UNIVERSITÄT
BAYREUTH

Digitally Sovereign Information Systems: Enabling Davids to Win Against Goliaths

Dissertation

zur Erlangung des Grades eines Doktors der Wirtschaftswissenschaft

der Rechts- und Wirtschaftswissenschaftlichen Fakultät

der Universität Bayreuth

Vorgelegt

von

Fabiane Marie Völter

aus

Esslingen am Neckar

Dekan:	Prof. Dr. Michael Grünberger
Erstberichterstatter:	Prof. Dr. Nils Urbach
Zweitberichterstatter:	Prof. Dr. Jens Strüker
Tag der mündlichen Prüfung:	10. Mai 2023

"There is an important lesson in all battles with giants. The powerful and the strong are not always what they seem."

(Malcom Gladwell, 2013)

Abstract

The digital transformation of both economies and personal lives carries various challenges, including adverse dependencies on digital platform providers, data privacy, and security. In an effort to address these concerns, digital sovereignty describes the triad of organisations, individuals, and societies being able to independently nurture their digital industries, self-determine the use of their data, and ensure the security of the latter. However, to date, the roles of information systems (ISs) as well as their management in striving for digital sovereignty have remained unclear. Thus, this dissertation aims to establish an understanding of digitally sovereign IS by following three research goals. First, I aim to shed light on the management of IS for digital sovereignty (RG1). Essay 1 addresses resource investments' effects on the machine learning lifecycle. Second, I seek to demonstrate the utilisation of IS for digital sovereignty (RG2). Essay 2 informs the design of a privacy-oriented IS that simultaneously allows for sensitive data exchange and the prevention of double-spending. Essay 3 evaluates the trustworthiness of technology aimed at providing digital sovereignty. Essays 4 and 5 address the application of the concept of self-sovereign identity in an organizational context. Specifically, Essay 4 observes the concept's affordances through the lens of affordance theory and Essay 5 investigates the concept's effect on agency costs. Essay 6 presents an investigation of the application of emerging technologies in practise. Lastly, I also address the aspect of security (RG3) as Essay 7 provides a research framework that analyses the current state of knowledge on the security concept of zero-trust. My dissertation contributes to an integrative understanding of digital sovereignty from an IS research perspective. I emphasise multiple angles of digital sovereignty by enabling the management as well as utilisation digital sovereign IS, addressing both the technical and the social subsystems including the interplays between them.

Keywords: Digital sovereignty, data privacy, data security, self-sovereign identity, blockchain technology, artificial intelligence.

Acknowledgements

Reflecting on the past three years of my time as a doctoral student, I wish to express my appreciation to all the persons who accompanied me during this journey.

First, my gratitude to my academic supervisor, Nils Urbach, for his advice and support in my research endeavours. I also thank Jens Strüker for being co-advisor on this dissertation. I acknowledge the support of the University of Bayreuth and Fraunhofer FIT in providing me with an environment to do my research. My gratitude to all the co-authors and colleagues with whom I undertook my research, for challenging my approaches and engaging in invaluable exchanges.

Second, I'm indebted to my friends, who have inspired and encouraged me not only throughout my academic journey, but long before. Lastly, I thank the members of my family, who have accompanied, supported, and believed in me from the start.

Bayreuth, March 2023

Fabiane Marie Völter

Contents

List of abbreviations

AI	Artificial intelligence
ANOVA	Analysis of variance
BYOD	Bring your own device
CSA	Computers-as-a-social actor
DLT	Distributed ledger technology
DSR	Design science research
EU	European Union
HCI	Human-Computer-Interaction
IoT	Internet of Things
IS(s)	Information system(s)
IT	Information technology
ML	Machine learning
PAT	Principal-agent theory
RBV	The resource-based view
RG(s)	Research goal(s)
RQ(s)	Research question(s)
SSI	Self-sovereign identity
U.S.	United States of America
VC(s)	Verifiable Credential(s)

Introduction to Digitally Sovereign Information Systems: Enabling Davids to Win Against Goliaths

Abstract

This thesis seeks to establish an understanding of digitally sovereign information systems (ISs), which encompasses both the management of IS to ensure digital sovereignty as well as the utilisation of IS for digital sovereignty. It contains seven essays, which are structured along three research goals. Accordingly, this thesis informs the IS management toward technological sovereignty as well as the utilisation of IS for data sovereignty and data security.

In the following introduction, I motivate the overall relevance of addressing digital sovereignty (Section 1), introduce and conceptualise digital sovereignty in light of IS research (Section 2), derive the three research goals (Section 3), present the seven essays' research methods (Section 4), summarise their results (Section 5), and conclude with a discussion of the essays' results, limitations, and an outlook on future research potentials (Section 6).

Keywords: Digital sovereignty, data privacy, data security, self-sovereign identity, blockchain technology, zero-trust, artificial intelligence.

Table of Contents – Introduction

1 Motivation

Both researchers and practitioners agree that the inability to access resources and markets can cause organisations to fail (Pfeffer and Salancik 1978; Tauscher and Kietzmann 2017; Sheppard 1995). This applies especially to resources for digital innovation and to digital markets, since a handful of players control these. For instance, Amazon's marketplace accounts for more than 50% of all e-commerce sales in the U.S. (Masters 2019). Various examples highlight that being cut off from their supreme access to customers can be an existential threat for retailers (Weise 2019). Furthermore, Amazon is also the dominant player in providing cloud computing services, claiming more than one-third of the global market share (Richter 2022). Similarly, Meta dominates the market for social networking services, accounting for 43% of global active users in January 2022 (Kemp 2023). Their large consumer bases allow them to collect vast amounts of data about their users' behaviours as well as metadata (Hermes et al. 2020a). Thus, a few dominant market players are controlling those resources and markets, which represent the foundation for the development of what is considered breakthrough technologies, such as diverse datasets (Jarke et al. 2019) and flexible computing infrastructure (Hermes et al. 2020a).

These observations point to several complications. First, the monopolistic control of critical resources and markets allows the few dominant market players to become gatekeepers for new market entries by constraining resources and, therefore, innovation capabilities (Clemons et al. 2022a). This applies specifically to the development of resource-intensive innovations, such as in the domain of machine learning (ML). For instance, ChatGPT was trained using vast amounts of data on a "supercomputer" developed by Microsoft exclusively for OpenAI (Langston 2020, p. 1). Also, the input data gathered from users serve to continually improve the model, which further fuel the development of superior technologies by dominant providers (Hermes et al. 2020a). Thus, organisations that do not offer inherently digital products and services, such as the hidden champions and family-owned businesses prevalent in Europe, are particularly vulnerable owing to their dependence on the service providers and, therefore, in the development of novel innovations (Jarke et al. 2019).

Second, the dominant platform providers' practices raise concerns about data privacy. Specifically, users cannot self-determinate what data are collected, what data are stored, and what purposes they are used for (Clemons et al. 2022a). Recent legislative changes in the U.S. (e.g., the CLOUD Act), which allows U.S. authorities to access data of U.S. companies even if these data are stored abroad, further highlight the uncertainty resulting from foreign data collection from a European perspective (Hermes et al. 2020b). These data privacy concerns apply not only to individual users but also to both private and public organisations pursuing the various services offered by large platform providers (Braun and Esswein 2012). Especially leakages and abuse of public organisations' data can have severe consequences, such as a political loss of control (Pickl 2019).

Data security represents the third concern regarding online platform dominance. Because large, siloed data collections by platform providers represent honey pots for attackers, the potential damage in case of a leak is massive (Lacity and Carmel 2022). Examples from the past raise concerns about the sufficient protection of the highly personal data collected, such as personal account information and payment data (Covert et al. 2020). For instance, among many others, Meta faced serious data leakages that left more than half a billion users' private data exposed (Bowman 2021). Security threats also affect organisations, since data loss can lead to reputational damages and business failures (Pickl 2019).

These challenges raise the question how both individuals and organisations can strive for a higher digital sovereignty level. The term digital sovereignty describes the ability of organisations, individuals, and societies to independently foster innovation in the absence of strategic dependencies on single providers or countries as well as the self-determined and secure administration of one's own data (Braud et al. 2021; Pickl 2019; Madiega 2020). Motivated by the need to create solutions for these challenges, this thesis seeks to help IS scholars and practitioners to understand and apply IS artefacts aimed at providing digital sovereignty as well as contextual factors relevant for achieving it. Accordingly, this thesis' overall research aim is:

To enable the management and utilisation of IS for digital sovereignty.

This overall aim guides the seven essays that address design- and management-oriented questions on digital sovereignty. In this way, I contribute to both my cumulative dissertation and the academic literature. Specifically, I seek to contribute

to the IS discourse by defining the meaning of the term digital sovereignty in light of IS research, informing choices regarding technological design and digital practises for achieving data privacy and security, and supporting organisations and politics in achieving digital sovereignty through the appropriate use of technology.

The remainder of this introduction to my thesis is structured as follows: First, I introduce the concept of digital sovereignty and conceptualise it in the context of IS research (Chapter 2). I then derive and motivate the three research goals and introduce the research questions (Chapter 3). Subsequently, I present the essays' research methods (Chapter 4) and results (Chapter 5). I conclude this introduction with a discussion of the results, limitations, and future research opportunities (Chapter 6). The seven essays follow after the introduction.

When referring to the essays, I use *we*, as they all involved joint work with co-authors. I have omitted the standard indications of these citations so as to improve the introduction's readability.

2 Background and conceptualisation

To provide a solid conceptual foundation for the remainder of this thesis, in the following I will define the concept digital sovereignty, introduce the notion of the IS artefact on which the essays rely, and conceptualise digital sovereignty in IS research.

2.1 Defining digital sovereignty

Originally coined as a term in political theory, *sovereignty* describes a supreme authority over a community that is based on some legitimacy, for instance, a constitution or hereditary law, and that applies to a specific territory, which may be a land mass, infrastructure, or airspace (Pohle and Thiel 2020).

The momentum to contextualise sovereignty to the digital world – i.e., to address *digital sovereignty* – is mainly driven by the observation that large platform providers' monopolistic tendencies hinder data ownership and control, create security risks, and prevent conditions of fair competition by creating strategic dependencies (Madiega 2020). Thus, digital sovereignty is considered a countermeasure against dependencies in the digital world (Couture and Toupin 2019). Policy actors understand digital sovereignty as the ability to defend liberal and democratic values as well as the accountability of sovereign power (Pohle and Thiel 2020). To base my thesis' results on a comprehensive conceptual foundation, I rely on the definition by Germany's government as well as political bodies of the European Union, who define digital sovereignty as the "ability and opportunity of individuals and organizations to perform their roles in the digital world in an independent, self-determined, and secure manner" (Goldacker 2017, p. 3; Madiega 2020, p. 1). While I acknowledge the term's original framing in politics, the latter definition allows to establish a reference to IS. In the following, I will introduce and describe each characteristic that the term digital sovereignty encompasses: independence, self-determination, and security.

First, independence refers to the capacity for technological innovation and, thus, the capacity to develop (digital) industries (Madiega 2020; Ramahandry et al. 2021). The first aspect of digital sovereignty is closely related to resource dependencies (Pfeffer and Salancik 1978). Specifically, it requires organisations to be independent regarding the sourcing of technology both concerning hardware (e.g., computing chips) and software (e.g., ML models). The independence aspect is also referred to as

technological sovereignty (Ramahandry et al. 2021). Current initiatives by the EU, such as the European Chips Act, which aims to increase the resilience of Europe's manufacturing industry by reducing the dependency on single providers, emphasise this goal (European Commission 2022). Also, current efforts around the development of a national cloud infrastructure, Gaia-X, seek to provide an alternative to computing infrastructure provided by U.S. corporations (Otto 2022).

Further, the latter initiative also targets the second aspect of digital sovereignty, self-determination, regarding the management and sharing of data, also referred to as *data sovereignty* (Braud et al. 2021). Data sovereignty affects both organisations and individuals. Regarding the former, data sovereignty describes the exchange of organisational data in ecosystems governed by negotiated and monitored data usage agreements (Jarke et al. 2019). Regarding the latter, data sovereignty refers to the self-determination of how one's personal data are used. The term data sovereignty relates closely to data privacy, which refers to an individual's ability to "personally control information about oneself" (Popovic et al. 2017, p. 1). Several emerging technologies such as blockchain as well as interaction paradigms, such as self-sovereign identities (SSI) promise to omit third parties in data management and data provisioning, and to allow for self-ownership of and control over personal data.

The third building block of digital sovereignty is *data security*, which refers to sovereignty over critical infrastructure (such as telecommunication networks) and resilience against cyber-attacks (Madiega 2020). Thus, the security of systems, networks, and data must be guaranteed (Ramahandry et al. 2021). As the definition of the term security in the context of digital sovereignty is broad (c.f. Ramahandry et al. 2021; Madiega 2020; Goldacker 2017), in this thesis, I will adapt a normative view on securing digital assets, following the general trend of IS research in information technology (IT) security (Hui et al. 2016).

In sum, the term digital sovereignty is multifaceted, but can be broken down into three core aspects: First, digital sovereignty refers to the capacity for technological innovation. As a result, technological innovation allows for the development of national (digital) industries. In turn, this allows respective organisations to locally (if not independently) source technologies (both software and hardware). Second, digital sovereignty requires that organisations and individuals be able to assert control over their own data. Third, besides privacy also security of data must be guaranteed.

2.2 IS research perspectives on digital sovereignty

To date, IS research has rarely touched on the concept of digital sovereignty. However, we can identify an association between digital sovereignty and research efforts in the IS literature concerning the momentum that is built on. For instance, Clemons et al. (2022b) recently called for investigating issues associated with social welfare computing. Unlike digital sovereignty, social welfare computing does not refer to the uses of technology for desirable outcomes (Clemons et al. 2022b); however, both concepts follow efforts that go beyond purely capitalist motives and seek to improve technology's contributions to society.

As IS research has not yet conceptualised its role in exploring digital sovereignty, I rely on Chatterjee et al.'s (2021) sociotechnical understanding of IS artefacts to identify relevant considerations of digital sovereignty from an IS research perspective (see Figure 1). While IS research offers a diverse discourse on the conceptualization of IS (c.f. Akhlaghpour et al. 2013; Orlikowski and Iacono 2001; Seidel et al. 2010), I follow Chatterjee et al.'s (2021) understanding as it allows to include both social, organisational, and societal aspects, which are relevant when considering digital sovereignty. In specific, Chatterjee et al. (2021) understand an IS artefact as a "superordinate system composed of social and technical subsystems" (p. 556). The subsystems are composed of individuals, structures, and their interrelationships (the social subsystem) as well as devices, tools, and techniques, which transform inputs into outputs (the technical subsystem). However, the subsystems are not enclosed elements but have open system boundaries, which allow for interactions with the surrounding environment as well as exchanges with further subsystems. Information shapes the latter interactions between the social and the technical subsystems and is also shaped by the ways of interaction between them. Information has a key role, since it promotes or inhibits a system's entropy, capturing the state and behaviour of the overall system.

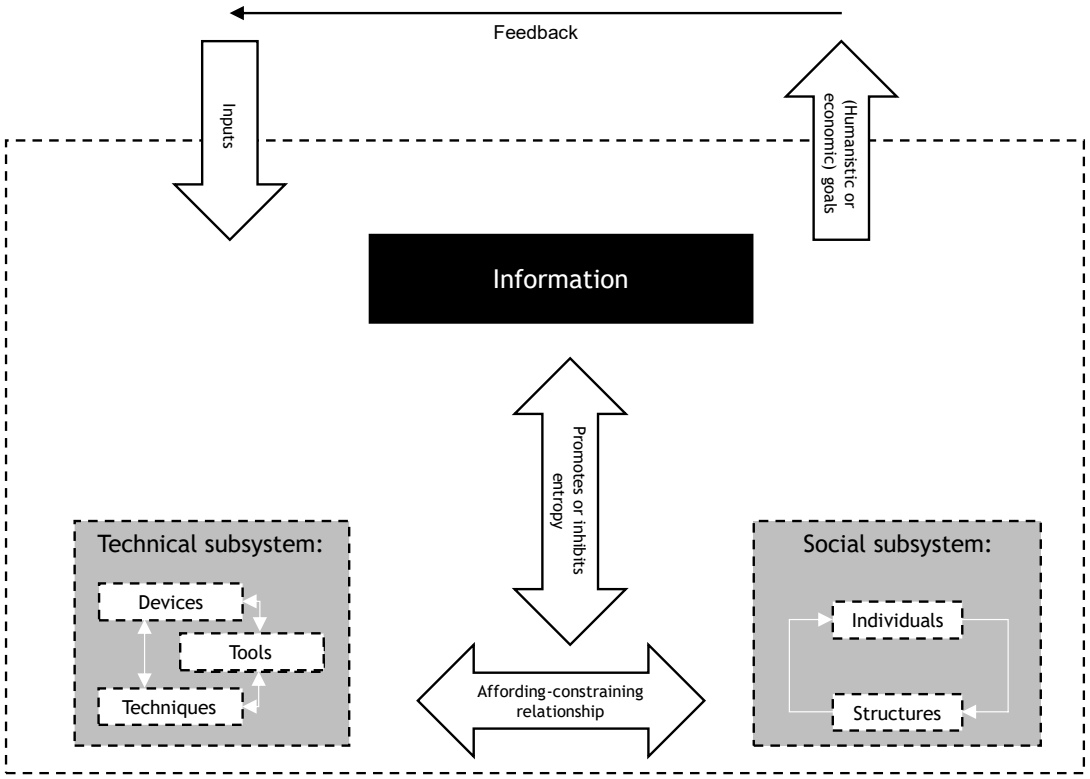

Figure 1. Information system following Chatterjee et al. (2021)

In the context of addressing digital sovereignty from an IS perspective, I identified related research streams that address both the social and the technical subsystems. On the one hand, several research streams that focus on the social subsystem such as management sciences provide insights into the effort of exploring digital sovereignty. Specifically, the management sciences offer much knowledge that can be relied on when addressing digital sovereignty issues. For instance, resource dependence theory has provided many insights into adverse dependencies between organisations (Barney 1991; Bharadwaj 2000; Das and Teng 2000; Grant 1991), which can also be transferred to digital services and products. In addition to management sciences, political sciences and legal studies also discuss digital sovereignty (Pohle and Thiel 2020). For instance, Trzaskowski (2022) shed light on regulation's role to limit monopolistic tendencies in two-sided digital markets.

On the other hand, the computer sciences, which address questions around the technical subsystem, have also contributed to our understanding of digital sovereignty. For instance, the discipline offers a broad range of research on security, aiming to ensure the confidentiality, integrity, and availability of information (Association for Computing Machinery 2023). Besides security methods, the computer sciences also provide systems and algorithms that contribute to privacy-preserving computations.

For instance, the discipline provides multiple conceptualisations and proposed methods, which allow the partial sharing of data called zero-knowledge proofs (Goldreich et al. 1991; Goldreich and Oren 1994; Goldwasser et al. 1985). Also, peer-to-peer networks and distributed systems, which lay the foundation for direct data exchange between peers without reliance on third-party providers, are a core topic in the computing sciences (Parameswaran et al. 2001; Fox 2001). Many of the above-mentioned proposed technical solutions (i.e., zero-trust solutions, distributed systems, zero-knowledge proofs) also touch on the same motives as the overall goal of achieving digital sovereignty: achieving data privacy and security as well as independence from third parties.

Thus, we can rely on related research streams that address the social and technical subsystems in isolation. However, when we observe the interplays between the social and the technical subsystems, which Chatterjee et al. (2021) consider a "fundamental issue" (p. 561) against the backdrop of digital sovereignty, we can draw on very little related work. Specifically, the IS literature has not offered a conceptualisation of digital sovereignty nor a positioning regarding its role in exploring digital sovereignty. However, IS research should significantly contribute to understanding digital sovereignty: solely observing either the technical or the social subsystem is not sufficient for achieving digital sovereignty – the interplays between them must be addressed if one is to grasp technological designs' implications on individuals, organisations, and society. Specifically, following Chatterjee et al.'s (2021) conceptualisation, we must observe IS from three perspectives if we are to establish a comprehensive understanding of digital sovereignty: First, efforts to achieve technological sovereignty (i.e., the ability to independently drive innovation) require that we understand the impacts of environmental constraints on the IS's input and their cascading effects within the sociotechnical system. Second, aiming for data sovereignty (i.e., data control and ownership, data privacy), we must understand how the technical subsystem impacts on information and therefore the relationships between information and the social subsystems. Specifically, we must grasp a technical subsystem's role in changing the data control and ownership within single or multiple social subsystems. Third, IT security for digital sovereignty requires that one comprehends how sociotechnical systems' boundaries can be protected.

I understand technological and data sovereignty as first-order objectives, since they form the core of digital sovereignty, and consider security as a second-order objective, since a lack of security renders the boundaries of and the interplays between the subsystems obsolete. The above conceptualisation of digital sovereignty in the context of IS research following Chatterjee et al. (2021) will serve as a basis for the remainder of this thesis.

3 Derivation of research questions

On the basis of my overall research aim – to understand the management and utilisation of IS for digital sovereignty – I derive my research goals (RG) along the three core elements of digital sovereignty: independence, self-determination, and IT security.

(RG1) *Understanding the management of IS for technological sovereignty.*
(RG2) *Understanding the utilisation of IS for data sovereignty.*
(RG3) *Understanding the utilisation of IS for IT security.*

I will now describe the research gaps and research questions for each essay, following the three RGs.

3.1 Understanding the management of IS for technological sovereignty

First, digital sovereignty requires the ability to independently foster innovation. As the inputs of an IS define its outputs (Chatterjee et al. 2021), innovation strongly depends on the ability to access all relevant resources that enable it. However, resources for developing and applying technologies that drive innovation vary in their strategic value (Bharadwaj 2000): while some resources can be bought externally without growing strategic dependencies, others cannot. This observation applies especially in the context of developing ML applications. For instance, access to scalable computing infrastructure is crucial (Bhattacharjee et al. 2017; Hazelwood et al. 2018) and requires significant investments (Baier and Seebacher 2019). At the same time, other resources are not as critical to the execution of the ML lifecycle, since they can be substituted or neglected, such as data-splitting tools. Thus, strategic decisions regarding an organisation's resource configuration require awareness of the resources' effects on the ML lifecycle. Further, being unaware of the latter also allows us to oversee critical monopolisation tendencies among providers, which can limit fair access to ML. A lack of awareness of resource dependencies regarding the ML lifecycle can negatively impact on an organisation's ability to independently drive innovations and, therefore, technological sovereignty. Thus, we ask:

How do resource investments impact the ML lifecycle?

3.2 Understanding the utilization of IS for data sovereignty

Whilst RG1 addresses the management of ML resources, the second pillar of digital sovereignty calls for investigating how technology can be utilised to enable digital sovereignty. Specifically, the latter calls for digital sovereignty regarding data sovereignty, which refers to the self-determined use of data and the ability of organisations, individuals, and societies to own and autonomously control the sharing of their data in negotiated terms (Jarke et al. 2019).

There are various technologies and concepts for improved data ownership and sharing. For instance, blockchain technology[1] was originally developed to perform value transactions between two parties without a reliance on a trusted intermediary[2] (Nakamoto 2008; Glaser 2017). While the technology's potential to reduce the dependency on third parties by preventing double-spending and establishing a single source of truth is widely acknowledged (Butijn et al. 2020; Rossi et al. 2019), its inability to delete entries makes it unfit for the exchange of sensitive data (Schellinger et al. 2022). In the following years, an alternative approach emerged: The concept of SSI allows for the self-determined exchange of sensitive data (Mühle et al. 2018), but at the same time does not prevent the double-spending of tokens. Thus, we can rely on technological concepts to prevent either double-spending or allow for the exchange of sensitive data.

However, to date, there is very little research into how to utilise both concepts to achieve the seemingly contradictory requirements of the prevention of double-spending and the exchange of sensitive data. This observation also holds true in the context of e-prescriptions. To date, the research has mainly focused on decentralised solutions, which neglect privacy-related challenges.

We respond to Chatterjee et al.'s (2021) call to gain an understanding of the technical subsystem. Thus, to improve our understanding of how blockchain technology and the SSI concept can be levered to achieve data sovereignty while preventing double-spending, in Essay 2, we ask:

[1] For simplicity, I use the term blockchain technology to refer to all types of distributed ledger technologies in the introduction of this dissertation.

[2] For a comprehensive explanation of the technologies, please see the individual essays.

How to design and implement a decentralised system for e-prescription management using blockchain technology and digital wallets?

While Essay 2 focuses on the technical design and implementation, we acknowledge the importance of its interactions with the social subsystem (Chatterjee et al. 2021). Thus, IS supporting the achievement of data sovereignty is of no use if the IS does not fulfil users' technology acceptance requirements. Specifically, past research has demonstrated that trust is a behavioural antecedent of the willingness to use technology (Gefen et al. 2003; Söllner et al. 2016). While we can build on much research on trust between people and technology (Söllner et al. 2016), we need to contextualise the latter in the technology under scrutiny, particularly concerning emerging technologies (Guggenberger et al. 2023). Specifically, we focus on trust as a crucial factor for acceptance, as blockchain technology is widely acknowledged to cause a shift from trust in intermediaries to trust in the technology itself (Ostern 2018). Thus, to inform the design of trustworthy technology for data sovereignty, we ask:

To what extent are established IS trust signals also effective in enhancing a user's trust level in blockchain applications?

After Essays 2 and 3 inform us about the design and implementation of the technology and concepts, we follow Chatterjee et al. (2021) in further investigating the interplays with the technical subsystem's organisational environment. Specifically, the technical subsystem delivers features and techniques that impact on the interaction with information. These features and techniques can be actualised by the social subsystem in a certain way. The latter instantiation is characterised by a relationship between affordance and experimentation: The technology provides affordances, which can be experimented with and actualised by the social subsystem (Du et al. 2019; Strong et al. 2014). Thus, to improve our understanding of organisations adopting SSI, we must understand the interactions between the technological system, its provided information, and the social context. Hence, we aim to observe how the affordances of an SSI-based system are experimented with and actualised. Thus, in Essay 4, we ask:

What are the affordances of SSI in an organisational ecosystem? How does the public sector experiment with and actualise these affordances?

For a holistic understanding of IS's role in enabling data sovereignty, we must understand not only the technical subsystem as well as its interplays with the social subsystem, but also information's role. This applies specifically to SSI-based systems,

since it shifts data ownership and control back to the end-user while ensuring the data's verifiability (Mühle et al. 2018). By impacting on the ownership, accessibility, and verifiability of information, it may also affect the relationships between information and one or multiple social subsystems. We chose to investigate this using the example of supplier information management, since buyer-seller relationships are characterised by high information asymmetry, which in turn, cause adverse selection (Pavlou et al. 2007; Bergen et al. 1992). Hence, we expect that an IS impacting on the ownership, accessibility, and verifiability of data impacts on the social subsystem, specifically, the relationship between buyers and suppliers. Thus, we ask:

How does self-sovereign identity affect adverse selection within buyer-supplier relationship management?

After having understood the inner workings of the IS, we must also understand how to utilise technologies in practise, specifically in light of the fact that to date, we can see only limited practical applications of technologies such as artificial intelligence (AI), internet of things (IoT) or distributed ledgers (DLT) for digital sovereignty. This applies not only to using technologies in isolation but also to their combined use. However, particularly in extraordinary circumstances such as pandemics, the thoughtful use of technologies is expected to support the response and management of crises, and, thus, be of value for individuals, organisations, and societies. Hence, we ask:

What role do IoT, AI, and DLT and their convergence play in combatting the COVID-19 pandemic or future crises?

Which resulting implications for research, practise, and policy can be identified?

3.3 Understanding the utilisation of IS for IT security

IT security represents the third pillar for achieving digital sovereignty: individuals, organisations, and societies must not only be able to independently foster innovative capacities and utilise IS for increasing data privacy but must also be able to ensure the latter information's confidentiality, integrity, and availability. Thus, we must understand how to protect an IS's permeable boundaries.

This is crucial, because the number of data breaches and hacking attacks have elevated in the past few years (DeCusatis et al. 2016; Moubayed et al. 2019; Shlapentokh-

Rothman et al. 2020). The increasing connectivity of devices driven by digitalisation generally but also recent trends such as the IoT and bring your own device (BYOD) more specifically, have led to a growth in both the size and the complexity of existing networks (Compastie et al. 2016; Moubayed et al. 2019). Accordingly, this trend represents a challenge for existing security solutions, which differentiate solely between internal and external devices: a single unsecured device poses a threat to the entire network (Chen et al. 2019; Mcginthy and Michaels 2019). Thus, to understand the protection of an IS's boundaries, we must turn to alternative, more promising solutions. For instance, the zero-trust paradigm is gaining interest from researchers and practitioners in their efforts to better secure organisational resources (Mehraj and Banday 2020; Zaheer et al. 2019). In contrast to existing IT security solutions distinguishing between trusted and untrusted devices, the core idea of zero-trust is that any request by any device must be evaluated and approved (DeCusatis et al. 2016; Moubayed et al. 2019). Nonetheless, to date, the research on the zero-trust concept has focused mainly on the technical subsystem, neglecting a sociotechnical perspective on the concept. To gain a holistic understanding of the zero-trust concept and, thus, determine its role in achieving digital sovereignty, we ask:

What is the current state of the knowledge about zero-trust, and what are avenues for future research?

An overview of the essays, their publication outlets, and their publication appears in Table 1.

Table 1. The seven essays and how they address the three research goals of this thesis

Title	Research questions	Publication outlet	VHB JQ3/ Scopus	Publication status
RG1: Understanding the management of IS for digital sovereignty.				
Essay 1: The impact of resource investments on the machine learning lifecycle: Bridging the gap between software engineering and management	How do resource investments impact the ML lifecycle?	Business Information Systems Engineering	B / 88% percentile	Under review (2nd round)
RG2: Understanding the utilisation of IS for data sovereignty.				
Essay 2: Harmonizing sensitive data exchange and double-spending prevention through blockchain and digital wallets: The case of e-prescription management	How to design and implement a decentralised system for e-prescription management using blockchain technology and digital wallets?	ACM Distributed Ledger Technologies: Research and Practice	n.a.	Published
Essay 3: Trusting the trust machine: Developing and evaluating trust signals of blockchain applications	To what extent are established IS trust signals also effective in enhancing a user's trust level in blockchain applications?	International Journal of Information Management	C/ 99% percentile	Published
Essay 4: Affordances, experimentation, and actualization of self-sovereign identity: A case study of the implementation and use of SSI	What are the affordances of SSI in an organisational ecosystem? How does the public sector experiment with and actualize these affordances?	Information & Organisation	B / 98% percentile	Under review
Essay 5: Know your supplier: A principal-agent perspective on self-sovereign identities in supplier management	How does Self-Sovereign Identity affect adverse selection within buyer-supplier relationship management?	Scientific journal	A / 86% percentile	In preparation for submission
Essay 6: Emerging digital technologies to combat future crises: Reviewing COVID-19 to be prepared for the future	What role do IoT, AI, and DLT and their convergence play in combatting the COVID-19 pandemic or future crises? Which resulting implications for research, practise, and policy can be identified?	International Journal of Innovation and Technology Management	C/ 48% percentile	Published
RG3: Understanding the utilisation of IS for IT security.				
Essay 7: Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust	What is the current state of the knowledge about zero-trust, and what are avenues for future research?	Computers & Security	n.a. / 99% percentile	Published

4 Research designs

I will now outline the essays' research methods. A summary of the research designs can be found in Table 2.

Table 2. Research methods of the seven essays

Title	Research designs
RG1: Understanding the management of IS for digital sovereignty.	
Essay 1: The impact of resource investments on the machine learning lifecycle: Bridging the gap between software engineering and management	**Design science research:** • Iterative development of a framework for resources and their effects • Systematic literature review to collect justificatory knowledge and to draft an initial framework • Expert interview study to refine and evaluate the framework
RG2: Understanding the utilisation of IS for data sovereignty.	
Essay 2: Harmonizing sensitive data exchange and double-spending prevention through blockchain and digital wallets: The case of e-prescription management	**Design science research:** • Problem identification in practise; literature analysis for the identification of solution objectives • Design of an architecture and the implementation of the prototype • Quantitative and qualitative evaluation, including security analysis
Essay 3: Trusting the trust machine: Developing and evaluating trust signals of blockchain applications	**Laboratory experimental study:** • Quantitative analysis to empirically validate trustworthiness • Between-groups experiment with four groups including three manipulations
Essay 4: Affordances, experimentation, and actualization of self-sovereign identity: A case study of the implementation and use of SSI	**Case study research:** • Triangulation of five data sources, including ten interviews with experts; open, axial, and selective coding of data • Deriving an understanding of the interrelationships between the technical and the social subsystems
Essay 5: Know your supplier: A principal-agent perspective on self-sovereign identities in supplier management	**Interview study:** • Interview study to derive the causal relationships between SSI, information-sharing, and agency costs through the lens of PAT • Derivation of a theoretical framework that highlights SSI's impacts on information-sharing and, therefore, agency costs
Essay 6: Emerging digital technologies to combat future crises: Reviewing COVID-19 to be prepared for the future	**Research commentary:** • Identification of the most effective means of leveraging technologies' potentials as well as derivation of implications for researchers, practitioners, and policy-makers
RG_3: Understanding the utilisation of IS for IT security.	
Essay 7: Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust	**Multivocal literature review:** • Analysis of the current state of research into zero-trust using the academic and the grey literature • Derivation of a research agenda for the further development of the field

Essays 1 and 2 follow the design science research (DSR) paradigm. We chose the DSR paradigm for Essay 1, since we aim to develop a framework for decision-makers that incorporates insights from both the literature and practitioners' expertise. The chosen DSR paradigm allows us to iteratively incorporate both knowledge streams in the rigorous design and evaluation of an artefact to solve relevant real-world problems (Hevner 2007). We follow the six stages of a DSR process (problem identification, objectives, design and development, demonstration, evaluation, and communication), as proposed by Peffers et al. (2007), and execute five design iterations: First, we conceptualised the problem space, including defining the relevant stakeholders, their needs, the research goal, and the to-be-fulfilled design requirements (Maedche et al. 2019). Second, we started the design and development phase by collecting justificatory knowledge through a literature review. The literature analysis' results – a set of identified resources – informed the initial framework draft during design iteration 1. During iteration 2, we structured the identified resources along the ML lifecycle as proposed by Amershi et al. (2019). To access new knowledge and to evaluate our framework, we conducted 12 interviews with experts over three iterations. We relied on the evaluation criteria for models by Sonnenberg and Vom Brocke (2012). The interview study's results informed the further development of our framework in iterations 3 to 5. As a result of the DSR process, we proposed an ML Effect Framework and introduced five effect classes, which clarify ML resource investments' impacts on the ML lifecycle.

In parallel to addressing the research gap outlined in Essay 1, we also aim to solve a real-world problem while also contributing to the theory in Essay 2. Specifically, we followed Peffers et al.'s (2007) six DSR research steps to investigate privacy-preserving data exchange while preventing double-spending. After defining a research problem that is of practical relevance, we conducted a literature review following Kitchenham and Charters (2007), which informed eight design objectives for the solution. On this basis, we developed a system architecture and implemented a prototype built on digital wallets and blockchain technology. We evaluated the artefact in a quantitative as well as a qualitative way along the defined evaluation criteria, which are based on the design objectives. Lastly, besides developing, implementing, and evaluating a system, we

generalised our knowledge by providing design principles that guide the design and development of IS artefacts with similar requirements.

Essay 3 follows a quantitative research approach for an empirical analysis of trust signals' effectiveness. The chosen between-groups experiment allowed us to determine the relationships between subjects and variables by manipulating the latter (Palvia et al. 2004). Our research approach following Lazar et al. (2017) has five stages. First, we examined the literature to inform the conceptual development of signals for trustworthiness. We identified familiarity, transparency, and past credible commitment as relevant trust signals, leading to four conditions, including one control group. Second, we drafted the experimental design and selected an appropriate sample group. Informed by similar experiments (c.f. Verberne et al. 2012), we chose a between-groups experiment and recruited 20 participants per condition. We built four prototypes, which each displayed varying or no trust signals. Third, after pre-testing, we conducted the experiment. After a short briefing on the scenario, which follows Weber et al. (2016), the participants interacted with the developed prototypes. Fourth, after the experiment, we measured the participants' trust in the system using a questionnaire proposed by Jian et al. (2000). To enhance our results' insightfulness, we also conducted semi-structured interviews with 12 participants. Lastly, we analysed the data, which revealed a significant difference between the trust levels in dependence of the respective condition.

In Essay 4 we conducted a holistic single-case study following the recommendations of Eisenhardt (1989) and Eisenhardt and Graebner (2007) to understand the actualisation and utilisation of the novel phenomenon of SSI through the lens of affordance theory (Gibson 1979; Markus and Silver 2008). We chose this research approach to collect rich qualitative evidence (Eisenhardt 1989; Yin 2014). Specifically, case study research established a detailed understanding of the interactions between the social and the technical subsystems within a natural setting (Benbasat et al. 1987; Klein and Myers 1999), which is why we considered it appropriate for our research objective. For conducting our study, we chose an applied research project, which aims to improve a tax verification process with the help of SSI-based tax registration certificates. We followed Yin's (2014) recommendations for data collection and tapped multiple data sources. Specifically, we conducted an interview study with all ten individuals involved in the research project, relying on researcher notes from formal

and informal meetings, project documentation (i.e., contractual agreements, project reports, protocols, and presentations), archival records about paper-based tax certificates and the technical artefact itself, including its technical documentation. We coded all data in three stages, involving open coding, axial coding, and selective coding (Corbin and Strauss 2014). The data analysis allowed us to provide insights into the affordances as well as the observed organisations' experimentation and the actualisation of the latter. In line with our sociotechnical conception of IS, we could derive an understanding of the interdependencies between the SSI system and the actors.

In parallel to Essay 4's research aim, we also investigated the relationship between the social context and the technological artefact in Essay 5. As we seek to capture the contextual complexity of the relationship, we chose a qualitative research approach, which allows for an in-depth observation. Specifically, we conducted an interview study following Myers and Newman (2007) to investigate the causalities between the application of SSI-based IS, information-sharing, and agency costs. We iteratively collected and analysed our data. Thus, we refined both the interview guide as well as our expert sampling definition after the first open coding. During each coding phase (open, axial, selective coding), the research team conducted joint coding workshops to increase the results' reliability (Lombard et al. 2002) and internal validity (Marton 2013). Resulting from the data analysis, we present a theoretical framework that demonstrates the causal relationships between the SSI-based IS, information-sharing, and agency costs.

In Essay 6, we analyse the potential of the IoT, AI, and DLT to tackle pandemic-related challenges of organisations, individuals, and society. Essay 6 is a research commentary, whose results rely on the authors' experience with the extant literature and their insights into the industry. However, we do not follow a single methodological approach.

Lastly, Essay 7 also relies on a qualitative empirical research approach. We sought to provide a comprehensive overview of and derive a research agenda for a novel phenomenon. As we wanted to include the most recent state of knowledge, we may rely not only on academic insights, since the peer-reviewed literature involves a more diligent and therefore lengthy publication process compared to the practitioner literature. Thus, we decided to conduct a multivocal literature review following Garousi

et al.'s (2019) guidelines, which allowed us to include findings from the practitioner literature in a rigorous way. The research process had three stages: First, during planning, we defined the literature analysis' scope and derived the corresponding research question. For deriving the research questions, we adopted the framework introduced by Risius and Spohrer (2017). Second, we gathered the literature: According to Kitchenham and Charters (2007), we collected the academic literature by searching through respective databases. For the grey literature, we conducted a web search (Garousi et al. 2019). Our initial search for the academic and the grey literatures yielded 1,318 and 184 items, respectively. After applying pre-defined exclusion and inclusion criteria as well as snowballing, our final literature set had 66 items. Third, we reviewed the identified items along our defined research framework. As a result, we were able to both draw a comprehensive, multifaceted picture of the literature and to systematically derive a research agenda that highlights avenues for future research that would enhance the research field.

In sum, this dissertation primarily relies on a pragmatist position (Goldkuhl 2012). Specifically, the research objectives, which are mainly motivated by observations from practice, reflect the ontological and epistemological assumptions of a pragmatist position (Goldkuhl 2012).

5 Summarising the results

I will now summarise the essays' results, which inform the management of IS to ensure digital sovereignty and the utilisation of IS for achieving digital sovereignty.

5.1 Essay 1: The impact of resource investments on the machine learning lifecycle: Bridging the gap between software engineering and management

In Essay 1, we provide a framework that will support decision-makers in their understanding of resource requirements and their impacts on the ML lifecycle. Specifically, the framework integrates resources relevant for the development of ML applications with the process and technical dependencies within the ML lifecycle. Building on the resource-based view (RBV) (Bharadwaj 2000), the framework arranges 30 primary and secondary resources along the three stages of the ML lifecycle: data management, model learning and verification, and model deployment. We identified direct effect classes, which connect primary resources along the ML lifecycle and secondary effect classes, which moderate the ML lifecycle's ability to generate output based on the given input.

We contribute to the literature and to practise in three ways: 1) Building on the software engineering perspective and on the management discourse, we are able to extend the list of relevant resources previously discussed in the context of big data analytics or AI (c.f. Mikalef and Gupta 2021; Gupta and George 2016; Weber et al. 2022). 2) We theorise on resources' effects, which allows us to understand the implications of resource allocation, bundling, and scaling. 3) In practise, our framework reduces the risk of inefficient resource investments by guiding the assessments of organisational readiness and maturity for developing and deploying ML applications.

5.2 Essay 2: Harmonizing sensitive data exchange and double-spending prevention through blockchain and digital wallets: The case of e-prescription management

In Essay 2, we explore how a single architecture can achieve both sensitive data exchange and can prevent double-spending. To address this challenge, we develop and implement a system that relies on the one hand on digital wallets for bilateral data

exchange and on the other hand on blockchain technology to prevent double-spending. Based on design requirements derived from the literature, we evaluated the system and conducted a security analysis. The qualitative analysis found that our proposed system can fulfil the requirements of disclosure control, the prevention of double-spending, verifiability, decentralisation, pharmacy independence, key management, and interoperability. Furthermore, a performance analysis with the distributed ledger performance scan (Sedlmeir et al. 2021) showed that our system provides sufficient scalability and performance for hundreds of millions of users. Building on our knowledge, we formulated design principles for more generalised learnings: First, verifiable credentials (VCs) stored in a digital wallet should be used to provide sensitive and verifiable user information. Second, vouchers can be implemented by creating a token and including its spending secret in the digital certificate. This is beneficial for usability and ease of implementation, since users do not require a mobile app beyond their digital wallet. Third, an ecosystem, in which VCs can be combined and used repeatedly in different contexts, is beneficial for users.

We contribute to the theory and practise in multiple ways: 1) We present generalisable knowledge on how sensitive data exchange can be guaranteed while also preventing double-spending. We extend both the literature and support practitioners in developing systems with similar design requirements. 2) We offer insights into the remaining challenges regarding the development of decentralised systems that combine sensitive data and business logic involving multiple stakeholders.

5.3 Essay 3: Trusting the trust machine: Developing and evaluating trust signals of blockchain applications

In Essay 3, we empirically evaluate the effectiveness of established IS trust formation factors in the context of blockchain technology. Our empirical evaluation of trust signals provides three results: 1) We found that the association with a familiar organisation does not impact on users' level of trust in blockchain technology. Thus, institutional trust is of little relevance. 2) While complexity negatively influences user trust in blockchain-based solutions, transparency and comprehensibility increase trust

in blockchain-based systems. 3) Displaying previous and concurrent transactions of other users increases perceptions of trust, reliability, and integrity.

Regarding theoretical lenses' applicability, we found that, compared to the "computer-as-a-social action" (CSA) paradigm (Benbasat and Wang 2005; Lankton et al. 2015), the approach stemming from Human-Computer Interaction (HCI) research (Söllner et al. 2012a; Söllner et al. 2012b) better describes trust in blockchain technology. Furthermore, our results show similarities to findings of trust in user-facing technologies. Thus, we highlight that investigating user-related aspects of blockchain technology is highly relevant, although it represents a non-user-facing technology (Ostern 2018).

We contribute to the blockchain management discourse by empirically evaluating trust signals, highlighting that not all insights from IS research on trust in IT artifacts apply to blockchain technology. We support practitioners in the design of trustworthy technology that emphasises and levers the underlying trust-stimulating characteristics of the technology.

5.4 Essay 4: Affordances, experimentation, and actualization of self-sovereign identity: A case study of the implementation and use of SSI

In Essay 4, we analysed the experimentation and actualization of the action possibilities of SSI in an organizational context to recognise its various affordances provided by SSI. Specifically, we found that 1) organisations can issue signed identity documents. Additionally, an identity holder can 2) verifiably present their identity independent from the identity provider and 3) selectively combine properties from certificates issued by different issuers. Furthermore, 4) verifiers can prove that they have received a verifiable presentation. The experimentation phase demonstrated that SSI can be used as a general-purpose tool for issuing and providing evidence. In addition, SSI ecosystems allows to take on flexible roles, allowing public organisations to become both issuer and verifier of certified information. Furthermore, we demonstrate that if both natural and legal entities benefit from SSI-based applications, the latter's scope can be further increased. At the same time, our case study also

highlights that regulatory challenges are still apparent when it comes to applying SSI in practise, specifically in the context of public organisations.

We contribute a better understanding of SSI's value and how organisations can approach its benefits. Further, we were able to validate the theoretical lens of affordance-experimentation-actualisation theory as proposed by Du et al. (2019), specifically regarding the existence of an experimentation phase.

5.5 Essay 5: Know your supplier: A principal-agent perspective on self-sovereign identities in supplier management

In Essay 5, we conduct an interview study to investigate the causal effects between the utilization of SSI and adverse selection in buyer-supplier relationships. We provide a research framework including five propositions demonstrating how the SSI affects adverse selection. In specific, we show how an SSI ecosystem, specifically the SSI infrastructure and trust service providers, provide signalling capabilities by enabling the communication of attested attributes and ensuring their credibility. Thus, in turn, buyers are able to assess potential partners and reduce their risk of selecting dishonest suppliers. As a result, SSI has a negative effect on adverse selection. Our findings highlight that technology itself is not sufficient to create credible information, but that some institution must also provide trust.

Our findings align with previous research on the usage of IT for the reduction of information asymmetries and the risk of adverse selection. By providing a comprehensive understating of the mechanisms by which ISs can reduce adverse selection, we contribute both to the theoretical body of knowledge on principal-agent theory (PAT) as well as on SSI.

5.6 Essay 6: Emerging digital technologies to combat future crises: Reviewing COVID-19 to be prepared for the future

In Essay 6, we investigate the role of emerging technologies, specifically IoT, AI, and DLT, and their convergence in addressing challenges related to the COVID-19 pandemic. In our commentary, we provide an overview of the potential that arises from the technologies' thoughtful use. Besides addressing the technologies' potentials in isolation as well as in combination, we also derive implications for research, practice, and policy makers. While I refer to the essay for a detailed discussion of all

propositions, I would like to emphasise two recommendations, which are specifically relevant in the context of digital sovereignty. First, we encourage to lever IoT for data creation. As data continues to be a scarce resource for AI developments, IoT could ensure the growth of a data basis, specifically in the context of extraordinary situations. At the same time, we emphasize the role of data privacy when collecting individuals' data on a large scale through IoT. Second, we also highlight that the utilization of DLT can benefit from SSI by ensuring a secure and privacy-preserving identity layer.

In sum, we contribute to the theory on the convergence of emerging digital technologies to enable their utilization to support individuals, organisations, and society in overcoming extraordinary circumstances.

5.7 Essay 7: Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust

In Essay 7, we develop a research framework for the zero-trust research area to structure the existing literature and identify future research avenues. Our findings reveal that the zero-trust paradigm has recently drawn much interest from both academia and practise. Regarding the research topics in focus, academics and practitioners have focused on the conceptual and technical aspects of zero-trust. While a limited number of practitioner studies have addressed implementation strategies, we also currently lack academic research into zero-trust through the lens of sociotechnical IS: specifically, we lack analyses of organisational as well as end-user-related aspects of the concept. Furthermore, the literature has focused on the paradigm's benefits and therefore provides a fairly one-sided view of zero-trust. Building on our analysis, we present exemplary research questions that may serve as an initial starting point for future research.

We contribute to the literature by 1) providing a multi-perspective overview of the current state of the knowledge on zero-trust and presenting a research framework that structures the research area. 2) We contribute to the research field by suggesting future research avenues that can enhance the field's maturity. 3) We support practitioners by providing a conceptual summary and consolidation. Thus, we enable the application of insights from the academic discourse in practise.

6 Discussion and conclusion

In the following, I will summarise this thesis' contents and aim in Section 6.1, discuss its contributions to theory and implications for practise (Section 6.2), outline its limitations (Section 6.3), and conclude by presenting future research opportunities (Section 6.4).

6.1 Summary

Chatterjee et al.'s (2021) sociotechnical understanding of IS has shaped this thesis, since each essay emphasises a specific element of the superordinate system.

First, we address the interactions of the IS with its environment and environmental constraints on inputs in Essay 1 by investigating resource investments' effects on the ML lifecycle. We emphasise the ability of single resources to affect the entire ML lifecycle and therefore their contributions to the overall synergy of the superordinate system (Chatterjee et al. 2021). Further, resource investments' effects, as investigated in Essay 1, demonstrate sociotechnical systems' multifinality and equifinality: we show that investments in single resources can have multiple effects on the ML lifecycle (e.g., the iterating and reusability effect of production data), reflecting the effects' multifinality. However, these effects may materialise over time, as for instance investments in flexible infrastructure may affect both the outcome of the ML lifecycle as well as future ML endeavours (equifinality).

Second, we observe the technical subsystem and its interactions with the social subsystem as well as its impacts on the relationship between the social subsystem and information. Specifically, Essays 2 and 3 inform the design of the technical subsystem. While in Essay 2 we focus on the development of a decentralised, privacy-oriented IS for the exchange of sensitive information, in Essay 3 we follow a behavioural approach for the evaluation of trust cues of blockchain technology to inform the design of trustworthy IS. Furthermore, as Chatterjee et al. (2021) highlighted, an affording-constraining relationship characterises the interactions between an IS's subsystems. We observe this relationship in more detail in Essay 3 and apply the lens of affordances to SSI-based IS in the context of the public sector. Information also has a key role in ISs, since it both shapes the interaction between the technical and the social subsystems, and is also shaped by the interactions between subsystems (Chatterjee et

al. 2021). In Essay 5, we apply PAT to observe how the use of an underlying technical subsystem impacts on information's role in social subsystems. Specifically, we highlighted how an SSI-based system affects the principal-agent relationship between supplier and customer through verifiable information. As a final contribution to RG2, in Essay 6 we derive recommendations for the use of emerging digital technologies to address pandemic-related challenges for organisations, individuals, and society.

Third, Essay 7 observes the entire superordinate system. The underlying research framework based on Risius and Spohrer (2017) allowed us to derive future research potentials on several levels of analysis, including technical, organisational, and social aspects of zero-trust applications.

6.2 Contributions to theory and implications for practise

This dissertation provides a conceptualisation of digital sovereignty from an IS research perspective and emphasises multiple angles to explore the digital sovereignty concept. I will structure the contributions of this dissertation's essays along the three research goals[3].

Addressing RG1, Essay 1 contributes to the identification of dependencies regarding resources relevant for the development of ML applications. Thus, I emphasise that environmental constraints on inputs of IS can threaten digital sovereignty.

Regarding RG2, Essays 2, 3, 4, 5 and 6 contribute to our theoretical understanding of how ISs can be utilized for digital sovereignty while observing both the technical and social subsystem as well as its interplays and information's role. Specifically, the essays that address RG2 make two primary contributions: On the one hand, Essays 2 and 3 inform the design of ISs designed for providing digital sovereignty. Specifically, Essay 2 theorises on the design of a technical subsystem that prevents double-spending while keeping transactions private, thereby also maximising users' privacy. This theoretical knowledge guides the design of systems that face similar challenges. Essay 3 contributes to the theoretical understanding of user-related aspects of technology for digital sovereignty, informing the design for trustworthiness of various ISs. On the other hand, the essays that address RG2 emphasise how changes to the

[3] Detailed descriptions of the essays' contributions to theory and implications for practice appear in the essays' discussion or conclusion sections.

technical subsystem (i.e., shifting to SSI-based systems) can impact on the relationship between social subsystems through a change in data access and the locus of data control. In particular, Essays 4 and 5 highlight that changing data access and control through the technical subsystem supports data sovereignty and thus digital sovereignty. Essay 6 contributes to our understanding of digital sovereignty by emphasizing how emerging digital technologies can be utilized for e.g., generating resources and providing data privacy in practise.

Concerning RG3, Essay 7 advances the zero-trust research field. Specifically, we emphasise the importance of protecting all perimeters in order to secure all the subsystems' boundaries, and, thus, interplays between the latter.

This thesis' essays have several managerial implications. First, we have reduced uncertainty in corporate and political decision-making regarding resource investments (Essay 1). Second, we help practitioners design technology for digital sovereignty (Essays 2 and 3) as well as its utilisation in an organisational (Essays 4 and 5) and societal (Essay 6) context. Third, Essay 7 enables the application of theoretical insights in practise by providing a conceptual summary and consolidation of the literature.

6.3 Limitations

I will now briefly present three overarching limitations of this thesis. For a detailed description of the specific limitations, please see the essays' discussion and conclusion sections.

First, common in the study of emerging technologies, most technologies and concepts observed in this thesis (i.e., blockchain technology and SSI) are not yet widely adopted in practise. Thus, our empirical insights partially stem from research projects that implemented prototypes rather than observing productive environments (i.e., Essays 3, 4, and 5). Thus, future research into blockchain technology and SSI in productive environments promises further interesting insights, which would also provide additional insights into user acceptance in practice (Guggenberger et al. 2023).

Second, this thesis focused on levering technology for digital sovereignty (Essays 2 to 7), with a lesser focus on the management of technology for digital sovereignty (Essay 1). Furthermore, we investigated how technologies can contribute to digital sovereignty but do not observe the achievement of total digital sovereignty. Thus,

future research should also address how the interplays between various building blocks allow us to fulfil the overall goal of achieving digital sovereignty and clarify what it means to achieve the latter.

Third, regarding the benefits of digital sovereignty, this thesis emphasises the value of data sovereignty for individuals (Essays 1, 2, 3 and 7), but does not necessarily answer data sovereignty's benefits for individual organisations. However, answering this question is crucial for motivating organisations to invest in digital sovereignty, as efforts do not necessarily pay out in the short term, but rather in the long term. Also, an individual organisation may not even benefit from being the only one striving for digital sovereignty – only united effort by all involved stakeholders may be profitable.

6.4 Future research

In this dissertation, I have addressed how technologies and paradigms can be utilised for the goal of digital sovereignty. I conclude by outlining the potentials for future research endeavours. Specifically, I emphasise the relevance of further specifying IS research's role in exploring digital sovereignty, and the need to adopt an interdisciplinary view as well as to continually explore novel technologies for digital sovereignty.

Although several studies have addressed partial aspects of digital sovereignty in IS, for instance for digital resilience (Boh et al. 2020) or social welfare computing (Clemons et al. 2022b), the *digital sovereignty* concept has not yet been established in IS research. On the one hand, digital sovereignty's practical relevance (c.f. Bendiek and Stürzer 2022, Braud et al. 2021, Goldacker 2017, Madiega 2020) underscores the urgency of addressing this shortcoming in IS research. On the other hand, IS research is particularly well-suited for engaging in the topic digital sovereignty: solely observing the technical or social subsystem is insufficient. In contrast, answering how digital technologies can enable digital sovereignty and how these technologies must be managed to ensure digital sovereignty requires acknowledging the implications of technological designs for individuals, organisations, and society – i.e., a sociotechnical understanding of IS. Thus, while I contributed an initial conceptualisation of digital sovereignty, I encourage IS scholars to further define IS research's role in understanding digital sovereignty. When doing so, researchers can draw on multiple existing studies. For instance, resource dependence theory (Pfeffer and Salancik 1978)

explains external constraints' effects on organisations. In light of addressing digital sovereignty, the theory can help IS researchers to manage adverse dependencies that are critical for technological sovereignty, data sovereignty, and security. Thus, when approaching digital sovereignty in IS research, scholars can stand on the shoulders of giants.

Second, an integrated observation of digital sovereignty requires an interdisciplinary perspective. For instance, regulation may be a building block for achieving digital sovereignty. The digital sovereignty concept is already a much-discussed element in the legal and political sciences (Pohle and Thiel 2020; Couture and Toupin 2019). I encourage IS researchers to adopt an interdisciplinary view on digital sovereignty so as to foster a holistic understanding of the concept.

Third, future research should examine not only the current technologies, concepts, and methods for digital sovereignty, but should continue observing novel tools. In the past years, we have observed several technologies and paradigms specifically aimed at providing more data sovereignty and security. Starting with blockchain technology fostering independence from intermediaries in payment processes (Nakamoto 2008), both researchers and practitioners have utilised the technology for a broad range of purposes that involve the omission of third-party providers. Blockchain technology also became the underlying trust infrastructure for identity provisioning, specifically in the context of SSI. However, to date, we observe that blockchain technology does not necessarily represent a technical component of SSI applications. The research proves that technological concepts designed for providing digital sovereignty keep evolving. Thus, future research should keep observing emerging technologies, concepts, and methods for digital sovereignty.

This thesis addresses the facilitation of digital sovereignty, providing a rich basis for future (IS) research. Since blockchain technology as well as the paradigms of SSI and zero-trust will not be the last concepts to address digital sovereignty, future research should provide theoretical and managerial guidance on technologies as well as how to manage the latter to support individuals and organisations and therefore societies in their transition to digital sovereignty.

References

Akhlaghpour S, Wu J, Lapointe L, Pinsonneault A (2013) The ongoing quest for the IT artifact: Looking back, moving forward. Journal of Information Technology 28(2):150–166.

Amershi S, Begel A, Bird C, DeLine R, Gall H, Kamar E, Nagappan N, Nushi B, Zimmermann T (2019) Software engineering for machine learning: A case study. In: Proceedings of the 41st International Conference on Software Engineering: Software Engineering in Practice, pp 291–300.

Association for Computing Machinery (2023) ACM computing classification system. https://dl.acm.org/ccs. Accessed 2023-03-19.

Baier L, Seebacher S (2019) Challenges in the deployment and operation of machine learning in practice. In: Proceedings of the 27th European Conference on Information Systems (ECIS).

Barney J (1991) Firm resources and sustained competitive advantage. Journal of Management 17(1):99–120.

Benbasat I, Goldstein DK, Mead M (1987) The case research strategy in studies of information systems. MIS Quarterly 11(3):369–386.

Benbasat I, Wang W (2005) Trust in and adoption of online recommendation agents. Journal of the Association for Information Systems 6(3):72–101.

Bendiek A, Stürzer I (2022) Advancing European internal and external digital sovereignty. https://www.swp-berlin.org/publications/products/comments/2022C20_EuropeanDigitalSovereignty.pdf. Accessed 2023-03-23.

Bergen M, Dutta S, Walker OC (1992) Agency relationships in marketing: A review of the implications and applications of agency and related theories. Journal of Marketing 56(3):1–24.

Bharadwaj AS (2000) A resource-based perspective on information technology capability and firm performance: An empirical investigation. MIS Quarterly 24(1):169–196.

Bhattacharjee B, Boag S, Doshi C, Dube P, Herta B, Ishakian V, Jayaram KR, Khalaf R, Krishna A, Li YB, Muthusamy V, Puri R, Ren Y, Rosenberg F, Seelam SR, Wang Y, Zhang JM, Zhang L (2017) IBM deep learning service. IBM Journal of Research and Development 61(4-5):1–11.

Boh WF, Constantinides P, Padmanabhan B, Viswanathan S (2020) Digital resilience: Call for papers. MIS Quarterly.

Bowman E (2021) After data breach exposes 530 million, Facebook says IT will not notify users. https://www.npr.org/2021/04/09/986005820/after-data-breach-exposes-530-million-facebook-says-it-will-not-notify-users. Accessed 2023-03-19.

Braud A, Fromentoux G, Radier B, Le Grand O (2021) The road to European digital sovereignty with Gaia-X and IDSA. IEEE Network 35(2):4–5.

Braun R, Esswein W (2012) Corporate risks in social networks – towards a risk management framework. In: Proceedings of the Americas Conference on Information Systems (AMCIS).

Butijn B-J, Tamburri DA, van Heuvel W-J den (2020) Blockchains: A systematic multivocal literature review. ACM Computing Surveys 53(3):1–37.

Chatterjee S, Sarker S, Lee MJ, 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.

Chen Y, Hu H, Cheng G (2019) Design and implementation of a novel enterprise network defense system by maneuvering multi-dimensional network properties. Frontiers of Information Technology & Electronic Engineering 20(2):238–252.

Clemons E, Schreieck M, Hermes S, Rowe F, Krcmar H (2022a) The cooperation paradox. Electronic Markets 32(2):459–471.

Clemons E, Schreieck M, Krcmar H, Bui T (2022b) Social welfare computing and the management and regulation of new online business models. Electronic Markets 32(2):411–414.

Compastie M, Badonnel R, Festor O, He R, Kassi-Lahlou M (2016) A software-defined security strategy for supporting autonomic security enforcement in distributed cloud. In: Proceedings of the 2016 IEEE International Conference on Cloud Computing Technology and Science (CloudCom), pp 464–467.

Corbin J, Strauss A (2014) Basics of qualitative research: Techniques and procedures for developing grounded theory. SAGE Publications.

Couture S, Toupin S (2019) What does the notion of "sovereignty" mean when referring to the digital? New Media & Society 21(10):2305–2322.

Covert Q, Steinhagen D, Francis M, Streff K (2020) Towards a triad for data privacy. In: Proceedings of the 53rd Hawaii International Conference on System Sciences (HICSS).

Das T, Teng B-S (2000) A resource-based theory of strategic alliances. Journal of Management 26(1):31–61.

DeCusatis C, Liengtiraphan P, Sager A, Pinelli M (2016) Implementing zero trust cloud networks with transport access control and first packet authentication. In: Proceedings of the 2016 IEEE International Conference on Smart Cloud (SmartCloud), pp 5–10.

Du W, Pan SL, Leidner DE, Ying W (2019) Affordances, experimentation and actualization of fintech: A blockchain implementation study. The Journal of Strategic Information Systems 28(1):50–65.

Eisenhardt KM (1989) Building theories from case study research. The Academy of Management Review 14(4):532.

Eisenhardt KM, Graebner ME (2007) Theory building from cases: Opportunities and challenges. Academy of Management Journal 50(1):25–32.

European Commission (2022) Digital sovereignty: Commission proposes chips act. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_729. Accessed 2023-03-19.

Fox G (2001) Peer-to-peer networks. Computing in Science & Engineering 3(3):75–77.

Garousi V, Felderer M, Mäntylä M (2019) Guidelines for including grey literature and conducting multivocal literature reviews in software engineering. Information and Software Technology 106:101–121.

Gefen D, Karahanna E, Straub D (2003) Trust and TAM in online shopping: An integrated model. MIS Quarterly 27(1):51–90.

Gibson JJ (1979) The ecological approach to visual perception. Psychology Press Taylor & Francis Group, London, UK, New York, NY, USA.

Glaser F (2017) Pervasive decentralisation of digital infrastructures: A framework for blockchain enabled system and use case analysis. In: Proceedings of the 50th Hawaii International Conference on System Sciences (HICSS), pp 1543–1552.

Goldacker G (2017) Digitale Souveräntität. https://www.cio.bund.de/Webs/CIO/DE/digitale-loesungen/digitale-souveraenitaet/digitale-souveraenitaet-node.html. Accessed 2023-03-19.

Goldkuhl G (2012) Pragmatism vs interpretivism in qualitative information systems research. European Journal of Information Systems 21(2):135–146.

Goldreich O, Micali S, Wigderson A (1991) Proofs that yield nothing but their validity or all languages in np have zero-knowledge proof systems. Journal of the ACM 38(3):690–728.

Goldreich O, Oren Y (1994) Definitions and properties of zero-knowledge proof systems. Journal of Cryptology 7(1):1–32.

Goldwasser S, Micali S, Rackoff C (1985) The knowledge complexity of interactive proof-systems. In: Proceedings of the 17th Annual ACM Symposium on Theory of Computing, pp 291–304.

Grant R (1991) The resource-based theory of competitive advantage: Implications for strategy formulation. California Management Review 33(3):114–135.

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: Proceedings of the 56th Hawaii International Conference on System Sciences (HICSS).

Gupta M, George JF (2016) Toward the development of a big data analytics capability. Information & Management 53(8):1049–1064.

Hazelwood K, Bird S, Brooks D, Chintala S, Diril U, Dzhulgakov D, Fawzy M, Jia B, Jia Y, Kalro A, Law J, Lee K, Lu J, Noordhuis P, Smelyanskiy M, Xiong L, Wang X (2018) Applied machine learning at Facebook: A datacenter infrastructure perspective. In: Proceedings of the IEEE International Symposium on High Performance Computer Architecture (HPCA), pp 620–629.

Hermes S, Clemons E, Schreieck M, Pfab S, Mitre M, Böhm M, Wiesche M, Krcmar H (2020a) Breeding grounds of digital platforms: Exploring the sources of American platform domination, China's platform self-sufficiency, and Europe's platform gap. In: ECIS 2020 Proceedings.

Hermes S, Töller N, Hein A, Weking J (2020b) Gaining control over critical platforms: A comparative case study of European consortia. In: ECIS 2020 Proceedings.

Hevner AR (2007) A three cycle view of design science research. Scandinavian Journal of Information Systems 19(2):4–10.

Hui K, Vance A, Zhdanov D (2016) Securing digital assets. In: Bush A, Rai A (eds) MIS Quaterly Research Curations.

Jarke M, Otto B, Ram S (2019) Data sovereignty and data space ecosystems. Business & Information Systems Engineering 61(5):549–550.

Jian J-Y, Bisantz A, Drury C (2000) Foundations for an empirically determined scale of trust in automated systems. International Journal of Cognitive Ergonomics 4(1):53–71.

Kemp S (2023) Most popular social networks worldwide as of January 2022, ranked by number of monthly active users. https://datareportal.com/reports/digital-2023-global-overview-report. Accessed 2023-03-19.

Kitchenham B, Charters S (2007) Guidelines for performing systematic literature reviews in software engineering. Software Engineering Group, School of Computer Science and Mathematics, Keele University.

Klein H, Myers M (1999) A set of principles for conducting and evaluating interpretive field studies in information systems. MIS Quarterly 23(1):67–93.

Lacity M, Carmel E (2022) Self-sovereign identity and verifiable credentials in your digital wallet. MIS Quarterly Executive 21(3):241–251.

Langston J (2020) Microsoft announces new supercomputer, lays out vision for future AI work. https://news.microsoft.com/source/features/ai/openai-azure-supercomputer/. Accessed 2023-03-19.

Lankton N, McKnight DH, Tripp J (2015) Technology, humanness, and trust: Rethinking trust in technology. Journal of the Association for Information Systems 16(10):880–918.

Lazar J, Feng JH, Hochheiser H (2017) Research methods in human computer interaction. Morgan Kaufmann, Boston, MA, USA.

Lombard M, Snyder-Duch J, Bracken CC (2002) Content analysis in mass communication: Assessment and reporting of intercoder reliability. Human Communication Research 28(4):587–604.

Madiega T (2020) Digital sovereignty for Europe. https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf. Accessed 2023-03-04.

Maedche A, Gregor S, Morana S, Feine J (2019) Conceptualization of the problem space in design science research. In: Proceedings of the 14th International Conference on Design Science Research in Information Systems and Technology (DESRIST), pp 18–31.

Markus ML, Silver M (2008) A foundation for the study of IT effects: A new look at Desanctis and poole's concepts of structural features and spirit. Journal of the Association for Information Systems 9(10):609–632.

Marton A (2013) Purposive selection and the quality of qualitative IS research. In: Proceedings of the 34th International Conference on Information Systems (ICIS).

Masters K (2019) These four companies still refuse to sell on Amazon, despite its market dominance. https://www.forbes.com/sites/kirimasters/2019/09/05/these-four-companies-still-refuse-to-sell-on-amazon-despite-its-market-dominance/?sh=6d725f3924fe. Accessed 2023-03-19.

Mcginthy JM, Michaels AJ (2019) Secure industrial internet of things critical infrastructure node design. IEEE Internet of Things Journal 6(5):8021–8037.

Mehraj S, Banday MT (2020) Establishing a zero trust strategy in cloud computing environment. In: Proceedings of the 2020 International Conference on Computer Communication and Informatics, pp 1–6.

Mikalef P, Gupta M (2021) Artificial intelligence capability: Conceptualization, measurement calibration, and empirical study on its impact on organizational creativity and firm performance. Information & Management 58(3):103434.

Moubayed A, Refaey A, Shami A (2019) Software-defined perimeter (SDP): State of the art secure solution for modern networks. IEEE Network 33(5):226–233.

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.

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

Nakamoto S (2008) Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf. Accessed 2021-08-08.

Orlikowski WJ, Iacono CS (2001) Research commentary: Desperately seeking the "IT" in IT research: A call to theorizing the IT artifact. Information Systems Research 12(2):121–134.

Ostern N (2018) Do you trust a trust-free technology? Toward a trust framework model for blockchain technology. In: Proceedings of the 39th International Conference on Information Systems (ICIS), 1- 17.

Otto B (2022) A federated infrastructure for European data spaces. Communications of the ACM 65(4):44–45.

Palvia P, Leary D, Mao E, Midha V, Pinjani P, Salam AF (2004) Research methodologies in MIS: An update. The Communications of the Association for Information Systems 14(1):58.

Parameswaran M, Susarla A, Whinston AB (2001) P2p networking: An information sharing alternative. Computer 34(7):31–38.

Pavlou, Liang, Xue (2007) Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. MIS Quarterly 31(1):105.

Peffers K, Tuunanen T, Rothenberger MA, Chatterjee S (2007) A design science research methodology for information systems research. Journal of Management Information Systems 24(3):45–77.

Pfeffer J, Salancik GR (1978) The external control of organizations: A resource dependence perspective. Stanford University Press, Stanford, CA, USA.

Pickl S (2019) Interview with Erich Vad on “political and security aspects of digitization”. Business & Information Systems Engineering 61(3):257–260.

Pohle J, Thiel T (2020) Digital sovereignty. Internet Policy Review 9(4):1–19.

Popovic A, Thong J, Wattal S (2017) Information privacy. In: Bush A, Rai A (eds) MIS Quarterly Research Curations.

Ramahandry T, Bonneau V, Bani E, Vlasov N, Flickenschild M, Batura O, Tcholtchev N, Lämmel P, Boerger, Michell (2021) Key enabling technologies for Europe's technological sovereignty. https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2021)697184. Accessed 2023-03-12.

Richter F (2022) Amazon, Microsoft & Google dominate cloud market. https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/. Accessed 2023-03-19.

Risius M, Spohrer K (2017) A blockchain research framework. Business & Information Systems Engineering 59(6):385–409.

Rossi M, Mueller-Bloch C, Thatcher JB, Beck R (2019) Blockchain research in information systems: Current trends and an inclusive future research agenda. Journal of the Association for Information Systems 20(9):1388–1403.

Schellinger B, Völter F, Urbach N, Sedlmeir J (2022) Yes, I do: Marrying blockchain applications with GDPR: January 3-7, 2022. In: Proceedings of the 55th Hawaii International Conference on System Sciences (HICSS).

Sedlmeir J, Ross P, Luckow A, Lockl J, Miehle D, Fridgen G (2021) The DLPS: A framework for benchmarking blockchains. In: Proceedings of the 54th Hawaii International Conference on System Sciences (HICSS), pp 6855–6864.

Seidel S, Müller-Wienbergen F, Becker J (2010) The concept of creativity in the information systems discipline: Past, present, and prospects. Communications of the Association for Information Systems 27:217–242.

Sheppard JP (1995) A resource dependence approach to organizational failure. Social Science Research 24(1):28–62.

Shlapentokh-Rothman M, Hemberg E, O'Reilly U-M (2020) Securing the software defined perimeter with evolutionary co-optimization. In: Proceedings of the 2020 Genetic and Evolutionary Computation Conference Companion, pp 1528–1536.

Söllner M, Benbasat I, Gefen D, Leimeister J, Pavlou P (2016) Trust. In: Bush A, Rai A (eds) MIS Quaterly Research Curations.

Söllner M, Hoffmann A, Hoffmann H (2012a) Twenty software requirement patterns to specify recommender systems that users will trust. In: Proceedings of the 20th European Conference on Information Systems (ECIS), 1-13.

Söllner M, Hoffmann A, Hoffmann H, Wacker A, Leimeister J (2012b) Understanding the formation of trust in IT artifacts. In: Proceedings of the 33rd International Conference on Information Systems (ICIS), 1-18.

Sonnenberg C, Vom Brocke J (2012) Evaluation patterns for design science research artefacts. In: Helfert M, Donnellan B (eds) Practical Aspects of Design Science. Springer, Berlin, Germany, pp 71–83.

Strong D, Volkoff O, Johnson S, Pelletier L, Tulu B, Bar-On I, Trudel J, Garber L (2014) A theory of organization-EHR affordance actualization. Journal of the Association for Information Systems 15(2):53–85.

Tauscher K, Kietzmann J (2017) Learning from failures in the sharing economy. MIS Quarterly Executive 16(4):253–264.

Trzaskowski J (2022) Data-driven value extraction and human well-being under EU law. Electronic Markets 32(2):447–458.

Verberne FMF, Ham J, Midden CJH (2012) Trust in smart systems: Sharing driving goals and giving information to increase trustworthiness and acceptability of smart systems in cars. Human Factors 54(5):799–810.

Weber I, Xu X, Riveret R, Governatori G, Ponomarev A, Mendling J (2016) Untrusted business process monitoring and execution using blockchain. In: Proceedings of the International Conference on Business Process Management (BPM), pp 329–347.

Weber M, Engert M, Schaffer N, Weking J, Krcmar H (2022) Organizational capabilities for AI implementation: Coping with inscrutability and data dependency in AI. Information Systems Frontiers:1–21.

Weise K (2019) Prime power: How Amazon squeezes the businesses behind its store. https://www.nytimes.com/2019/12/19/technology/amazon-sellers.html. Accessed 2023-03-19.

Yin RK (2014) Case study research: Design and methods. SAGE Publications, Los Angeles, CA, USA, London, UK, New Delhi, India, Singapore, Washington DC, WA, USA.

Zaheer Z, Chang H, Mukherjee S, van der Merwe J (2019) eZTrust: Network-independent zero-trust perimeterization for microservices. In: Proceedings of the 2019 ACM Symposium on SDN Research, pp 49–61.

The impact of resource investments on the machine learning lifecycle: Bridging the gap between software engineering and management[4]

Authors

Duda, Sebastian; Hofmann, Peter; Urbach, Nils; Völter, Fabiane; Zwickel, Amelie.

Abstract

An organization's ability to develop Machine Learning (ML) applications depends on its available resource base. Without awareness and understanding of all relevant resources as well as their impact on the ML lifecycle, we risk inefficient allocations as well as missing monopolization tendencies. To counteract these risks, we develop a framework that interweaves the relevant resources with the procedural and technical dependencies within the ML lifecycle. To rigorously develop and evaluate we follow the Design Science Research paradigm and build on a literature review and an interview study. In doing so, we bridge the gap between the software engineering and management perspective to advance the ML management discourse. Our results extend the literature by introducing not yet discussed but relevant resources, describing six direct and indirect effects of resources on the ML lifecycle, and revealing the resources' contextual properties. Furthermore, the framework is useful in practice to support organizational decision-making and contextualize monopolization tendencies.

Keywords: ML management, machine learning lifecycle, artificial intelligence, resource-based view, design science research.

[4] This essay has been published in:
Duda S, Hofmann P, Urbach N, Völter F, Zwickel A (2023) The impact of resource allocation on the machine learning lifecycle. Business & Information Systems Engineering.

Harmonizing sensitive data exchange and double-spending prevention through blockchain and digital wallets: The case of e-prescription management[5]

Authors

Schlatt, Vincent; Sedlmeir, Johannes; Traue, Janina; Völter, Fabiane

Abstract

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

Keywords: Distributed ledger, privacy, security, self-sovereign identity, tokens.

---

[5] This essay has been published in:
Schlatt V, Sedlmeir J, Traue J, Völter F (2022) Harmonizing sensitive data exchange and double-spending prevention through blockchain and digital wallets: The case of e-prescription management. Distributed Ledger Technologies: Research and Practice.

Trusting the trust machine: Evaluating trust signals of blockchain applications[6]

Authors

Völter, Fabiane; Urbach, Nils; Padget, Julian

Abstract

Information systems research emphasizes that blockchain requires trust in the technology itself. However, we lack knowledge on the applicability of established trust cues to blockchain technology. Thus, this paper's objective is to empirically evaluate the effectiveness of several established IS trust formation factors on end user trust. We do so by conducting a between-groups experiment. While we can validate the applicability of previous IS trust research for blockchain technology to some extent, we find that trust signals emphasizing the technology's underlying trust-building characteristics are most effective. Hence, we highlight the need for contextualization of trust research on blockchain technology. We provide both researchers and practitioners with insights for building trustworthy blockchain applications that enable trust-less interactions not only in theory but in practice.

Keywords: Blockchain technology, trust signals, end users' trust, trustworthiness, distributed ledger.

[6] This essay has been published in:
Völter F, Urbach N, Padget J (2021) Trusting the trust machine: Evaluating trust signals of blockchain applications. International Journal of Information Management 68:1–13.

Affordances, experimentation, and actualization of self-sovereign identity: A case study of the implementation and use of SSI [7]

Authors

Guggenberger, Tobias; Völter, Fabiane; Urbach, Nils

Extended Abstract

The concept of self-Sovereign Identity (SSI) promises to remedy the high complexity, costs, limited portability and reliability of current identity management (IdM) systems (Mühle et al. 2018). In essence, practitioners claim that SSI allows for portable and reliable digital identities that are in the end user's control (Reed and Preukschat 2021). An identity system as promised could decrease complexity and, thus, save costs for involved organizations as well as increase users' ability to control their own identity data (Wang and Filippi 2020). Due to these promises, the public sector is increasingly interested in SSI, as identity provision is at the core of its tasks (c.f. European Commission 2022; eIDAS Expert Group of the EU 2022; Federal Ministry of the Interior and Community 2021; Federal Ministry for Economic Affairs and Energy 2021).

However, while the public and private sectors heavily invest in SSI, little insights prevail on the concept's offerings for organizations as no productive SSI applications exist as of today. Specifically, a detailed understanding of the application and the value provided by SSI for organizations remains unclear (Cucko and Turkanovic 2021). Furthermore, academics and practitioners lack insights into the actualization of SSI's offerings to redesign existing and establish new business processes and systems (Leidner et al. 2018). Following the theoretical lens of affordance-experimentation-actualization (A-E-A) by Du et al. (2019), effective implementation of SSI can be understood as a process in which the actor, in our case, an organization, can experiment with the concept and actualize its affordances. To gain a better

[7] 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.

understanding of organizations adopting SSI, we, thus, ask the following research questions:

What are the affordances of SSI in an organizational context?

How does the public sector experiment with and actualize these affordances?

To answer the research questions, we conducted a holistic single-case study on a project implementing SSI within the public sector (Yin 2014; Eisenhardt 1989). In specific, we followed Yin's (2014) recommendations for data collection and tapped multiple data sources. Furthermore, we rely on A-E-A theory as a lens to shed insights on the novel phenomenon of SSI in line with Leidner (2020).

Our contribution is twofold: First, we contribute a better understanding of SSI's value and how organisations can approach its benefits. Second, we confirm the theoretical lens of affordance-experimentation-actualisation theory as proposed by Du et al. (2019), specifically with regards to the existence of the experimentation phase.

Keywords: Blockchain, case study, identity management, self-sovereign identity, public sector

References

Cucko S, Turkanovic M (2021) Decentralized and self-sovereign identity: Systematic mapping study. IEEE Access 9:139009–139027.

Du W, Pan SL, Leidner DE, Ying W (2019) Affordances, experimentation and actualization of fintech: A blockchain implementation study. The Journal of Strategic Information Systems 28(1):50–65.

eIDAS Expert Group of the EU (2022) European digital identity architecture and reference framework – outline. https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-architecture-and-reference-framework-outline.

Eisenhardt KM (1989) Building theories from case study research. The Academy of Management Review 14(4):532.

European Commission (2022) European blockchain services infrastructure. https://digital-strategy.ec.europa.eu/en/policies/european-blockchain-services-infrastructure. Accessed 2023-03-22.

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. Accessed 2023-03-19.

Federal Ministry of the Interior and Community (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. Accessed 2023-03-19.

Leidner DE (2020) What's in a contribution? Journal of the Association for Information Systems 21(1):238–245.

Leidner DE, 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.

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.

Reed D, Preukschat A (2021) Self-sovereign identity: Decentralized digital identity and verifiable credentials. Manning Publications, Boston, MA, USA.

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 2:28.

Yin RK (2014) Case study research: Design and methods. SAGE Publications, Los Angeles, CA, USA, London, UK, New Delhi, India, Singapore, Washington DC, WA, USA.

Know your supplier: A principal-agent perspective on self-sovereign identities in supplier management[8]

Authors

Guggenberger, Tobias; Stramm, Jan; Urbach, Nils; Völter, Fabiane

Abstract

Information asymmetry between buyers and suppliers can lead to adverse selection during relationship formation (Akerlof 1978; Jensen and Meckling 1976; Rothschild and Stiglitz 1976). Using credentials serves as a means to mitigate this asymmetry by signaling the characteristics of the parties involved (Terlaak and King 2006). Although digitized credentials provide operational advantages, they only partially mitigate the problem of adverse selection, because the verification of these credentials' legitimacy requires considerable resources, leaving room for deceitful suppliers to present falsified credentials. As a result, bad actors among suppliers can secure contracts and therefore competitive advantages while deteriorating or defecting after contract conclusion (Moratis 2018). Such fraudulent practices not only undermine genuine suppliers who have invested significantly in acquiring the presented competencies, but can also create substantial risks for the ongoing buyer-supplier relationship performance (Koh et al. 2012). In light of these challenges, there has been a growing interest in research aimed at developing advanced and secure ISs to decrease information asymmetries and curb adverse selection, especially through blockchain technology (Koh et al. 2012; Treiblmaier and Garaus 2023; Treiblmaier 2018; Dutta et al. 2020; Bauer et al. 2022). In specific, the novel blockchain-based self-sovereign identity paradigm (SSI) presents a potential solution to facilitate the efficient sharing of the required information in the digital sphere in a machine-processable and cryptographically verifiable way (Mühle et al. 2018; Reed and Preukschat 2021). Yet, the underlying relationships between these concepts and how they reduce adverse selection remain unclear, specifically regarding the application of SSI in organizational contexts. This knowledge gap prevents the purposive use of SSI for effective buyer-

[8] At the time of publishing 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.

supplier relationship formation. Thus, we ask:

How can digital credentials within blockchain-based SSI affect adverse selection during buyer-supplier relationship formation?

In order to answer our research question, we conducted an inductive qualitative empirical study through the lens of agency theory. Our empirical foundation includes semi-structured interviews with experts in OM, specifically within SCM and SSI development, and is enriched by insights from multiple SSI projects in Germany. As a result, we present a research model that demonstrates the causal relationships between SSI, signaling, and adverse selection.

This study makes two primary contributions: First, we enhance the understanding of the role of credentials within blockchain-based SSI as credible digital signals for counteracting adverse selection. By means of a thorough exploration grounded in agency theory, we underline the pivotal role of cryptographically signed credentials in increasing the credibility of information exchanged between entities within the digital realm. We find that the advantages of these credentials don't rely solely on technological (blockchain) features but also on the complex network of trusted credential issuers, who play a pivotal role in establishing trust through these credentials. Therefore, the effectiveness of the SSI system is rooted in the enhanced digital signaling of attributes, facilitated by automated information delivery, and the provision of trustworthy and verifiable data. Second, our discoveries have the potential to redefine practices and strategies in the context of establishing buyer-supplier relationships. This integration of blockchain-based SSI into the process of buyer-supplier relationship formation extends the influence of SSI into the academic discussions within operations management.

Keywords: Adverse selection, signalling, organisational identities, self-sovereign identities, digital supplier management

References

Akerlof GA (1978) The market for "lemons": Quality uncertainty and the market mechanism. In: Diamond P, Rothschild M (eds) Uncertainty in Economics. Elsevier, pp 235–251.

Bauer I, Parra-Moyano J, Schmedders K, Schwabe G (2022) Multi-party certification on blockchain and its impact in the market for lemons. Journal of Management Information Systems 39(2):395–425.

Dutta P, Choi T-M, Somani S, Butala R (2020) Blockchain technology in supply chain operations: Applications, challenges and research opportunities. Transportation research. Part E, Logistics and transportation review 142:102067.

Jensen MC, Meckling WH (1976) Theory of the firm: Managerial behavior, agency costs and ownership structure. Journal of Financial Economics 3(4):305–360.

Koh TK, Fichman M, Kraut RE (2012) Trust across borders: Buyer-supplier trust in global business-to-business e-commerce. Journal of the Association for Information Systems 13(11):886–922.

Moratis L (2018) Signalling responsibility? Applying signalling theory to the ISO 26000 standard for social responsibility. Sustainability 10(11):4172.

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.

Reed D, Preukschat A (2021) Self-sovereign identity: Decentralized digital identity and verifiable credentials. Manning Publications, Boston, MA, USA.

Rothschild M, Stiglitz J (1976) Equilibrium in competitive insurance markets: An essay on the economics of imperfect information. The Quarterly Journal of Economics 90(4):629.

Terlaak A, King AA (2006) The effect of certification with the ISO 9000 quality management standard: A signaling approach. Journal of Economic Behavior & Organization 60(4):579–602.

Treiblmaier H (2018) The impact of the blockchain on the supply chain: A theory-based research framework and a call for action. Supply Chain Management: An International Journal 23(6):545–559.

Treiblmaier H, Garaus M (2023) Using blockchain to signal quality in the food supply chain: The impact on consumer purchase intentions and the moderating effect of brand familiarity. International Journal of Information Management 68:102514.

Emerging digital technologies to combat future crises: Reviewing COVID-19 to be prepared for the future[9]

Authors

Guggenberger, Tobias; Lockl, Jannik; Röglinger, Maximilian; Schlatt, Vincent; Sedlmeir, Johannes; Stoetzer, Jens-Christian; Urbach, Nils; Völter, Fabiane

Abstract

In 2020, the world has witnessed an unprecedented global pandemic with COVID-19. It has led nations to take measures that have an enormous impact on individuals, society, and the economy. Researchers and practitioners responded rapidly, evaluating opportunities to capitalize on technology for tackling associated challenges. We investigate the innovative potentials of three emerging digital technologies – namely, the Internet of Things, artificial intelligence, and distributed ledgers – to tackle pandemic-related challenges. We present our findings on the most effective means of leveraging each technology's potential, the implications for use in crises, and the convergence of the three technologies.

Keywords: Artificial intelligence; blockchain; COVID-19; distributed ledger technology; open innovation; emerging digital technology; internet of things.

[9] This essay has been published in:
Guggenberger T, Lockl J, Röglinger M, Schlatt V, Sedlmeir J, Stoetzer J-C, Urbach N, Völter F (2021) Emerging digital technologies to combat future crises: Learnings from COVID-19 to be prepared for the future. International Journal of Innovation and Technology Management 18(04):1–27.

Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust[10]

Authors

Buck, Christoph; Olenberger, Christian; Schweizer, André; Völter, Fabiane; Eymann, Torsten

Abstract

In response to weaknesses of current network security solutions, the zero-trust model follows the idea that no network – whether internal or external – is trustworthy. The concept of zero-trust is enjoying increasing attention in both research and practice due to its promise to fulfil complex new network security requirements. Despite zero-trust's advantages over traditional solutions, it has not yet succeeded in replacing existing approaches. Uncertainty remains regarding the concept's distinct benefits and drawbacks for organisations and individuals, which hinders a holistic understanding of zero-trust and wide-spread adoption. Research can make valuable contributions to the field by systematically providing new insights into zero-trust. To support researchers in this endeavour, we aim to consolidate the current state of the knowledge about zero-trust and to identify gaps in the literature. Thus, we conduct a multivocal literature review, analysing both academic and practice-oriented publications. We develop a research framework for zero-trust to structure the identified literature and to highlight future research avenues. Our results show that the academic literature has focused mainly on the architecture and performance improvements of zero-trust. In contrast, the practice-oriented literature has focused on organisational advantages of zero-trust and on potential migration strategies. However, economic analyses and

[10] This essay has been published in:
Buck C, Olenberger C, Schweizer A, Völter F, Eymann T (2021) Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust. Computers & Security 110(C):102436.

user-related studies have been neglected by both academia and practice. Future research may rely on our findings to advance the field in meaningful ways.

Keywords: Zero-trust, network security, access control, software-defined perimeter, SDP, literature review