Fostering Digital Trust in the Digital Age: On the Design and Management of Emerging Decentralized Information Systems

Dissertation

zur Erlangung des Grades eines Doktors der Wirtschaftswissenschaft

der Rechts- und Wirtschaftswissenschaftlichen Fakultät

der Universität Bayreuth

Vorgelegt

von

Simon Feulner

aus

Frankfurt am Main

Dekan:	Prof. Dr. Claas Christian Germelmann
Erstberichterstatter:	Prof. Dr. Nils Urbach
Zweitberichterstatter:	Prof. Dr. Jens Strüker
Tag der mündlichen Prüfung:	20.02.2025

Decentralization – or distributed processing, or distributed computing, or whatever – is a good solution sometimes, but they are only good solutions to some problems. As in most things we do, the important work is in deciding whether the solutions we like fit the problems we have.

Robert L. Patrick, 1976

Abstract

Trust is fundamental to personal, economic, and professional interactions, yet establishing trust can be challenging in the physical world and even more so in the digital realm. In digital interactions, individuals often lack the means to directly assess trustworthiness and must instead rely on the reputations of their transaction partners. However, widespread failures in both the private and public sectors have significantly eroded public trust. Emerging decentralized technologies such as blockchain and self-sovereign identity (SSI) offer promising solutions to this issue by fostering digital trust by means of enhanced user control, transparency, and the reduction of centralized control. Despite these promises, organizations still struggle to lever blockchain and SSI for building trustful digital processes, products, and services. The effective design and management of decentralized ISs remain key challenges that require dedicated guidance. This dissertation addresses these challenges by pursuing three primary research goals (RGs).

RG1 deepens our understanding of blockchain's potentials to enable trustful digital interactions without the need for a trusted central party. Essay 1 investigates the roles of intermediaries in blockchain-based ecosystems and examines blockchain's capacity for disintermediation. RG2 focuses on guiding organizations in designing trustworthy decentralized ISs. Essay 2 presents a framework for SSI-based digital KYC processes and derives generic design principles (DPs). Essay 3 proposes an SSI-based framework for event ticketing to resolve trust issues in secondary ticket markets. Essay 4 introduces a holistic, SSI-based digital car identity framework to facilitate trustworthy and privacy-preserving interactions between humans, organizations, and machines. RG3 investigates how organizations can effectively manage decentralized ISs. Essay 5 explores how the public sector can successfully innovate with decentralized ISs, while Essay 6 examines the governance of blockchain-based systems. Essay 7 delves into how public sector organizations can identify and lever the affordances of SSI. By addressing these goals, this dissertation provides both theoretical insights and practical guidance for designing and managing emerging decentralized ISs to foster trust in digital interactions.

Keywords: Blockchain, self-sovereign identity, decentralization, digital trust, design, management.

Acknowledgments

Looking back on the past four years as a doctoral student, I am filled with gratitude for the incredible support, guidance, and encouragement I have received throughout this journey. I sincerely thank everyone who has had a role in making this dissertation possible.

I thank my academic supervisor, Nils Urbach, for his advice, mentorship, and support over the past four years. I also thank Jens Strüker for taking on the role of co-supervisor. My gratitude to the Frankfurt University of Applied Sciences, the University of Bayreuth, and Fraunhofer FIT for providing me with such a creative and supportive environment for my research.

My gratitude to my friends, co-authors, and colleagues. It is a privilege to work alongside such talented, intelligent, and warm-hearted individuals. This dissertation would not have been possible without your invaluable support, encouragement, and advice. Every day I'm inspired anew by how much I can learn from every one of you.

My heartfelt gratitude and appreciation to my family: To my parents, Werner and Waltraud, for their unwavering love, encouragement, and trust in me. To my siblings, Lisa and Daniel, and their partners, Julian and Sina, thank you for your love, constant support, and for always being there to listen. I am profoundly grateful to my nieces – Ida, Betti, Klara, and Lotta – whose wonderful spirits and joyous presences have brightened even the most challenging of days. A special note of appreciation to my sister, Hanna, for her exceptional empathy, love, and invaluable support. Your care and understanding have provided immense comfort throughout this journey.

Finally, my deepest gratitude to my fiancée, Lili, for your boundless love, unwavering support, and incredible patience and encouragement. You have lifted me up during the toughest moments and celebrated every success by my side. Your belief in me has been a gift beyond words, and I am profoundly grateful for your presence in my life.

Frankfurt, January 2025

Simon Feulner

Abbreviations and Initializations

A-E-A	affordance-experimentation-actualization
DeFi	decentralized finance
DSR	design science research
DP(s)	design principle(s)
EUDI-Wallet	the European Digital Identity Wallet
GDPR	the General Data Protection Regulation
IoT	Internet of things
IM	identity management
IS(s)	information system(s)
IT(s)	information technology/ies
KYC	know your customer
P2P	peer-to-peer
PoC	proof of concept
PoW	proof of work
RG(s)	research goal(s)
SSI	self-sovereign identity
SSO	single sign-on
UTAUT	the Unified Theory of Acceptance and Use of Technology
VCs	verifiable credentials
VPs	verifiable presentations
ZKP(s)	zero-knowledge proof(s)

Table of Contents

Introduction to *Fostering Digital Trust in the Digital Age: On the Design and Management of Emerging Decentralized Information Systems*

Abstract

This cumulative dissertation seeks to guide organizations in designing and managing emerging decentralized information systems (ISs). It consists of seven essays, organized around three primary research goals. Through its findings, this dissertation contributes to IS research by shedding light on the potential roles and impacts of emerging decentralized ISs in fostering digital trust.

In the following introduction, I motivate the relevance of research on emerging decentralized ISs and digital trust (Section 1), outline conceptual and technical foundations (Section 2), illustrate the gaps in research and questions addressed by this dissertation (Section 3), present the applied research methods (Section 4), summarize the seven essays' results (Section 5), and conclude with a discussion of the essays' results and contributions, limitations, and potential avenues for further research (Section 6).

Keywords: Blockchain, self-sovereign identity, decentralization, digital trust, design, management.

Table of Contents – Introduction

1 Motivation

In the digital age, digital technologies and rapid technological advancements have become integral to our daily lives. As these digital technologies become embedded in every aspect of our society, and as human interactions increasingly take place online, new complexities arise. In particular, the absence of tangible, visual cues in digital interactions complicate the process of building trust, making traditional trust signals both harder to interpret and easier to manipulate (Sasse & Kirlappos, 2014). Recent surveys have recorded a worrying decline in trust in technology, science, and social institutions (Edelman, 2021; KMPG, 2022; Public Affairs Council, 2021; World Economic Forum, 2022). Failures of private and public sector organizations – from governance lapses and ethical misconduct to technical issues such as artificial intelligence (AI) mishaps, privacy breaches, and severe security incidents – have significantly eroded public confidence (World Economic Forum, 2022). A stark example of this erosion of trust can be seen in the financial sector; the 2007/8 global financial crisis severely damaged public confidence in financial institutions, leading to widespread calls for greater transparency, higher integrity, and increased oversight (Cheng, 2020).

It was into this environment of financial instability and diminishing confidence in traditional financial institutions that Bitcoin was introduced by Satoshi Nakamoto in 2008. Bitcoin promises an alternative financial system independent of centralized control by banks or governments (Gramlich et al., 2023). This cryptocurrency operates on blockchain technology, which utilizes transparent and immutable distributed ledgers and decentralized consensus mechanisms to ensure trustworthiness without the need for a trusted central authority. Owing to its promises to resolve trust issues in various industries and applications, including supply chain management, the Internet of things (IoT), and healthcare (Attaran, 2022; Lacity, 2018; Lockl et al., 2020), *The Economist* (2015) called blockchain a “trust machine.”

The emergence of blockchain-based IS and the growing blockchain community subsequently sparked a broader movement for decentralization and propelled the development of further decentralized technologies, particularly in the area of decentralized identity management (IM). Most notably, self-sovereign identity (SSI) emerged, aiming to give individuals full control over their digital identities and allowing them to manage and share their information securely without relying on a centralized authority

(Mühle et al., 2018). A common thread across these emerging decentralized technologies is their potentials to foster digital trust by providing users with greater control and transparency while also reducing centralized parties' power and control. As Lumineau et al. (2021, p. 515) put it, they "offer a way to address a crisis of confidence in traditional institutions [...] especially given that individuals often desire greater access to and transparency of information that has been controlled mostly by large entities."

Despite these promises, however, public and private sector organizations still struggle to lever blockchain and SSI for building trustful digital processes, products, and services (Al-Shamsi et al., 2022; Guggenberger et al., 2023). This is partly owing to the fact that designing decentralized ISs requires different approaches and paradigms (Udokwu et al., 2020). New prescriptive knowledge (e.g. in the form of reference architectures and frameworks) and design theories (e.g. in the form of DPs) are required to enable organizations in building effective decentralized and trustworthy ISs (Nærland et al., 2017; vom Brocke et al., 2020). Further, companies face additional managerial challenges. In particular, organizations often struggle to assess the value of blockchain and SSI-based use and business cases, or to successfully manage implementation projects owing to the high levels of complexity, uncertainty, and ambiguity involved when innovating with these emerging decentralized technologies (Guggenberger, 2023; Rotolo et al., 2015; Zavolokina et al., 2020). New approaches and methods are required to effectively manage IS levering blockchain and SSI. This dissertation, which comprises seven individual essays, seeks to derive valuable insights and to contribute to societal advancements by examining "how to design and manage emerging decentralized IS to foster trust in digital interactions."

The remainder of the introduction to my dissertation is structured as follows: Section 2 provides the conceptual and technical foundations of emerging decentralized ISs and digital trust. Section 3 illustrates the gaps in research and questions addressed in the seven essays, while Section 4 explains the reasoning for the applied research methods. Section 5 presents the seven essays' results, followed by a concluding discussion on my dissertation's contributions to theory and practice, limitations, and potential avenues for further research.

2 Background

2.1 Conceptualizing Decentralized Information Systems

ISs are integral to the functioning of modern organizations, enabling businesses to efficiently collect, process, and analyze information. With the rapid advancement of technology, ISs' importance has grown exponentially, making them indispensable tools for enhancing productivity, lowering costs, and fostering innovation. Chatterjee et al. defined IS as "superordinate systems composed of social and technical subsystems, with information playing a key role that captures the state and behavior of these superordinate systems" (Chatterjee et al., 2021, p. 556). Thus, ISs not only have a technical component, comprising of devices, tools, and techniques that transform inputs into outputs (Sykes et al., 2014), but also a social component, consisting of individuals (and their skills, knowledge, and values), structures, as well as their interrelationships (Lee et al., 2015).

Following seminal work by Baran (1964) and Leifer (1988), ISs can be can be broadly classified into centralized, distributed[1], and decentralized systems. *Centralized ISs* consist of a central processing unit that manages data processing and storage (Akoka, 1978; Baran, 1964). *Distributed ISs* spread data processing and storage across multiple nodes, incorporating central hubs to coordinate activities and manage resources while local terminals handle specific tasks at various locations (Leifer, 1988; Nack, 1982). *Decentralized ISs* operate without a central authority or central hubs for processing information, distributing control and decision-making across all nodes (Agre, 2003; Durr, 1987; Leifer, 1988).

While the sharp classification of ISs into centralized, distributed, and decentralized ISs is a valuable initial orientation, a spectrum from centralized to decentralized systems depicts reality better (Ein-Dor & Segev, 1978) – both the technical and social subsystem of an IS can be characterized by varying degrees of decentralization. For the social subsystem, key influencing factors include the degree of decentralization of 1) the organization in which an IS is implemented, 2) the IS development and implementation efforts, and 3) the IT department. For the technical subsystem, the degree of

[1] Baran and Leifer both distinguish between centralized, distributed, and decentralized IS. However, ISs defined by Baran as distributed are defined by Leifer as decentralized, and vice versa. I follow Leifer's definitions.

decentralization is influenced by 1) the extent to which computer equipment is geographically dispersed and 2) the extent to which data are concentrated in databases (Ein-Dor & Segev, 1978; Walsham, 1993).

Questions regarding the decentralization of IS initially focused on configurations in individual companies. The rise of the Internet and web technologies subsequently enabled organizations to interconnect their systems, share data, and collaborate more effectively (Atluri et al., 2007). Further, peer-to-peer (P2P) systems emerged, allowing end-users to share digital resources directly (Agre, 2003; Buchegger & Datta, 2009). However, the debate around decentralization only gained significant momentum in recent years owing to shifting political and economic environments, most notably with the emergence of blockchain and SSI, as I will discuss in the next sections.

2.2 Foundations of Blockchain

In October 2008, a white paper titled Bitcoin: A Peer-to-Peer Electronic Cash System (Nakamoto, 2008) was released on a cryptography mailing list. It outlined a revolutionary digital currency system enabling online payments to be transferred directly between parties without the involvement of a financial institution. Bitcoin's underlying technology, known as blockchain, has since attracted a great deal of interest in both research and practice. A blockchain is a distributed digital ledger that maintains a record of all transactions across a network of computers (F. Glaser, 2017). It functions within a peer-to-peer network, with each participant retaining a complete copy of the blockchain. To validate new transactions, blockchains employ a consensus mechanism. In Bitcoin's case, this mechanism is known as proof of work (PoW), where miners solve intricate mathematical problems to append new blocks to the blockchain. This process ensures that all transactions are verified and agreed upon by the majority of the network (Butijn et al., 2021; Kolb et al., 2021). To ensure immutability, each block includes a cryptographic hash of the preceding block. The linkage of blocks through cryptographic hashes forms a chain, making it extremely difficult for any malicious actor to alter the data without altering all subsequent blocks, which would require immense computational power (Butijn et al., 2021; F. Glaser, 2017).

Blockchain technology is often described as a breakthrough development with the potential to disrupt existing businesses and industries (Beck & Müller-Bloch, 2017; Lage et al., 2022). This technology promises to enable trusted transactions and data-sharing

across organizational boundaries where parties need not rely on a central authority or intermediaries. Thus, blockchain may pave the way for more sophisticated and trusted decentralized applications and systems (Lage et al., 2022). Particularly the following key features are at the center of attention:

- **Transparency:** Blockchain's inherent transparentness ensures that all participants have access to the same data, potentially promoting accountability and reducing the potentials for fraud (Beck & Müller-Bloch, 2017).
- **Immutability:** Once recorded on a blockchain, data cannot be changed or removed, guaranteeing the integrity and authenticity of the information. This is crucial for applications that require reliable audit trails (Lashkari & Musilek, 2021).
- **Automation:** Blockchains can utilize smart contracts to automate processes and transactions, reducing the need for manual interventions and intermediaries, potentially lowering costs and increasing efficiency (Khan et al., 2021).

Owing to these features, both practitioners and researchers have explored the uses of blockchain in various fields such as supply chains, finance, or healthcare. For instance, in a case study, Lacity and van Hoek (2021) investigated how Wallmart Canada applied blockchain technology to improve freight invoice processing. This blockchain-based approach has significantly improved efficiency in Walmart Canada's logistics, allowing it to cut disputed invoice rates from over 70% to less than 2%. Similarly, Chronicled's MediLedger uses blockchain to ensure compliance with Food and Drug Administration (FDA) regulations for medicine traceability by enhancing transparency and security in the pharmaceutical supply chain (Mattke et al., 2019). Gramlich et al. (2023) contributed to our understanding of the promises and challenges of decentralized finance (DeFi) by providing a multivocal literature. In particular, they highlighted the potentials of a decentralized and democratized financial system based on blockchain. Attaran (2022), among others, studied opportunities and challenges of applying blockchain as an underlying, trusted infrastructure for managing patients' health records, maintaining comprehensive medical histories, and securely granting access to health data.

While blockchain technology is still emerging and evolving, it faces various technical challenges that may hinder its widespread adoption. First, scalability remains a significant issue, as blockchain networks can become slow and inefficient with increasing

numbers of transactions, leading to delays and higher costs (Lim et al., 2018). Second, usability and key management pose significant challenges, since managing cryptographic keys can be challenging and daunting for users. These keys are similar to highly sensitive passwords, but instead of being stored in a familiar way (e.g. saved in a browser), they require secure handling through specialized software or hardware, such as wallets. If users lose these keys or fail to properly store them, they may permanently lose access to their accounts or funds. Further, poorly protected keys can be stolen by hackers, leading to unauthorized access and potential financial loss (Fridgen et al., 2019). Third, privacy protection is a concern, as blockchain's transparentness can lead to the exposure of transaction details and user identities, making it hard to maintain confidentiality (Rieger et al., 2019). Finally, the oracle problem presents a further challenge, as blockchain relies on external data sources (oracles) to interact with the outside world, which can introduce vulnerabilities and trust issues if the data provided are inaccurate or are manipulated (Caldarelli, 2020; Lumineau et al., 2021).

2.3 Foundations of Self-Sovereign Identity

Another significant development in decentralized IS is the concept of SSI. In recent years, digital identities are increasingly controlled by companies such as Facebook or Google. These trusted third parties offer user-friendly single sign-on (SSO) solutions, enabling the use of digital identities across company and system boundaries (Schlatt et al., 2022). However, such services are problematic from the privacy and security perspective, as demonstrated for instance by the massive data breach in 2018 that impacted on more than 50 million Facebook users (Newman, 2020). SSI can be regarded as a paradigm shift in digital IM, giving users full control over their digital identities (Wang & Filippi, 2020). It allows individuals to manage and share their digital credentials and attestations without the need to rely on trusted third parties, akin to managing physical identity documents such as plastic cards in physical wallets (Schlatt et al., 2022).

Physical documents – such as standardized ID cards – are represented in SSI using a tamper-proof format called verifiable credentials (VCs) (Preukschat & Reed, 2021; Sporny et al., 2022). Instead of relying on third parties for storing and transferring information, credential holders manage their VCs in an identity wallet or digital wallet, typically on their mobile phones (Lesavre, 2020). Credential-holders can prove certain

claims to relying parties by transmitting so-called verifiable presentations (VPs). A verifiable presentation can thereby contain claims from multiple VCs. Public key cryptography is then used to verify the credentials' integrity and authenticity (Ehrlich et al., 2021). In some SSI implementations, blockchain serves as a technological backbone owing to its decentralized, transparent and immutable nature. For instance, some SSI projects apply blockchains to record institutions' public keys (Ehrlich et al., 2021) or to record revocation information in a highly trusted decentralized infrastructure (Feulner et al., 2022).

The SSI paradigm offers promising features that align with contemporary demands for privacy, security, efficiency, and compliance. By using cryptographic techniques, SSI ensures that personal data are only accessible by authorized parties, significantly reducing the risk of data breaches and identity theft (Schlatt et al., 2022). Further, users can selectively disclose information, sharing only the necessary details for a particular transaction or interaction, thereby minimizing the exposure of sensitive data (Der et al., 2017). SSI also holds potentials for improving interoperability across different platforms and services. Utilizing standardized protocols such as VCs, SSI allows for seamless and secure interactions across diverse systems without requiring users to create multiple accounts and remember multiple passwords. This approach enhances user convenience and reduces friction in digital interactions (Ehrlich et al., 2021; Feulner et al., 2022).

Several governmental and corporate initiatives, along with academic studies, are actively exploring SSI's potentials (Ehrlich et al., 2021). Germany's government, for instance, invested no less than €45 million to develop secure digital identities. This investment is being channeled into several funded projects that are exploring the development and application of SSI solutions across various domains (Federal Ministry for Economic Affairs and Energy, 2021). Researchers have also studied the application of SSI for various usage cases such as improving know your customer (KYC) processes (Schlatt et al., 2022), IoT interactions (Fedrecheski et al., 2020), event ticketing systems (Feulner et al., 2022) or seamless mobility-as-a-service solutions (Hoess et al., 2024). Recently, the European Commission has even decided to initiate the European Digital Identity Wallet (EUDI-Wallet), an ambitious SSI-based initiative to provide EU citizens with a secure, unified digital identity wallet by 2026 (European Commission,

2024). These initiatives highlight the growing recognition of SSI's potentials to transform digital IM.

While its potentials are widely recognized, the SSI paradigm and particularly its current practical implementations still pose challenges. First, managing backups and cryptographic keys is a critical challenge for SSI. Users are responsible for storing and protecting their private keys, which are essential for accessing and controlling their digital identities. Loss or compromise of these keys can lead to permanent loss of access to identity credentials and associated data (Lesavre, 2020). Second, SSI systems aim to ensure that identity credentials are securely bound to the rightful owner and prevent unauthorized sharing. This challenge involves implementing strong authentication methods to verify that the person who presents the credential is in fact its owner. While biometrics, multifactor authentication, and secure devices can help, these methods must be user-friendly and widely accessible to ensure that they are adopted (Camenisch & Lysyanskaya, 2001; Hardman et al., 2019). Third, regulatory challenges arise from the lack of clear guidance and standards for SSI implementation. Different jurisdictions have varying data protection laws and identity verification requirements, creating a fragmented regulatory landscape. This uncertainty can hinder the development and adoption of SSI solutions, as organizations may struggle to comply with multiple and sometimes conflicting regulations (Preukschat & Reed, 2021).

2.4 Emerging Decentralized Information Systems as Enablers of Digital Trust

Trust has pivotal roles in various aspects of our daily lives, including personal, economic, and professional relationships and interactions. Trust can be defined as "the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor" (Mayer et al., 1995, p. 712). The level of trust placed in other parties is subjective and is influenced by (in)direct knowledge of past interactions. A strong reputation, built over time through consistent positive interactions, can significantly enhance perceived trustworthiness. Conversely, a poor reputation, resulting from negative behaviors or unreliability, can undermine trust and make others hesitant to engage (Aberer & Despotovic, 2001; Mattila & Seppälä, 2016; Yan & Holtmanns, 2013). In addition to reputation-based mechanisms, trust is often established and reinforced by legal

frameworks, particularly in business settings or financial matters. These legal frameworks ensure that any misconduct can be penalized through legal actions (Yan & Holtmanns, 2013).

While building trust is often hard in the physical world, things become even more complicated in the digital world. In remote digital interactions, gathering reliable information for establishing and cultivating trust is challenging, because information can be easily tampered with and fake identities can be used (Yan & Holtmanns, 2013). Mattila and Seppälä (2016) argued that building digital trust requires security, identifiability, and traceability. Security in digital interaction means that the utilized systems and data as well as the provided products and services are protected against attacks, manipulation, and interruptions. It also means that individuals maintain control over the privacy of their personal data. For building digital trust, the parties involved further require ways to ensure that their transaction partners are in fact who they claim to be. Finally, traceability enables parties in digital interactions to transparently verify whether commitments are met within the agreed terms and conditions (Dobrygowski, 2022; Mattila & Seppälä, 2016).

As it is often hard for individuals to evaluate these features, they have little choice but to rely on their transaction partners' reputations (Mattila & Seppälä, 2016). However, the emergence of blockchain and SSI-based ISs may well positively disrupt the creation of digital trust. As discussed above, blockchains provide an effective way to transparently and immutably record information and ensure that code-based rules and agreements are automatically enforced by the decentralized network (Filippi & Wright, 2018; Lumineau et al., 2021). SSI enables parties to reliably and securely prove certain claims about their identity in the digital world without relying on centralized authorities (Schlatt et al., 2022). Thus, both blockchain and SSI have the potentials to facilitate digital interactions where trust is embedded in the decentralized provision and operation of the technological infrastructure rather than in centralized intermediaries.

3 Deriving the Research Goals, Gaps, and Questions

In this dissertation, I investigate *how to design and manage emerging decentralized ISs to foster trust in digital interactions*. Following on from my overarching research aim, I derive three distinct research goals:

RG1: Understand blockchain's potentials to enable trustful digital interactions without the need for a trusted central party.

*RG2: Guide organizations in **designing** trustworthy decentralized ISs.*

*RG3: Guide organizations in **managing** emerging decentralized ISs.*

To achieve these research goals, I identify gaps in the research and derive research questions, which I address in this dissertation through seven individual essays. In the following, I describe the specific research gaps and corresponding research questions addressed in each of the essays.

3.1 RG1: Understand the potentials of blockchain for enabling trustful digital interactions without the need for a trusted central party

Since the advent of blockchain technology in 2008, its potentials to disrupt traditional business models and industries have been widely acknowledged by researchers and practitioners (Beck et al., 2018; Schweizer et al., 2020). A core feature of blockchain is its decentralized design, potentially enabling participants to conduct trustful digital transactions without the need for a trusted third party. This has led many to view the removal of intermediaries, also denoted as disintermediation, as a fundamental aspect of blockchain's impacts on businesses (Chalmers et al., 2021).

However, the research into intermediation's roles in blockchain remains highly fragmented, with a wide range of propositions, approaches, and perspectives. While a significant portion of the literature posits that disintermediation is intrinsic to blockchain technology (Chalmers et al., 2021; Pereira et al., 2019; Perscheid et al., 2020), other researchers suggest a more nuanced perspective. These studies suggest that blockchain often reconfigures rather than eliminates intermediaries, introducing new roles or redefining existing ones to address gaps left by decentralized processes (Chong et al., 2019; Zeiß et al., 2024). This phenomenon is also referred to as re-intermediation. Despite growing recognition that blockchain can both displace and create intermediaries,

existing research provides limited insights into the specific conditions under which new intermediaries emerge and how these roles differ from traditional gatekeepers. Furthermore, there is a lack of evidence on how different blockchain architectures, stakeholder interactions, and regulatory pressures influence the transition from disintermediation to re-intermediation. This gap hinders organizations' ability to anticipate how blockchain might reshape business models or redefine institutional roles.

Thus, the existing studies have not provided a comprehensive framework for understanding the varied and evolving roles of intermediaries in blockchain-enabled ecosystems. To fill this gap in the research, we[2] ask:

How and under what conditions do blockchain solutions transition from disintermediation to re-intermediation, and what factors most significantly drive this transition? (Essay 1)

3.2 RG2: Guide organizations in designing trustworthy decentralized information systems

Emerging decentralized ISs such as blockchain and SSI provide an alternative approach for building trust in digital interactions, potentially decreasing the reliance on trusted third parties. While organizations can typically draw on extensive experience in the design of centralized ISs, designing decentralized ISs remains a particular concern (Beck et al., 2017; Rossi et al., 2019; Sedlmeir et al., 2021). The emerging nature of blockchain and SSI further increases the complexity, as these technologies are often characterized by rapidly evolving technical standards, limited interoperability, and missing or underspecified regulatory guidelines (Preukschat & Reed, 2021; Rieger et al., 2019; Sedlmeir et al., 2022). This makes it hard for organizations to develop robust and scalable decentralized solutions that meet organizational goals, regulatory requirements, and users' expectations.

Enabling trustworthy digital interactions is particularly important in the context of KYC processes. Various regulations require financial institutions to perform in-depth due diligence to verify the identity of their customers and understand their activities' purposes (Arasa, 2015; Arner et al., 2018). Traditional KYC processes, which often

[2] As all the essays in this dissertation are the result of collaborative work and thus written in co-authorship, I use the plural *we* when referring to these studies' results.

necessitate physical presence or video calls for identity verification, are costly, time-consuming, and inconvenient for customers (Zetzsche et al., 2018). Efforts to digitalize the KYC process have had limited success. For instance, banks have attempted to create digital customer identities from analog proofs such as passports. However, these approaches are still error-prone, repetitive, and hindered by the lack of shared standards and interbank collaboration, limiting KYC data's reusability across institutions (Arner et al., 2018; Jessel et al., 2018). Centralized digital solutions – such as those implemented in India and Australia – have been proposed to streamline the KYC process (Zetzsche et al., 2018). While these solutions can reduce costs and accelerate onboarding, they are fraught with risks relating to data privacy and security. Reports of data leaks and misuse have eroded trust in centralized systems, and concerns about the centralization of power further impede their widespread adoption (Rieger et al., 2019; Swinhoe & Hill, 2022; Zavolokina et al., 2020).

One emerging alternative is the concept of SSI. Instead of relying on centralized KYC providers, SSI enables users to manage and selectively share their own KYC-related information. Despite SSI's potentials, research in this area remains nascent and fragmented. A recent study by Soltani et al. (2018) explored SSI-based eKYC onboarding, but did not fully addressed user orientation, comprehensive coverage of the KYC process, or platform independence. Further, Soltani et al. overlooked the practical implications for banks and blockchain's broader role in facilitating SSI. Thus, the IS research still lacks a generic and validated framework to guide the design of SSI solutions for eKYC processes. There is also a need for generic DPs that can be applied to blockchain-based SSI solutions across various sectors. To fill this gap in the research, we ask:

How to design and conceptualize trustworthy digital KYC processes built on blockchain-based SSI, and which generic DPs can be derived? (Essay 2)

Digital trust also holds significant potentials in the event ticketing market. Current event ticketing systems face significant challenges, particularly owing to the prevalence of scalping and fraud in the secondary market. Bots, which account for approximately 40% of traffic on ticketing portals (Imperva, 2019), create fake identities to purchase tickets in bulk and resell them at inflated prices (Glaap & Heilgenberg, 2019). Customers' trust is further undermined as a result of counterfeit or invalid tickets, with no effective way for consumers to verify the authenticity of tickets on the secondary market (Regner et al., 2019). Several approaches have been proposed to address these

issues, such as dynamic QR codes (Hookings, 2019). However, these solutions often prove cumbersome, costly, or easily circumvented by savvy scalpers, who can create multiple accounts or can transfer login credentials (GUTS Tickets, 2020).

Blockchain technology has also been suggested as a potential solution for improving ticket ownership verification and the regulation of secondary markets (Cha et al., 2018; Li et al., 2019; Regner et al., 2019). By levering smart contracts and nonfungible tokens (NFTs), event organizers could theoretically enforce rules and price limits transparently. Nonetheless, blockchain-based systems face their own challenges, particularly concerning data protection regulations such as GDPR and the ease with which blockchain accounts can be created and transferred, thereby ineffectively addressing the issue of weak identity binding (Corsi et al., 2019; Regner et al., 2019).

SSI presents a novel approach to these challenges by enabling stronger user-to-ticket binding. With SSI, users manage their identity-related documents (including digital tickets) in a digital wallet on their smartphones. This system could potentially offer a more secure, efficient, and privacy-preserving way to control ticket ownership and the secondary market. However, while the SSI concept is promising, both research and practice still need guidance in designing SSI-based event ticketing systems to effectively address prevailing challenges such as ticket fraud and scalping. There is also a lack of generic DPs for applications in event ticketing and similar contexts that require efficient, privacy-oriented, and reliable identity verification. To address this gap in the research, we ask:

How to design and conceptualize trustworthy digital event ticketing systems built on SSI, and which generic DPs can be derived? (Essay 3)

Current car IM systems face significant challenges, in both their physical and digital implementations (Castella-Roca et al., 2017). Physical identifiers – such as license plates, inspection stickers, and parking permits – are prone to theft, damage, and counterfeiting, leading to trust issues owing to unauthorized uses, fraudulent claims, and tampering with essential vehicle records such as odometer readings (Alessandria & Vizzarri, 2021). Such vulnerabilities contribute to substantial financial losses, as evidenced by odometer fraud of an estimated €58 billion in Europe in 2017 and global car insurance fraud of $83 billion in 2021 (Benedek et al., 2022; Borkowski, 2019).

Further, reliance on manual verification processes makes these systems inefficient and error-prone.

While they are more advanced, digital car identifiers are not without issues. Components such as black boxes, onboard serial numbers, and SIM cards introduce privacy risks and are often managed through centralized databases. This centralized approach creates single points of failure, exposing sensitive data to potential breaches, unauthorized access, or misuse (Rabby et al., 2019). Further, scalability remains a challenge, as centralized systems struggle to accommodate fluctuating traffic volumes and diverse data processing needs (Santana et al., 2018). Thus, existing systems have failed to balance the needs for privacy, security, and interoperability, leaving users and organizations exposed to fraud, inefficiencies, and privacy breaches.

Emerging decentralized identity systems, specifically SSI, offer a potential solution. SSI enables users to manage their identity credentials independently, ensuring security and privacy without any reliance on centralized storage (Preukschat & Reed, 2021). This decentralized model has proven effective in other domains and is gaining traction under frameworks such as the EU's eIDAS 2.0 regulation. However, the application of SSI to car IM remains underexplored, leaving questions about its feasibility, scalability, and integration with existing systems. To address this gap in the research, we ask:

How to leverage SSI to design a holistic and privacy-preserving framework for managing digital car identities? (Essay 4)

3.3 RG3: Guide organizations in managing emerging decentralized information systems

Owing to the paradigm shift toward decentralized systems, organizations innovating through emerging decentralized ISs are facing a number of new managerial challenges, such as identifying and evaluating viable usage and business cases for their respective application domains or assessing the impacts of adopting these technologies on their organization (Du et al., 2019; Gatteschi et al., 2020; Long et al., 2023; Zavolokina et al., 2020). Companies must further ensure that they build and operate decentralized IS in trustworthy, effective, and sustainable ways, for instance by establishing suitable development and governance structures (Beck et al., 2018; Zavolokina et al., 2020).

Innovating by means of emerging decentralized ISs in the public sector presents a unique set of challenges, despite the significant potentials for improving public services such as education, healthcare, social security, and public safety. Digital innovation offers opportunities to deliver these services more efficiently, cost-effectively, and in ways that are more citizen-centric and trustworthy (Eggers et al., 2024). However, many governments face substantial difficulties in integrating these innovations into their existing frameworks (Amend et al., 2025; Goh & Arenas, 2020; Pahlka, 2023).

The primary obstacles stem from deep-seated structural and cultural barriers within government organizations (Meijer, 2015; Pahlka, 2023), which are often the result of complex and sometimes conflicting policies that shape governmental operations. Such policies influence organizational structures, leading to rigid processes, top-down decision-making, complex IT architectures, and inflexible budgeting procedures (Goh & Arenas, 2020; Scott et al., 2016). These factors collectively foster a bureaucratic culture that resists change and innovation, making it hard for governments to adopt new technologies and approaches (Caudle et al., 1991; Goh & Arenas, 2020; Thacher & Rein, 2004).

Emerging technologies such as blockchain and SSI exacerbate these challenges owing to their early-stage development and the often-exaggerated narratives surrounding their potentials (Shiller, 2019; Vassilakopoulou et al., 2023). Early in their lifecycles, these technologies are not only immature but also poorly understood, which leads to a flood of hyperbolic claims about their transformative capabilities. These claims are often vague and lack practical coherence, particularly when driven by broad public discourse (Miranda et al., 2022; Shiller, 2019; Wang, 2010). This creates a polarized environment in which initial enthusiasm is often followed by a wave of skepticism and criticism, further complicating the adoption process (Swanson & Ramiller, 2004; Swanson & Ramiller, 1997).

Thus, practitioners and researchers lack insights into how governments can successfully navigate these structural and cultural barriers to effectively innovate by means of emerging decentralized ISs. This includes identifying viable usage cases that align with government needs, overcoming organizational resistance and securing the necessary political and public support. It is crucial to address these gaps so as to enable public sector organizations to lever the full potentials of emerging decentralized ISs. Thus, we ask:

How can public sector organizations successfully innovate by means of emerging decentralized ISs? (Essay 5)

The need for new and effective management insights and approaches is also evident in the context of building and governing trustworthy decentralized intergovernmental ISs. The increasing digitalization of public sector services requires substantial investment and coordination across various levels of government. However, translating these investments into more secure, trustworthy, and efficient services is complex, particularly when cooperation across different levels of government is necessary (Pahlka, 2023; Roth et al., 2023). Each level of government – federal, state, or local – operates under distinct legal competencies and budgets, leading to separate ISs that are often incompatible with one another. This separation results in fragmented and multilayered IT architectures that hinder efficient information exchange and complicate modernization efforts (Pahlka, 2023). One emerging solution to these challenges is the use of blockchain. Blockchains, with their decentralized and transparent nature, offer a promising avenue for improving intergovernmental collaboration (Rieger et al., 2019; Roth et al., 2023). They can enable secure and tamper-proof information exchange across different governmental ISs, ensuring that data integrity is maintained (Roth et al., 2023). Further, blockchains can facilitate automated and rules-based processes by means of smart contracts, reducing the need for manual intervention and thereby increasing intergovernmental services' efficiency and reliability (Rieger et al., 2019).

However, the implementation of blockchain-based approaches in a multilevel governmental context raises questions about interoperability with existing IT systems, joint development efforts, and effective governance. Ensuring interoperability with existing systems is very challenging, because the multilayeredness of many legacy IT systems often results in legacy IT systems that are harder to adapt and extend than the legal frameworks they support (Pahlka, 2023). Also, trustworthy development is crucial, as the success of intergovernmental blockchain systems depends on each participating entity's willingness to share data and collaborate transparently. Further, there is a need to establish clear governance frameworks that define the roles and responsibilities of different governmental entities in deploying and maintaining a blockchain-based solution (Beck et al., 2018; Zavolokina et al., 2020). Thus, while blockchain holds promise for enhancing intergovernmental collaboration, further insights are needed to address the challenges of building and governing these systems.

To fill this gap in the research, we ask:

How to build and govern blockchain-based intergovernmental ISs? (Essay 6)

As digital interactions increasingly dominate our lives, managing digital identities in trustworthy ways has become a critical and contested issue. Traditional IM systems such as federated systems place significant control over user data in the hands of enterprises, raising concerns about privacy and security (Maler & Reed, 2008). To address these issues, the SSI concept has emerged, shifting control of digital identities from centralized entities to individuals. SSI promises to reduce operational complexity and lower costs, and to enhance user control and portability of identity data (Mühle et al., 2018; Preukschat & Reed, 2021), making it an attractive solution for public sector organizations responsible for identity provision.

Despite the public sector's growing interest in SSI, demonstrated by significant investments, there is a notable gap in the research regarding understanding how public sector organizations can discover and actualize the affordances provided by SSI. While SSI's benefits for users are well recognized, little is known about how these benefits translate into organizational value in the public sector, particularly given the scarcity of productive SSI applications today (Cucko & Turkanovic, 2021). The process of realizing SSI's potentials in public sector organizations involves more than just adopting new technologies; it requires a deep understanding of how SSI can reshape business processes and systems. This includes recognizing and actualizing SSI affordances (Leidner et al., 2018). However, the path from experimentation to actualization is complex and underexplored, particularly regarding the human and organizational capabilities needed to effectively harness SSI (Du et al., 2019).

While there has been technical research into SSI and its potential opportunities, we still lack a holistic understanding of SSI's value and practical guidance for implementing SSI-based applications in the public sector. It is crucial to address this gap, particularly given the significant financial investment required for large-scale SSI systems, such as the EUDI-Wallet, which is estimated to cost more than €600 million (European Commission, 2021). Research is needed to reduce the complexity and risks associated with SSI implementation, ensuring that public sector organizations can fully lever its affordances to deliver more secure, efficient, and citizen-centric services. To address this gap in the research, we ask:

Which affordances does SSI offer within an organizational setting?

How can the public sector experiment with and actualize the SSI affordances?

(Essay 7)

Table 1 presents a summary of the seven essays included in this cumulative dissertation and how they address my research goals. A list of my other publications, which are not part of this dissertation, is provided in Appendix B.

Table 1: Overview over the Seven Research Essays, which Address the Identified Research Goals

Title	**Publication outlet**	**VHB JQ4 ranking**	**Publication status**
RG1: Understand blockchain's potentials for enabling trustful digital interactions without the need for a trusted central party			
Essay 1: Beyond Disintermediation: A Multiple Case Study of Emerging Intermediary Roles in Blockchain Applications	Electronic Markets	B	Under Review
Building on: Shedding light on the blockchain disintermediation mystery: A review and future research agenda	Proceedings of the 30th European Conference on Information Systems (ECIS)	A	Published
RG2: Guide organizations in designing trustworthy decentralized ISs			
Essay 2: Designing a Framework for Digital KYC Processes Built on Blockchain-Based Self-Sovereign Identity	Information & Management	B	Published
Essay 3: Exploring the Use of Self-Sovereign Identity for Event Ticketing Systems	Electronic Markets	B	Published
Essay 4: Driving Self-Sovereign Identity: Designing a Car Identity Management Framework	Business & Information Systems Engineering	B	Under review
RG3: Guide organizations in managing emerging decentralized ISs			
Essay 5: Recoding Asylum Management – How Germany's Federal Government Approached Innovation with Emerging IT	Scientific Journal	n/a	In preparation for submission
Essay 6: Bringing Government in the Digital Age – Insights from Germany's Asylum Procedure	MISQE	B	Published
Essay 7: Affordances, Experimentation and Actualization of Self-Sovereign Identity: A Case Study of the Implementation and Use of SSI in the Public Sector	Government Information Quarterly	B	Under review

4 Research Designs

In this section, I will outline the research designs employed in the seven essays to address my research goals and questions. In what follows, I will provide detailed explanations of the individual research approaches, data collection methods, and analytical techniques used to ensure reliable and valid findings. Table 2 summarizes the chosen research designs.

Table 2: Research Designs of the Seven Research Essays

Title	Research design
RG1: Understand blockchain's potentials for enabling trustful digital interactions without the need for a trusted central party	
Essay 1: Beyond Disintermediation: A Multiple Case Study of Emerging Intermediary Roles in Blockchain Applications	**Case study research** • Triangulation of various data sources, including eight interviews with experts. • Open, axial, and selective coding of the data. • Deriving an updated view of disintermediation in the context of blockchain-based ISs.
RG2: Guide organizations in designing trustworthy decentralized ISs	
Essay 2: Designing a Framework for Digital KYC Processes Built on Blockchain-Based Self-Sovereign Identity	**Design science research** • Problem identification and derivation of seven DOs based on a review of the KYC literature and insights from three interviews with experts. • Iterative development of an SSI-based eKYC framework. • Formative and summative artifact evaluation; 10 interviews with experts, analyzed using open and axial coding.
Essay 3: Exploring the Use of Self-Sovereign Identity for Event Ticketing Systems	**Design science research** • Examining the ticketing literature to identify key challenges, including scalping and ticket bots, and deriving five DOs. • Designing a framework and implementing a PoC for SSI-based event ticketing systems. • Providing a criteria-based artifact evaluation along the DOs based on eight interviews with experts.
Essay 4: Driving Self-Sovereign Identity: Designing a Car Identity Management Framework	**Design science research** • Identification of challenges and related DOs based on a literature review and expert interviews. • Iterative development of an SSI-based car IM framework. • Formative and summative artifact evaluation based on 10 interviews with experts, analyzed using open and axial coding.

Title	Research design
RG3: Guide organizations in managing emerging decentralized ISs	
Essay 5: Recoding Asylum Management – How Germany's Federal Government Approached Innovation with Emerging IT	**Clinical IS research** • Actively participating in the Federal Blockchain Infrastructure Asylum (FLORA) project; providing advisory services and working closely with project stakeholders. • Gathering extensive data on the innovation process over six years, including 98 semi-structured interviews and 1,000+ project pages. • Data analysis using a two-stage coding process and following the guidelines for grounded theory development.
Essay 6: Bringing Government in the Digital Age – Insights from Germany's Asylum Procedure	**Case study research** • Inductive research design to develop a deep understanding of how to build and govern blockchain-based intergovernmental ISs. • Triangulation of various data sources, including 98 interviews, direct observations from sprint reviews and management meetings, and project documentation such as conceptual and legal documents, meeting minutes, technical documentation, and white papers. • Data analysis using open and axial coding.
Essay 7: Affordances, Experimentation and Actualization of Self-Sovereign Identity: A Case Study of the Implementation and Use of SSI in the Public Sector	**Case study research** • Single-case study focused on a project aiming at improving tax verification processes by implementing SSI. • Several data collection methods, including 10 semi-structured interviews with experts, documentation, archival records, observations, and technical artifacts. • Three-phase coding approach using open, axial, and selective coding.

In Essay 1, we adopted the case study methodology to investigate blockchain technology's impacts on disintermediation. This approach allows us to draw insights from real-world situations and explore complex practical problems. Given the diverse effects of different blockchain technologies on disintermediation, we choose a multiple-case study approach to capture a broad range of impacts (R. Yin, 2008). We begin by reviewing the literature to identify any existing theories or hypotheses relating to our topic, as recommended by Eisenhardt (1989), though we found none that directly address blockchain and disintermediation. However, the literature on electronic markets provides a conceptual background. We then use theoretical sampling to select two cases from the finance and supply chain industry, which have been described as the most promising sectors for blockchain use cases (Chong et al., 2019). We also chose these sectors because they involve intermediaries in value creation, making them ideal for studying blockchain's effects on disintermediation (Allen & Santomero, 1997; Cole & Aitken, 2020). For data collection, we gather public information and project documentation, and conduct eight semi-structured interviews with experts over three months. The interviews, lasting between 35 and 60 minutes, provide 91 pages of transcripts, offering detailed insights into each case. We analyze the data using a three-

stage coding process of open, axial, and selective coding, as recommended by Corbin and Strauss (1990) as well as B. Glaser and Strauss (2017). In the open coding phase, we label relevant data passages, then refine these codes and develop categories during axial coding. Finally, in the selective coding phase, we unify the categories to prepare for our case write-up. We ensure reliable and rigorous findings through multiple workshops with all involved researchers. Following from our analysis, we provide an updated view of disintermediation in the context of blockchain systems that proposes a distinction between centralized and decentralized intermediation.

Essays 2, 3, and 4 each employ a design science research (DSR) approach to accumulate prescriptive knowledge on the design of emerging decentralized ISs. The DSR approach is well-suited for addressing unsolved 'wicked' problems in IS through an iterative build-and-evaluate process (Hevner et al., 2004). DSR outcomes typically include IT artifacts – such as constructs, models, methods, or instantiations – that provide both practical and theoretical contributions (Hevner et al., 2004; March & Smith, 1995).

In Essay 2, we follow the widely accepted DSR process model proposed by Peffers et al. (2007) to design a framework for digital KYC processes built on blockchain-based SSI. Peffers et al.'s (2007) approach has six sequential steps, allowing for an iterative and rigorous approach to developing a relevant IT artifact. The process typically begins with the identification of a research problem of practical relevance. In the case of KYC processes, this involves challenges such as low efficiency, security vulnerabilities, poor user experiences, and data protection issues. Based on these identified challenges, we define solution objectives to guide the creation of a meaningful artifact. These objectives are derived from a comprehensive review of the related literature and regulatory requirements concerning digital identification and authentication, leading to the design and development of our SSI-based eKYC framework.

The evaluation phase is crucial for testing the artifact's effectiveness and ensuring that it meets the defined objectives. This phase includes both formative and summative evaluations (Sonnenberg & vom Brocke, 2012; Venable et al., 2016), conducted through interviews with experts in KYC and SSI. The interviews allow us to assess the artifact's functionality, accuracy, reliability, utility, and fit within the organizational context. In sum, we record 320 interview minutes (an average of 35.6 minutes per interview). For data analysis, we employ grounded theory techniques, specifically open

and axial coding (Saldaña, 2016). This process involves creating 30 categories and 300 subcategories, which are later reassembled during axial coding to provide a more coherent understanding of the data (Corbin & Strauss, 2015; Saldaña, 2016). Building on our derived insights, we develop nascent DPs for blockchain-based SSI, contributing to both practical solutions and theoretical advancements in the field (Gregor & Hevner, 2013).

In Essay 3, we again draw on the DSR approach and follow Peffers et al.'s (2007) guidelines to develop and evaluate a novel SSI-based event ticketing framework. The first step involves identifying the problem, focusing on significant challenges in current event ticketing systems. Through an in-depth examination of both the event ticketing literature and existing systems, we identify scalping, ticket fraud, a lack of transparency in secondary markets, and difficulties in implementing centralized exchange models as the most critical challenges in event ticketing (Schneiderman, 2016; Waterson, 2016). Based on our understanding of the problem and on established requirements for event ticketing systems and secondary market control (Courty, 2019; Puigserver et al., 2012), we formulate five main design objectives (DOs) and several detailed subrequirements to guide the creation of our SSI-based ticketing framework. In the next step, we design and develop the SSI-based event ticketing framework, which we instantiate as a proof of concept (PoC). The design draws on foundational work in event ticketing (Courty, 2019) and seminal work on the foundations and applications of SSI (Preukschat & Reed, 2021; Schlatt et al., 2022). We then demonstrate the PoC to a panel of experts in SSI and event ticketing, gathering their feedback to iteratively refine the artifact. The following evaluation focuses on ensuring the artifact's understandability, applicability, and functionality, proving its effectiveness in addressing the identified challenges (Sonnenberg & vom Brocke, 2012). To gather rich data for the evaluation, we conduct qualitative interviews with carefully selected experts with extensive experience in SSI or event ticketing (Schultze & Avital, 2011). We chose these experts to provide diverse perspectives, ensuring that the evaluation considers both domain-specific and technical perspectives (Morse, 1990). We transcribe and analyze the interviews, which average 55 minutes each, using grounded theory techniques (Corbin & Strauss, 2015). We begin with open coding to identify initial categories and subcategories (Saldaña, 2016) and then employ axial coding to explore relationships and synthesize the findings into more abstract insights (Charmaz, 2006; Corbin & Strauss, 2015). From this analysis, we derive nascent DPs for efficient, reliable, and privacy-oriented ticket and

identity verification. These DPs provide a foundation for broader application and theoretical discussion, extending our framework's utility beyond the immediate case study. Finally, we communicate our research's results, contributing practical solutions and theoretical advancements to the field of event ticketing and digital IM.

In Essay 4, we also use a DSR approach based on Peffers et al. (2007) to ensure rigor and real-world applicability when designing a digital car IM framework (Hevner et al., 2004; vom Brocke et al., 2020). Our research process begins with identifying research problems and challenges in car IM, such as privacy concerns, inefficient verification, and the risks of manipulation. Based on the literature and regulatory directives, we define seven DOs to guide the framework's development. Building on these objectives, we design the IM framework as a tangible DSR artifact. The framework undergoes iterative evaluation through interviews with experts – essential for verifying that the DOs are well defined and that the artifact meets its intended purpose. We conduct three iterative cycles of semi-structured expert interviews, involving 10 experts with a combined interview duration of more than 455 minutes. The participants were selected based on their expertise in SSI, electric vehicle (EV) charging infrastructure, and smart mobility, providing insights into both theoretical soundness and technical feasibility. After reaching saturation in the evaluation phase, we perform deductive coding to map expert insights to the DOs and framework elements (Saldaña, 2016). This iterative approach ensures a robust and comprehensive IM framework grounded in both practice and theory. To enhance the theoretical contributions of the artifact, we develop three DPs for applying SSI in car IM and similar contexts where seamless interactions between diverse identity types is essential.

In Essay 5, we use a clinical research approach to examine how public sector organizations can successfully innovate by means of emerging decentralized ISs. Unlike other paradigms, clinical research emphasizes practical interventions where researchers actively collaborate with practitioners to solve real-world problems (Ågerfalk & Karlsson, 2020; Baskerville et al., 2023). In our case, three co-authors actively participate in the FLORA project conducted by Germany's Federal Office for Migration and Refugees, providing advisory services and working closely with project stakeholders from 2018 to 2024. The FLORA project was initiated in response to the challenges faced during Germany's asylum procedures, particularly during the 2015–2016 refugee crisis. The project sought to streamline the exchange of procedural information between the

Federal Office and state-level migration authorities, which had previously relied on outdated and inefficient methods such as paper lists and fax messages. By levering blockchain, the FLORA project sought to create a secure, transparent, and efficient system for sharing information across the various authorities involved in the asylum process. This initiative was part of the Federal Office's broader effort to modernize its IT infrastructure and enhance intergovernmental cooperation. The close collaboration with the Federal Office allow us to gather extensive data on the innovation process over six years, including 98 semi-structured interviews. These interviews were designed to be open-ended, encouraging participants to discuss their experiences freely, providing rich insights into the FLORA project's challenges and successes (Myers & Newman, 2007; Schultze & Avital, 2011). To ensure rich and accurate findings, we also examine more than 1,000 pages of project documentation, including conceptual, legal, and technical documents, as well as direct observations from project meetings, workshops, and sprint reviews. This allows us to triangulate our findings and gain a comprehensive understanding of the project's dynamics (Kuckartz & Rädiker, 2022). For data analysis, we employ a two-stage coding process, following Corbin and Strauss's (1990) guidelines for grounded theory development. We begin with open coding to identify initial themes and then use axial coding to explore deeper constructs, relationships, and theoretical explanations. The first and second authors lead the coding of interview transcripts and documents, while the third author, who was closely involved with the project, adds insights from participant observations. We use the MAXQDA software toolkit to manage the data and support the coding process. The findings are iteratively reviewed and refined by all authors, ensuring a comprehensive understanding of the challenges and strategies for successfully innovating by means of emerging ITs in a government context.

In Essay 6, we employ an inductive research design to develop a deep understanding of how to build and govern blockchain-based intergovernmental ISs, again focusing on the FLORA blockchain project by Germany's Federal Office for Migration and Refugees. Our longitudinal single-case study (R. K. Yin, 2017) spans six years, from the project's inception in early 2018 to its rollout across several German states by 2024. We selected the FLORA project owing to its potential to provide rich insights into the application of private blockchains. Analogous to Essay 5, we draw on the available data sources from our deep involvement with the FLORA project, involving 98 semi-structured interviews at various stages of the project. These interviews provide diverse

perspectives on building and governing blockchain-based intergovernmental ISs, including inputs from Federal Office employees, external consultants, researchers, IT service providers, senior management, and case workers. In addition to the interviews, we again draw on more than 1,000 pages of project documentation, including conceptual and legal documents, meeting minutes, technical documentation, and white papers. We also rely on direct observations from sprint reviews, workshops, and management meetings. We record, transcribe, and analyze interviews using grounded theory methods, supported by the MAXQDA software toolkit. Our data analysis begins with consolidating and clarifying the data, followed by a two-stage coding process (Corbin & Strauss, 1990). We start with open coding to identify initial concepts and then proceed to axial coding to explore themes, relationships, and aggregate dimensions. The first and second authors lead the coding process, while the third author contributes additional insights from participant observations. The iterative review of the findings with all authors and comparisons with academic literature ensures robust findings.

In Essay 7, we again employ a case study research design to explore the emerging phenomenon of SSI affordances in the public sector context. Case studies are well-suited for exploratory research, as they allow for the in-depth examination of complex socio-technical systems within their natural settings (Benbasat et al., 1987; Gephart, 2004; Majchrzak et al., 2000). As case studies generally aim for a detailed examination of the socio-technical context of IS use (Klein & Myers, 1999; Orlikowski & Iacono, 2001), they represent a common approach to study affordances in the IS research (Du et al., 2019; Keller et al., 2019; Seidel et al., 2013). Our single-case study focuses on a project initiated by a tax authority in Germany aimed at improving tax verification processes by implementing SSI. This project, which ran for six months, involved multiple stakeholders, including public institutions, researchers, and technology providers, making it a rich environment for studying SSI's affordances and how the public sector can experiment with and actualize these. To obtain a rich data set, we follow R. K. Yin (2014) and rely on several data collection methods, including data from interviews, documentation, archival records, observations, and technical artifacts. Specifically, we conduct semi-structured interviews with 10 key stakeholders involved in the project who represent a diverse range of organizations, including the tax authority, technology partners, and academic researchers. The interviews were designed to capture a comprehensive view of the project from multiple angles, ensuring that we could observe the actualization process holistically. Each interview follows a structured guide that

included questions about the expectations of different stakeholders, the challenges faced, and the SSI system's perceived effectiveness. We developed the guide based on Rubin and Rubin's (2012) methodology to ensure thorough coverage of the topics relevant to our research questions. During the interviews, we encourage participants to discuss their experiences in-depth, allowing us to gather rich qualitative data. This approach also enables us to explore the nuanced perspectives of different stakeholders, including their views on SSI's roles in enhancing tax administration processes. To ensure accurate and reliable data, we conduct follow-up interviews when necessary to clarify any ambiguities arising during the analysis. This iterative process of data collection and verification is essential in refining our understanding of the case. For data analysis, we adopt a three-phase coding approach based on Corbin and Strauss (2015). Initially, we use open coding to generate preliminary codes that reflect various aspects of affordances, experimentation, and actualization. These codes are then refined through axial coding, where we group them into higher-order themes. Finally, selective coding allows us to establish relationships between these themes, leading to a deeper understanding of how the public sector organization has experimented with and actualized SSI's affordances.

5 Summary of the Results

I will now summarize the findings from the seven essays, which explore how to design and manage emerging decentralized ISs to enable trustful digital interactions.

5.1 Essay 1: Beyond Disintermediation: A Multiple Case Study of Emerging Intermediary Roles in Blockchain Applications

In Essay 1, we explore how blockchain technology transforms market intermediation by analyzing two case studies: TradeLens, a permissioned blockchain platform in the global shipping industry, and MakerDAO, a decentralized finance protocol. Both cases reveal how blockchain-driven systems often reconfigure rather than eliminate intermediaries, creating new forms of governance, compliance, and technical dependencies.

TradeLens digitized and streamlined shipping processes using a permissioned blockchain, aiming to reduce inefficiencies and delays. However, it introduced new intermediaries, with IBM and Maersk acting as gatekeepers managing governance, membership, and data stewardship. MakerDAO, operating on a permissionless blockchain, was designed for decentralized issuance of the stablecoin DAI. Despite its decentralized intent, MakerDAO developed dependencies on centralized actors like stablecoin providers, external oracles, and influential token holders to ensure stability and governance.

Our analysis identified two archetypes of re-intermediation in blockchain ecosystems, each representing distinct trajectories. The permissioned blockchain archetype, exemplified by TradeLens, reflects a centralized re-intermediation approach common in business-to-business blockchain applications. Initially, TradeLens faced concerns from potential participants about the high degree of centralization, fearing it might lead to power imbalances. In response, the platform gradually incorporated more decentralized governance elements to address these concerns, allowing participating entities to exert greater influence. This trajectory illustrates a shift from a centralized structure toward a more balanced model of governance, while still maintaining some degree of central control to ensure compliance and operational stability.

The permissionless blockchain archetype, represented by MakerDAO, follows a different path. MakerDAO, like many projects in the DeFi space, operates on a public permissionless blockchain protocol governed by a democratic yet complex system. Despite its fundamentally decentralized governance, many users rely on centralized

intermediaries—such as stablecoin providers and external oracles—to participate effectively. This reliance reflects a move from a purely decentralized intermediation approach toward a hybrid model, where certain centralized actors re-emerge to address specific operational, regulatory, or technical needs.

While both archetypes exemplify re-intermediation, their trajectories diverge. Permissioned systems like TradeLens evolve from centralized to increasingly decentralized re-intermediation, integrating broader stakeholder influence over time. In contrast, permissionless systems like MakerDAO transition from decentralized models to hybrid structures, reintroducing centralized intermediaries where necessary.

Through these insights, we challenge the deterministic view of blockchain as a purely disintermediating technology (Chalmers et al., 2021). Instead, we underscore how blockchain reconfigures intermediation, redistributing authority and trust while addressing practical and compliance-related constraints. Through this nuanced perspective, we inform both the design of blockchain solutions and theoretical discussions on intermediation in digital markets.

5.2 Essay 2: Designing a Framework for Digital KYC Processes Built on Blockchain-Based Self-Sovereign Identity

In Essay 2, we develop a framework aimed at enhancing the KYC process by implementing an end-to-end digital solution that levers blockchain-based SSI. Recognizing the nascency of the research into SSI, particularly in application design, we build on work by Soltani et al. (2018) that initially explored SSI in the KYC context. Our approach expands on their findings by focusing on the specific needs of banks and other key stakeholders. Using a DSR approach, we design and evaluate a comprehensive framework that includes both a generic architecture and process design utilizing blockchain-based SSI. The evaluation indicates that our framework can significantly reduce cost and time expenditures and can contribute to better user experiences and increased security during the KYC process. For banks and regulators, fully digital verification provides a significant advantage over paper documents by improving data accuracy and eliminating manual processing errors. We also find that our SSI-based approach can significantly improve digital trust. Fake credentials cannot be created, because they require a credential issuer's signature in order to be valid. Also, ownership of credentials can be cryptographically verified. Linking multiple credentials through attributes

such as a holder's name, biometrics, or secure hardware makes it hard to share or sell them.

However, our research also highlights additional conceptual challenges that need to be addressed before SSI can be effectively implemented in real-world systems, particularly regarding establishing governance frameworks and conducting a more in-depth regulatory analysis. While we identify potential synergies between SSI and regulation, significant challenges remain, particularly in developing a broad SSI-based ecosystem and ensuring that it is user-friendly while maintaining strong privacy and security protections.

In addition to the conceptualized and evaluated architecture and set of processes (Gregor & Hevner, 2013), we make three key contributions to the academic body of knowledge. First, our analysis highlights the challenges of relying solely on blockchain for exchanging personal data, particularly in digital IM systems. We demonstrate how these challenges can be addressed by applying SSI on top of the blockchain layer, which harnesses blockchain's benefits while mitigating its known issues regarding scalability and privacy. Second, we explored the design implications of SSI-based solutions built on blockchain for KYC processes, identifying three DPs (Gregor et al., 2020) that elevates our IT artifact for broad theoretical discussion: (1) Utilize blockchain only for public data, (2) anticipate an ecosystem of various ledgers, and (3) enable decentralization at the edge. Finally, we provide recommendations for future research into blockchain and SSI, enabling scholars to build on our findings and further expand the knowledge base (vom Brocke et al., 2020).

5.3 Essay 3: Exploring the Use of Self-Sovereign Identity for Event Ticketing Systems

In Essay 3, we follow a rigorous DSR approach to build and evaluate an SSI-based event ticketing framework. As a result of our event ticketing framework, ticket owners cannot simply pass on their ticket to a third party. Instead, they must request a transfer through the ticket issuer, which allows issuers, holders, and organizers to verify ownership. This ensures that only legitimate ticket holders can enter the venue, preventing the fraudulent multiple reselling of tickets. Also, by implementing a random reallocation of tickets to prevent side-payments, this approach ensures that the price and resale restrictions are extremely hard to circumvent (Courty, 2019). Thus, ticket scalping and

black-market activities can be effectively prevented. Because tickets cannot be resold at a profit or only with a small margin, it is also no longer profitable to operate ticket bots to get a competitive advantage and buy large numbers of tickets, increasing the chance of regular ticket buyers receiving a ticket. Our findings demonstrate that SSI-based event ticketing can significantly increase trust when buying tickets online, particularly in the secondary ticket market. This framework benefits visitors by reducing ticket fraud and scalping while offering user-friendly identity verification. While ticket issuers gain more control over secondary market transactions, and event organizers benefit from efficient entrance verification and greater fan satisfaction, some challenges remain. To purchase SSI-based event tickets, users first need to have the appropriate identity credentials. Yet once they are equipped with a digital wallet and foundational credentials – as proposed with the EUDI-Wallet – the onboarding process with the ticket issuer can be fully automated. As a further challenge, tickets cannot be freely transferred or gifted to others. Tickets can only be sold through the official secondary market, where they must be randomly reallocated so as to fully prevent scalping. While this ensures that visitors can receive compensation, it prevents them from changing companions after the ticket purchase, which may be undesirable for some spectators.

We make three primary contributions to the existing knowledge base. First, we introduce a novel SSI-based event ticketing approach. By developing and evaluating a PoC, we demonstrate this approach's feasibility in addressing event ticketing issues such as scalping and fraud (Drechsler & Hevner, 2018). SSI provides reliable and efficient user identification, making it a suitable solution for implementing the centralized exchange model proposed by Courty (2019). Second, by deriving new DPs, we gain valuable insights for digital IM solutions in event ticketing and similar scenarios that require efficient, privacy-oriented, and reliable identity verification. These principles are: (1) facilitate digital credential-bundling and verification, (2) bind credentials to users using existing credentials with a high assurance level, and (3) use public and privacy-preserving revocation registries to manage resale activities. Third, we provide theoretical insights into SSI's value for event ticketing. By proposing revocation registries, we extend Courty's model with an alternative method for linking visitors to their tickets without explicitly storing ticket holders in a (de)centralized ledger. The SSI-based approach also offers great flexibility, as additional credentials (such as vaccination certificates) can be requested without compromising efficiency or privacy.

5.4 Essay 4: Driving Self-Sovereign Identity: Designing a Car Identity Management Framework

In Essay 4, we present a novel framework for car IM based on the principles of SSI, addressing the limitations of both analog and centralized digital approaches. Traditional car IM systems, which rely on physical identifiers and inspection documents, suffer from limitations in security, scalability, and adaptability to modern vehicle ecosystems. Similarly, existing digital solutions often depend on centralized architectures, exposing them to vulnerabilities such as data breaches, scalability issues, and a lack of user control over sensitive data.

To address these challenges and improve trust in car identity systems, we develop our framework using the DSR methodology and expert-driven evaluations. This approach allows us to create a practical decentralized IM system that integrates tools such as VCs, machine identity wallets, and infrastructure devices for verifying identity. Our framework is designed to prioritize privacy, reliability, and scalability while enabling seamless and trustworthy interactions across individual, organizational, and machine identities.

Besides the rigorously designed and evaluated car IM framework, we contribute three key DPs, elevating our artifact for further theoretical discussions: (1) utilize standardized SSI protocols to enable seamless interactions between heterogeneous identity types, (2) lever SSI's user-centric approach for enhanced privacy benefits, and (3) use the cryptographic features of SSI to establish trust in the reliability and integrity of data. While our framework is designed for the car IM context, we also demonstrate its broader implications. Holistic IM systems such as ours can unify diverse identity types, filling a gap in the academic research and enabling cross-contextual applications.

However, we acknowledge several challenges to implementation. The framework requires significant infrastructural advancements, such as decentralized public registries and the widespread adoption of identity wallets. The complexity of managing digital identities independently may hinder user acceptance, highlighting the need for educational efforts and intuitive designs. Technical challenges – including stable wireless communication in dynamic environments such as moving vehicles – also require further investigation.

Looking ahead, we identify several avenues for future research. Simplifying SSI infrastructure, optimizing identity wallets for IoT and embedded systems as well as

improving holistic systems' usability could facilitate broader adoption. As autonomous vehicles and smart environments continue to evolve, the importance of seamless, interoperable IM will grow. In our view, our SSI-based framework not only provides a foundational architecture for secure digital interactions, but also fosters improved trust among users, organizations, and machines in increasingly dynamic ecosystems.

5.5 Essay 5: Recoding Asylum Management – How Germany's Federal Government Approached Innovation with Emerging IT

In Essay 5, we conduct a clinical research approach at the Federal Office for Migration and Refugees in Germany to investigate how governments can effectively innovate by means of emerging technologies such as blockchain. Such projects often face significant challenges owing to entrenched structural and cultural barriers (Cinar et al., 2019; Goh & Arenas, 2020; Kamal, 2006) as well as issues associated with immature or hyped emerging technologies (Miranda et al., 2022; Wang, 2010). Based on our direct involvement in the development, piloting, and implementation of Germany's FLORA system, we investigate how these challenges materialized and how the FLORA team successfully addressed them. Building on these insights, we outline four key lessons for governments to effectively innovate by means of emerging technologies:

Lesson Learned 1: How to develop a government use case

Innovation discourse often highlights compelling and inspiring stories about emerging technologies' potentials, but these narratives are predominantly tailored to the private sector. However, governments must reinterpret and adapt these stories to create use cases that address their distinct needs, including fulfilling public service goals, aligning with operational constraints, and adhering to strict policy requirements. We find that this adaptation is crucial for demonstrating the technology's value as well as secure stakeholder support and funding. While private-sector examples may serve as inspiration, they must be translated to fit the public sector context. This process can benefit from ideation workshops, PoCs, and pilot projects to test and refine the technology in real-world settings. Notably, the use case should both improve performance and demonstrate how the technology fits in the public sector's organizational structure and processes.

Lesson Learned 2: How to overcome structural barriers

Emerging technologies are often immature, and governments that seek to adopt them

will encounter various uncertainties and structural challenges. These range from concerns about regulatory compliance, to interoperability with existing IT systems and rigid budgeting processes, to a lack of necessary skills and capabilities (Baskerville & Myers, 2009; Wang, 2010). We find that a key step in overcoming structural barriers is forming interdisciplinary teams that integrate legal, technological, and procedural expertise. It is crucial that these teams be effectively managed, with clear structures and processes that support iterative problem-solving, exploration of solutions, and collective learning. One strategy is to delegate experimental work to subprojects operating alongside the main project. However, this approach is only successful if the subprojects are staffed with individuals who have the requisite expertise. In cases where such expertise is lacking, governments must establish systems for collaborating effectively with technology consultants and IT service providers.

Lesson Learned 3: How to overcome cultural barriers

Government authorities typically operate in a cultural framework that emphasizes risk aversion, consistency, and procedural integrity. While these values are essential for maintaining dependable public services, they can hinder unbiased engagement with new technologies. To bridge the gap between agile innovation processes and the traditional culture of stewardship, we find that project managers should engage in cultural sensemaking activities. This may include involving users and employee representatives in iterative feedback loops to address concerns about the new technology. Further, managers can lever innovation stories about the technology to facilitate cultural change by illustrating how the technology can lead to a more desirable way of working. These stories, particularly when aligned with the core values of the government authority – such as promoting 'cooperation' – can help foster acceptance and drive cultural shifts.

Lesson Learned 4: How to secure stakeholder buy-in

Government innovation projects involving emerging ITs often face substantial stakeholder skepticism (Wang, 2010). These projects' inherent uncertainty often raises concerns about their effectiveness and prompts questions about the potential misuse of taxpayer funds. To gain broad stakeholder support, we find that innovation managers should adopt the role of 'political entrepreneur' and should engage in strategic political activities. This involves engaging with users, partner authorities, and the public. Additionally, transparency measures – such as publishing white papers and media articles – can help alleviate public concerns.

5.6 Essay 6: Bringing Government in the Digital Age – Insights from Germany's Asylum Procedure

In Essay 6, we conduct a longitudinal single-case study based on Germany's FLORA project to develop an in-depth understanding of how to build and govern a blockchain-based intergovernmental IS. The FLORA system primarily seeks to share procedural information between the involved agencies in the asylum-seeking procedures. It creates a 'shared source of truth' through secure, timely, and reliable distribution and persistent tracking of process status messages. FLORA's introduction eliminated most previously used Excel-based lists and streamlined the exchange of procedural information. FLORA has also improved the quality of information (significantly improved information accuracy and completeness), has sped up the procedures by up to 50%, and has reduced the risks for procedural errors and data privacy violations.

However, the development of the FLORA project presented numerous challenges, particularly regarding building and governing a blockchain-based intergovernmental IS. In our case study, we illustrate how the Federal Office approached these challenges, and derive three recommendations for successfully building and governing intergovernmental ISs:

Recommendation 1: Determine the suitability of decentralized over centralized solutions

We find that centralized IT systems, while often regarded as cost-effective solutions for managing multiple agencies, tend to conceal significant hidden costs in the context of intergovernmental ISs. These hidden costs arise from the necessity of aligning diverse procedures and data models across various government bodies, as well as the need for new legal frameworks to facilitate centralized data management. To navigate these obstacles, the FLORA project adopted a decentralized data-sharing approach. This decision not only minimized the need for new legal bases, but also reduced the costs associated with standardizing disparate local data models and procedures across agencies. Yet the FLORA case reveals that the use of blockchain technology introduces its own set of challenges, particularly in adhering to stringent privacy regulations. Blockchain's inherent append-only structure directly conflicts with the regulatory requirement to erase personal data once the legal basis for its storage expires. To address this concern, the Federal Office implemented a pseudonymization solution that preserved procedural data while ensuring that personal identifiers could be erased as required by law.

Recommendation 2: Advocate for modularity to break up multilayered legacy architectures

Another significant challenge revealed in our case study is the complexity of integrating FLORA with existing legacy IT systems. Many legacy systems are deeply entangled with older legal frameworks, making them hard to modify or replace. Over time, these systems have accumulated layers of technology that add to their rigidity. We illustrate how FLORA tackled this challenge by emphasizing loose coupling and modularity, allowing the new system to interact with legacy systems without replicating their data. This design ensured that FLORA could be updated and maintained over time without requiring a complete overhaul of existing systems. For instance, FLORA levers Hyperledger Fabric as the primary framework for sharing and storing procedural data, as it is well-suited to the multilevel requirements of federal data processing. However, the system's design remains flexible, allowing this blockchain component to be replaced with a more streamlined or efficient solution, should a better option become available in the future.

Recommendation 3: Start with a software-as-a-service model and then gradually move to a flexible integration model

The governance of the blockchain-based systems presented yet another challenge. The legal separation of responsibilities among different governmental bodies often complicates the alignment of technical and financial responsibilities. In our case study, we reveal how the Federal Office implemented a 'one-for-all' approach to overcome this issue, where it temporarily assumed the majority of the technical and financial responsibilities during the system's early development phases. This strategy enabled the project to move forward without waiting for full alignment among all agencies involved. As the system matured, the responsibilities were gradually redistributed among the participating agencies. In line with this approach, FLORA employed a software-as-a-service model during its initial project phases, allowing the partner agencies to adopt the system without needing to immediately integrate it with their legacy IT systems. This incremental transition lowered the usual barriers to adoption, allowing the agencies to gradually determine their desired integration level and to manage the necessary budgeting, staffing, and contracting processes accordingly.

5.7 Essay 7: Affordances, Experimentation and Actualization of Self-Sovereign Identity: A Case Study of the Implementation and Use of SSI in the Public Sector

In Essay 7, we conduct a case study to explore how public sector organizations can identify and implement the affordances offered by SSI. From a technological perspective, this helps us understand SSI's capabilities and limitations by focusing on how goal-oriented public sector entities perceive and interact with SSI. From an organizational perspective, this approach sheds light on how these institutions can overcome barriers such as technical, political, and cultural challenges, while also addressing user needs when designing digital innovations.

Our study offers three primary theoretical contributions. First, we contribute to SSI research by identifying four organizational-level SSI affordances, revealing how public sector organizations can engage with and benefit from SSI. Notably, we expand SSI research by showing that SSI allows verifiers to not only reliably confirm identity credentials, but also to prove that they received a verifiable presentation. This is particularly important for compliance-heavy contexts such as KYC, where auditability and traceability are essential. Second, we contribute to the affordance-experimentation-actualization (A-E-A) theory by showing how affordance discovery, experimentation, and actualization are interconnected over time. Specifically, we provide insights into how the experimentation phase helps align the technical, political, and cultural factors in an organization. In turn, this alignment enables organizations to discover and actualize SSI's affordances. By presenting empirical evidence of this iterative process, our study highlights the practical relevance of A-E-A theory in fostering organizational innovation. Third, we contribute to the public sector innovation literature by developing an affordance-based framework tailored to public sector organizations. This framework helps these entities to better understand the affordances available to them, offering guidance for creating user-centric public services. Our findings emphasize that an affordance-based approach is valuable in overcoming technical, cultural, and political barriers that are often overlooked in traditional features-driven strategies. This perspective can help prevent innovation failures and can improve trust in digital public services.

6 Discussion and Conclusion

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

6.1 Summary

In this dissertation, I investigate how to design and manage emerging decentralized ISs to foster trust in digital interactions. To achieve this overarching aim, I define three distinct research goals: understand blockchain's potentials for enabling trustful digital interactions without the need for a trusted central party (RG1), guide organizations in designing trustworthy decentralized ISs (RG2), and guide organizations in managing emerging decentralized ISs (RG3). I explore the corresponding research questions using a range of research methods, including DSR, case studies, and clinical IS research. These methodologies provide a comprehensive approach to tackling complex issues in the field. In this dissertation, I present the findings of my research through seven individual essays. Essay 1 analyzes the potentials of blockchain for conducting trustful digital transactions without the need for trusted third parties. Building on these findings, Essays 2, 3, and 4 provide concrete solution designs and DPs to guide organizations in designing effective emerging decentralized IS in the contexts of KYC, event ticketing, and smart cars. Finally, Essays 5, 6, and 7 clarify how organizations can effectively manage emerging decentralized ISs by providing in-depth insights into large-scale real-world implementation projects, actionable recommendations, and tailored innovation frameworks.

6.2 Contributions to Theory and Implications for Practice

In the seven essays that underpin this cumulative dissertation, I adopt a socio-technical perspective on ISs (Chatterjee et al., 2021) to address the overarching research aim as well as to contribute to both theory and practice.

Essay 1 answers several calls to investigate how blockchain affects intermediation and thus the role of trusted third parties in digital interactions (RG1) (Lumineau et al., 2021; Rossi et al., 2019). While previous studies have suggested that blockchain has the potentials to disrupt various sectors by eliminating the need for trusted third

parties (Chalmers et al., 2021; Pereira et al., 2019), Essay 1 contributes to this academic discourse by offering a more nuanced and in-depth understanding, illustrating how blockchain can take over and redefine certain market functions, but also recognizing the various scenarios in which it may not satisfactorily fulfill these roles. Thus, Essay 1 offers theoretical explanations for blockchain's overall limited impacts on disintermediation observed in practice to date (The Wall Street Journal, 2022).

Essays 2, 3, and 4 respond to researchers' calls that ISs be designed in more trustworthy ways (RG2) (Sasse & Kirlappos, 2014; Shin, 2022; Söllner et al., 2016). These essays contribute concrete solution designs for trustworthy decentralized ISs as well as more broadly applicable design knowledge by abstracting and generalizing the findings in the form of DPs (Gregor & Hevner, 2013; Gregor et al., 2020). Essay 2 identifies the weaknesses of pure blockchain-based approaches for improving KYC (Norvill et al., 2019; Parra Moyano & Ross, 2017) and contributes a regulatory compliant, SSI-based KYC design that improves digital trust in the KYC process for both banks and customers. Essay 3 enhances the current understanding of how to design event ticketing systems that foster user trust in purchasing tickets online, particularly in the secondary market, by contributing a rigorously designed and evaluated SSI-based event ticketing framework and corresponding DPs. Essay 4 contributes a novel, SSI-based framework for digital car identities to enable trustworthy and privacy-preserving digital interactions and verifications among persons, organizations, and machines.

Essay 5, 6, and 7 contribute to the managerial discourse on emerging decentralized ISs (RG3). Essay 5 provides in-depth insights into the various challenges of successfully innovating by means of emerging technologies in the public sector (Goh & Arenas, 2020; Meijer, 2015). It further contributes resolution strategies for how to effectively address these challenges. Essay 6 contributes to the understanding of how to build and govern blockchain-based intergovernmental ISs by providing valuable insights and actionable recommendations for practitioners distilled from a six-year case study on a blockchain-based, intergovernmental IS applied in Germany's asylum procedures. Essay 7 investigates managerial challenges relating to the adoption of SSI in the public sector. It identifies four organizational-level SSI affordances, provides an affordance-based framework for public sector innovations, and demonstrates how this approach contributes to overcoming technical, cultural, and political barriers to innovation.

6.3 Limitations

Investigating emerging decentralized ISs is inherently complex and presents challenges. This complexity stems not only from the intricacy of blockchain and SSI as well as their rapid advancements (Bhutta et al., 2021; Lashkari & Musilek, 2021; Schardong & Custódio, 2022), but also from the dynamic interactions between technologies, organizations, and individuals (Baskerville et al., 2018; Österle et al., 2011). Acknowledging these factors, I will now address this dissertation's limitations. While the specific limitations of each essay are addressed there, I will now focus on the overarching limitations of the dissertation as a whole.

This research's first limitation is the predominant use of qualitative-empirical methods, such as case studies and DSR. Qualitative methods are well-suited for exploring emerging and complex phenomena, such as decentralized ISs, where structured, in-depth understanding is essential. These methods enabled a detailed examination of real-world implementations and contextual factors, offering rich insights into the practical challenges and dynamics faced by organizations and individuals. However, these methods are limited in their ability to quantify certain impacts. Quantitative analyses could enrich the findings by offering statistical evidence for instance of user behaviors and trust dynamics, further strengthening this dissertation's conclusions.

Another limitation of my research is that the developed artifacts are implemented only as prototypes, without being evaluated in real-world settings. While these prototypes provide valuable insights into the design and functionality of decentralized ISs, they lack validation in practical, operational environments; this limits the ability to assess their long-term effectiveness and scalability. I seek to mitigate this limitation by incorporating practical insights through interviews with experts, which provide valuable perspectives and feedback from professionals in the field. Despite this, real-world testing would have provided a more robust evaluation of the artifact's performance and impacts.

Another limitation is that the results and findings reflect the current state of decentralized technologies, which are rapidly evolving. While I seek to provide abstract and generalizable knowledge, for instance by deriving DPs, future technological advancements may render some of my conclusions less applicable. Thus, while I seek to achieve broad applicability, the research remains inherently shaped by the technological constraints of its time.

6.4 Potential Avenues for Future Research

With this dissertation, I seek to provide a solid theoretical foundation for fostering digital trust through rigorously designed and effectively managed decentralized ISs. Still, the abovementioned limitations open valuable opportunities to address identified challenges and refine the proposed solutions. Thus, I conclude the introduction to my dissertation with avenues for future research.

First, the practical relevance and effectiveness of the artifacts developed in this dissertation should be rigorously tested in real-world settings. While this dissertation provides insights into a large-scale blockchain-based project in Essays 5 and 6, real-world implementations of SSI systems remain relatively scarce so far. Given the emerging importance of initiatives such as the EUDI-Wallet and corresponding large-scale pilot projects, these contexts provide valuable opportunities to explore the real-world effectiveness, scalability, and user acceptance of SSI-based systems.

Second, technological advancements in decentralized systems and cryptographic techniques have the potentials to effectively address prevailing challenges and limitations of decentralized IS and therefore require further investigation. One such significant development is the rise of zero-knowledge proofs (ZKPs), which presents promising avenues for addressing scalability and privacy issues in decentralized ISs (Babel & Sedlmeir, 2023; Gross et al., 2021). Scalability is a long-standing issue in decentralized ISs, particularly in blockchain, where every transaction must be verified and recorded by all nodes, resulting in slower processing times and higher resource consumption. ZKPs such as ZK-SNARKs have the potentials to reduce the data that need to be shared across the network, thereby improving scalability. ZKPs could also be applied to balance transparency and privacy requirements. While we applied nascent ZKP-based algorithms in our prototypes in Essays 2 and 3, further investigation should focus for instance on the applicability, scalability, and performance of ZKPs in real-world applications.

Third, the qualitative-exploratory research approach in my dissertation should be complemented by additional research approaches, since methodological pluralism yields more comprehensive and nuanced results (Mingers, 2001). Future research could incorporate additional research approaches, including quantitative methods to complement and extend the findings. For instance, controlled experiments may be used to compare user trust between traditional centralized systems and decentralized

alternatives. In this regard, existing trust-based research models – such as TAM (Davis, 1989; Venkatesh & Bala, 2008), Trust-TAM (Gefen et al., 2003), and UTAUT (Venkatesh et al., 2003) – could be applied to assess trust formation, user perceptions, and the adoption of decentralized ISs in more structured and measurable ways.

Digital Trust is a very valuable asset, particularly in today's world, where rapid technological advancements and digital innovations increasingly shape our lives. By addressing key challenges and proposing innovative solutions when designing and managing emerging decentralized ISs, I trust that this dissertation will motivate future research to further improve our understanding of how to enable digital trust in the digital age.

References

Aberer, K., & Despotovic, Z. (2001). Managing trust in a peer-2-peer information system. In H. Paques, L. Liu, D. Grossman, & C. Pu (Eds.), *Proceedings of the tenth international conference on Information and knowledge management* (pp. 310–317). ACM. https://doi.org/10.1145/502585.502638

Ågerfalk, 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

Agre, P. E. (2003). P2P and the promise of internet equality. *Communications of the ACM*, *46*(2), 39–42. https://doi.org/10.1145/606272.606298

Akoka, J. (1978). *Centralization Versus Decentralization of Information Systems: A Critical Survey and an Annotated Bibliography*.

Alessandria, M. L., & Vizzarri, A. (2021). Self-Sovereign Identity and Blockchain applications for the automotive sector. In *2021 AEIT International Conference on Electrical and Electronic Technologies for Automotive (AEIT AUTOMOTIVE)* (pp. 1–6). IEEE. https://doi.org/10.23919/AEITAUTOMOTIVE52815.2021.9662861

Allen, F., & Santomero, A. (1997). The theory of financial intermediation. *Journal of Banking & Finance*, *21*(11), 1461–1485. https://doi.org/10.1016/S0378-4266(97)00032-0

Al-Shamsi, M., Al-Emran, M., & Shaalan, K. (2022). A Systematic Review on Blockchain Adoption. *Applied Sciences*, *12*(9), 4245. https://doi.org/10.3390/app12094245

Amend, J., Feulner, S., Rieger, A., Roth, T., Guggenberger, T., & Fridgen, G. (2025). Bringing Government into the Digital Age: Insights from Germany's Asylum Procedure. *MIS Quarterly Executive*.

Arasa, R. (2015). Determinants of Know Your Customer (KYC) Compliance among Commercial Banks in Kenya. *Journal of Economics and Behavioral Studies*, *7*(2(J)), 162–175. https://doi.org/10.22610/jebs.v7i2(J).574

Arner, D. W., Zetzsche, D. A., Buckley, R. P., & Barberis, J. N. (2018). The Identity Challenge in Finance: From Analogue Identity to Digitized Identification to Digital KYC Utilities. *SSRN Electronic Journal*. Advance online publication. https://doi.org/10.2139/ssrn.3224115

Attaran, M. (2022). Blockchain technology in healthcare: Challenges and opportunities. *International Journal of Healthcare Management*, *15*(1), 70–83. https://doi.org/10.1080/20479700.2020.1843887

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

Baran, P. (1964). On Distributed Communications Networks. *IEEE Transactions on Communications*, *12*(1), 1–9. https://doi.org/10.1109/TCOM.1964.1088883

Baskerville, R., Baiyere, A., Gregor, S., Hevner, A., & Rossi, M. (2018). Contributions : Finding a Balance between Artifact and Theory. In https://api.semanticscholar.org/CorpusID:49413596

Baskerville, R., & Myers, M. D. (2009). Fashion waves in information systems research and practice. *MIS Quarterly*, *33*(4), 647–662.

Baskerville, R., vom Brocke, J., Mathiassen, L., & Scheepers, H. (2023). Clinical research from information systems practice. *European Journal of Information Systems*, *32*(1), 1–9. https://doi.org/10.1080/0960085X.2022.2126030

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. (2017). Blockchain as Radical Innovation: A Framework for Engaging with Distributed Ledgers as Incumbent Organization. In *Proceedings of the Annual Hawaii International Conference on System Sciences, Proceedings of the 50th Hawaii International Conference on System Sciences (2017)*. Hawaii International Conference on System Sciences. https://doi.org/10.24251/HICSS.2017.653

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

Benbasat, J., Goldstein, D., & Mead, M. (1987). The Case Research Strategy in Studies of Information Systems. *MIS Quarterly*, *11*, 369–386. https://api.semanticscholar.org/CorpusID:7288871

Benedek, B., Ciumas, C., & Nagy, B. Z. (2022). Automobile insurance fraud detection in the age of big data – a systematic and comprehensive literature review. *Journal of Financial Regulation and Compliance*, *30*(4), 503–523. https://doi.org/10.1108/JFRC-11-2021-0102

Bhutta, M. N. M., Khwaja, A. A., Nadeem, A., Ahmad, H. F., Khan, M. K., Hanif, M. A., Song, H., Alshamari, M., & Cao, Y. (2021). A Survey on Blockchain Technology: Evolution, Architecture and Security. *IEEE Access*, *9*, 61048–61073. https://doi.org/10.1109/ACCESS.2021.3072849

Borkowski, P. (2019). Reducing Odometer Fraud in the EU Second-Hand Passenger Car Market Through Technical Solution. In G. Sierpiński (Ed.), *Advances in Intelligent Systems and Computing. Integration as Solution for Advanced Smart Urban Transport Systems* (Vol. 844, pp. 184–194). Springer International Publishing. https://doi.org/10.1007/978-3-319-99477-2_17

Butijn, B.-J., Tamburri, D. A., & van Heuvel, W.-J. den (2021). Blockchains. *ACM Computing Surveys*, *53*(3), 1–37. https://doi.org/10.1145/3369052

Caldarelli, G. (2020). Understanding the Blockchain Oracle Problem: A Call for Action. *Information*, *11*(11), 509. https://doi.org/10.3390/info11110509

Camenisch, J., & Lysyanskaya, A. (2001). An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation. In G. Goos, J. Hartmanis, J. van Leeuwen, & B. Pfitzmann (Eds.), *Lecture Notes in Computer Science. Advances in Cryptology — EUROCRYPT 2001* (Vol. 2045, pp. 93–118). Springer Berlin Heidelberg. https://doi.org/10.1007/3-540-44987-6_7

Castella-Roca, J., Mut-Puigserver, M., Payeras-Capella, M. M., Viejo, A., & Angles-Tafalla, C. (2017). Secure and Anonymous Vehicle Access Control System to Traffic-Restricted Urban Areas. In *2017 26th International Conference on Computer Communication and Networks (ICCCN)* (pp. 1–7). IEEE. https://doi.org/10.1109/ICCCN.2017.8038491

Caudle, S. L., Gorr, W. L., & Newcomer, K. E. (1991). Key Information Systems Management Issues for the Public Sector. *MIS Quarterly*, *15*(2), 171. https://doi.org/10.2307/249378

Cha, S.-C., Peng, W.-C., Hsu, T.-Y., Chang, C.-L., & Li, S.-W. (2018). A Blockchain-Based Privacy Preserving Ticketing Service. In *2018 IEEE 7th Global Conference on Consumer Electronics (GCCE)* (pp. 585–587). IEEE. https://doi.org/10.1109/GCCE.2018.8574479

Chalmers, D., Matthews, R., & Hyslop, A. (2021). Blockchain as an external enabler of new venture ideas: Digital entrepreneurs and the disintermediation of the global music industry. *Journal of Business Research*, *125*, 577–591. https://doi.org/10.1016/j.jbusres.2019.09.002

Charmaz, K. (2006). *Constructing grounded theory: A practical guide through qualitative analysis* (1. publ). *Introducing qualitative methods*. SAGE Publ.

Chatterjee, S., Sarker, S., Lee, M., Xiao, X., & Elbanna, A. (2021). A possible conceptualization of the information systems (IS) artifact: A general systems theory perspective. *Information Systems Journal*, *31*(4), 550–578. https://doi.org/10.1111/isj.12320

Cheng, S. (2020). *Regaining Trust*. https://blogs.cfainstitute.org/marketintegrity/2020/04/07/regaining-trust/

Chong, A. Y. L., Lim, E. T. K., Hua, X., Zheng, S., & Tan, C.-W. (2019). Business on Chain: A Comparative Case Study of Five Blockchain-Inspired Business Models. *Journal of the Association for Information Systems*, 1308–1337. https://doi.org/10.17705/1jais.00568

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

Cole, R., & Aitken, J. (2020). The role of intermediaries in establishing a sustainable supply chain. *Journal of Purchasing and Supply Management*, *26*(2), 100533. https://doi.org/10.1016/j.pursup.2019.04.001

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

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

Corsi, P., Lagorio, G., & Ribaudo, M. (2019). TickEth, a ticketing system built on ethereum. In C.-C. Hung & G. A. Papadopoulos (Eds.), *Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing* (pp. 409–416). ACM. https://doi.org/10.1145/3297280.3297323

Courty, P. (2019). Ticket resale, bots, and the fair price ticketing curse. *Journal of Cultural Economics*, *43*, 1–19. https://doi.org/10.1007/s10824-019-09353-4

Cucko, S., & Turkanovic, M. (2021). Decentralized and Self-Sovereign Identity: Systematic Mapping Study. *IEEE Access*, *9*, 139009–139027. https://doi.org/10.1109/ACCESS.2021.3117588

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

Der, U., Jähnichen, S., & Sürmeli, J. (2017). *Self-sovereign Identity $-$ Opportunities and Challenges for the Digital Revolution*. https://doi.org/10.48550/arXiv.1712.01767

Dobrygowski, D. (2022). *Earning Digital Trust: Decision-Making for Trustworthy Technologies*. https://www3.weforum.org/docs/WEF_Earning_Digital_Trust_2022.pdf

Drechsler, A., & Hevner, A. (2018). Utilizing, Producing, and Contributing Design Knowledge in DSR Projects. In S. Chatterjee, K. Dutta, & R. P. Sundarraj (Eds.), *Lecture Notes in Computer Science. Designing for a Digital and Globalized World* (Vol. 10844, pp. 82–97). Springer International Publishing. https://doi.org/10.1007/978-3-319-91800-6_6

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

Durr, M. (1987). Peer Networks Gain Ground. *Computerworld*, *21*(4).

The Economist. (2015). *The trust machine: The technology behind bitcoin could transform how the economy works*. https://www.economist.com/leaders/2015/10/31/the-trust-machine

Edelman, R. (2021). *2021 Edelman Trust Barometer: Trust in Technology*. https://www.edelman.com/trust/2021-trust-barometer/trust-technology

Eggers, W., Dinnessen, F., Price, M., & Rodrigues, G. (2024). *Government at warp speed: How agencies are accelerating public service delivery and reducing burdens on citizens and businesses*. https://www2.deloitte.com/us/en/insights/industry/public-sector/government-trends.html#government-at-warp-speed

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

Ein-Dor, P., & Segev, E. (1978). Centralization, decentralization and management information systems. *Information & Management*, *1*(3), 169–172. https://doi.org/10.1016/0378-7206(78)90004-6

Eisenhardt, K. (1989). Building theories from case study research. *Academy of Management Review*(14), Article 4, 532–550. https://api.semanticscholar.org/CorpusID:55396735

European Commission. (2021). *EBSI: Experience the future with the European Blockchain Services Infrastructure*. https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI

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 and Energy. (2021). *Showcase Program "Secure Digital Identities"*. https://www.digitale-technologien.de/DT/Navigation/EN/ProgrammeProjekte/AktuelleTechnologieprogramme/Sichere_Digitale_Identitaeten/sichere_digitale_ident.html

Federal Ministry of the Interior. (2021). *Was sind die Schaufenster „Sichere Digitale Identitäten“ und was haben sie mit dem Projekt zu tun?* https://www.personalausweisportal.de/SharedDocs/faqs/Webs/PA/DE/Haeufige-Fragen/11_projekt_digitale_identitaeten/PDI7_Foerderprogramm_Schaufenster.html

Fedrecheski, G., Rabaey, J. M., Costa, L. C. P., Calcina Ccori, P. C., Pereira, W. T., & Zuffo, M. K. (2020). Self-Sovereign Identity for IoT environments: A Perspective. In *2020 Global Internet of Things Summit (GIoTS)* (pp. 1–6). IEEE. https://doi.org/10.1109/GIOTS49054.2020.9119664

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. https://doi.org/10.1007/s12525-022-00573-9

Filippi, P. de, & Wright, A. (2018). *Blockchain and the Law*. Harvard University Press. https://doi.org/10.2307/j.ctv2867sp

Fridgen, G., Guggenberger, N., Hoeren, T., Prinz, W., Urbach, N., Baur, J., Brockmeyer, H., Gräther, W., Rabovskaja, E., Schlatt, V., Schweizer, A., Sedlmeir, J., & Wederhake, L. (2019). *Chancen und Herausforderungen von DLT (Blockchain) in Mobilität und Logistik*. https://www.fim-rc.de/Paperbibliothek/Veroeffentlicht/1106/wi-1106.pdf

Gatteschi, V., Lamberti, F., & Demartini, C. (2020). Blockchain Technology Use Cases. In S. Kim & G. C. Deka (Eds.), *Studies in Big Data. Advanced Applications of Blockchain Technology* (Vol. 60, pp. 91–114). Springer Singapore. https://doi.org/10.1007/978-981-13-8775-3_4

Gefen, Karahanna, & Straub (2003). Trust and TAM in Online Shopping: An Integrated Model. *MIS Quarterly*, *27*(1), 51. https://doi.org/10.2307/30036519

Gephart, R. P. (2004). Qualitative research and the Academy of Management Journal. *Academy of Management Journal*, *47*(4), 454–462.

Glaap, R., & Heilgenberg, M.-C. (2019). Digitales Ticketing. In L. Pöllmann & C. Herrmann (Eds.), *Der digitale Kulturbetrieb* (pp. 127–159). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-24030-1_7

Glaser, B., & Strauss, A. (2017). *Discovery of Grounded Theory: Strategies for Qualitative Research*. Routledge.

Glaser, F. (2017). Pervasive Decentralisation of Digital Infrastructures: A Framework for Blockchain enabled System and Use Case Analysis. In *Proceedings of the Annual Hawaii International Conference on System Sciences, Proceedings of the 50th Hawaii International Conference on System Sciences (2017)*. Hawaii International Conference on System Sciences. https://doi.org/10.24251/HICSS.2017.186

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

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). https://doi.org/10.1007/s12525-023-00637-4

Gregor, S., & Hevner, A. (2013). Positioning and Presenting Design Science Research for Maximum Impact. *MIS Quarterly*, *37*, 337–356. https://doi.org/10.25300/MISQ/2013/37.2.01

Gregor, S., Kruse, L., & Seidel, S. (2020). Research Perspectives: The Anatomy of a Design Principle. *Journal of the Association for Information Systems*, *21*, 1622–1652. https://doi.org/10.17705/1jais.00649

Gross, J., Sedlmeir, J., Babel, M., Bechtel, A., & Schellinger, B. (2021). Designing a Central Bank Digital Currency with Support for Cash-Like Privacy. *SSRN Electronic Journal*. Advance online publication. https://doi.org/10.2139/ssrn.3891121

Guggenberger, T. (2023). *On the Design and Management of Blockchain-Based Information Systems*. https://doi.org/10.15495/EPub_UBT_00007254

Guggenberger, T., Neubauer, L., Stramm, J., Völter, F., & Zwede, T. (2023). Accept Me as I Am or See Me Go: A Qualitative Analysis of User Acceptance of Self-Sovereign Identity Applications. In T. Bui (Ed.), *Proceedings of the Annual Hawaii International Conference on System Sciences, Proceedings of the 56th Hawaii International Conference on System Sciences*. Hawaii International Conference on System Sciences. https://doi.org/10.24251/HICSS.2023.793

GUTS Tickets. (2020). *FAQ — Can scalpers bypass the system by buying tickets on single use sim cards and selling these?* https://blog.guts.tickets/faq-can-scalpers-bypass-the-system-by-buying-tickets-on-throw-away-simcards-and-selling-these-f24e9a27e2b7

Hardman, D., Harchandani, L., Othman, A., & Callahan, J. (2019). Using Biometrics to Fight Credential Fraud. *IEEE Communications Standards Magazine*, *3*(4), 39–45. https://doi.org/10.1109/MCOMSTD.001.1900033

Hevner, A., March, S., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly*, *28*(78), Article 1, 75–105. https://doi.org/10.2307/25148625

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

Hookings, M. (2019). *The O2 and The SSE Arena, Wembley, launch fan-first ticketing approach with AXS*. https://www.eventindustrynews.com/news/the-o2-and-the-sse-arena-wembley-launch-fan-first-ticketing-approach-with-axs

Imperva. (2019). *How bots affect ticketing*. https://www.imperva.com/resources/resource-library/reports/how-bots-affect-ticketing/

Jessel, B., Lowmaster, K., & Hughes, N. (2018). Digital identity: The foundation for trusted transactions in financial services. *Journal of Financial Transformation*(47), 143–150.

Kamal, M. M. (2006). IT innovation adoption in the government sector: identifying the critical success factors. *Journal of Enterprise Information Management*, *19*(2), 192–222. https://doi.org/10.1108/17410390610645085

Keller, R., Stohr, A., Fridgen, G., Lockl, J., & Rieger, A. (2019). Affordance-Experimentation-Actualization Theory in Artificial Intelligence Research - A Predictive Maintenance Story. *ICIS 2019 Proceedings*.

Khan, S. N., Loukil, F., Ghedira-Guegan, C., Benkhelifa, E., & Bani-Hani, A. (2021). Blockchain smart contracts: Applications, challenges, and future trends. *Peer-to-Peer Networking and Applications*, *14*(5), 2901–2925. https://doi.org/10.1007/s12083-021-01127-0

Klein, H., & Myers, M. (1999). A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems. *MIS Quarterly*, *23*, 67–94. https://api.semanticscholar.org/CorpusID:2404895

KMPG. (2022). *KPMG Cyber trust insights 2022: Building trust through cybersecurity and privacy*. https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2022/10/kpmg-cyber-trust-insights-2022.pdf

Kolb, J., AbdelBaky, M., Katz, R. H., & Culler, D. E. (2021). Core Concepts, Challenges, and Future Directions in Blockchain. *ACM Computing Surveys*, *53*(1), 1–39. https://doi.org/10.1145/3366370

Kuckartz, U., & Rädiker, S. (2022). *Qualitative Inhaltsanalyse. Methoden, Praxis, Computerunterstützung: Grundlagentexte Methoden* (5. Auflage). *Grundlagentexte Methoden*. Beltz Juventa. http://www.content-select.com/index.php?id=bib_view&ean=9783779955337

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

Lacity, M. C., & van Hoek, R. (2021). How Walmart Canada Used Blockchain Technology to Reimagine Freight Invoice Processing. *MIS Quarterly Executive*, 219–233. https://doi.org/10.17705/2msqe.00050

Lage, O., Saiz-Santos, M., & Zarzuelo, J. M. (2022). Decentralized platform economy: emerging blockchain-based decentralized platform business models. *Electronic Markets*, *32*(3), 1707–1723. https://doi.org/10.1007/s12525-022-00586-4

Lashkari, B., & Musilek, P. (2021). A Comprehensive Review of Blockchain Consensus Mechanisms. *IEEE Access*, *9*, 43620–43652. https://doi.org/10.1109/ACCESS.2021.3065880

Lee, A. S., Thomas, M., & Baskerville, R. (2015). Going back to basics in design science: from the information technology artifact to the information systems artifact. *Information Systems Journal*, *25*(1), 5–21. https://doi.org/10.1111/isj.12054

Leidner, D. E., Gonzalez, E., & Koch, H. (2018). An affordance perspective of enterprise social media and organizational socialization. *The Journal of Strategic Information Systems*, *27*(2), 117–138. https://doi.org/10.1016/j.jsis.2018.03.003

Leifer, R. (1988). Matching Computer-Based Information Systems with Organizational Structures. *MIS Quarterly*, *12*(1), 63. https://doi.org/10.2307/248805

Lesavre, L. (2020). *A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems*. https://doi.org/10.6028/NIST.CSWP.01142020

Li, X., Niu. J., & Han, Y. (2019). Secure Electronic Ticketing System based on Consortium Blockchain. *KSII Transactions on Internet and Information Systems*, *13*(10). https://doi.org/10.3837/tiis.2019.10.022

Lim, S. Y., Tankam Fotsing, P., Almasri, A., Musa, O., Mat Kiah, M. L., Ang, T. F., & Ismail, R. (2018). Blockchain Technology the Identity Management and Authentication Service Disruptor: A Survey. *International Journal on Advanced Science, Engineering and Information Technology*, *8*(4-2), 1735–1745. https://doi.org/10.18517/ijaseit.8.4-2.6838

Lockl, J., Schlatt, V., Schweizer, A., Urbach, N., & Harth, N. (2020). Toward Trust in Internet of Things Ecosystems: Design Principles for Blockchain-Based IoT Applications. *IEEE Transactions on Engineering Management*, *67*(4), 1256–1270. https://doi.org/10.1109/TEM.2020.2978014

Long, Y., Feng, T., Fan, Y., & Liu, L [Lijun] (2023). Adopting blockchain technology to enhance green supply chain integration: The moderating role of organizational culture. *Business Strategy and the Environment*, *32*(6), 3326–3343. https://doi.org/10.1002/bse.3302

Lumineau, F., Wang, W., & Schilke, O. (2021). Blockchain Governance—A New Way of Organizing Collaborations? *Organization Science*, *32*(2), 500–521. https://doi.org/10.1287/orsc.2020.1379

Majchrzak, A., Rice, R., Malhotra, A., King, N., & Ba, S. (2000). Technology Adaptation: The Case of a Computer-Supported Inter-Organizational Virtual Team. *MIS Quarterly*, *24*, 569–600. https://doi.org/10.2307/3250948

Maler, E., & Reed, D. (2008). The Venn of Identity: Options and Issues in Federated Identity Management. *IEEE Security & Privacy Magazine*, *6*(2), 16–23. https://doi.org/10.1109/MSP.2008.50

March, S., & Smith, G. (1995). Design and natural science research on information technology. *Decision Support Systems*, *15*(4), 251–266. https://doi.org/10.1016/0167-9236(94)00041-2

Mattila, J., & Seppälä, T. (2016). *Digital Trust, Platforms, and Policy*. https://doi.org/10.13140/RG.2.1.1565.1928

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

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An Integrative Model of Organizational Trust. *The Academy of Management Review*, *20*(3), 709. https://doi.org/10.2307/258792

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

Mingers, J. (2001). Combining IS Research Methods: Towards a Pluralist Methodology. *Information Systems Research*, *12*(3), 240–259. https://doi.org/10.1287/isre.12.3.240.9709

Miranda, S., Wang, D., & Tian, C. (2022). Discursive Fields and the Diversity-Coherence Paradox: An Ecological Perspective on the Blockchain Community Discourse. *MIS Quarterly*, *45*, 1421–1452. https://doi.org/10.25300/MISQ/2022/15736

Morse, J. (1990). *Qualitative Nursing Research: A Contemporary Dialogue* (1st ed.). SAGE Publications Incorporated. https://ebookcentral.proquest.com/lib/kxp/detail.action?docID=6950689

Mühle, A., Grüner, A., Gayvoronskaya, T., & Meinel, C. (2018). A survey on essential components of a self-sovereign identity. *Computer Science Review*, *30*, 80–86. https://doi.org/10.1016/j.cosrev.2018.10.002

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

Nack, J. (1982). Newton's Laws of Data Processing. *The Economics of Information Processing*.

Nærland, K., Mueller-Bloch, C., Beck, R., & Palmund, S. (2017). Blockchain to Rule the Waves – Nascent Design Principles for Reducing Risk and Uncertainty in Decentralized Environments. In *International Conference on Interaction Sciences*.

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

Newman, L. (2020). *Think Twice Before Using Facebook, Google, or Apple to Sign In Everywhere*. https://www.wired.com/story/single-sign-on-facebook-google-apple/#:~:text=In%20September%202018%2C%20Facebook%20disclosed,the%20incident%20underscored%20the%20potential

Norvill, R., Steichen, M., Shbair, W. M., & State, R. (2019). Demo: Blockchain for the Simplification and Automation of KYC Result Sharing. In *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* (pp. 9–10). IEEE. https://doi.org/10.1109/BLOC.2019.8751480

Orlikowski, W., & Iacono, S. (2001). Research Commentary: Desperately Seeking the "IT" in IT Research - A Call to Theorizing the IT Artifact. *Information Systems Research*, *12*, 121–134. https://api.semanticscholar.org/CorpusID:10833059

Österle, H., Becker, J., Frank, U., Hess, T., Karagiannis, D., Krcmar, H., Loos, P., Mertens, P., Oberweis, A., & Sinz, E. J. (2011). Memorandum on design-oriented information systems research. *European Journal of Information Systems*, *20*(1), 7–10. https://doi.org/10.1057/ejis.2010.55

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

Parra Moyano, J., & Ross, O. (2017). KYC Optimization Using Distributed Ledger Technology. *Business & Information Systems Engineering*, *59*(6), 411–423. https://doi.org/10.1007/s12599-017-0504-2

Peffers, K., Tuunanen, T., Rothenberger, M., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems*, *24*, 45–77.

Pereira, J., Tavalaei, M. M., & Ozalp, H. (2019). Blockchain-based platforms: Decentralized infrastructures and its boundary conditions. *Technological Forecasting and Social Change*, *146*, 94–102. https://doi.org/10.1016/j.techfore.2019.04.030

Perscheid, G., Ostern, N., & Moormann, J. (2020). Towards a taxonomy of decentralized platform-based business models. In

Preukschat, A., & Reed, D. (2021). *Self-sovereign identity: Decentralized digital identity and verifiable credentials*. Manning.

Public Affairs Council. (2021). *Public Affairs Pulse Survey Report*. https://pac.org/wp-content/uploads/Pulse_2021_Report.pdf

Puigserver, M., Payeras-Capellà, M. M., Ferrer-Gomila, J., Vives Guasch, A., & Castellà-Roca, J. (2012). A survey of electronic ticketing applied to transport. *Computers & Security*, *31*, 925–939. https://doi.org/10.1016/j.cose.2012.07.004

Rabby, M. K. M., Islam, M. M., & Imon, S. M. (2019). A Review of IoT Application in a Smart Traffic Management System. In *2019 5th International Conference on Advances in Electrical Engineering (ICAEE)* (pp. 280–285). IEEE. https://doi.org/10.1109/ICAEE48663.2019.8975582

Regner, F., Urbach, N., & Schweizer, A. (2019). NFTs in Practice - Non-Fungible Tokens as Core Component of a Blockchain-based Event Ticketing Application. In *International Conference on Interaction Sciences*. https://api.semanticscholar.org/CorpusID:204860347

Rieger, A., Guggenmos, F., Lockl, J., Fridgen, G., & Urbach, N. (2019). Building a Blockchain Application that Complies with the EU General Data Protection Regulation. *MIS Quarterly Executive*, *18*(4), 263–279. https://doi.org/10.17705/2msqe.00020

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

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

Rotolo, D., Hicks, D., & Martin, B. R. (2015). What is an emerging technology? *Research Policy*, *44*(10), 1827–1843. https://doi.org/10.1016/j.respol.2015.06.006

Rubin, H. J., & Rubin, I. S. (2012). *Qualitative interviewing: The art of hearing data* (Third edition). Sage.

Saldaña, J. (2016). *The coding manual for qualitative researchers* (3. edition). Sage.

Santana, E. F. Z., Chaves, A. P., Gerosa, M. A., Kon, F., & Milojicic, D. S. (2018). Software Platforms for Smart Cities. *ACM Computing Surveys*, *50*(6), 1–37. https://doi.org/10.1145/3124391

Sasse, M. A., & Kirlappos, I. (2014). Design for Trusted and Trustworthy Services: Why We Must Do Better. In R. H. R. Harper (Ed.), *Trust, Computing, and Society* (pp. 229–249). Cambridge University Press. https://doi.org/10.1017/CBO9781139828567.015

Schardong, F., & Custódio, R. (2022). Self-Sovereign Identity: A Systematic Review, Mapping and Taxonomy. *Sensors (Basel, Switzerland)*, *22*(15). https://doi.org/10.3390/s22155641

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

Schneiderman, E. (2016). *What's blocking New Yorkers from getting tickets*. https://ag.ny.gov/sites/default/files/reports/Ticket_Sales_Report.pdf

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

Schweizer, A., Knoll, P., Urbach, N., Gracht, H. A. von der, & Hardjono, T. (2020). To What Extent Will Blockchain Drive the Machine Economy? Perspectives From a Prospective Study. *IEEE Transactions on Engineering Management*, *67*(4), 1169–1183. https://doi.org/10.1109/TEM.2020.2979286

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

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

Sedlmeir, J., 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

Seidel, S., Recker, J., & vom Brocke, J. (2013). Sensemaking and Sustainable Practicing: Functional Affordances of Information Systems in Green Transformations. *MIS Quarterly*, *37*, 1275–1299. https://api.semanticscholar.org/CorpusID:2871814

Shiller, R. J. (2019). *Narrative economics: How stories go viral & drive major economic events*. Princeton University Press.

Shin, D. (2022). How do people judge the credibility of algorithmic sources? *AI & SOCIETY*, *37*(1), 81–96. https://doi.org/10.1007/s00146-021-01158-4

Söllner, M., Hoffmann, A., & Leimeister, J. M. (2016). Why different trust relationships matter for information systems users. *European Journal of Information Systems*, *25*(3), 274–287. https://doi.org/10.1057/ejis.2015.17

Soltani, R., Trang Nguyen, U., & An, A. (2018). A New Approach to Client Onboarding Using Self-Sovereign Identity and Distributed Ledger. In *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)* (pp. 1129–1136). IEEE. https://doi.org/10.1109/Cybermatics_2018.2018.00205

Sonnenberg, C., & vom Brocke, J. (2012). Evaluations in the Science of the Artificial - Reconsidering the Build-Evaluate Pattern in Design Science Research. In *International Conference on Design Science Research in Information Systems and Technology*. https://api.semanticscholar.org/CorpusID:43568491

Sporny, M., Longley, D., & chadwick, D. (2022). *Verifiable Credentials Data Model 1.1*. https://www.w3.org/TR/vc-data-model/

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

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

Swinhoe, D., & Hill, M. (2022). *https://www.csoonline.com/article/534628/the-biggest-data-breaches-of-the-21st-century.html*. https://www.csoonline.com/article/534628/the-biggest-data-breaches-of-the-21st-century.html

Sykes, T. A., Venkatesh, V., & Johnson, J. L. (2014). Enterprise System Implementation and Employee Job Performance: Understanding the Role of Advice Networks. *MIS Quarterly*, *38*(1), 51–72. https://doi.org/10.25300/MISQ/2014/38.1.03

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

Udokwu, C., Anyanka, H., & Norta, A. (2020). Evaluation of Approaches for Designing and Developing Decentralized Applications on Blockchain. In *Proceedings of the 2020 4th International Conference on Algorithms, Computing and Systems* (pp. 55–62). ACM. https://doi.org/10.1145/3423390.3426724

Vassilakopoulou, P., Haug, A., Salvesen, L. M., & Pappas, I. O. (2023). Developing human/AI interactions for chat-based customer services: lessons learned from the Norwegian government. *European Journal of Information Systems*, *32*(1), 10–22. https://doi.org/10.1080/0960085X.2022.2096490

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. https://doi.org/10.1057/ejis.2014.36

Venkatesh, Morris, & Davis (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly*, *27*(3), 425. https://doi.org/10.2307/30036540

Venkatesh, V., & Bala, H. (2008). Technology Acceptance Model 3 and a Research Agenda on Interventions. *Decision Sciences*, *39*(2), 273–315. https://doi.org/10.1111/j.1540-5915.2008.00192.x

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. https://doi.org/10.17705/1jais.00611

The Wall Street Journal. (2022). *Blockchain Fails to Gain Traction in the Enterprise*. https://www.wsj.com/articles/blockchain-fails-to-gain-traction-in-the-enterprise-11671057528

Walsham, G. (1993). Decentralization of information systems in developing countries: power to the people? *Journal of Information Technology*, Article 8.

Wang (2010). Chasing the Hottest IT: Effects of Information Technology Fashion on Organizations. *MIS Quarterly*, *34*(1), 63. https://doi.org/10.2307/20721415

Wang, F., & Filippi, P. de (2020). Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion. *Frontiers in Blockchain*, *2*, Article 28. https://doi.org/10.3389/fbloc.2019.00028

Waterson, M. (2016). *Independent review of consumer protection measures concerning online secondary ticketing facilities*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/525885/ind-16-7-independent-review-online-secondary-ticketing-facilities.pdf

World Economic Forum. (2022). *Earning Digital Trust: Earning Digital Trust: Decision-Making for Trustworthy Technologies*. https://www3.weforum.org/docs/WEF_Earning_Digital_Trust_2022.pdf

Yan, Z., & Holtmanns, S. (2013). Trust Modeling and Management. In J. Bishop (Ed.), *Examining the Concepts, Issues, and Implications of Internet Trolling* (pp. 279–303). IGI Global. https://doi.org/10.4018/978-1-4666-2803-8.CH018

Yin, R. (2008). *Case Study Research: Design and Methods*. SAGE Publications.

Yin, R. K. (2014). *Case study research: Design and methods* (5. edition). Sage.

Yin, R. K. (2017). *Case Study Research and Applications* (6th ed.). SAGE Publications US.

Zavolokina, L., Ziolkowski, R., & Bauer, I. (2020). Management, Governance, and Value Creation in a Blockchain Consortium. *MIS Quarterly Executive*, *19*(1), 1–17. https://doi.org/10.17705/2msqe.00022

Zeiß, C., Schaschek, M., Straub, L., Tomitza, C., & Winkelmann, A. (2024). Re-intermediation of the crypto asset ecosystem by banks: An empirical study on acceptance drivers among the populace. *Electronic Markets*, *34*(1). https://doi.org/10.1007/s12525-024-00720-4

Zetzsche, D., Buckley, R., & Arner, D. (2018). Digital ID and AML/CDD/KYC utilities for financial inclusion, integrity and competition. *Journal of Financial Transformation*, 133–142.

Appendices

Appendix A: Declarations of Co-Authorship and the Individual Contributions

I will now describe the co-authors' contributions to the essays.

Essay 1: Beyond Disintermediation: A Multiple Case Study of Emerging Intermediary Roles in Blockchain Applications

This research paper was co-authored by Simon Feulner, Jens-Christian Stoetzer, Tobias Guggenberger, and Nils Urbach. The co-authors contributed as follows:

Simon Feulner (co-author)

Simon Feulner co-developed the research project. He participated in regular discussion rounds and contributed to developing 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. Thus, Simon's co-authorship is reflected in the entire research project.

Jens-Christian Stoetzer (co-author)

Jens-Christian Stoetzer co-developed the research project. He participated in regular discussion rounds and helped develop the paper's theoretical foundations, content, and structure. He engaged in textual elaboration, particularly in the introduction, theoretical background, methodology, results, discussion, and conclusion sections. Thus, Jens-Christian'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's co-authorship is reflected in the entire research project.

Nils Urbach (co-author)

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

Essay 2: Designing a Framework for Digital KYC Process Built on Blockchain-Based Self-Sovereign Identity

This research paper was co-authored by Vincent Schlatt, Johannes Sedlmeir, Simon Feulner, and Nils Urbach. The co-authors contributed as follows:

Vincent Schlatt (co-author)

Vincent Schlatt co-developed the research project. He contributed by providing ongoing guidance on the design and development of the proposed architecture and set of processes. Further, he took part in the evaluation of the proposed artifacts. Together with the co-authors, he developed the design principles resulting from our research. He also engaged in the revision of the paper and in formulating its theoretical contributions. Therefore, Vincent's co-authorship is reflected in the entire research project.

Johannes Sedlmeir (co-author)

Johannes Sedlmeir co-developed the research project. He contributed to the technical background and analyzed, improved, and described the artifact's technical properties. He also derived the design principles from an analysis of the interview transcripts. Together with the other first author, he created the initial manuscript draft and refined the DOs, method, criteria-based evaluation, and design principles sections. Thus, Johannes's co-authorship is reflected in the entire research project.

Simon Feulner (subordinate co-author)

Simon Feulner initiated and co-developed the research project. He contributed by developing the paper's theoretical foundations, designing, developing, and testing the IT artifact, conducting and analyzing the interviews with the experts, developing the theoretical contributions, and engaging in most of the textual elaboration. Also, he participated in research discussions and provided feedback on the paper's content and structure. Thus, Simon's co-authorship is reflected in the entire research project.

Nils Urbach (subordinate 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.

Essay 3: Exploring the Use of Self-Sovereign Identity for Event Ticketing Systems

This research paper was co-authored by Vincent Schlatt, Johannes Sedlmeir, Simon Feulner, and Nils Urbach. The co-authors contributed as follows:

Simon Feulner (leading co-author)

Simon Feulner initiated and developed the research project. He contributed by developing the paper's theoretical foundations, designing, developing, and testing the IT artifact, conducting and analyzing the interviews with the experts, developing the theoretical contributions, and engaging in most of the textual elaboration. He also participated in research discussions and provided feedback on the paper's content and structure. Thus, Simon's co-authorship is reflected in the entire research project.

Johannes Sedlmeir (subordinate co-author)

Johannes Sedlmeir co-developed the research project. He contributed by participating in research discussions and co-shaping the paper's content and structure. Together with the co-authors, he developed the design principles resulting from our research. Also, he engaged in the revision of the paper and in formulating its theoretical contributions. Therefore, Johannes's co-authorship is reflected in the entire research project.

Vincent Schlatt (subordinate co-author)

Vincent Schlatt co-developed the research project. He contributed by participating in research discussions and co-shaping the paper's content and structure. Together with the co-authors, he developed the design principles resulting from our research. Also, he engaged in the revision of the paper and in formulating its theoretical contributions. Therefore, Vincent's co-authorship is reflected in the entire research project.

Nils Urbach (subordinate 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's co-authorship is reflected in the entire research project.

Essay 4: Driving Self-Sovereign Identity: Designing a Car Identity Management Framework

This research paper was co-authored by Hendrik Pfaff, Simon Feulner, Vincent Schaaf, Tobias Guggenberger, and Nils Urbach. The co-authors contributed as follows:

Hendrik Pfaff (co-author)

Hendrik Pfaff co-developed the research project. He contributed by developing the paper's theoretical foundations, designing, developing, and testing the IT artifact, conducting and analyzing the interviews with the experts, developing the theoretical contributions, and engaging in most of the textual elaboration. He also participated in research discussions and provided feedback on the paper's content and structure. Thus, Hendrik's co-authorship is reflected in the entire research project.

Simon Feulner (co-author)

Simon Feulner initiated and co-developed the research project. He participated in regular discussion rounds and contributed to developing the paper's theoretical foundations, content, and structure. Together with the co-authors, he developed the design principles resulting from our research. Further, he engaged in textual elaboration, particularly in the introduction, theoretical background, methodology, results, evaluation, discussion, and conclusion sections. Thus, Simon's co-authorship is reflected in the entire research project.

Vincent Schaaf (co-author)

Vincent Schaaf co-developed the research project. He participated in regular discussion rounds and contributed to developing the paper's theoretical foundations, content, and structure. Together with the co-authors, he developed the design principles resulting from our research. Also, he engaged in textual elaboration, particularly in the introduction, theoretical background, methodology, results, evaluation, discussion, and conclusion sections. Thus, Vincent'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's co-authorship is reflected in the entire research project.

Nils Urbach (co-author)

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

Essay 5: Recoding Asylum Management – How Germany's Federal Government Approached Innovation with Emerging IT

The research paper was co-authored by Julia Amend, Simon Feulner, Alexander Rieger, Tamara Roth, and Nils Urbach. The co-authors contributed as follows:

Julia Amend (co-author)

Julia Amend initiated and co-developed the research project. She participated in regular discussion rounds and contributed to developing the paper's theoretical foundations, content, and structure. Further, she engaged in textual elaboration, particularly in the introduction, theoretical background, methodology, results, discussion, and conclusion sections. Thus, Julia's co-authorship is reflected in the entire research project.

Simon Feulner (co-author)

Simon Feulner also initiated and co-developed the research project. He participated in regular discussion rounds and contributed to developing 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. Thus, Simon's co-authorship is reflected in the entire research project.

Alexander Rieger (co-author)

Alexander Rieger co-developed the research project. He participated in regular discussion rounds and contributed to developing 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. Thus, Alexander's co-authorship is reflected in the entire research project.

Tamara Roth (co-author)

Tamara Roth co-developed the research project. She participated in regular discussion rounds and helped develop the paper's theoretical foundations, content, and structure. She also engaged in textual elaboration, particularly in the introduction, theoretical background, methodology, results, discussion, and conclusion sections. Thus, Tamara's co-authorship is reflected in the entire research project.

Nils Urbach (co-author)

Nils Urbach participated in selected research discussions, provided feedback on the

paper's content and structure, and reviewed the manuscript. Thus, Nils's co-authorship is reflected in the entire research project.

Essay 6: Bringing Government into the Digital Age: Insights from Germany's Asylum Procedure

This research paper was co-authored by Julia Amend, Simon Feulner, Alexander Rieger, Tamara Roth, Tobias Guggenberger, and Gilbert Fridgen. The authors contributed as follows:

Julia Amend (co-author)

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

Simon Feulner (co-author)

Simon Feulner initiated and co-developed the research project. He participated in regular discussion rounds and contributed to developing 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, Simon's co-authorship is reflected in the entire research project.

Alexander Rieger (co-author)

Alexander Rieger 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, Alexander's co-authorship is reflected in the entire research project.

Tamara Roth (co-author)

Tamara Roth co-developed the research project. She participated in regular discussion rounds and helped develop the paper's theoretical foundations, content, and structure. Further, she engaged in textual elaboration, particularly in the introduction,

theoretical background, methodology, results, discussion, and conclusion sections. She also participated in research discussions and co-shaped the paper's content and structure. Thus, Tamara's co-authorship is reflected in the entire research project.

Tobias Guggenberger (co-author)

Tobias Guggenberger 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, Tobias's co-authorship is reflected in the entire research project.

Gilbert Fridgen (co-author)

Gilbert Fridgen participated in selected research discussions, provided feedback on the paper's content and structure, and reviewed the manuscript. Thus, Gilbert's co-authorship is reflected in the entire research project.

Essay 7: Affordances, Experimentation and Actualization of Self-Sovereign Identity: A Case Study of the Implementation and Use of SSI in the Public Sector

This research paper was co-authored by Simon Feulner, Jonathan Lautenschlager, Tobias Guggenberger, Fabiane Völter, and Nils Urbach. 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 the revision of the paper and in formulating its theoretical contributions. Thus, Simon's 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 the revision of the paper and in formulating its theoretical contributions. Thus, Jonathan's 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, Tobias's 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 regular discussion rounds and helped develop the paper's theoretical foundations, content, and structure. Further, she engaged in textual elaboration, particularly in the introduction, theoretical background, methodology, results, discussion, and conclusion

sections. She also participated in research discussions and co-shaped the paper's content and structure. Thus, Fabiane's co-authorship is reflected in the entire research project.

Nils Urbach (co-author)

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

Appendix B: Other Publications by the Author

Table 2: Overview over Other Publications by the Author

Reference	Title	Publication outlet
Feulner, S., Guggenberger, T., Stoetzer, J.-C., & Urbach, N. (2022)	Shedding Light on the Blockchain Disintermediation Mystery: A Review and Future Research Agenda	*Proceedings of the 30th European Conference on Information Systems (ECIS)*
Amend, J. et al. (2022)	Federal Blockchain Infrastructure Asylum (FLORA) – Piloting and evaluation of the FLORA support system in the context of the AnkER facility Dresden	BAMF white paper
Amend, J. et al. (2022)	Opportunities and challenges of using blockchain technology in public administration – Insights from the FLORA project of Germany's Federal Office for Migration and Refugees	BAMF white paper
Urbach, N. et al. (2024)	EU Digital Identity Wallet: Anwendungsfälle, Nutzungspotenziale und Herausforderungen für Unternehmen	Fraunhofer white paper
Gimpel, H. et al. (2024)	(Generative) AI Competencies for Future-Proof Graduates: Inspiration for Higher Education Institutions	Hohenheim Discussion Papers in Business, Economics, and Social Sciences
Becker et al. (2024)	Lohnt sich Microsoft 365 Copilot? Eine Potenzialanalyse für Unternehmen und Bildungseinrichtungen	Bayreuther Arbeitspapiere zur Wirtschaftsinformatik
Feulner et al. (2024)	Self-Sovereign Identity for Digital KYC	Book chapter in: Decentralized Technologies – Financial Sector in Change

Beyond Disintermediation: A Multiple Case Study of Emerging Intermediary Roles in Blockchain Applications[3]

Authors

Simon Feulner, Jens-Christian Stoetzer, Tobias Guggenberger, Nils Urbach

Extended Abstract

Blockchain technology has garnered significant attention from both academia and industry due to its potential to profoundly transform markets, organizational structures, and societal interactions. Initially praised for its capability to remove traditional intermediaries through decentralization—a phenomenon known as disintermediation—blockchain promised direct, trustless transactions and a fundamental shift in existing business models (Chalmers et al., 2021). However, as blockchain applications matured, researchers and practitioners observed the emergence of a more complex reality: instead of entirely eliminating intermediaries, blockchain often leads to a reconfiguration or introduction of new intermediary roles, a process termed re-intermediation (Feulner et al., 2022; Zeiß et al., 2024).

Despite recognizing the dual dynamics of disintermediation and re-intermediation, prior studies have provided limited clarity regarding the specific conditions under which blockchain-driven re-intermediation occurs, as well as the characteristics distinguishing new intermediaries from traditional gatekeepers. Furthermore, the literature lacks comprehensive insights into how different blockchain architectures, regulatory environments, and stakeholder interactions shape the transition from disintermediation towards re-intermediation (Chalmers et al., 2021). Thus, there remains a significant research gap concerning the interplay of these factors in determining the fate and function of intermediaries in blockchain ecosystems. Consequently, we ask the following research question:

"How and under what conditions do blockchain solutions transition from disintermediation to re-intermediation, and what factors most significantly drive this transition?"

[3] At the time of publishing this thesis, this essay is under review for publication in a scientific journal. Thus, I provide an extended abstract that covers the essay's content.

To investigate this question, we adopted a positivist multiple case study methodology (Dubé & Paré, 2003; Yin, 2009), analyzing two distinct blockchain applications in depth. Specifically, we compared TradeLens, a permissioned blockchain solution in the shipping industry, with MakerDAO, a decentralized finance protocol characterized by permissionless governance. Our methodological choice allowed us to closely examine real-world implementations, capturing the dynamics of intermediary transformation in differing organizational and technological contexts.

We contribute an integrative theoretical framework emphasizing that blockchain's impact on intermediation is conditional, shaped significantly by governance structures, regulatory requirements, and technological complexity. This framework extends existing literature by moving beyond a binary interpretation of disintermediation, providing practitioners and academics a more comprehensive understanding of blockchain's nuanced influence on market intermediation. Ultimately, our study underlines the necessity of considering broader organizational and regulatory contexts when evaluating blockchain's disruptive potential, offering critical guidance for organizations navigating the evolving landscape of intermediation.

Keywords: Intermediation; Disintermediation; Electronic Markets; Blockchain; Multiple Case Study

References

Chalmers, D., Matthews, R., & Hyslop, A. (2021). Blockchain as an external enabler of new venture ideas: Digital entrepreneurs and the disintermediation of the global music industry. *Journal of Business Research*, *125*, 577–591. https://doi.org/10.1016/j.jbusres.2019.09.002

Dubé, L., & Paré, G. (2003). Rigor in Information Systems Positivist Case Research: Current Practices, Trends, and Recommendations. *MIS Quarterly*, *27*(4), 597. https://doi.org/10.2307/30036550

Feulner, S., Guggenberger, T., Stoetzer, J.-C., & Urbach, N. (2022). Shedding Light on the Blockchain Disintermediation Mystery: A Review and Future Research Agenda. In *ECIS,* Timisoara, Romania. https://aisel.aisnet.org/ecis2022_rp/13

Yin, R. K. (2009). *Case study research: Design and methods* (4. ed.). *Applied social research methods series: Vol. 5*. Sage.

Zeiß, C., Schaschek, M., Straub, L., Tomitza, C., & Winkelmann, A. (2024). Re-intermediation of the crypto asset ecosystem by banks: An empirical study on acceptance drivers among the populace. *Electronic Markets*, *34*(1). https://doi.org/10.1007/s12525-024-00720-4

Designing a Framework for Digital KYC Processes Built on Blockchain-Based Self-Sovereign Identity[4]

Authors

Vincent Schlatt, Johannes Sedlmeir, Simon Feulner, Nils Urbach

Abstract

Know your customer (KYC) processes place a great burden on banks, because they are costly, inefficient, and inconvenient for customers. While blockchain technology is often mentioned as a potential solution, it is not clear how to use the technology's advantages without violating data protection regulations and customer privacy. We demonstrate how blockchain-based self-sovereign identity (SSI) can solve the challenges of KYC. We follow a rigorous design science research approach to create a framework that utilizes SSI in the KYC process, deriving nascent design principles that theorize on blockchain's role for SSI.

Keywords: Digital certificate, Digital wallet, Decentralized identity, Distributed ledger technology, Verifiable credential

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

Exploring the use of self-sovereign identity for event ticketing systems[5]

Authors

Simon Feulner, Johannes Sedlmeir, Vincent Schlatt, Nils Urbach

Abstract

Ticket fraud and ticket scalping activities often cause high costs as well as trust concerns for fans buying event tickets, especially in the secondary ticketing market. To address these issues, several publications and projects have proposed using blockchain technology to enable digital trust and ticket verifiability and thus to improve event ticketing systems. However, these approaches exhibit considerable privacy challenges and fall short concerning reliable, efficient visitor identification, which is necessary for controlling secondary market transactions. We demonstrate how a novel paradigm for end-user digital identity management, called self-sovereign identity (SSI), can be utilized to gain secondary market control. To do so, we follow a rigorous design science research approach to build and evaluate an SSI-based event ticketing framework. Our findings demonstrate that SSI-based event ticketing can enable efficient secondary market control by facilitating a practical implementation of the centralized exchange model. To generalize our results, we derive design principles for the efficient, reliable, and privacy-oriented ticket and identity verification and the use of revocation registries.

Keywords: Bot prevention, Digital identity management, Digital wallet, Secondary market control, Ticket scalping, Verifiable credentials

[5] This essay has been published in: Feulner, S., Sedlmeir, J., Schlatt, V. & Urbach, N. (2022). Exploring the use of self-sovereign identity for event ticketing systems. Electron Markets 32, 1759–1777 (2022). https://doi.org/10.1007/s12525-022-00573-9

Driving Self-Sovereign Identity: Designing a Car Identity Management Framework[6]

Authors

Hendrik Pfaff, Simon Feulner, Vincent Schaaf, Tobias Guggenberger, Nils Urbach

Abstract

Effective identity management is crucial for secure, reliable, and trustworthy interactions in both physical and digital domains. Traditional identification methods for vehicles, such as license plates, VIN numbers, and physical permits, face significant limitations. Physical identifiers can easily be damaged, stolen, or counterfeited, facilitating unauthorized use, insurance fraud, and identity falsification. Similarly, digital identifiers such as SIM cards or telematics systems pose challenges regarding privacy, scalability, and security (Castella-Roca et al., 2017; Kailus et al., 2024).

Despite recognition of these issues, current literature lacks a comprehensive, integrated solution capable of addressing the complexity of modern vehicle ecosystems, particularly the seamless integration and simultaneous management of diverse identity types such as individuals, organizations, and machines. While various approaches have been explored (Alessandria & Vizzarri, 2021; Castella-Roca et al., 2017), they often remain fragmented and fail to provide an effective, scalable solution that guarantees both user privacy and interoperability within increasingly digitalized environments. The absence of an integrated framework that leverages decentralized identity management paradigms significantly limits advancements in secure and privacy-preserving interactions among entities within automotive ecosystems. Addressing this research gap, this study explores the following research question:

"How to leverage SSI to design a holistic and privacy-preserving framework for managing digital car identities?"

We employ an iterative Design Science Research method as proposed by Peffers et al. (2007) to answer the research question. Through structured expert interviews, we iteratively evaluate both the initial design objectives and the developed framework.

The key contribution of this research is the presentation of a comprehensive SSI-based

[6] At the time of publishing this thesis, this essay is under review for publication in a scientific journal. Thus, I provide an extended abstract that covers the essay's content.

framework specifically tailored for digital car IM. The framework integrates multiple identity types into a cohesive system. It offers a set of effective tools, including the standardized use of verifiable credentials, delegation of credentials to machine identity wallets, and deployment of infrastructure devices capable of identity verification. This combination ensures privacy, scalability, and reliability within decentralized environments. Moreover, the research distills three essential Design Principles from the framework evaluation. First, it highlights the importance of standardized SSI protocols to facilitate seamless interoperability among different identity types, enabling smooth interactions across complex ecosystems. Second, it emphasizes the user-centric nature of SSI, granting users full control over their data and significantly enhancing privacy. Finally, the study identifies cryptographic elements of SSI, particularly zero-knowledge proofs and public key infrastructures, as vital for ensuring data integrity and establishing robust trust mechanisms.

Keywords: Self-Sovereign Identity, Car Identity Management, Base Identity, Privacy, Design Science Research

References

Alessandria, M. L., & Vizzarri, A. (2021). Self-Sovereign Identity and Blockchain applications for the automotive sector. In *2021 AEIT International Conference on Electrical and Electronic Technologies for Automotive (AEIT AUTOMOTIVE)* (pp. 1–6). IEEE. https://doi.org/10.23919/AEITAUTOMOTIVE52815.2021.9662861

Castella-Roca, J., Mut-Puigserver, M., Payeras-Capella, M. M., Viejo, A., & Angles-Tafalla, C. (2017). Secure and Anonymous Vehicle Access Control System to Traffic-Restricted Urban Areas. In *2017 26th International Conference on Computer Communication and Networks (ICCCN)* (pp. 1–7). IEEE. https://doi.org/10.1109/ICCCN.2017.8038491

Kailus, A., Kern, D., & Krauß, C. (2024). Self-sovereign Identity for Electric Vehicle Charging. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (14585 LNCS, pp. 137–162). Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/978-3-031-54776-8_6

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

Recoding Asylum Management - How Germany's Federal Government Approached Innovation with Emerging IT[7]

Authors

Julia Amend, Simon Feulner, Tamara Roth, Alexander Rieger, Nils Urbach

Abstract

Public sector organizations face increasing pressure to innovate digitally, leveraging emerging decentralized information systems such as blockchain or self-sovereign identity technologies to enhance efficiency, transparency, and citizen trust. Innovations enabled by decentralized ISs promise substantial improvements in crucial public services including education, healthcare, migration management, and public safety. Despite such potentials, public organizations frequently encounter significant challenges in adopting these technologies (Goh & Arenas, 2020; Pahlka, 2023). Such obstacles primarily originate from entrenched structural and cultural constraints inherent to public institutions, characterized by rigid hierarchies, complex regulations, inflexible budgeting, and risk-averse organizational cultures (Meijer, 2015). Additionally, decentralized ISs are typically immature and often surrounded by exaggerated public narratives regarding their transformative capabilities. This immaturity fuels cycles of heightened expectations followed by skepticism, creating polarized environments that further complicate practical integration (Caudle et al., 1991; Thacher & Rein, 2004). Consequently, governmental organizations often experience uncertainty regarding viable use cases, struggle to obtain internal and external stakeholder support, and lack effective strategies to overcome resistance to change. These issues collectively represent a critical research gap, as existing scholarship provides limited empirical guidance on how public sector organizations can realistically navigate such barriers to successfully innovate through decentralized ISs. Addressing this gap, our study investigates the following research question:

How can public sector organizations successfully innovate by means of emerging decentralized ISs?

[7] At the time of publication of this thesis, this essay is in preparation for submission to a scientific journal. Thus, I provide an extended abstract that covers the essay's content.

Methodologically, we employed a clinical research approach (Baskerville et al., 2023) characterized by active, collaborative engagement with practitioners to address real-world innovation challenges. This involved participating in Germany's Federal Office for Migration and Refugees' FLORA project, which aimed to modernize asylum procedures using blockchain technology. Our empirical basis comprises extensive qualitative data collected between 2018 and 2024, including 98 interviews, over 1,000 pages of project documentation, and direct observations. Data analysis followed grounded theory principles to ensure systematic triangulation and theoretical rigor.

Our study explicitly provides four contributions to research and practice: First, we address the lack of clear public-sector-specific guidance on developing viable use cases. We demonstrate that translating private-sector innovation narratives into concrete government applications is essential for successful innovation. Second, we provide insights into overcoming structural barriers, emphasizing the necessity of interdisciplinary teams, iterative problem-solving, and strategic collaboration with external technology experts. Third, our research illuminates effective ways of managing cultural barriers by highlighting the role of cultural sensemaking. We show how public managers can leverage innovation narratives aligned with core governmental values to foster organizational acceptance and engagement with decentralized ISs. Fourth, we advance understanding of how to secure stakeholder buy-in in politically sensitive environments. We highlight the necessity for project leaders to engage as political entrepreneurs, strategically managing communication and transparency to overcome skepticism, thereby ensuring sustained political and public support. By explicitly addressing these four areas, our study provides actionable insights for scholars and practitioners navigating the complex realities of digital innovation in the public sector.

Keywords: Emerging IT, blockchain, clinical IS research, government innovation, structural barriers, cultural barriers

References

Baskerville, R., vom Brocke, J., Mathiassen, L., & Scheepers, H. (2023). Clinical research from information systems practice. *European Journal of Information Systems*, *32*(1), 1–9. https://doi.org/10.1080/0960085X.2022.2126030

Caudle, S. L., Gorr, W. L., & Newcomer, K. E. (1991). Key Information Systems Management Issues for the Public Sector. *MIS Quarterly*, *15*(2), 171. https://doi.org/10.2307/249378

Corbin, J., & Strauss, A. (1990). Grounded theory research: Procedures, canons, and evaluation criteria. *Qualitative Sociology*, *13*(1), 3–21.

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

Huber, G. P., & Power, D. J. (1985). Retrospective reports of strategic-level managers: Guidelines for increasing their accuracy. *Strategic Management Journal*, *6*(2), 171–180.

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

Pahlka, J. (2023). *Recoding America: Why Government Is Failing in the Digital Age and How We Can Do better*. Metropolitan Books.

Rousseau, D. M., Manning, J., & Denyer, D. (2008). 11 Evidence in Management and Organizational Science: Assembling the Field's Full Weight of Scientific Knowledge Through Syntheses. *The Academy of Management Annals*, *2*(1), 475–515. https://doi.org/10.1080/19416520802211651

Schein, E. H. (2008). Clinical Inquiry/Research. In *The SAGE Handbook of Action Research* (pp. 266–279). SAGE Publications Ltd. https://doi.org/10.4135/9781848607934.n26

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

Bringing Government into the Digital Age: Insights from Germany's Asylum Procedure[8]

Authors

Julia Amend, Simon Feulner, Tobias Guggenberger, Alexander Rieger, Tamara Roth, Gilbert Fridgen

Abstract

Governments spend billions to bring their services into the digital age. But government IT projects can be challenging when the law requires cooperation across multiple levels of government while each level must maintain distinct IT systems. This article examines how Germany's Federal Office for Migration and Refugees successfully navigated these challenges when it implemented FLORA, an inter-governmental IT system that supports the coordination of asylum procedures. FLORA improves the exchange and quality of procedural information, accelerates the procedure by up to 50 percent, and mitigates error and data privacy concerns. Based on our insights into the FLORA project, we provide three recommendations for successfully building inter-governmental IT systems.

Keywords: Government services, Government IT systems, Decentralized IT architecture, Private blockchain, Asylum management.

[8]This essay has been published in: Amend, J., Feulner, S., Rieger, A., Roth, T., Fridgen, G. & Guggenberger, T. (2025). How Germany Successfully Implemented Its Intergovernmental FLORA System. MIS Quarterly Executive: Vol. 24: Iss. 1, Article 8.

Affordances, Experimentation and Actualization of Self-Sovereign Identity: A Case Study of the Implementation and Use of SSI in the Public Sector[9]

Authors

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

Abstract

In an increasingly digitalized society, managing digital identities securely and trustworthily is a pressing and highly debated issue. Traditional identity management systems, such as federated identity frameworks, grant centralized entities substantial control over user data, raising significant privacy, security, and user autonomy concerns (Reed & Preukschat, 2021). Self-Sovereign Identity has emerged as a promising alternative, aiming to shift control over identity data back to individuals. SSI systems promise enhanced user control, portability of identity credentials, operational efficiency, and reduced costs (Mühle et al., 2018), thereby making them particularly attractive to public sector organization. Yet, despite increasing interest and substantial public investments, there remains a notable lack of empirical understanding of how public organizations can realize and actualize the organizational affordances of SSI. Most existing research focuses on technical aspects or individual-level benefits, overlooking the complex socio-technical dynamics and organizational-level requirements crucial to successful adoption. Specifically, little is known about how public sector organizations can effectively identify, experiment with, and actualize the affordances offered by SSI, navigating technical limitations, political considerations, cultural barriers, and stakeholder needs. Given these gaps, our research addresses two research questions:

(1) Which affordances does SSI offer within an organizational setting?

(2) How can the public sector experiment with and actualize SSI affordances?

We explore these questions using an exploratory, qualitative single-case study approach (Yin, 2014), focusing on a six-month SSI implementation project initiated by a German tax authority. This rich empirical context involved diverse stakeholders,

9 At the time of publishing this thesis, this essay is under review for publication in a scientific journal. Thus, I provide an extended abstract that covers the essay's content.

including government officials, researchers, and technology providers, allowing us to comprehensively examine how organizational actors perceive, experiment with, and actualize SSI affordances. Our data collection included semi-structured interviews with key stakeholders, extensive documentation, archival materials, observations, and technical artifacts, analyzed through a rigorous three-phase coding process following grounded theory principles.

Our study explicitly makes three theoretical and practical contributions: First, we extend existing SSI research by identifying and elaborating four distinct organizational-level affordances of SSI. In particular, we highlight how SSI not only enables secure verification of digital identities but also provides critical auditability and traceability features. Second, we contribute to affordance-experimentation-actualization theory (Du et al., 2019) by providing empirical insights into the iterative, interconnected processes through which public sector organizations navigate the complexities of SSI adoption. We demonstrate how experimentation with SSI affordances acts as a crucial mechanism, aligning technical capabilities with organizational, political, and cultural factors, thus facilitating successful actualization. Third, we contribute to the public sector innovation literature by introducing an affordance-based framework explicitly tailored to public organizations. This framework guides public institutions in systematically identifying and actualizing technology affordances in a manner sensitive to the public sector's unique organizational dynamics. In sum, our research bridges critical gaps by providing practical guidance for the effective adoption of SSI in public sector contexts, highlighting both theoretical advancements and tangible managerial implications.

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

References

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

Mühle, A., Grüner, A., Gayvoronskaya, T., & Meinel, C. (2018). A survey on essential components of a self-sovereign identity. *Computer Science Review*, *30*, 80–86. https://doi.org/10.1016/j.cosrev.2018.10.002

Reed, D., & Preukschat, A. (2021). *Self-Sovereign Identity: Decentralized Digital Identity and Verifiable Credentials* (1st edition). Manning Publications. https://learning.oreilly.com/library/view/-/9781617296598/?ar

Yin, R. K. (2014). *Case study research: Design and methods* (5. edition). SAGE.