Lautenschlager, Hannes Voucko-Glockner, Tobias Plank, Tobias Guggenberger, and Nils Urbach. The co-authors contributed as follows:

**Vincent Schaaf (co-author)**

Vincent Schaaf co-developed the research project. He contributed by structuring the results of the literature review, developing the motivation and theoretical contribution of the paper. Additionally, he engaged in textual elaboration, participated in research discussions and provided feedback on the paper's content and structure. Thus, Vincent Schaaf's co-authorship is reflected in the entire research project.

**Jonathan Lautenschlager (co-author)**

Jonathan Lautenschlager co-developed the research project. He contributed by structuring the results of the literature review, developing the motivation and theoretical contribution of the paper. Additionally, he engaged in textual elaboration, participated in research discussions and provided feedback on the paper's content and structure. Thus, Jonathan Lautenschlager's co-authorship is reflected in the entire research project.

**Hannes Voucko-Glockner (co-author)**

Hannes Voucko-Glockner co-initiated and co-developed the research project. He contributed by conducting the literature review, analyzing the results and deriving avenues for future research. Additionally, he engaged in textual elaboration, participated in research discussions and provided feedback on the paper's content and structure. Thus, Hannes Voucko-Glockner's co-authorship is reflected in the entire research project.

**Tobias Plank (co-author)**

Tobias Plank co-initiated and co-developed the research project. He contributed by conducting the literature review, analyzing the results, and deriving avenues for future research. Additionally, he engaged in textual elaboration, participated in research discussions and provided feedback on the paper's content and structure. Thus, Tobias Plank's co-authorship is reflected in the entire research project.

**Tobias Guggenberger (co-author)**

Tobias Guggenberger supervised the research project and provided mentorship. Further, he participated in research discussions, provided feedback on the paper's content

and structure and engaged in textual elaboration. Thus, Tobias Guggenberger's co-authorship is reflected in the entire research project.

**Nils Urbach (co-author)**

Nils Urbach supervised the research project and provided mentorship. Further, he participated in research discussions, provided feedback on the paper's content and structure, and engaged in textual elaboration. Thus, Nils Urbach's co-authorship is reflected in the entire research project.

## Appendix B: Other publications by the author

Table 2: Overview of other publications by the author

| Reference | Title | Publication outlet |
|---|---|---|
| Jonas, C., Lautenschlager, J., Eymann, T. (2021) | Die Entwicklung bayerischer Hochschulrechenzentren – Handlungsempfehlungen aus einer Fallstudie für ein professionelles IT-Servicemanagement | *HMD-Praxis der Wirtschafts-informatik (VHB 2024 – C)* |
| Strüker, J. et al. (2021) | Self-sovereign identity: Foundations, applications, and potentials of portable digital identities | White Paper (Available in English and German) |
| Stramm, J., Lautenschlager, J., Keppler, L. (2024) | Blockchain Technology | Book Chapter |
| Urbach, N. et al. (2024) | EU Digital Identity Wallet: Anwendungsfälle, Nutzungspotenziale und Herausforderungen für Unternehmen | White Paper |
| Körner, M. et al (2025) | A digital infrastructure for integrating decentralized assets into redispatch. Decentralized Redispatch (DEER): Interfaces for providing flexibility | White Paper |
| Gramlich et al. (2025) | On the role of tokenization for pursuing environmental sustainability | Book Chapter |
| Lautenschlager et al. (2025) | From Project Design to Retirement: The Role of Blockchain along the Voluntary Carbon Credit Lifecycle | Book Chapter |

## The transparency challenge of blockchain in organizations[2]

### Authors

Johannes Sedlmeir, Jonathan Lautenschlager, Gilbert Fridgen, Nils Urbach

### Published in

Electronic Markets

### Abstract

This position paper discusses the challenges of blockchain applications in businesses and the public sector related to an excessive degree of transparency. We first point out the types of sensitive data involved in different patterns of blockchain use cases. We then argue that the implications of blockchains' information exposure caused by replicated transaction storage and execution go well beyond the often-mentioned conflicts with the GDPR's "right to be forgotten" and may be more problematic than anticipated. In particular, we illustrate the trade-off between protecting sensitive information and increasing process efficiency through smart contracts. We also explore to which extent permissioned blockchains and novel applications of cryptographic technologies such as self-sovereign identities and zero-knowledge proofs can help overcome the transparency challenge and thus act as catalysts for blockchain adoption and diffusion in organizations.

Keywords: Confidentiality; Data protection; Digital wallet; Distributed ledger technology; Privacy; Verifiable computation

[2] This essay has been published in: Sedlmeir, J., Lautenschlager, J., Fridgen, G., & Urbach, N. (2022). The transparency challenge of blockchain in organizations. *Electronic Markets*, *32*(3), 1779-1794.

## Self-sovereign identity and digital wallets[3]

### Authors

Matthias Babel, Lukas Willburger, Jonathan Lautenschlager, Fabiane Völter, Tobias Guggenberger, Marc Fabian Körber, Johannes Sedlmeir, Jens Strüker, Nils Urbach

### Published in

Electronic Markets

### Abstract

Current approaches to managing digital identities struggle to meet the demands of ongoing digital transformation. They either create fragmented identities tied to specific online services, making it difficult for users to manage, or they raise concerns about being locked into corporate identity providers and data protection issues. Additionally, they provide limited support for machine-verifiable identity attributes. This reliance on third parties for managing machine identities can put companies at a market disadvantage. Therefore, there is a pressing need for a unified identity management solution that allows for the portable and interoperable use of verifiable identity data across services. The recently announced European Digital Identity Wallet marks a significant step forward in digital identity management. This initiative aims to provide EU citizens with a unified, secure, and convenient way to access both public and private online services, thereby enhancing the efficiency and security of digital interactions and prioritizing user needs. Self-sovereign identity (SSI) forms the basis for such a wallet-based identity ecosystem that supports electronic market growth. However, as a relatively new concept, SSI still lacks a unified theoretical analysis and a thorough exploration of its value propositions for digital ecosystems and networked businesses.

Keywords: DID, eIDAS, Identity ecosystem, Privacy, User centricity, Verifiable credential, Zero-knowledge proof

[3] This essay has been published in: Babel, M., Willburger, L., Lautenschlager, J., Völter, F., Guggenberger, T., Körner, M. F., ... & Urbach, N. (2025). Self-sovereign identity and digital wallets. Electronic Markets, 35(1), 1-14.

# Toward Seamless Mobility-as-a-Service: Providing Multimodal Mobility Through Digital Wallets[4]

**Authors**

Alexandra Hoess, Jonathan Lautenschlager, Johannes Sedlmeir, Gilbert Fridgen, Vincent Schlatt, Nils Urbach

**Published in**

Business & Information Systems Engineering

**Abstract**

With growing awareness of sustainability and convenience expectations, customers are increasingly demanding integrated and seamless mobility in the form of mobility-as-a-service (MaaS). However, as centralized MaaS platforms have thus far failed to integrate a critical share of mobility service providers (MSPs), travelers lack opportunities to efficiently combine the various mobility services required for seamless end-to-end itinerary coverage. Particularly, MSPs often refuse to collaborate by devolving control over customer interfaces or sensitive data owing to threats of market power concentration. While alternative blockchain-based approaches aim to provide equal market access, they cannot sufficiently align competing business goals and face substantial problems resulting from the replicated processing of sensitive data. Both researchers and practitioners have recently suggested decentralized digital identity management enabled by digital wallets as a promising mechanism to exchange verifiable identity attributes while mitigating problems related to data aggregation. Following a design science research approach, the article accordingly explores how digital wallets can address the shortcomings of existing approaches to MaaS. It contributes a novel IS architecture and principles for a design at the nexus of centralized and decentralized solutions to mitigate tensions between cooperation and competition. Further, the findings indicate that when building decentralized solutions, one should also consider components beyond blockchain and smart contracts.

Keywords: Coopetition, Digital identity, Digital wallet, MaaS, Self-sovereign identity

[4] This essay has been published in: Hoess, A., Lautenschlager, J., Sedlmeir, J., Fridgen, G., Schlatt, V., & Urbach, N. (2024). Toward seamless mobility-as-a-service: providing multimodal mobility through digital wallets. *Business & Information Systems Engineering*, 1-22.

## Striking a Balance: Designing a Blockchain-Based Solution to Navigate Coopetition Dynamics in Supply Chain Management[5]

### Authors

Jonathan Lautenschlager, Jan Stramm, Tobias Guggenberger, Nils Urbach

### Accepted in

Electronic Markets

### Abstract

Coopetition dynamics, which refer to the simultaneous competition and cooperation, increasingly affect the management of digital supply chains. Current research profoundly explores the benefits and drawbacks of using blockchain systems in coopetition strategies to boost cooperation and automation in supply chains. However, these systems often do not adequately address how to manage competition dependencies, which practitioners need to address when considering adopting a blockchain solution that contains excessive disclosure of sensitive information during the data exchange within a transparent network. This paper examines how to protect such sensitive information essential for maintaining competitive dynamics. Following a design science research approach, we suggest a blockchain architecture specifically tailored to the construction industry. We focus on components that manage competition and privacy-enhancing technologies that address the trade-off between cooperation benefits and the need to protect sensitive business data, which is especially crucial in supply chain automation. This study contributes to the current scientific discourse by designing and deriving implementation guidelines for a solution that incorporates the benefits while addressing the potential drawbacks of blockchain technology through coopetitive data exchange to diffuse blockchain solutions into practice successfully.

Keywords: Coopetition, Blockchain Technology, Data Transparency, Delivery Invoices, Construction Industry, Supply Chain Automation

[5] This essay has been accepted in: Lautenschlager, J., Stramm, J., Guggenberger, T., & Urbach, N. (2025). Striking a balance: Designing a blockchain-based solution to navigate coopetition dynamics in supply chain management. *Electronic Markets*. Forthcoming.

## Interoperability in Digital Identity Ecosystems[6]

### Authors

Martin Brennecke, Tobias Guggenberger, Jonathan Lautenschlager, Nils Urbach

### Submitted to

Journal of the Association of Information Systems

### Abstract

As digital identities become integral to public services, economic participation, and user-centric digital infrastructures, governments, private sector actors, and civil society are investing in the development of digital identity ecosystems (Ceccagnoli et al., 2012). Among these, wallet-based identity ecosystems, which are built on self-sovereign identity principles, offer a decentralized alternative to platform-based models (Rieger et al., 2024). However, the increasing heterogeneity in technical standards, governance arrangements, and stakeholder interests leads to fragmentation and poses a major barrier to interoperability, a key enabler of value creation and trust in these ecosystems (Allen et al., 2014). Addressing this challenge, we conceptualize interoperability as a dynamic equilibrium as a subject to cycles of stabilization and destabilization rather than a static outcome of standardization efforts. Using the lens of information ecology theory, which views digital ecosystems as holarchically structured systems, we investigate how interoperability is shaped by multilevel socio-technical interactions.

We conduct an embedded single-case study of the German federal showcase program Secure Digital Identities, comprising four heterogeneous sub-ecosystems, each with distinct technical architectures, governance models, and regional scopes (Yin, 2018). Based on 24 expert interviews and extensive document analysis over a four-year period, we identify mechanisms through which interoperability is co-developed, challenged, and realigned (Hanseth et al., 2021). These include holon-specific activities (e.g., development, technical adaptation), peer-level interactions (e.g., negotiation, harmonization), part-whole coordination (e.g., governance, integration), and temporal

[6] At the time of submitting this thesis, the corresponding essay is under peer review for potential publication in an academic journal. Consequently, an extended abstract is provided to outline the essay's main content.

change (e.g., adoption, disruption).

We contribute a conceptual framework that explains how interoperability in decentralized digital identity ecosystems emerges from recursive, distributed processes rather than top-down control. Our findings have implications for research on digital innovation and interoperability governance, and provide practical guidance for policymakers and ecosystem designers seeking to foster sustainable, cross-domain identity infrastructures.

Keywords: Digital identity ecosystems, information ecology theory, digital innovation, digital identities, wallet-based digital identity

## References

Allen, D. K., Karanasios, S., & Norman, A. (2014). Information Sharing and Interoperability: The Case of Major Incident Management. *European Journal of Information Systems*, *23*(4), 418–432.

Ceccagnoli, M., Forman, C., Huang, P., & Wu, D. J. (2012). Cocreation of Value in a Platform Ecosystem: The Case of Enterprise Software. *MIS Quarterly*, *36*(1), 263.

Hanseth, O., & Rodon, J. M. (2021). The Dynamics of Architecture-Governance Configurations: An Assemblage Theory Approach. *Journal of the Association for Information Systems*, *22*(1), 130–155.

Rieger, A., Roth, T., Sedlmeir, J., Fridgen, G., & Young, A. (2024). Organizational Identity Management Policies. *Journal of the Association for Information Systems*, *25*(3), 522–527.

Yin, R. K. (2018). *Case Study Research and Applications: Design and Methods* (6th ed.). Sage.

## Self-Sovereign Identity in the Public Sector: Affordances, Experimentation, and Actualization[7]

### Authors

Simon Feulner, Tobias Guggenberger, Jonathan Lautenschlager, Nils Urbach, Fabiane Völter

### Published in

Government Information Quarterly

### Abstract

The emerging concept of Self-Sovereign Identity (SSI) promises more portable, secure, and convenient identity services. The public sector, in particular, invests heavily to innovate with this emerging concept. However, an in-depth understanding of SSI's value and how offerings are utilized is lacking, causing complexities and insecurities in designing and implementing SSI-based applications in the public sector. Thus, we conducted a case study which aimed at utilizing SSI for tax registration purposes on online marketplaces. We chose affordance-experimentation-actualization (A-E-A) theory to explore SSI implementation and utilization. As a result, we identify four organizational-level SSI affordances and offer insights into how public sector organizations can innovate with and benefit from SSI by developing an affordance-based innovation framework. Lastly, we contribute to A-E-A theory by revealing how the experimentation phase shapes the organizational context by increasing technical, cultural, and political fit.

Keywords: Case Study, Self-Sovereign Identity, Emerging IT, Affordance, Open Innovation, Public Sector

[7] This essay has been published in: Feulner, S., Guggenberger, T., Lautenschlager, J., Urbach, N., & Völter, F. (2025). Self-sovereign identity in the public sector: Affordances, experimentation, and actualization. *Government Information Quarterly*, *42*(3), 102052.

# A Multivocal Literature Review on Capturing Value Propositions for Private Organizations in a CBDC Ecosystem[8]

**Authors**

Vincent Schaaf, Jonathan Lautenschlager, Hannes Voucko-Glockner, Tobias Plank, Tobias Guggenberger, Nils Urbach

**Published in**

Communications of the Association for Information Systems

**Abstract**

Central Bank Digital Currencies (CBDC) are a novel phenomenon gaining widespread attention from academics and practitioners in recent years. CBDCs combine FinTech and Decentralized Finance aspects in the form of a technology- enabled financial system promising to transform financial infrastructure with the close bound to central banks and governments of fiat currencies. However, CBDCs and explicit concepts are still in their infancy, and many questions remain unanswered. While current practice and research primarily focus on designing specific CBDC systems or the governmental role, the role of companies and the private sector in the CBDC ecosystem still needs to be explored. This paper aims to fill this gap by shedding light on private organizations' value propositions in CBDC ecosystems. We aggregate these value propositions first-hand by surveying the current literature base and second-hand by mapping the needs of a CBDC ecosystem to value propositions companies might offer to fulfil these needs.

Keywords: CBDC, Blockchain, Value Proposition, Financial Sector

[8] This essay has been published in: Schaaf, V., Lautenschlager, J., Voucko-Glockner, H., Plank, T., Guggenberger, T., & Urbach, N. (2025). A Multivocal Literature Review on Capturing Value Propositions for Private Organizations in a CBDC Ecosystem. *Communications of the Association for Information Systems*, 57(1), 14.