UNIVERSITÄT
BAYREUTH

The Whole Is More Than the Sum of Its Parts: On the Design of Decentralized Information Systems

Dissertation

zur Erlangung des Grades eines Doktors der Wirtschaftswissenschaft

der Rechts- und Wirtschaftswissenschaftlichen Fakultät

der Universität Bayreuth

Vorgelegt

von

Vincent Erich Schlatt

aus

München

Dekan:	Prof. Dr. Jörg Schlüchtermann
Erstberichterstatter:	Prof. Dr. Nils Urbach
Zweitberichterstatter:	Prof. Dr. Jens Strüker
Tag der mündlichen Prüfung:	15.06.2022

We're all part of a masterplan.

Noel Gallagher

Table of Contents

Abstract

Decentralized information systems (IS) strongly gained prominence through the rise in popularity of cryptocurrencies. Yet, the potential of such systems, specifically those based on blockchain technology, may reach far beyond this context. However, the rapid pace of development, the emergence of new concepts, and mixed appraisals of the actual potential complicate the application of decentralized IS in different contexts. Motivated by these challenges, this dissertation aims to guide organizations and individuals in designing decentralized IS to shape digitalization beneficially.

I structure this dissertation along four research questions, which I approach in four essays. To achieve the overall research goal, the individual research contributions range from analytical to prescriptive. Because the often promoted strong security provided by blockchain-based systems seems contradictory to popular security incidents, Essay 1 aims to analyze the attack vectors of blockchain systems and derive research avenues on the cybersecurity of blockchain-based systems for the IS community. Aiming to provide prescriptive knowledge on the design of decentralized IS, Essays 2–4 provide design artifacts for decentralized IS in different contexts of digitalization. The developed artifacts aim to guide organizations and individuals in the design and development of blockchain-based systems in the Internet of Things (Essay 2) and systems building on the combination of blockchain technology and SSI in the banking (Essay 3) and healthcare sectors (Essay 4).

Thus, I provide novel theoretical and practical insights on the design, development, and evaluation of decentralized IS with a focus on blockchain technology. I contribute a socio-technical perspective to research on decentralized IS through integrative research approaches, partly involving practitioners. Therefore, the essays in this dissertation contribute theoretically solid and practice-inspired knowledge through analytical as well as prescriptive research on the design of decentralized IS.

Keywords: Cybersecurity, decentralization, distributed ledger technology, information systems, self-sovereign identity

Acknowledgments

This dissertation is the result of a journey with many ups and downs. I am grateful for the people accompanying me along the way - it would have not been possible without you.

I would like to express my heartfelt gratitude to my academic supervisor Nils Urbach. Thank you for your inspiration and the opportunity to learn and follow my interests. I value you not only as an academic, but also as a person - may many others enjoy your supervision after me! In addition, I would like to wholeheartedly thank Jens Strüker for taking the role of co-advisor of this dissertation. I am also thankful for the support of the University of Bayreuth and Fraunhofer FIT in writing this dissertation.

I am indebted to thank my friends, who make my time on this earth very special. Your company during good times and support during bad ones are invaluable to me. I will try to offer the same to you. I strongly hope you all feel addressed by this.

To my partner, Lea, I am grateful for having been able to spend a large portion of my time as a doctoral candidate with you. I thank you for your love, support, and for making me smile even during difficult times.

Lastly, I would like to try to express my appreciation and gratefulness for my family. To my brother, who always has my back, to my parents, who were there for me for longer than I can remember, and to my grandparents.
I could not imagine life without knowing you by my side. This dissertation is for you.

Bayreuth, 03.05.2022
Vincent Schlatt

Introduction to
The Whole Is More Than the Sum of Its Parts: On the Design of Decentralized Information Systems

Abstract

This dissertation aims to guide organizations and individuals in designing decentralized IS with a focus on blockchain technology. It comprises four research essays, which have either been published in or submitted to distinguished research journals. The individual essays contribute theoretically solid and practice-inspired knowledge through analytical as well as prescriptive research on the design of decentralized IS. The introduction to this dissertation consists of six sections. I motivate the research in this dissertation in Section 1. Section 2 provides the background on decentralized IS with a focus on blockchain technology. Section 3 illustrates the research gaps addressed in the dissertation, whereas Section 4 introduces its structure and research methodology. The results in the four research essays are summarized in Section 5 and discussed in Section 6.

Keywords: Blockchain, decentralization, digitalization, information systems, self-sovereign identity

Table of Contents

1 Motivation

The exponential growth of technical capabilities brings significant changes to society (Kurzweil, 2005). For instance, the advancement and convergence of information technology (IT) lead to an ongoing digitalization of people's personal and professional lives (Legner et al., 2017). The amalgamation of IT, people, and organizational concepts creates increasingly complex information systems (IS) of socio-technical nature (Davis and Olson, 1985; Hevner et al., 2004; Lee, 1999; Österle et al., 2011). Given these systems' rising importance in everyday life, the question on how to design IS that shape digitalization beneficially has been of interest in research and practice for decades (Hevner et al., 2004; March and Smith, 1995; Nunamaker Jr et al., 1990; Österle et al., 2011).

Different designs of IS have been proposed along with ongoing technological development. In 1964, computer scientist Paul Baran broadly distinguished between centralized, decentralized, and distributed systems. Ever since, there have been discussions about which system design is preferable to others (Ein-Dor and Segev, 1978; Rockart and Leventer, 1976). The arguments given often went beyond technical considerations: for example, political stances and organizational structures have been shown to be influential forces, too (Agre, 2003; Hugoson, 2007). Thus, designs of IS must reflect a variety of influential elements.

The early designs of IS were strongly centralized (Leifer, 1988). However, as early as 1985, researchers warned about the risks associated with centralizing control and insight over transactions in IS, illustrating scenarios such as the possibility to manipulate elections based on computer systems' user profiles (Chaum, 1985). Recent incidents illustrate that this fear has become a reality (e.g., Isaak and Hanna, 2018). In fact, the Internet itself is not supposed to rely on any central actors but to offer an open networking architecture (Leiner et al., 2009). However, governing institutions with significant power over the Internet emerged quickly (De Nardis, 2014). In modern IS leveraging the Internet, such as digital platforms, network effects and resulting winner-take-all situations arising from centralized designs often lead to a strong centralization of power (Ruutu et al., 2017; Tiwana, 2013). In

summary, the commercialization and politicizing of the Internet ignited a strong tendency towards the centralization of IS, with all its side effects.

Yet, there are—and have been—alternative approaches to centralized designs of IS. Early on, IS were developed to take power away from central actors (Chaum, 1985). Driven by the goal of developing digital cash transaction systems without the need for central intermediaries, decentralized IS in particular got a strong boost through the invention of blockchain technology as the backbone of the cryptocurrency Bitcoin in 2008 (Nakamoto, 2008). Soon after, many decentralized IS based on blockchain technology emerged beyond cryptocurrencies (Casino et al., 2019; Hughes et al., 2019). Although technologically not necessarily dependent, the movement for decentralization sparked by blockchain technology triggered the development of other decentralized IS, such as self-sovereign identity (SSI) (Mühle et al., 2018; Preukschat and Reed, 2021). As Beck et al. (2017, p.381) put it, the "implications of creating a reliable, trustworthy distributed record system, or ledger, may be fundamental to how we organize interpersonal and interorganizational relationships".

Apart from increasing effectiveness and efficiency in organizations (Hevner et al., 2004), socio-technical design artifacts are supposed to result in widespread societal change (Hevner and Gregor, 2020). Ultimately, designing such artifacts should serve human purposes (March and Smith, 1995). Given this background, the need for research on the design of decentralized IS based on blockchain technology, which take power away from central actors, strongly gained relevance in diverse areas of society (Beck et al., 2017; Sedlmeir et al., 2021b). With this dissertation[1], I thus aim to contribute to this literature by shedding light on *how to design decentralized IS based on blockchain technology to shape digitalization beneficially*.

I structure the rest of this manuscript as follows: Section 2 provides the necessary context to understand the history of decentralized IS with a focus on blockchain. Section 3 illustrates the research gaps addressed in the dissertation, whereas Section 4 introduces its structure and research methodology. The results in the four research essays included in this dissertation are summarized in Section 5 and discussed in Section 6.

1 On addressing the results of the individual essays comprising this dissertation, I use *we* to refer to the authors, because all essays were written in co-authorship. The following sections are partly comprised of content taken from these essays. To improve the readability of the text, I omit the standard labeling of these citations.

2 Background

This section presents the background necessary to grasp the context of the individual essays comprising this dissertation. The introductory subsection presents different perspectives on decentralized IS in prior research. The following subsections explore blockchain technology and its contribution to research on decentralized IS in the past decade.

2.1 Perspectives on Decentralized IS

Different understandings and, thus, research strands of IS exist in academia (Boell and Cecez-Kecmanovic, 2015): Highlighting the information processing aspect of IS, some authors, such as Dumas et al. (2005) and Alter (2008), take a *process view* on IS and claim that processing information is the defining activity of any IS. Further delineating the nature of IS, the authors adopting a *technology view* understand IS as IT embedded in organizations (Symons, 1991), whereas the authors adopting a *social view* see IS as social systems and the embedded IT as one of multiple, equally important elements thereof (Land, 1985; Land, 1992). Finally, those with a *socio-technical view* integrate these perspectives and additionally take the interactions between the latter two into account (Bostrom and Heinen, 1977; Lee, 2001; Orlikowski, 1992). Although semantically distinct, all definitions indicate that IS extend beyond merely technical systems. In this dissertation, I follow a socio-technical view on IS, which is claimed to be highly suitable for developing accepted and value-adding IS (Baxter and Sommerville, 2011). Thus, I understand IS as containing both social and technical components, which interact with and mutually influence each other (Bostrom and Heinen, 1977; Orlikowski, 1992).

As Österle et al. (2011) note, IS broadly involve three interacting elements: IT, people, and organizations. While people and organizational concepts became increasingly central to IS research in the past decades, calls to shift attention to IT systems as the core subject of scientific endeavor emerged, because IT is considered to be the enabling component which digitalization revolves around (Benbasat and Zmud, 2003; Grover and Lyytinen, 2015;

Orlikowski and Iacono, 2001). In this dissertation I follow this view and emphasize the technical (IT) components of IS while nevertheless taking the social context into account.

Given this background, three distinct configurations of IS prevail: *centralized*, *decentralized*, and *distributed* (Baran, 1964; Ein-Dor and Segev, 1978; Leifer, 1988). While the exact definitions differ, I refer to Baran (1964)'s seminal definition of IS network topology and Leifer (1988)'s account of IS to distinguish between the three. Centralized systems organize reliant terminals around a central processing unit and, thus, contain a single point of failure (Baran, 1964). Distributed systems, however, can contain multiple hubs, which terminals revolve around.[1] Decentralized IS do not rely on any central party that information needs to be passed through, but are made of relatively equal components communicating directly with each other (Leifer, 1988).

Practical examples of decentralized IS are numerous, and past research in the IS domain reflects their IT, people, and organization components. For instance, Bloomfield and Coombs (1992) take a social perspective on IS and discuss the impact of introducing IT systems to organizations on the decentralization of power within the organizations. Thus, for the authors, decentralization refers to an organizational aspect rather than a technical property. Moreover, from a business-centric perspective, Kahai et al. (2003) shed light on the views and intentions of IT executives on the use of decentralized IS in their organizations. From a technical perspective, especially peer-to-peer (P2P) systems as prime examples of decentralized IS were discussed extensively in the literature (e.g., Fox, 2001). Finally, taking a socio-technical approach, Walsham (1993) researches the impact of decentralized IS on the empowerment of social groups through the technical property of decentralization. Thus, the author's work combines the technical property of decentralization and its impact on social aspects, thereby illustrating socio-technical research on IS.

Although before 2008 there had been only occasional academic reflections on decentralized IS, the research on this topic was given unprecedented impetus by the invention of Bitcoin, which is discussed in the next section.

2.2 Foundations of Blockchain Technology

Blockchain technology builds upon a combination of technologies that were already available before the invention of Bitcoin, which is presumably the first application of blockchain

1 Baran (1964) indeed calls this architecture *decentralized*. However, for consistency, in this dissertation I adhere to the nomenclature offered by Leifer (1988).

technology. Although Nakamoto (2008) is credited with bringing together all necessary pieces to create a distributed and tamper-resistant ledger of transactions, initial approaches to tackling related issues had existed for almost two decades (Chaum et al., 1988; Haber and Stornetta, 1990). Blockchain is one possible and probably the best known form of distributed ledger technology (DLT). [2] From a technological perspective, blockchain technology provides a distributed and replicated append-only database that groups transactions in blocks, which are stored on all nodes of a P2P network (Butijn et al., 2020). Removing the need for a central trusted authority (Nakamoto, 2008), the nodes of the P2P network repeatedly coordinate the state of the blockchain system by following a consensus protocol (Chanson et al., 2019; Glaser, 2017). Each block in a blockchain is linked to the previous block through a cryptographic hash; the blockchain, thereby, creates a tamper-resistant historical data record (Butijn et al., 2020).

Because of their technical structure, blockchain systems have important properties. Resulting from the resistance against crashes or the malicious behavior of a subset of nodes, blockchain systems are highly available and decentralized digital infrastructures (Amend et al., 2021). To participate in consensus or to interact with the P2P network and authorize transactions, the users of a blockchain system must authenticate using public-key cryptography. As a result, blockchain systems also offer an integrated public key infrastructure (Merkle, 1978). In summary, whereas blockchain systems are physically decentralized, the consensus mechanism ensures the creation of a single source of truth (Rossi et al., 2019). The combination of a consensus mechanism and the use of hash references provides a tamper-resistant data record in an absolute order (Butijn et al., 2020).

Since the emergence of Bitcoin as a system for financial transactions (Nakamoto, 2008), research as well as practice soon started to investigate the technology's potential beyond financial applications to provide decentralized digital infrastructures and improve cross-organizational processes (Fridgen et al., 2018; Hughes et al., 2019; Tandon et al., 2021). In this context, smart contracts, which are computer programs that are executed redundantly on the nodes of the P2P network in a blockchain system (Buterin et al., 2014; Lockl et al., 2020), are a particularly relevant innovation. Smart contracts enable a large variety of transactions beyond financial values (Beck et al., 2018), including the exchange of generic digital assets. These so-called *tokens* are value containers that represent digital or non-digital objects and that are transferable between the participants in a blockchain system (Oliveira et al., 2018; Pilkington, 2016). The opportunities related to the "tokenization"

2 The exact definitions of DLT and blockchain differ. For simplicity, in this dissertation I refer to blockchain technology, while sometimes describing infrastructures some authors call DLTs.

of physical and digital objects are considered an essential economic trend (Sunyaev et al., 2021).

Despite these developments, blockchain technology has several open challenges (Kannengießer et al., 2020). Whereas energy consumption is problematic only for a subset of consensus mechanisms called proof of work (Sedlmeir et al., 2020), blockchains in general present challenges in scalability and data visibility because of the inherent redundant storage and execution of transactions (Kannengießer et al., 2020; Kolb et al., 2020). Information transparency implies significant challenges in both personal data protection and business data protection. This issue is aggravated by the immutability of blockchains, which inhibits the retrospective deletion of information stored on a blockchain (Schellinger et al., 2022). Consequently, the use of blockchains should be sensibly considered regarding the processing of sensitive information.

Nevertheless, blockchain-based systems have become increasingly relevant in business and society. Their applications aim at leveraging the inherent characteristics of the technology, such as decentralization, tamper-resistance, and transparency (Hughes et al., 2019; Schweizer et al., 2017). As a result, blockchain-based systems contain an increasing amount of value, both monetary and in the form of business process information. For example, the German Federal Office for Migration and Refugees has developed a blockchain-based system for managing the highly sensitive personal information of refugees seeking asylum (Guggenmoos et al., 2020), and the value of cryptocurrencies has increased dramatically in the past decade. However, this ever-rising value stored in blockchain systems creates increasingly attractive targets for attackers, and several prominent cybercrimes on blockchain systems were reported recently (Feder et al., 2017; Mehar et al., 2019).

Despite the relevance of such incidents, the cybersecurity of blockchain-based systems has been considered strong by IS research so far (Frizzo-Barker et al., 2020; Hughes et al., 2019). Yet, several researchers called for a more critical perspective (Beck et al., 2017; Hughes et al., 2019) and additional research on the security of blockchain (Mendling et al., 2018), which constitutes an important motivator for this dissertation.

2.3 Blockchain as a Catalyst for Decentralized IS

By triggering a shift towards decentralization, blockchain technology served as a catalyst for the development of decentralized IS in general (Beck et al., 2017). In digital identity management, SSI offers verifiable digital identities for organizations, people, and networked

machines. Accounting for their decentralization aspect, such SSIs are not tied to a certain place or organization and can be used across domains with the identity owners' consent (Allen, 2016). SSI involves three distinct types of entities (Mühle et al., 2018): the issuer of an identity document, the holder of the respective document, and the verifier of properties described in the document. Tamper-resistant identity documents relate to verifiable credentials (VCs), which are cryptographically signed digital objects containing claims about their holders' identity and authorizations (Ehrlich et al., 2021; Preukschat and Reed, 2021; Sporny et al., 2019). Holders store these VCs in an application called digital wallet. To prove properties, or claims, described in their VCs to a verifier, holders generate verifiable presentations (VPs), which they present to the verifier. VPs are tamper-proof attestations derived from one or multiple VCs addressing the requirements of a verifier (Hardman, 2019; Preukschat and Reed, 2021; Sporny et al., 2019).

While these building blocks provide a solid foundation for an SSI system, a neutral infrastructure is still required: information about the issuers of VCs, such as their signing keys, and information about the revocation status of VCs must be publicly available to verify the correctness of VPs. By proving knowledge of the issuer's digital signature and non-inclusion of the issuer's VC in a public but privacy-protecting revocation registry (in the form of a cryptographic accumulator), holders can convince a verifier that their VC has not been revoked without having to contact the credential issuer (Schlatt et al., 2021). Furthermore, schemas of VCs must be publicly available to allow verifiers to vet the authenticity of VPs. Because of its properties as a decentralized and highly available data structure, blockchain technology is often used for this purpose (Ferdous et al., 2019; Mühle et al., 2018). SSI lately gained traction in a variety of use cases, often building on blockchain technology (Kuperberg, 2019). Thus, conceptually, blockchain technology often constitutes an important element of decentralized IS.

Beyond digital identities, blockchain has served as a motivator to decentralize other emerging technologies as well. This observation applies especially to technologies typically built on centralized infrastructures because of computing power restraints. For instance, the current architectures for the Internet of Things (IoT) typically rely on transmitting device data to centralized cloud servers for processing (Kshetri, 2017). Using cloud services in this scenario is supposed to enhance the IoT in terms of storage, computation, and communication capability (Botta et al., 2014). Yet, this approach typically generates data silos and requires trust in third parties operating the cloud servers (Shafagh et al., 2017), which also represent single points of failure (Taylor et al., 2020). In this light, using blockchain in the IoT could provide advancements through distributing data and decentralizing operations,

thus replacing a central cloud infrastructure. Similarly, artificial intelligence (AI) often relies on processing large datasets through centralized infrastructures. Salah et al. (2019) examine to what extent the properties of blockchain technology can support decentralizing AI methods, whereas Karger (2020) observe the reciprocal relationships and possible connections between the two emerging technologies. In summary, in the past decade, blockchain technology has started to significantly contribute to the designs of decentralized IS.

3 Derivation of Research Gaps and Research Questions

To investigate *how to design decentralized IS based on blockchain-technology to shape digitalization beneficially*, in this dissertation I aim to answer four related research questions through individual essays. Their research contributions shift from analytical (i.e., examining and conceptualizing attacks on blockchain-based systems) to prescriptive (i.e., giving design principles and guidelines for blockchain-based decentralized IS) (Gregor, 2006). In this section, I discuss the concrete research gaps and research questions in this dissertation.

3.1 Challenges in Designing Secure Decentralized Systems

Cybersecurity has gained relevance since the rise of networked computer systems and is becoming increasingly important due to the ubiquity of digitalization. As a result, security is a foundational objective for the design of any IS (Baskerville, 1993). As outlined before, IS research has almost unanimously considered the security of blockchain-based IS as particularly strong (Frizzo-Barker et al., 2020; Hughes et al., 2019). Nevertheless, motivated by prominent security incidents and critical technical publications, several researchers began to call for a more critical perspective (Beck et al., 2017; Hughes et al., 2019) and additional research on the security of blockchain-based systems (Mendling et al., 2018). Few descriptive technical surveys on the security of blockchain-based IS exist, whereas the IS research community lacks a systematic overview of attack vectors and resulting research avenues for this topic. However, research on the security of blockchain technology is required to increase acceptance of blockchain technology (Saad et al., 2020) and trust in its applications (Hughes et al., 2019). Therefore, while the security of blockchain-based systems seems "virtually indisputable" in IS literature, it is starting to be considered a risk as well (Frizzo-Barker et al., 2020, p. 9). IS researchers and practitioners alike should holistically consider the cybersecurity threats to blockchain-based systems to design, develop, and evaluate applications based on such systems (Warkentin and Orgeron, 2020). To fill this research gap, we aim to answer the following question:

What are the known attack vectors of blockchain systems, and which IS research avenues on the cybersecurity of blockchain-based systems can be derived?

3.2 Designing Decentralized Systems to Support Digitalization

Digitalization has become omnipresent in our society and permeates almost every aspect of our lives (Legner et al., 2017). However, in the context of digitalization, the traditionally centralized design of IS can be problematic. With the emergence of blockchain technology, decentralized IS gained popularity, aiming to resolve the shortcomings of their centralized counterparts. Yet how to design such blockchain-based decentralized IS in different contexts of business and society has remained a blurry question (Beck et al., 2017; Sedlmeir et al., 2021b), not least because of the variety of domain-specific requirements.

For instance, the applications of the IoT are diverse and present in many aspects of our society (Gubbi et al., 2013). However, current architectures for the IoT typically rely on transmitting device data to centralized cloud servers for processing (Kshetri, 2017). This approach typically generates data silos and requires trust in third parties operating the cloud servers (Shafagh et al., 2017), which also represent single points of failure (Taylor et al., 2020), in addition to lacking transparency (Kshetri, 2017). Recently, blockchain technology has been proposed to replace centralized cloud structures as the backend in the IoT (Fernández-Caramés and Fraga-Lamas, 2018; Kshetri, 2017; Makhdoom et al., 2019), because this technology was designed to provide trust through tamper resistance and the availability of data in a decentralized way (Abadi et al., 2018; Cong and He, 2019).

Although blockchain may solve the problems of current IoT architectures related to data integrity and availability (Liu et al., 2017; Reyna et al., 2018), research on the practical, theoretical, and managerial implications of this setting remains scarce (Chanson et al., 2019; Rossi et al., 2019). A literature review by Conoscenti et al. (2016) identified the tamper-resistant logging of data collected by devices and related events as one particularly promising use case for blockchain in the IoT, but most research hitherto seems to concentrate on resolving infrastructural issues of the IoT through blockchain (e.g., Lin et al., 2018; Roy and Kumar, 2019). The few existing research efforts on respective IoT data logging applications suggest solutions that are still reliant on centralized cloud services (Bocek et al., 2017; Samaniego and Deters, 2016; Taylor et al., 2020). Given this background, we formulate the following research questions to address the identified research gaps:

How can blockchain-based systems be conceptualized to improve sensor data integrity and availability in the IoT?

What are nascent design principles of blockchain-based IoT ecosystems?

Another highly centralized digital process is know your customer (KYC), which is imperative for financial service providers according to financial regulations in most of the world. This process is problematic for banks, because it is cost-intensive and time-consuming for them and inconvenient for their customers (Zetzsche et al., 2018). Therefore, there have been several attempts to improve it. For example, a central utility that collects and provides identity-related data for an electronic KYC (eKYC) process, as in India or Australia, is often mentioned as a solution to the aforementioned problems (Arner et al., 2019; Perlman and Gurung, 2019; Zetzsche et al., 2018), because it can reduce costs and significantly shorten KYC onboarding processes (Rajput and Gopinath, 2017). However, leaks and misuses of personal data have lowered confidence of both banks and customers in centralized solutions creating data silos (Swinhoe, 2020). Moreover, in some jurisdictions such a centralized service run by the government is legally not feasible (Rieger et al., 2019).

Though both researchers and practitioners have identified blockchain technology as a potential solution to those problems induced by centralized solutions, it is well-known that this technology's built-in transparency and append-only structure aggravates privacy-related problems (Rieger et al., 2019). Particularly, the European General Data Protection Regulation (GDPR) grants individuals the *right to be forgotten*, which means that they can demand that their private data be deleted at any time as soon as the purpose for their storage has expired. As data stored on a blockchain practically cannot be erased, implementations such as Moyano and Ross (2017)'s, where eKYC-related information is stored transparently on-chain, are not a viable solution. As an alternative, one could think of depositing the KYC information in a standardized way at the one and only entity involved in each of its KYC processes: the customer. These considerations lead to the concept of SSI. While research studies on the problem and approaches to SSI-based eKYC onboarding have recently emerged (Soltani et al., 2018), they have not covered topics such as user orientation, the entire KYC process, or platform independence. Furthermore, Soltani et al. (2018) focused on implementing the user-oriented principles of SSI without acknowledging that SSI is a tool to achieve an improved KYC process from the perspective of banks. For the reasons mentioned above, both research and practice need a generic and validated framework that guides SSI solutions' design for entire eKYC processes, as well as an overview of the resulting implications, to assess the potential benefits and learn how to leverage them.

In addition, we still lack generic design principles (DPs) to guide the development of SSI solutions based on blockchain technology that can also be used in other sectors (Liu et al., 2020). We therefore ask, *how to design a framework for an eKYC process built on blockchain-based SSI and which generic DPs can be derived?*

The healthcare sector is a further example of ongoing digitalization, which affects its stakeholders in various ways. In this context, the need to balance privacy requirements and digital healthcare provisioning can be complex (Guggenberger et al., 2021), which becomes evident in the digitalization of medical prescriptions. Medical prescriptions are typically physical, paper-based documents signed or sealed by a qualified physician, which patients present to pharmacies or health service providers to obtain treatment. However, such paper-based medical prescriptions suffer from various drawbacks. They are slow to process (Seaberg et al., 2021) and susceptible to manipulation, unauthorized reproduction, and errors (Mundy and Chadwick, 2002). Additionally, paper-based prescriptions can hardly integrate with telemedicine—which increased by a factor of 78 from February to April 2020, at the beginning of the Covid-19 pandemic (Bestsennyy et al., 2021))—and impede automatic checks for cross-reactions of pharmaceuticals (Aldughayfiq and Sampalli, 2021). Consequently, several attempts to introduce medical prescriptions in an electronic format have emerged. These digital references or documents allow for automatic validity checks and are typically stored in databases run by parties regarded as trustworthy, to prevent fraud and the abuse of sensitive data (Aldughayfiq and Sampalli, 2021). As such, existing approaches to electronic prescriptions (e-prescriptions) rely on highly centralized infrastructures and data silos. Accordingly, they serve as attractive targets for attackers aiming to capture sensitive health information on a large scale (Le Bris and El Asri, 2016; Lord, 2020). Moreover, they pose the socio-economic threat of creating monopolies or oligopolies (Wu and Tsai, 2018) and ethical issues associated with privacy concerns (Aldughayfiq and Sampalli, 2021). Also, centralized implementations of e-prescriptions are often not interoperable, because they create lock-in effects. To eliminate these drawbacks of centralized approaches, researchers recently proposed alternative solutions based on decentralized infrastructures. These approaches rely on distributed data storage and aim to provide higher security, privacy, and interoperability compared to centralized approaches (Stafford and Treiblmaier, 2020). As such, decentralized solutions address several issues of both paper-based and centralized electronic approaches to medical prescriptions.

Extant literature often uses a blockchain as the underlying decentralized infrastructure. Yet, the use of blockchain exacerbates privacy concerns (He et al., 2019; Stafford and Treiblmaier, 2020). This affects not only patients' confidentiality requirements but also

the compliance with regulations such as the EU GDPR, the California Consumer Privacy Act (CCPA), or the US Health Insurance Portability and Accountability Act (HIPAA). SSI offers standards and protocols for end-to-end encrypted bilateral communication and practices for selective and verifiable information disclosure based on digital certificates (Ferdous et al., 2019; Sporny et al., 2019). However, preventing the double-spending of e-prescriptions that are purely based on digital certificates is not possible solely through bilateral communication, because one pharmacy cannot know whether an e-prescription has already been presented and redeemed at another pharmacy. We hence propose that the combination of blockchain technology for double-spending prevention and SSI digital wallets for the verifiable exchange of sensitive e-prescription data and key management potentially offers properties solving the shortcomings of the current solutions to e-prescription management. Thus, we pose the following research question: *How to design and implement a decentralized system for e-prescription management using blockchain technology and digital wallets?*

4 Dissertation Structure and Research Designs

This dissertation consists of four research essays, each aiming to answer one of the research questions derived in chapter 3. The essays follow this introduction[1], which serves as an overview of my dissertation. Thus, the structure of this dissertation reflects its cumulative nature. Table 1 summarizes the publication history of each essay and how it addresses the research goal. Chapter 8 gives a summary of my other publications that are not part of this dissertation.

Table 1: Overview of the essays comprising this dissertation.

RQ	Title	Publication Outlet	Status
1	Attacking the Trust Machine: Developing an Information Systems Research Agenda for Blockchain Cybersecurity	International Journal of Information Management *Ranking: VHB-JOURQUAL3: C, Scopus: 99% percentile*	Published
2.1 **2.2**	Toward Trust in Internet of Things Ecosystems: Design Principles for Blockchain-Based IoT Applications	IEEE Transactions on Engineering Management *Ranking: VHB-JOURQUAL3: B, Scopus: 76% percentile*	Published
3	Designing a Framework for Digital KYC Processes Built on Blockchain-Based Self-Sovereign Identity	Information & Management *Ranking: VHB-JOURQUAL3: B, Scopus: 96% percentile*	Published
4	Harmonizing Sensitive Data Exchange and Double-Spending Prevention: The Case of E-Prescription Management	Scientific Journal *Ranking: N/A*	Under Review

The goal of contributing both analytical (*Essay 1*) and prescriptive insights (*Essays 2–4*) determined the choice of research designs in this dissertation (Gregor, 2006). Because of the interdisciplinary nature of IS and their strong embedding in society, which is reflected in the research questions in this dissertation, I follow Mingers (2001) and propose that research on IS should favor a pluralism of research methods and take inspiration from a range of academic fields. Thus, the results of this dissertation are drawn from the application of

1 For copyright reasons, the public version of this dissertation contains only summaries of the published papers.

several research methods. From a philosophical perspective, IS research can be interpreted as containing elements from both natural and social sciences (Mingers, 2004), which is reflected in the socio-technical view taken in this dissertation (Bostrom and Heinen, 1977). While there are debates about its implications for the choice of research methods (Mingers, 2004), I was inspired by a pragmatist point of view in the choice of my research designs (Beck et al., 2018; Goldkuhl, 2012; Mingers, 2004). Thus, I was strongly motivated by the practical relevance of my research outcome while using scientific rigor to achieve this goal (Mingers, 2004).

The research procedure of *Essay 1* is divided into two stages. First, we identified concrete attacks and attack vectors on blockchain systems through a structured literature review (SLR). This stage strongly reflects the analytical nature of the essay. Second, we derived an IS research framework and agenda for the cybersecurity of blockchain-based systems to generalize our findings and provide prescriptive knowledge. To conduct our SLR, we followed the widely accepted approach of Webster and Watson (2002). Thus, as an initial step, we extracted search terms from the research question at hand and then refined them by including insights from existing attack overviews. Subsequently, we created a Boolean search string based on these terms, which we applied to search appropriate databases for titles, abstracts, and keywords. We selected the ACM Digital Library, IEEE Xplore, and arXiv to cover papers with a technical focus, and AISel and Web of Science to cover relevant IS journals and conferences specifically. The databases returned 5332 results using the identified search string. We deliberately considered both journal publications and conference proceedings for our SLR, because research on blockchain is still in its infancy and evolving quickly (Rossi et al., 2019). After filtering the relevant data from the identified literature, we were left with 161 manuscripts for the final analysis. We followed the guidelines in Nickerson et al. (2013) to derive a concise, robust, comprehensive, and explanatory systematization for classifying the identified attacks along distinct attack vectors.

By analyzing commonalities, characteristics, and specificities across the identified attacks and attack vectors, and conceptualizing related research frameworks given this background, we derived a comprehensive research framework for IS research on the cybersecurity of blockchain systems. Following this conceptual research framework, we proposed a research agenda offering fruitful avenues for IS researchers aiming to shed light on perspectives on the cybersecurity of blockchain-based systems. To give substantiate our guidance to researchers, we provided six research propositions in line with the research framework proposed.

Essays 2–4 adhere to a design science research (DSR) approach, thus reflecting my intention of contributing prescriptive knowledge through the development of design guidelines for blockchain-based IS. This approach is compatible with the pragmatist stance taken in my dissertation (Goldkuhl, 2012), because DSR is ultimately concerned with creating IT artifacts that solve practical problems (Baskerville, 2008; Hevner et al., 2004; March and Smith, 1995). In line with DSR, the insights gained from the DSR process must be applicable to more generic settings (Jones and Gregor, 2007). Also, the design artifacts should result in profound disruptions to traditional ways of doing business (Hevner and Gregor, 2020). The research contribution of DSR is highly contested. This is because, on the one hand, it is hard to determine what exactly a theoretical contribution in DSR is (Gregor and Hevner, 2013) and, on the other hand, it is hard to balance concrete, practical contributions to a rapidly changing technology environment while at the same time providing a sufficient level of generalization for theory (Baskerville et al., 2018). To address these challenges, I aimed to contribute concrete IT artifacts, such as architectural or process designs and implementations of decentralized IS based on blockchain (Gregor and Hevner, 2013). Additionally, to elevate these IT artifacts for further theoretical discussion, I aimed to derive DPs (Gregor and Hevner, 2013; Hevner et al., 2004), thus contributing nascent design theory in the form of operational principles (Gregor and Hevner, 2013).

In *Essay 2*, we aimed to answer early calls for design-oriented research on blockchain (Glaser, 2017; Lindman et al., 2017). To this end, we applied the DSR process by Peffers et al. (2007), which is suitable to prototype-centric research endeavors (e.g., Reinecke and Bernstein, 2013). In line with the chosen research method, we first identified the challenges of current cloud-based IoT architectures. Then, we derived the objectives of a potential solution to the problem by inferring them from design principles proposed in the literature on blockchain and IoT, leading to nine objectives to be fulfilled by a suitable artifact. The derived objectives set the foundation for developing a blockchain-based prototype system for providing data availability and integrity in the IoT. The evaluation of the system comprised multiple cycles.

First, we employed logical reasoning along evaluation criteria as one approach to evaluating the general applicability of the system and its impact on data availability and integrity. Furthermore, we conducted structured expert interviews that also comprised collecting quantified ratings of the prototype along a Likert scale. In addition, we conducted semi-structured interviews with experts of different nationalities and with different industry backgrounds to enhance and confirm our findings ex post (Gregor and Hevner, 2013). We subsequently derived design principles (Gregor and Hevner, 2013) for blockchain-based

IoT systems. We applied the evaluation and design and development steps iteratively so we could continuously adapt and re-evaluate our artifact (Beck et al., 2013). Finally, we communicated our work through publishing our results.

In *Essay 3*, we again drew on the DSR process model of Peffers et al. (2007) to facilitate the development of a relevant IT artifact created by a rigorous method. Our process again has six steps arranged in sequential order and incorporates an iterative research procedure by design (Peffers et al., 2007). First, our examination of the current KYC process revealed issues of practical relevance, such as low process efficiency, security challenges, poor user experiences, and data protection concerns. Next, we defined solution objectives to address the stated challenges and to create a meaningful artifact. Recent research into DSR has encouraged researchers to build their work on prior DSR within the respective domain (Vom Brocke et al., 2020). We therefore derived solution objectives by studying the related literature and regulatory requirements, both for the KYC process and for digital identification and authentication, resulting in six main objectives for the KYC framework and several requirements for each main objective. Based on these objectives and on theory, we designed and developed the SSI-based eKYC framework. In a subsequent evaluation, which was necessary to test whether an artifact achieved the purpose of its creation and to prove this achievement using rigorous methods (Venable et al., 2012), we aimed at better understanding the problem at hand to thus realize improved outcomes (Hevner et al., 2004).

Our evaluation consisted of several iterative evaluation steps, starting ex ante with the formative evaluation of the design objectives through interviews with experts (Sonnenberg and Vom Brocke, 2012; Venable et al., 2016). We also conducted six additional interviews to evaluate our framework ex post by demonstrating it to the interviewees and incorporating their feedback. We chose to conduct qualitative interviews, a frequently used method in IS research, because they generate rich data (Myers and Newman, 2007). We gathered the opinions of experts on KYC and SSI on the practical applicability of our framework in existing settings and bank structures, and on its technical maturity and feasibility. We recorded 320 interview minutes (an average of 35.6 minutes per interviewee). The interviews were recorded, transcribed, and later analyzed using MAXQDA software. For data analysis, we used both open and axial coding (Saldaña, 2015).

To elevate the implicit knowledge contribution of our IT artifact to more abstract and generalizable knowledge allowing for theoretical discussion (Gregor and Hevner, 2013), we then developed nascent DPs for blockchain-based SSI, because this technical approach is both novel and increasingly discussed, while currently no general DPs exists in the literature.

Finally, we shared the findings of our research with the relevant audience (Hevner et al., 2004). The applied DSR process was iterative and its steps conducted partly in parallel, because the results of the evaluation phase reshaped the created artifact (Beck et al., 2013).

In *Essay 4*, we aimed to answer our research question by employing both an SLR and a DSR approach, designing, implementing, and evaluating a system for e-prescriptions based on blockchain technology and digital wallets. We conducted an SLR to identify relevant work investigating the potential of decentralized approaches for e-prescriptions management systems following the guidelines proposed by Kitchenham and Charters (2007). Accordingly, we derived our search string based on our research question (Kitchenham and Charters, 2007). We screened the databases ACM Digital Library, AISeL, arXiv, IEEE Xplore, Google Scholar, ScienceDirect, and Web of Science, because they represent the prevailing databases in the computer science and information systems research domain. The initial search yielded 6,009 results in total.

First, we excluded the papers that did not focus on solutions for e-prescriptions. Second, following the goal of our literature review to identify existing propositions for e-prescriptions, we also excluded papers that did not cover a specific solution architecture or that gave guidance on architecture design. Last, we excluded duplicates from our article set. We found that although blockchain is often mentioned as a viable technology for the healthcare sector in general (Engelhardt, 2017; Katuwal et al., 2018; Seitz and Wickramasinghe, 2020), extant literature only rarely explicitly proposes architectures for the management of e-prescriptions. Instead, the current literature centers on blockchain-enabled medical supply chains (Jamil et al., 2019; Mattke et al., 2019; Ruby et al., 2020), electronic health records (Chenthara et al., 2020; Zhang et al., 2018), and the management of medication histories(Kim et al., 2019; Raghavendra, 2019). Furthermore, some authors address e-prescriptions explicitly, but they focus on implementations and requirements in a specific country, hindering the generalization of their findings (Mahatpure et al., 2019).

We, again, adhered to the DSR model proposed by Peffers et al. (2007) to guide our research, which consists of six partly overlapping as well as iterative steps. As we identified by reviewing recent literature, solutions for e-prescriptions are prone to security incidents, lack interoperability, are associated with socio-economic risks, and are sensitive to fraud. Thus, the design of systems for e-prescriptions solving these issues is a problem of practical relevance. Next, we derived requirements for our solution by reviewing existing proposals for implementing e-prescriptions identified in an SLR. We defined 8 design objectives for our proposed solution. Adhering to these design objectives, we developed a system architecture

and instantiated it by implementing a prototype based on blockchain technology and digital wallets. We thus contribute both an architectural design and a prototype as IT artifacts. To evaluate the fulfilment of our design objectives and to highlight its advantages as well as the remaining shortcomings, we evaluated the artifacts both quantitatively and qualitatively along the criteria defined by the design objectives (Sonnenberg and Vom Brocke, 2012). To infer a contribution to theory, we subsequently derived DPs to offer more generalizable knowledge on the implications of designing and developing IT artifacts with similar requirements (Gregor and Hevner, 2013), such as privacy protection and double-spending prevention. Finally, we presented our artifact through publication.

5 Summary of Results

This section summarizes the results in the four research essays; as laid out in section 4, multiple research methods have led to their discovery. Yet, in all essays we adopted a pragmatist position.

5.1 Essay 1: Attacking the Trust Machine: Developing an Information Systems Research Agenda for Blockchain Cybersecurity

In *Essay 1*, we employed an SLR to analyze the literature on attacks targeting blockchain-based systems, extracting 87 distinct attacks. The first and second attack vectors comprise the P2P network representing the basic layer for data storage and exchange between nodes (15 attacks assigned) and the consensus mechanism for reaching agreement on the system's current state (27 attacks), respectively. The virtual machine (VM) and corresponding programming language of a blockchain system constitute the third attack vector (10 attacks). Building on these foundations, the infrastructure responsible for implementing application logic represents the fourth attack vector, subsuming smart contracts (16 attacks) and off-chain programs (11 attacks). Finally, client applications or wallets enabling users to interact with blockchain-based systems constitute the fifth attack vector (8 attacks).

We derived a framework for IS research on the cybersecurity of blockchain-based systems by conceptualizing existing blockchain research frameworks based on insights gained from analysing the attacks identified in our SLR. We divided the entities relevant for research on the cybersecurity of blockchain-based systems into (1) a human fraction, comprising users of blockchain applications, developers of blockchain-based systems, and attackers; and (2) an IT fraction, comprising blockchain infrastructure and blockchain applications running on top of the protocol (Rossi et al., 2019). Reciprocal effects characterize the relationships between the entities in the cybersecurity research framework. Building on the research framework derived, we contributed a nascent agenda for IS research on its cybersecurity. We developed six research propositions, each aligning with one or more elements in the framework (Hughes et al., 2019).

This article has three main contributions: First, we provide a structured overview and an analysis of the attacks on blockchain-based systems derived from a comprehensive literature review. Second, we contribute a framework guiding future research in the field of blockchain cybersecurity from an IS perspective. Third, we derive a comprehensive research agenda suggesting corresponding research avenues. In doing so, we introduced a socio-technical perspective on failures of IS (Bostrom and Heinen, 1977) to research on cybersecurity of blockchain-based systems, because these must be understood as socio-technical systems (Ehrenberg and King, 2020). Also, recently, scholars urged IS researchers to emphasize this theoretical stance (Sarker et al., 2019). The derived research framework and its theoretical grounding have a practical impact, too. We proposed that the interplay of the individual components in the blockchain technology stack and the relevant attacks for each resulting layer leads to different impacts on and involvement of the human and IT actors within the research framework. We divided the technology stack derived into three superordinate layers, for each of which specific attack types prevail. The affected and the primarily involved entities in the attacks, which we describe in our research framework, differ for each layer.

5.2 Essay 2: Toward Trust in Internet of Things Ecosystems: Design Principles for Blockchain-Based IoT Applications

Essay 2 investigates blockchain as an infrastructural approach for supporting IoT ecosystems in tamper-resistant sensor data logging. We initially derived 7 design objectives from the literature on IoT and blockchain technology to be achieved by a relevant implementation, which served as our primary design artifact. The implementation consists of three major components: An IoT sensor data logger module (component 1) is responsible for reading temperature and humidity data using a sensor board, which communicates with a Raspberry Pi single-board computer. We configured the Raspberry Pi as a light-client node for an Ethereum blockchain, which constitutes the blockchain layer serving as data storage and processing infrastructure through two smart contracts (component 2). A monitoring dashboard module (component 3) communicates with both contracts, displaying the sensor data and related information to an end user through a web application. After employing expert evaluation comprising two rounds of interviews, we distilled three design principles for blockchain-based systems in the IoT from our design. These entail ensuring the *modularity* of components, *data parsimony* in on-chain data storage, and the *availability* of components other than the blockchain system.

The theoretical contribution of the proposed artifact is twofold: First, our evaluation showed that our prototype system satisfies the basic design objectives from both IoT and blockchain domains, increasing data integrity and particularly data availability in the IoT. Nevertheless, we showed that the system also has deficits, such as high operating costs and limited scalability, which narrow its range of practical applicability. Through designing, developing, and evaluating the prototype, we expanded the field of DSR in the domains of blockchain and the IoT, adding to the limited body of knowledge in these still nascent fields. Second, we devised three generic design principles for blockchain-based IoT ecosystems resulting from a thorough evaluation approach, thus increasing the theoretical contribution of our design artifact (Gregor and Hevner, 2013).

In addition to its theoretical contribution, our research also provides valuable insights for practitioners in the fields of blockchain and IoT. In particular, we outlined a corporate strategy for developing blockchain-based systems in the IoT that builds on dedicated *technological experimentation* within organizations. Furthermore, we advised practitioners to *pre-evaluate technologies both generically and within context* before designing blockchain-based IoT ecosystems. We also recommended that practitioners *focus on comparably mature and open-source technologies* when choosing suitable blockchain protocols. Finally, *cooperation with other organizations* seems mandatory for transferring a reasonable system into production, because the value of the ecosystem increases with the number of participants.

In sum, *Essay 2* represents an early example of research on blockchain technology and the implications of largely outsourcing computational processes to a blockchain system's VMs. The designed system's evaluation indicates several challenges of using this approach, which is contrary to several prominent proposals in research at the time of writing.

5.3 Essay 3: Designing a Framework for Digital KYC Processes Built on Blockchain-Based Self-Sovereign Identity

In *Essay 3*, we designed a framework to improve the shortcomings in the KYC process through an end-to-end digital process built on blockchain-based SSI. Building on the work by Soltani et al. (2018), we emphasized banks' requirements on eKYC. We used a DSR approach based on Peffers et al. (2007), designing and evaluating a framework for KYC processes built on blockchain-based SSI, including a generic architecture and process design. Our evaluation suggests that our design can significantly contribute to a more

efficient KYC process that also addresses stakeholders' other requirements. However, we have illustrated that there are further conceptual challenges to be solved for use in real systems and settings, especially regarding the necessary governance frameworks and a more detailed regulatory analysis. Whereas our research suggests synergies between SSI and regulation, challenges remain, especially establishing a general SSI-based ecosystem and making SSI as user-friendly as possible without sacrificing privacy and security. From the DSR process, we derived three design principles: *using blockchain only for public data*, *anticipating an ecosystem of various ledgers*, and *enabling decentralization at the edge*.

Besides the conceptualized and evaluated architecture and set of processes (Gregor and Hevner, 2013) for the KYC case, we have made three primary contributions to the academic body of knowledge. First, our examination revealed the challenges of using DLT for the exchange of personal data in general and digital identity management systems in particular. We have also shown how these problems can be solved by using SSI on top of the blockchain layer. Second, we have revealed implications of designing SSI-based solutions built on blockchain in contexts of KYC by deriving three design principles, which allowed us to elevate our IT artifact for more abstract and generalizable theoretical discussion (Gregor and Hevner, 2013). Third, we suggested avenues for relevant further research on blockchain and SSI, enabling researchers to base their work on our results and thus generate additional knowledge (Vom Brocke et al., 2020). Our conception and evaluation of the SSI-based KYC framework allows practitioners to gain valuable insights regarding design choices, DLT's role, the intricacies of regulation, and related challenges and opportunities for banks and customers. Our results indicate that SSI-based eKYC processes can both reduce cost and time expenditures and contribute to better user experiences and increased security during the KYC process. In addition, we have also demonstrated how the use of SSI can improve the different onboarding processes and their interplay with an existing SSI ecosystem.

Drawing on the lessons learned in *Essay 2*, for the design of the decentralized IS conceptualized in *Essay 3* we made only minimal use of blockchain as a data store. Instead, we decentralized the storage of information even more, through outsourcing it to data owners themselves by implementing the system on the principles of SSI, and relying on blockchain technology only for storing small amounts of public data.

5.4 Essay 4: Harmonizing Sensitive Data Exchange and Double-spending Prevention: The Case of e-Prescription Management

To solve the challenges of harmonizing sensitive data exchange and double-spending prevention, we studied the case of e-prescriptions and designed and implemented a decentralized e-prescription management system using blockchain technology and SSI digital wallets. We evaluated the proposed system along requirements derived from a literature review. As our evaluation suggests, SSI can avoid data silos and provide a standardized interface for the exchange of verifiable information, whereas blockchains can solve the challenge of transferring value in a decentralized system. In contrast, blockchains cannot be used for the exchange of verifiable, sensitive information because of their inherent replication and immutability; yet, they allow for control on the number of usages of VCs across different bilateral interactions. Consequently, we derived the following corresponding design principles: *(1)* Use verifiable credentials stored in a digital wallet to provide sensitive and verifiable user information to services. *(2)* Implement vouchers through creating a token and adding its spending secret to the digital certificate. This benefits usability and ease of implementation because users do not require a mobile app beyond their digital wallet. *(3)* Create additional value by building an ecosystem in which VCs can be combined and used repeatedly in different contexts.

Thus, we contributed both a generic design and an illustrative implementation of an e-prescription management system. Our findings offer insights into the opportunities and remaining challenges of developing decentralized IS dealing with sensitive data and business logic that involves multiple stakeholders. Our design and implementation also aid practitioners in developing IS beyond the health sector with similar requirements. Our findings indicate that, first, the role and necessity of applying blockchain technology in the context of SSI systems remain debatable. Second, SSI and blockchain technologies are characterized by open-source software philosophies and are often freely available. Moreover, the respective technologies do not include a centralized, controlling party by design. Therefore, the stakeholders need to establish adequate governance structures to ensure the creation of a functioning ecosystem. Third, prior research indicates that the acceptance and usefulness of e-prescriptions increases when the required functionalities are embedded in a larger ecosystem (Tamblyn et al., 2006). This could, for example, include generic systems for managing and exchanging patient health data. To this end, the generic nature of the components used in SSI systems can provide several promising opportunities.

Fourth, by combining SSI and blockchain, we suppose that our solution should address several regulations, especially those of the EU GDPR.

Combining the insights obtained in *Essays 2 et seq.*, for the design proposed in *Essay 4* we refined the role of blockchain technology in decentralized IS. Whereas SSI offers the opportunity to distribute the information of individual entities to their respective infrastructures as VC, most implementations to date do not offer the option of guaranteeing single use of the respective VCs. We solved this problem by linking the VC to a blockchain-based token that can be spent only once, thus proposing a promising combination of the two decentralized IS.

6 Discussion and Conclusion

This section concludes the introduction of my dissertation. After summarizing the contents of this introduction, I discuss the theoretical and practical implications of my dissertation as a whole. To conclude, I reflect on the limitations of my research and describe opportunities for future research.

6.1 Summary

Guided by the central research aim of elucidating *how to design decentralized IS based on blockchain technology to shape digitalization beneficially*, in this dissertation I elaborated on analyzing cybersecurity challenges of blockchain-based systems and developing design knowledge on these systems in different application domains. Previous work on designing IS and early research on designing blockchain-based systems in particular provided the primary lenses for my scientific discourse. Motivated by four research questions, this dissertation consists of four corresponding essays. In *Essay 1*, we analyzed the attacks on blockchain-based systems and assigned them to common attack vectors, subsequently deriving a research framework and agenda for IS research on the cybersecurity of blockchain-based systems. In *Essays 2–3* we developed design guidelines for decentralized IS based on blockchain technology in the realms of IoT, eKYC, and digital healthcare, respectively.

6.2 Contributions to Theory and Implications for Practice

In light of its overarching research aim, this dissertation contributes to both theory and practice. Taking a socio-technical perspective on IS (Bostrom and Heinen, 1977), I aimed to answer calls for design knowledge on decentralized blockchain-based IS (Beck et al., 2017; Sedlmeir et al., 2021b) through research influenced by pragmatism (Goldkuhl, 2012). Thus, the four essays in this dissertation offer abstract and generically applicable design knowledge derived through rigorous method (Gregor and Hevner, 2013), therefore laying a foundation for future research on this topic (Vom Brocke et al., 2020). Concurrently,

they provide guidance for practitioners on how to design decentralized blockchain-based IS systems, by working with concrete IT artifacts and including insights from practice in formative and summative evaluations.

This dissertation makes four main theoretical contributions to the literature. First, I introduce and develop a socio-technical perspective to IS research on blockchain-based systems (Bostrom and Heinen, 1977). This is particularly reflected in the introduction of a socio-technical research framework on blockchain-based IS' security and related avenues for future research in *Essay 1*, as well as in embedding IT artifacts inside specific application areas, as in *Essays 2–4*. Thus, I answer recent calls for a stronger focus on understanding IS as socio-technical systems by research (Sarker et al., 2019). Second, I abstract and generalize insights from developing technical artifacts in *Essays 2–4* to more broadly applicable design knowledge, such as DPs (Gregor and Hevner, 2013). Observed over time, the essays' findings regarding the design of decentralized IS based on blockchain build on each other; for instance, because *Essay 2* investigates and critically evaluates the use of a blockchain as the main backend infrastructure, it only plays a supportive part through storing SSI elements in *Essay 3*. *Essay 4* in turn combines an SSI infrastructure with a blockchain-based token, illustrating the iterative quest for the most suitable configuration of both decentralized technologies in practical settings (Beck et al., 2013). Third, I provide insights into the design process for IT systems facing both low solution maturity and high application domain maturity (Gregor and Hevner, 2013). Thus, research on emerging technology beyond the technologies in this dissertation can benefit from my findings by reproducing its research procedures. Fourth, I critically evaluate the role and promises of blockchain technology in IS, which is in stark contrast to the almost euphoric understanding of the technology in prior IS literature (Frizzo-Barker et al., 2020; Hughes et al., 2019). Thus, I aim to promote a more differentiated understanding of blockchain technology in IS and urge scholars to adhere to critical realism in their research (Mingers, 2004).

In addition, my dissertation makes three main practical contributions. First, I offer a comprehensive overview of the attacks and attack vectors on blockchain-based systems, thereby guiding practitioners on how to secure their systems against possible attacks. In doing so, I offer an integrative perspective on the socio-technical aspects of cybersecurity (Baxter and Sommerville, 2011; Bostrom and Heinen, 1977). Second, I provide concrete guidelines for the design of blockchain-based decentralized IS. This allows practitioners to build on my insights and adapt them to their particular environment (Gregor and Hevner, 2013; Hevner et al., 2004; March and Smith, 1995). Third, by taking a pragmatist position in designing and developing decentralized IS based on blockchain technology, I enable practitioners

to apply the methods for establishing systems based on the emerging technology used in my dissertation. Blockchain and SSI are both technologies of early maturity. Thus, the practical guidelines and insights from my essays should prove useful for those aiming to develop systems facing similar immaturity.

6.3 Limitations

The design of decentralized IS is a complex and challenging task. Just like in any IS, the influential factors from the IT, people, and organizations comprising the system must be aligned to solve a specific challenge (Österle et al., 2011). However, this is particularly complex given that these elements are under constant change (Baskerville et al., 2018). In light of this complexity, my research is not without limitations. Next, I discuss the general limitations of this dissertation, because the specific limitations of my essays are discussed within.

A limitation to the applicability and relevance of my findings in practice relates to the nature of my research settings. Because I investigated emerging technology paradigms and theory, the artifacts resulting from my research were not evaluated in actual use, but largely remained proofs of concept. A practical perspective was introduced by including insights from and assessment of practitioners through expert interviews (*Essays 2 and 3*), as well as performance simulation (*Essay 4*). Yet, the artifacts were not employed in settings relating to their intended use in practice. Nevertheless, I acknowledge that the mutual impacts and relations between entities within IS can be observed best in their natural setting and context (Darke et al., 1998; Myers, 1997).

Furthermore, the results presented in this dissertation reflect the state of technology, theory, and empirical insight at a point in time. Thus, certain results may change through developments in either of these, rendering prior research less relevant. As the term indicates, emerging technologies evolve. Therefore, this observation is especially relevant in the context of my dissertation. For instance, the realization of a proposed switch to a proof-of-stake consensus algorithm in Ethereum[1] may render some results of *Essay 1* less relevant already. To counterbalance the impact of specific developments in IT, people, or organizations, I aimed at deriving abstract and generic knowledge through developing research frameworks or DPs (Gregor and Hevner, 2013).

1 https://ethereum.org/en/upgrades/merge/

The methodology employed in the research throughout my dissertation is mainly qualitative-empirical. Given the research aim, this kind of methodology facilitated context-rich insights into the questions investigated. However, the outcomes are naturally limited by the context given through our insights and those of the interviewed experts as well as of the available theory. To soften this limitation, care has been taken in the selection of interviewees as well as available theory through a stringent literature collection methodology, and in the formation of interdisciplinary research teams with varying levels of experience.

6.4 Future Research

In light of the original research goal motivating this dissertation, and the remaining limitations, several opportunities for future research emerge.

A coherent assessment of the impact of the artifacts developed in this dissertation requires their embedding in realistic, practical settings (Darke et al., 1998; Myers, 1997). Thus, pursuing research on the practical implementation of the developed artifacts is a main direction for future research. Practice-oriented research approaches, such as action design research (ADR) (Sein et al., 2011) or case study research (Eisenhardt, 1989; Yin, 2011), can provide rich insights and elevate both the theoretical and the practical impact of my dissertation. With growing technical maturity, more real-world implementations of decentralized IS based on blockchain technology will emerge, as well as corresponding research settings. In the context of my dissertation, they could, for example, include adding real-world attacks to the dataset and updating the derived artifacts (*Essay 1*) or employing the designs developed in settings representing their actual intended use (*Essays 2–4*).

IT is constantly developing and changing. During the writing of this dissertation, blockchain technology alone experienced several advancements. For instance, scalability has consistently been considered a limitation of blockchain technology (e.g., Xie et al., 2019), which is also strongly reflected in the evaluation of *Essay 2*. However, recent technical advancements, such as in the field of ZK-rollups (Gudgeon et al., 2020; Sedlmeir et al., 2021a), significantly advanced the scalability of blockchain-based systems to competitive levels. Comparable to this development, privacy has often been considered diametrical to the transparency usually required in blockchain systems. Technological developments leveraging zero-knowledge proof (ZKP) (e.g., in Zcash) revert this (Hopwood et al., 2022). Research should observe and incorporate these developments, constantly re-evaluating the

outcome of prior studies in longitudinal observations. This practice may consequently support the identification of generalizable knowledge.

This dissertation mainly builds on constructivist methodology, evident in the choice of research methods used. Yet, research indicates that methodical pluralism leads to richer results (Mingers, 2001). With a growing maturity of blockchain technology, more data and practical implementations will be observable in practice, and theory will begin to substantiate. This may allow for more choice in research methods and, in particular, quantitative observations over longer periods of time. Thus, insights on the design of decentralized IS can be gained through the thorough analysis of successful implementations and combination of several research methods. Research in comparable technology domains that have undergone similar developments serves as a motivating example (e.g. Rymaszewska et al., 2017 for the IoT).

While the dynamically changing environment of decentralized IS can be difficult to oversee in its entirety, I am convinced it is one promising field with the potential to provide meaningful advance for humanity. Thus, I hope this dissertation contributes a useful part to the whole of research on designing decentralized IS.

7 References

Abadi, F., Ellul, J., and Azzopardi, G. (2018). "The Blockchain of Things, Beyond Bitcoin: A Systematic Review". In: *The 1st International Workshop on Blockchain for the Internet of Things*. IEEE.

Agre, P. E. (2003). "P2P and the Promise of Internet Equality". In: *Communications of the ACM* 46 (2), pp. 39–42.

Aldughayfiq, B. and Sampalli, S. (2021). "Digital Health in Physicians' and Pharmacists' Office: A Comparative Study of e-Prescription Systems' Architecture and Digital Security in Eight Countries". In: *OMICS: A Journal of Integrative Biology* 25 (2), pp. 1–21.

Allen, C. (2016). *The Path to Self-Sovereign Identity*. `http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html`. Online; accessed 2021-11-23.

Alter, S. (2008). "Defining Information Systems as Work Systems: Implications for the IS Field". In: *European Journal of Information Systems* 17 (5), pp. 448–469.

Amend, J., Fridgen, G., Rieger, A., Roth, T., and Stohr, A. (2021). "The Evolution of an Architectural Paradigm – Using Blockchain to Build a Cross-Organizational Enterprise Service Bus". In: *54th Hawaii International Conference on System Sciences*, pp. 4301–4310.

Arner, D. W., Zetzsche, D. A., Buckley, R. P., and Barberis, J. N. (2019). "The Identity Challenge in Finance: From Analogue Identity to Digitized Identification to Digital KYC Utilities". In: *European Business Organization Law Review* 20 (1), pp. 55–80.

Baran, P. (1964). "On Distributed Communications Networks". In: *IEEE Transactions on Communications Systems* 12 (1), pp. 1–9.

Baskerville, R. (1993). "Information Systems Security Design Methods: Implications for Information Systems Development". In: *ACM Computing Surveys* 25 (4), pp. 375–414.

Baskerville, R. (2008). "What Design Science Is Not". In: *European Journal of Information Systems* 17 (5), pp. 441–443.

Baskerville, R., Baiyere, A., Gregor, S., Hevner, A. R., and Rossi, M. (2018). "Design Science Research Contributions: Finding a Balance Between Artifact and Theory". In: *Journal of the Association for Information Systems* 19 (5), p. 3.

Baxter, G. and Sommerville, I. (2011). "Socio-technical Systems: From Design Methods to Systems Engineering". In: *Interacting with computers* 23 (1), pp. 4–17.

Beck, R., Avital, M., Rossi, M., and Thatcher, J. B. (2017). "Blockchain Technology in Business and Information Systems Research". In: *Business & Information Systems Engineering* 59 (6), pp. 381–384.

Beck, R., Müller-Bloch, C., and King, J. L. (2018). "Governance in the Blockchain Economy: A Framework and Research Agenda". In: *Journal of the Association for Information Systems* 19 (10), p. 1.

Beck, R., Weber, S., and Gregory, R. W. (2013). "Theory-Generating Design Science Research". In: *Information Systems Frontiers* 15 (4), pp. 637–651.

Benbasat, I. and Zmud, R. W. (2003). "The Identity Crisis Within the IS Discipline: Defining and Communicating the Discipline's Core Properties". In: *MIS Quarterly*, pp. 183–194.

Bestsennyy, O., Gilbert, G., Harris, A., and Rost, J. (2021). *Telehealth: A Quarter-Trillion-Dollar post-COVID-19 Reality?* `https://www.mckinsey.com/industries/healthcare-systems-and-services/our-insights/telehealth-a-quarter-trillion-dollar-post-covid-19-reality`. Online; accessed 2021-11-23.

Bloomfield, B. P. and Coombs, R. (1992). "Information Technology, Control and Power: The Centralization and Decentralization Debate Revisited". In: *Journal of Management Studies* 29 (4), pp. 459–459.

Bocek, T., Rodrigues, B. B., Strasser, T., and Stiller, B. (2017). "Blockchains Everywhere – a Use-Case of Blockchains in the Pharma Supply-Chain". In: *2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*, pp. 772–777.

Boell, S. K. and Cecez-Kecmanovic, D. (2015). "What Is an Information System?" In: *48th Hawaii International Conference on System Sciences*, pp. 4959–4968.

Bostrom, R. P. and Heinen, J. S. (1977). "MIS Problems and Failures: A Socio-Technical Perspective, Part II: The Application of Socio-Technical Theory". In: *MIS Quarterly* 1 (3), pp. 11–28.

Botta, A., Donato, W. de, Persico, V., and Pescapé, A. (2014). "On the Integration of Cloud Computing and Internet of Things". In: *2014 International Conference on Future Internet of Things and Cloud (FiCloud)*, pp. 23–30.

Buterin, V. et al. (2014). *A Next-Generation Smart Contract and Decentralized Application Platform*. `https://ethereum.org/669c9e2e2027310b6b3cdce6e1c52962/Ethereum_Whitepaper_-_Buterin_2014.pdf`. Online; accessed 2022-06-25.

Butijn, B.-J., Tamburri, D. A., and Heuvel, W.-J. v. d. (2020). "Blockchains: A Systematic Multivocal Literature Review". In: *ACM Computing Surveys* 53 (3), pp. 1–37.

Casino, F., Dasaklis, T. K., and Patsakis, C. (2019). “A Systematic Literature Review of Blockchain-Based Applications: Current Status, Classification and Open Issues”. In: *Telematics and Informatics* 36, pp. 55–81.

Chanson, M., Bogner, A., Bilgeri, D., Fleisch, E., and Wortmann, F. (2019). “Blockchain for the IoT: Privacy-Preserving Protection of Sensor Data”. In: *Journal of the Association for Information Systems* 20 (9), pp. 1272–1307.

Chaum, D. (1985). “Security Without Identification: Transaction Systems to Make Big Brother Obsolete”. In: *Communications of the ACM* 28 (10), pp. 1030–1044.

Chaum, D., Fiat, A., and Naor, M. (1988). “Untraceable Electronic Cash”. In: *Conference on the Theory and Application of Cryptography*. Springer, pp. 319–327.

Chenthara, S., Ahmed, K., Wang, H., Whittaker, F., and Chen, Z. (2020). “Healthchain: A Novel Framework on Privacy Preservation of Electronic Health Records Using Blockchain Technology”. In: *PLoS one* 15 (12), pp. 1–35.

Cong, L. W. and He, Z. (2019). “Blockchain Disruption and Smart Contracts”. In: *The Review of Financial Studies* 32 (5), pp. 1754–1797.

Conoscenti, M., Vetro, A., and De Martin, J. C. (2016). “Blockchain for the Internet of Things: A Systematic Literature Review”. In: *IEEE/ACS 13th International Conference of Computer Systems and Applications*, pp. 1–6.

Darke, P., Shanks, G., and Broadbent, M. (1998). “Successfully Completing Case Study Research: Combining Rigour, Relevance and Pragmatism”. In: *Information Systems Journal* 8 (4), pp. 273–289.

Davis, G. and Olson, M. (1985). *Management Information Systems: Conceptual Foundations, Structure, and Development*. McGraw-Hill, New York, NY.

De Nardis, L. (2014). *The Global War for Internet Governance*. Yale University Press.

Dumas, M., Van der Aalst, W. M., and Ter Hofstede, A. H. (2005). *Process-Aware Information Systems: Bridging People and Software Through Process Technology*. John Wiley & Sons.

Ehrenberg, A. J. and King, J. L. (2020). “Blockchain in Context”. In: *Information Systems Frontiers* 22 (1), pp. 29–35.

Ehrlich, T., Richter, D., Meisel, M., and Anke, J. (2021). “Self-Sovereign Identity als Grundlage für universell einsetzbare digitale Identitäten”. In: *HMD Praxis der Wirtschaftsinformatik* 58 (2), pp. 247–270.

Ein-Dor, P. and Segev, E. (1978). “Centralization, Decentralization and Management Information Systems”. In: *Information & Management* 1 (3), pp. 169–172.

Eisenhardt, K. M. (1989). “Building Theories From Case Study Research”. In: *Academy of Management Review* 14 (4), pp. 532–550.

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

Feder, A., Gandal, N., Hamrick, J. T., and Moore, T. (2017). "The Impact of DDoS and Other Security Shocks on Bitcoin Currency Exchanges: Evidence From MT. Gox". In: *Journal of Cybersecurity* 3 (2), pp. 137–144.

Ferdous, M. S., Chowdhury, F., and Alassafi, M. O. (2019). "In Search of Self-Sovereign Identity Leveraging Blockchain Technology". In: *IEEE Access* 7, pp. 103059–103079.

Fernández-Caramés, T. M. and Fraga-Lamas, P. (2018). "A Review on the Use of Blockchain for the Internet of Things". In: *IEEE Access* 6, pp. 32979–33001.

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

Fridgen, G., Radszuwill, S., Urbach, N., and Utz, L. (2018). "Cross-Organizational Workflow Management Using Blockchain Technology? Towards Applicability, Auditability, and Automation". In: *51st Hawaii International Conference on System Sciences*, pp. 3507–3516.

Frizzo-Barker, J., Chow-White, P. A., Adams, P. R., Mentanko, J., Ha, D., and Green, S. (2020). "Blockchain as a Disruptive Technology for Business: A Systematic Review". In: *International Journal of Information Management* 51, p. 102029.

Glaser, F. (2017). "Pervasive Decentralisation of Digital Infrastructures: A Framework for Blockchain Enabled System and Use Case Analysis". In: *50th Hawaii International Conference on System Sciences*, pp. 1543–1552.

Goldkuhl, G. (2012). "Pragmatism vs Interpretivism in Qualitative Information Systems Research". In: *European Journal of Information Systems* 21 (2), pp. 135–146.

Gregor, S. (2006). "The Nature of Theory in Information Systems". In: *MIS Quarterly* 30 (3), pp. 611–642.

Gregor, S. and Hevner, A. R. (2013). "Positioning and Presenting Design Science Research for Maximum Impact". In: *MIS Quarterly* 37 (2), pp. 337–355.

Grover, V. and Lyytinen, K. (2015). "New State of Play in Information Systems Research". In: *MIS Quarterly* 39 (2), pp. 271–296.

Gubbi, J., Buyya, R., Marusic, S., and Palaniswami, M. (2013). "Internet of Things (Iot): A Vision, Architectural Elements, and Future Directions". In: *Future Generation Computer Systems* 29 (7), pp. 1645–1660.

Gudgeon, L., Moreno-Sanchez, P., Roos, S., McCorry, P., and Gervais, A. (2020). "Sok: Layer-two Blockchain Protocols". In: *International Conference on Financial Cryptography and Data Security*. Springer, pp. 201–226.

Guggenberger, T., Lockl, J., Röglinger, M., Schlatt, V., Sedlmeir, J., Stoetzer, J.-C., Urbach, N., and Völter, F. (2021). "Emerging Digital Technologies to Combat Future Crises: Learnings From COVID-19 to be Prepared for the Future". In: *International Journal of Innovation and Technology Management* 4 (18).

Guggenmoos, F., Lockl, J., Rieger, A., Wenninger, A., and Fridgen, G. (2020). "How to Develop a GDPR-Compliant Blockchain Solution for Cross-Organizational Workflow Management: Evidence from the German Asylum Procedure". In: *53th Hawaii International Conference on Systems Science*, pp. 4023–4032.

Haber, S. and Stornetta, W. S. (1990). "How to Time-stamp a Digital Document". In: *Conference on the Theory and Application of Cryptography*. Springer, pp. 437–455.

Hardman, D. (2019). *A Gentle Introduction to Verifiable Credentials*. `https://www.evernym.com/blog/gentle-introduction-verifiable-credentials/`. Online; accessed 2021-11-23.

He, M., Han, X., Jiang, F., Zhang, R., Liu, X., and Liu, X. (2019). "BlockMeds: A Blockchain-Based Online Prescription System with Privacy Protection". In: *International Conference on Service-Oriented Computing*, pp. 299–303.

Hevner, A. R. and Gregor, S. (2020). "Envisioning Entrepreneurship and Digital Innovation through a Design Science Research Lens: A Matrix Approach". In: *Information & Management* 59 (3), p. 103350.

Hevner, A. R., March, S. T., Park, J., and Ram, S. (2004). "Design Science in Information Systems Research". In: *MIS Quarterly* 28 (1), pp. 75–105.

Hopwood, D., Bowe, S., Hornby, T., and Wilcox, N. (2022). *Zcash Protocol Specification*. `https://zips.z.cash/protocol/protocol.pdf`. Online; accessed 2022-05-01.

Hughes, L., Dwivedi, Y. K., Misra, S. K., Rana, N. P., Raghavan, V., and Akella, V. (2019). "Blockchain Research, Practice and Policy: Applications, Benefits, Limitations, Emerging Research Themes and Research Agenda". In: *International Journal of Information Management* 49, pp. 114–129.

Hugoson, M.-Å. (2007). "Centralized Versus Decentralized Information Systems". In: *IFIP Conference on History of Nordic Computing*. Springer, pp. 106–115.

Isaak, J. and Hanna, M. J. (2018). "User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection". In: *Computer* 51 (8), pp. 56–59.

Jamil, F., Hang, L., Kim, K., and Kim, D. (2019). "A Novel Medical Blockchain Model for Drug Supply Chain Integrity Management in a Smart Hospital". In: *Electronics* 8 (5), pp. 1–32.

Jones, D. and Gregor, S. (2007). "The anatomy of a design theory". In: *Journal of the Association for Information Systems* 8 (5), pp. 312–335.

Kahai, P. S., Carr, H. H., and Snyder, C. A. (2003). "Technology and the Decentralization of Information Systems". In: *Information Systems Management* 20 (3), pp. 51–60.

Kannengießer, N., Lins, S., Dehling, T., and Sunyaev, A. (2020). "Trade-Offs Between Distributed Ledger Technology Characteristics". In: *ACM Computing Surveys* 53 (2), pp. 1–37.

Karger, E. (2020). "Combining Blockchain and Artificial Intelligence – Literature Review and State of the Art". In: *41st International Conference on Information Systems*, pp. 1–17.

Katuwal, G. J., Pandey, S., Hennessey, M., and Lamichhane, B. (2018). *Applications of Blockchain in Healthcare: Current Landscape & Challenges*. `https://arxiv.org/pdf/1812.02776`. Online; accessed 2021-11-23.

Kim, J. W., Lee, A. R., Kim, M. G., Kim, I. K., and Lee, E. J. (2019). "Patient-Centric Medication History Recording System Using Blockchain". In: *IEEE International Conference on Bioinformatics and Biomedicine*, pp. 1513–1517.

Kitchenham, B. A. and Charters, S. (2007). "Guidelines for Performing Systematic Literature Reviews in Software Engineering". In: *EBSE Technical Report EBSE-2007-01*.

Kolb, J., Abdel Baky, M., Katz, R. H., and Culler, D. E. (2020). "Core Concepts, Challenges, and Future Directions in Blockchain: A Centralized Tutorial". In: *ACM Computing Surveys* 53 (1), pp. 1–39.

Kshetri, N. (2017). "Can Blockchain Strengthen the Internet of Things?" In: *IT Professional* 19 (4), pp. 68–72.

Kuperberg, M. (2019). "Blockchain-Based Identity Management: A Survey From the Enterprise and Ecosystem Perspective". In: *IEEE Transactions on Engineering Management* 67 (4), pp. 1008–1027.

Kurzweil, R. (2005). *The Singularity Is Near: When Humans Transcend Biology*. Penguin.

Land, F. (1985). "Is an Information Theory Enough?" In: *The Computer Journal* 28 (3), pp. 211–215.

Land, F. (1992). "The Information Systems Domain". In: *Information Systems Research – Issues, Methods and Practical Guidelines*. Ed. by R. Galliers. Alfred Waller Ltd., Warwick, pp. 6–13.

Le Bris, A. and El Asri, W. (2016). *State of Cybersecurity & Cyber Threats in Healthcare Organizations*. `https://blogs.harvard.edu/cybersecurity/files/2017/01/risks-and-threats-healthcare-strategic-report.pdf`. Online; accessed 2021-11-23.

Lee, A. (1999). "Inaugural Editor's Comments". In: *MIS Quarterly*, pp. v–xi.

Lee, A. S. (2001). "Editor's Comments: Research in Information Systems: What We Haven't Learned". In: *MIS Quarterly* 25 (4), p. v.

Legner, C., Eymann, T., Hess, T., Matt, C., Böhmann, T., Drews, P., Mädche, A., Urbach, N., and Ahlemann, F. (2017). "Digitalization: Opportunity and Challenge for the Business and Information Systems Engineering Community". In: *Business & Information Systems Engineering* 59 (4), pp. 301–308.

Leifer, R. (1988). "Matching Computer-Based Information Systems With Organizational Structures". In: *MIS Quarterly* 12 (1), pp. 63–73.

Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., Postel, J., Roberts, L. G., and Wolff, S. (2009). "A Brief History of the Internet". In: *ACM SIGCOMM Computer Communication Review* 39 (5), pp. 22–31.

Lin, C., He, D., Huang, X., Choo, K.-K. R., and Vasilakos, A. V. (2018). "BSeIn: A Blockchain-Based Secure Mutual Authentication With Fine-Grained Access Control System for Industry 4.0". In: *Journal of network and computer applications* 116, pp. 42–52.

Lindman, J., Tuunainen, V. K., and Rossi, M. (2017). "Opportunities and Risks of Blockchain Technologies – A Research Agenda". In: *50th Hawaii International Conference on System Sciences*, pp. 1533–1542.

Liu, B., Yu, X. L., Chen, S., Xu, X., and Zhu, L. (2017). "Blockchain Based Data Integrity Service Framework for Iot Data". In: *2017 IEEE International Conference on Web Services*, pp. 468–475.

Liu, Y., Lu, Q., Paik, H.-Y., Xu, X., Chen, S., and Zhu, L. (2020). "Design Pattern as a Service for Blockchain-Based Self-Sovereign Identity". In: *IEEE Software* 37 (5), pp. 30–36.

Lockl, J., Schlatt, V., Schweizer, A., Urbach, N., and Harth, N. (2020). "Toward Trust in Internet of Things (IoT) Ecosystems: Design Principles for Blockchain-Based IoT Applications". In: *IEEE Transactions on Engineering Management* 67 (4), pp. 1256–1270.

Lord, N. (2020). *Top 10 Biggest Healthcare Data Breaches of All Time*. `https://digitalguardian.com/blog/top-10-biggest-healthcare-data-breaches-all-time`. Online; accessed 2021-11-23.

Mahatpure, J., Motwani, M., and Shukla, P. K. (2019). "An Electronic Prescription System Powered by Speech Recognition, Natural Language Processing and Blockchain Technology". In: *International Journal of Scientific & Technology Research* 8 (8), pp. 1454–1462.

Makhdoom, I., Abolhasan, M., Abbas, H., and Ni, W. (2019). "Blockchain's Adoption in Iot: The Challenges, and a Way Forward". In: *Journal of Network and Computer Applications* (125), pp. 251–279.

March, S. T. and Smith, G. F. (1995). "Design and Natural Science Research on Information Technology". In: *Decision Support Systems* 15 (4), pp. 251–266.

Mattke, J., Maier, C., and Hund, A. (2019). "How an Enterprise Blockchain Application in the U.S. Pharmaceuticals Supply Chain is Saving Lives". In: *MIS Quarterly Executive* 18 (4), pp. 245–261.

Mehar, M. I., Shier, C. L., Giambattista, A., Gong, E., Fletcher, G., Sanayhie, R., Kim, H. M., and Laskowski, M. (2019). "Understanding a Revolutionary and Flawed Grand Experiment in Blockchain: The DAO Attack". In: *Journal of Cases on Information Technology* 21 (1), pp. 19–32.

Mendling, J., Weber, I., Aalst, W., vom Brocke, J., Cabanillas, C., Daniel, F., Debois, S., Di Ciccio, C., Dumas, M., Dustdar, S., Gal, A., García-Bañuelos, L., Governatori, G., Hull, R., La Rosa, M., Leopold, H., Leymann, F., Recker, J., Reichert, M., and Zhu, L. (2018). "Blockchains for Business Process Management – Challenges and Opportunities". In: *ACM Transactions on Management Information Systems* 9 (1), pp. 1–16.

Merkle, R. C. (1978). "Secure Communications Over Insecure Channels". In: *Communications of the ACM* 21 (4), pp. 294–299.

Mingers, J. (2001). "Combining IS Research Methods: Towards a Pluralist Methodology". In: *Information Systems Research* 12 (3), pp. 240–259.

Mingers, J. (2004). "Real-izing Information Systems: Critical Realism as an Underpinning Philosophy for Information Systems". In: *Information and Organization* 14 (2), pp. 87–103.

Moyano, J. P. and Ross, O. (2017). "KYC Optimization Using Distributed Ledger Technology". In: *Business & Information Systems Engineering* 59 (6), pp. 411–423.

Mühle, A., Grüner, A., Gayvoronskaya, T., and Meinel, C. (2018). "A Survey on Essential Components of a Self-Sovereign Identity". In: *Computer Science Review* 30, pp. 80–86.

Mundy, D. and Chadwick, D. W. (2002). "A System for Secure Electronic Prescription Handling". In: *The Hospital of the Future, Second International Conference On The Management Of Healthcare And Medical Technology*.

Myers, M. D. (1997). "Qualitative Research in Information Systems." In: *MIS Quarterly* 21 (2).

Myers, M. D. and Newman, M. (2007). "The Qualitative Interview in Is Research: Examining the Craft". In: *Information and Organization* 17 (1), pp. 2–26.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://bitcoin.org/bitcoin.pdf. Online; accessed 2018-07-31.

Nickerson, R. C., Varshney, U., and Muntermann, J. (2013). "A Method for Taxonomy Development and Its Application in Information Systems". In: *European Journal of Information Systems* 22 (3), pp. 336–359.

Nunamaker Jr, J. F., Chen, M., and Purdin, T. D. (1990). "Systems Development in Information Systems Research". In: *Journal of Management Information Systems* 7 (3), pp. 89–106.

Oliveira, L., Zavolokina, L., Bauer, I., and Schwabe, G. (2018). "To Token or Not to Token: Tools for Understanding Blockchain Tokens". In: *39th International Conference on Information Systems*, pp. 1–17.

Orlikowski, W. J. (1992). "The Duality of Technology: Rethinking the Concept of Technology in Organizations". In: *Organization Science* 3 (3), pp. 398–427.

Orlikowski, W. J. and Iacono, C. S. (2001). "Research Commentary: Desperately Seeking " It" in It Research-a Call to Theorizing the It Artifact". In: *Information Systems Research* 12 (2), p. 121.

Österle, H., Becker, J., Frank, U., Hess, T., Karagiannis, D., Krcmar, H., Loos, P., Mertens, P., Oberweis, A., and Sinz, E. J. (2011). "Memorandum on Design-Oriented Information Systems Research". In: *European Journal of Information Systems* 20 (1), pp. 7–10.

Peffers, K., Tuunanen, T., Rothenberger, M. A., and Chatterjee, S. (2007). "A Design Science Research Methodology for Information Systems Research". In: *Journal of Management Information Systems* 24 (3), pp. 45–77.

Perlman, L. and Gurung, N. (2019). *Focus Note: The Use of eKYC for Customer Identity and Verification and AML*. https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3370665_code505438.pdf?abstractid=3370665&mirid=1. Online; accessed: 2020-07-24.

Pilkington, M. (2016). "Blockchain Technology: Principles and Applications". In: *Research Handbook on Digital Transformations*. Cheltenham, UK: Edward Elgar Publishing.

Preukschat, A. and Reed, D. (2021). *Self-Sovereign Identity: Decentralized Digital Identity and Verifiable Credentials*. Shelter Island, NY: Manning.

Raghavendra, M. (2019). "Can Blockchain Technologies Help Tackle the Opioid Epidemic: A Narrative Review". In: *Pain Medicine* 20 (10), pp. 1884–1889.

Rajput, A. and Gopinath, K. (2017). "Towards a More Secure Aadhaar". In: *International Conference on Information Systems Security*. Springer, pp. 283–300.

Reinecke, K. and Bernstein, A. (2013). "Knowing What a User Likes: A Design Science Approach to Interfaces that Automatically Adapt to Culture". In: *MIS Quarterly* 37 (2), pp. 427–453.

Reyna, A., Martin, C., Chen, J., Soler, E., and Diaz, M. (2018). "On Blockchain and Its Integration With Iot. Challenges and Opportunities". In: *Future Generation Computer Systems* 88, pp. 173–190.

Rieger, A., Guggenmos, F., Lockl, J., Fridgen, G., and and Urbach, N. (2019). "Building a Blockchain Application that Complies with the EU General Data Protection Regulation". In: *MIS Quarterly Executive* 18 (4), pp. 263–279.

Rockart, J. F. and Leventer, J. S. (1976). *Centralization vs Decentralization of Information Systems: A Critical Survey of Current Literature*. MIT Center for Information Systems Research.

Rossi, M., Mueller-Bloch, C., Thatcher, J. B., and Beck, R. (2019). "Blockchain Research in Information Systems: Current Trends and an Inclusive Future Research Agenda". In: *Journal of the Association for Information Systems* 20 (9), pp. 1390–1405.

Roy, G. G. R. and Kumar, S. B. R. (2019). "An Architecture to Enable Secure Firmware Updates on a Distributed-Trust IoT Network Using Blockchain". In: *International Conference on Computer Networks and Communication Technologies*, pp. 671–679.

Ruby, B., Ganesh, K., Murugamantham, B., and Murugan, A. (2020). "Authentic Drug Usage and Tracking with Blockchain Using Mobile Apps". In: *International Journal of Interactive Mobile Technologies* 14 (17), pp. 20–31.

Ruutu, S., Casey, T., and Kotovirta, V. (2017). "Development and Competition of Digital Service Platforms: A System Dynamics Approach". In: *Technological Forecasting and Social Change* 117, pp. 119–130.

Rymaszewska, A., Helo, P., and Gunasekaran, A. (2017). "Iot Powered Servitization of Manufacturing – An Exploratory Case Study". In: *International Journal of Production Economics* 192, pp. 92–105.

Saad, M., Spaulding, J., Njilla, L., Kamhoua, C., Shetty, S., Nyang, D. H., and Mohaisen, D. (2020). "Exploring the Attack Surface of Blockchain: A Comprehensive Survey". In: *IEEE Communications Surveys & Tutorials* 22 (3), pp. 1977–2008.

Salah, K., Rehman, M. H. U., Nizamuddin, N., and Al-Fuqaha, A. (2019). "Blockchain for AI: Review and Open Research Challenges". In: *IEEE Access* 7, pp. 10127–10149.

Saldaña, J. (2015). *The Coding Manual for Qualitative Researchers*. Sage.

Samaniego, M. and Deters, R. (2016). "Blockchain as a Service for IoT". In: *IEEE International Conference on Internet of Things (iThings)*, pp. 433–436.

Sarker, S., Chatterjee, S., Xiao, X., and Elbanna, A. R. (2019). "The Sociotechnical Axis of Cohesion for the IS Discipline: Its Historical Legacy and its Continued Relevance". In: *MIS Quarterly* 43.

Schellinger, B., Völter, F., Urbach, N., and Sedlmeir, J. (2022). "Yes, I Do: Marrying Blockchain Applications with GDPR". In: *55th Hawaii International Conference on System Sciences*, pp. 4631–4640.

Schlatt, V., Sedlmeir, J., Feulner, S., and Urbach, N. (2021). "Designing a Framework for Digital KYC Processes Built on Blockchain-Based Self-Sovereign Identity". In: *Information & Management*.

Schweizer, A., Schlatt, V., Urbach, N., and Fridgen, G. (2017). "Unchaining Social Businesses: Blockchain as the Basic Technology of a Crowdlending Platform". In: *38th International Conference on Information Systems*, pp. 1–21.

Seaberg, R. W., Seaberg, T. R., and Seaberg, D. C. (2021). "Use of Blockchain Technology for Electronic Prescriptions". In: *Blockchain in Healthcare Today*.

Sedlmeir, J., Buhl, H. U., Fridgen, G., and Keller, R. (2020). "The Energy Consumption of Blockchain Technology: Beyond Myth". In: *Business & Information Systems Engineering* 62 (6), pp. 599–608.

Sedlmeir, J., Buhl, H. U., Fridgen, G., and Keller, R. (2021a). *Recent Developments in Blockchain Technology and Their Impact on Energy Consumption*. `arXivpreprintarXiv:2102.07886`. Online; accessed 2021-11-23.

Sedlmeir, J., Smethurst, R., Rieger, A., and Fridgen, G. (2021b). "Digital Identities and Verifiable Credentials". In: *Business & Information Systems Engineering* 63 (5), pp. 603–613.

Sein, M. K., Henfridsson, O., Purao, S., Rossi, M., and Lindgren, R. (2011). "Action Design Research". In: *MIS Quarterly* 35 (1), pp. 37–56.

Seitz, J. and Wickramasinghe, N. (2020). "Opportunities for Using Blockchain Technology in E-Health: E-Prescribing in Germany". In: *Delivering Superior Health and Wellness Management with IoT and Analytics*. Heidelberg: Springer, pp. 299–316.

Shafagh, H., Burkhalter, L., Hithnawi, A., and Duquennoy, S. (2017). "Towards Blockchain-Based Auditable Storage and Sharing of Iot Data". In: *2017 Cloud Computing Security Workshop*, pp. 45–50.

Soltani, R., Nguyen, U. T., and An, A. (2018). "A New Approach to Client Onboarding Using Self-Sovereign Identity and Distributed Ledger". In: *International Conference on Internet of Things and Green Computing and Communications and Cyber, Physical and Social Computing and Smart Data*. IEEE, pp. 1129–1136.

Sonnenberg, C. and Vom Brocke, J. (2012). "Evaluations in the Science of the Artificial – Reconsidering the Build-Evaluate Pattern in Design Science Research". In: *International Conference on Design Science Research in Information Systems*. Springer, pp. 381–397.

Sporny, M., Longley, D., and Chadwick, D. (2019). *Verifiable Credentials Data Model 1.0*. `https://www.w3.org/TR/vc-data-model/`. Online; accessed 2020-07-24.

Stafford, T. F. and Treiblmaier, H. (2020). "Characteristics of a Blockchain Ecosystem for Secure and Sharable Electronic Medical Records". In: *IEEE Transactions on Engineering Management* 67 (4), pp. 1340–1362.

Sunyaev, A., Kannengießer, N., Beck, R., Treiblmaier, H., Lacity, M., Kranz, J., Fridgen, G., Spankowski, U., and Luckow, A. (2021). "Token Economy". In: *Business & Information Systems Engineering* 63 (4), pp. 457–478.

Swinhoe, D. (2020). *The 15 Biggest Data Breaches of the 21st Century*. `https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html`. Online; accessed: 2020-07-24.

Symons, V. (1991). "Impacts of Information Systems: Four Perspectives". In: *Information and Software Technology* 33 (3), pp. 181–190.

Tamblyn, R., Huang, A., Kawasumi, Y., Bartlett, G., Grad, R., Jacques, A., Dawes, M., Abrahamowicz, M., Perreault, R., Taylor, L., et al. (2006). "The Development and Evaluation of an Integrated Electronic Prescribing and Drug Management System for Primary Care". In: *Journal of the American Medical Informatics Association* 13 (2), pp. 148–159.

Tandon, A., Kaur, P., Mäntymäki, M., and Dhir, A. (2021). "Blockchain Applications in Management: A Bibliometric Analysis and Literature Review". In: *Technological Forecasting and Social Change* 166, p. 120649.

Taylor, P. J., Dargahi, T., Dehghantanha, A., Parizi, R. M., and Choo, K.-K. R. (2020). "A Systematic Literature Review of Blockchain Cyber Security". In: *Digital Communications and Networks* 6 (2), pp. 147–156.

Tiwana, A. (2013). *Platform Ecosystems: Aligning Architecture, Governance, and Strategy*. Morgan Kaufmann Publishers Inc.

Venable, J., Pries-Heje, J., and Baskerville, R. (2012). "A Comprehensive Framework for Evaluation in Design Science Research". In: *International Conference on Design Science Research in Information Systems*. Springer, pp. 423–438.

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

Vom Brocke, J., Winter, R., Hevner, A., and Maedche, A. (2020). "Special Issue Editorial – Accumulation and Evolution of Design Knowledge in Design Science Research: A Journey Through Time and Space". In: *Journal of the Association for Information Systems* 21 (3), p. 9.

Walsham, G. (1993). "Decentralization of Is in Developing Countries: Power to the People?" In: *Journal of Information Technology* 8 (2), pp. 74–81.

Warkentin, M. and Orgeron, C. (2020). "Using the Security Triad to Assess Blockchain Technology in Public Sector Applications". In: *International Journal of Information Management* 52, p. 102090.

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

Wu, H.-T. and Tsai, C.-W. (2018). "Toward Blockchains for Health-care Systems: Applying the Bilinear Pairing Technology to Ensure Privacy Protection and Accuracy in Data Sharing". In: *IEEE Consumer Electronics Magazine* 7 (4), pp. 65–71.

Xie, J., Yu, F. R., Huang, T., Xie, R., Liu, J., and Liu, Y. (2019). "A Survey on the Scalability of Blockchain Systems". In: *IEEE Network* 33 (5), pp. 166–173.

Yin, R. K. (2011). *Applications of Case Study Research*. Sage.

Zetzsche, D. A., Buckley, R. P., and Arner, D. W. (2018). "Digital ID and AML/CDD/KYC utilities for financial inclusion, integrity and competition". In: *Journal of Economic Transformation*, pp. 133–142.

Zhang, P., Schmidt, D. C., White, J., and Lenz, G. (2018). "Blockchain Technology Use Cases in Healthcare". In: *Advances in Computers*. Vol. 111. Amsterdam: Elsevier, pp. 1–41.

8 Appendix

8.1 Declarations of Co-Authorship and Individual Contributions

The essays comprising this cumulative dissertation were written in co-authorship. To delineate the individual contributions, I will hereafter provide details on the research settings and my involvement in the respective projects.

Essay 1: Attacking the Trust Machine: Developing an Information Systems Research Agenda for Blockchain Cybersecurity

In this essay, I collaborated with three co-authors to achieve the stated research goal. After a prior version of the manuscript with reduced content has been published jointly by the authors in 2021, I took over the lead role in developing the research project further. As the leading author of the essay, I initiated and developed the project to a journal publication. I was strongly involved in analyzing and structuring the results of the literature review and developed the research framework and agenda. Furthermore, I engaged in textual elaboration throughout the essay and performed the revisions. Thus, my leading co-authorship is reflected in the entire essay.

Essay 2: Toward Trust in Internet of Things Ecosystems: Design Principles for Blockchain-Based IoT Applications

This essay represents the collaboration of five co-authors. I originated the research project by conceptualizing, developing, and evaluating a blockchain-based system for the IoT. Thus, I was responsible for design-oriented tasks, the development, and the evaluation of the resulting artifact. Furthermore, I formulated the main sections of the paper and engaged significantly in the revisions. Thus, my co-authorship is reflected in the research project.

Essay 3: Designing a Framework for Digital KYC Process Built on Blockchain-Based Self-Sovereign Identity

This essay results from the collaboration of four co-authors. I contributed by providing continuous guidance on the design and development of the proposed architecture and set of

processes. Furthermore, I took part in the evaluation of the proposed artifacts. Together with the co-authors, I developed the design principles resulting from our research. In addition, I engaged in the revision of the paper and in formulating its theoretical contribution. Therefore, my co-authorship shaped the entire research project.

Essay 4: Harmonizing Sensitive Data Exchange and Double-Spending Prevention: The Case of E-Prescription Management

In this research essay, I was one of four co-authors taking part in its development. I co-initiated the research project and was responsible for textual elaboration and analysis. Furthermore, I took a role in developing the motivation and requirements, as well as discussion sections of the manuscript. I also took a role in introducing the theoretical perspective and formulating the design principles. As a result, my co-authorship is reflected in the entire research project.

8.2 Related Publications

Table 2: Overview of published articles.

Reference	Title	Publication Outlet
Schlatt, V., Schweizer, A., Fridgen, G. & Urbach, N. (2016)	Blockchain: Grundlagen, Anwendungen und Potenziale	Fraunhofer Whitepaper
Schweizer, A., Schlatt V., Fridgen, G. & Urbach, N. (2017)	Unchaining Social Businesses: Blockchain as the Basic Technology of a Crowdlending Platform	Proceedings of the 38th International Conference on Information Systems
Fridgen, G. et al. (2019)	Chancen und Herausforderungen von DLT (Blockchain) in Mobilität und Logistik	Machbarkeitsstudie für das Bundesministerium für Verkehr und digitale Infrastruktur
Fridgen, G., Röhlen, J., Guggenberger, T., Schlatt, V., & Schulze, M. (2019)	Überprüfung der Machbarkeit eines offenen und dezentralen Mobilitätssystems	Fraunhofer Whitepaper
Guggenberger, T. et al. (2020)	SSI@LfSt: Einsatz der Blockchain-Technologie in der Steuerverwaltung	Whitepaper für das Bayerische Landesamt für Steuern
Guggenberger, T., Lockl, J., Schlatt, V. & Urbach, N. (2020)	Damals wie heute? - Ein Rückblick der Risiken und Potenziale der Blockchain-Technologie	it-daily
Guggenberger, T. et al. (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
Guggenberger, T., Schlatt, V., Schmid, J., & Urbach, N. (2021)	A Structured Overview of Attacks on Blockchain Systems	Proceedings of the Pacific Asia Conference on Information Systems
Hoess, A., Schlatt, V., Rieger, A., & Fridgen, G. (2021)	The Blockchain Effect: From Inter-Ecosystem to Intra-Ecosystem Competition	Proceedings of the 29th European Conference on Information Systems
Geske, F., Hofmann, P., Laemmermann, L., Schlatt, V. & Urbach, N. (2021)	Gateways to Artificial Intelligence: Developing a Taxonomy for AI Service Platforms	Proceedings of the 29th European Conference on Information Systems
Strüker, J. et al. (2021)	Self-Sovereign Identity: Grundlagen, Anwendungen und Potenziale portabler digitaler Identitäten	Fraunhofer Whitepaper

Table 3: Overview of unpublished articles.

Reference	**Title**	**Publication Outlet**
Feulner, S., Sedlmeir, J., Schlatt, V. & Urbach, N.	Exploring the Use of Self-Sovereign Identity for Event Ticketing Systems	*Under Review*
Hoess, A., Lautenschlager, J., Sedlmeir, J., Fridgen, G., Schlatt, V. & Urbach, N.	Routing the Way to Seamless Mobility-as-a-Service: Providing Multimodal Mobility through SSI and Digital Wallets	*Under Review*
Guggenberger, T., Schlatt, V. & Urbach, N.	Designing a Cross-Organizational Identity Management System: Utilizing SSI for the Certification of Retailer Attributes	*Under Review*
Fischer-Brandies, L., Schellinger, B., Schlatt, V., Strüker, J. & Urbach, N.	Untangling the Concept of Blockchain-Based Tokens - A Systematic Literature Review	*Under Review*

Attacking the Trust Machine: Developing an Information Systems Research Agenda for Blockchain Cybersecurity

Authors:
Vincent Schlatt; Tobias Guggenberger; Jonathan Schmid; Nils Urbach

Published in:
International Journal of Information Management

Abstract:
Blockchain-based systems become increasingly attractive targets for cybercrime due to the rising amount of value transacted in respective systems. However, a comprehensive overview of existing attack vectors and a directive discussion of resulting research opportunities are missing. Employing a structured literature review, we extract and analyze 87 relevant attacks on blockchain-based systems and assign them to common attack vectors. We subsequently derive a research framework and agenda for information systems research on the cybersecurity of blockchain-based systems. We structure our framework along the users, developers, and attackers of both blockchain applications and blockchain infrastructure, highlighting the reciprocal relationships between these entities. Our results show that especially socio-technical aspects of blockchain cybersecurity are underrepresented in research and require further attention.

Keywords:
Blockchain; IT security; structured literature review; research agenda

Toward Trust in Internet of Things Ecosystems: Design Principles for Blockchain-Based IoT Applications

Authors:
Jannik Lockl; Vincent Schlatt; André Schweizer; Nils Urbach; Natascha Harth

Published in:
IEEE Transactions on Engineering Management

Abstract:
The Internet of Things (IoT) describes the concept of physical objects equipped with identifying, sensing, networking, and processing capabilities being connected to the Internet. Architectures for the IoT typically rely on transmitting data to centralized cloud servers for processing. Although cloud services are supposed to enhance the IoT in storage, computation, and communication capabilities, this approach often generates isolated data silos and requires trust in third parties operating the cloud servers, which become single point of failure. In addition, centralized cloud-based applications lack transparency and allow for undetected manipulation and concealment of IoT data. To overcome these downsides, we develop and evaluate a blockchain-based IoT sensor data logging and monitoring system, employing a design science research approach. In this article, we show that such systems should provide modularity, data parsimony, and availability in addition to domain-specific principles. The prototype improves data integrity and availability but uncovers challenges, such as high operating costs through smart contract computation fees. Furthermore, semistructured interviews with practitioners allowed us to derive insights for developing blockchain-based IoT ecosystems and reveal that cooperation with organizations is key for transferring solutions into production. We contribute to the IoT knowledge base by providing design principles as well as managerial and technological recommendations.

Keywords:
Blockchain; internet of things; design principles; design science research; distributed information systems; distributed ledger technology; peer-to-peer computing

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

Authors:
Vincent Schlatt; Johannes Sedlmeir; Simon Feulner; Nils Urbach

Published in:
Information & Management

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

Keywords:
Banking; digital certificate; digital wallet; decentralized identity; distributed ledger technology; verifiable credential

Harmonizing Sensitive Data Exchange and Double-Spending Prevention: The Case of E-Prescription Management

Authors:
Vincent Schlatt; Johannes Sedlmeir; Janina Traue; Fabiane Völter

Under review:
Scientific Journal

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 are medical prescriptions. However, current implementations of electronic prescription management systems typically create centralized data silos, leaving user data vulnerable to cybersecurity incidents and impeding interoperability. Research has also proposed decentralized solutions based on blockchain technology, but privacy-related challenges have often been ignored. We conduct design science research to develop and implement a system for the exchange of electronic prescriptions that builds on two blockchains and a digital wallet app. Our solution combines the bilateral, verifiable, and privacy-focused exchange of information between doctors, patients, and pharmacies through verifiable credentials with a token-based, anonymized double-spending check. Our qualitative and quantitative evaluations suggest that this architecture can improve existing approaches to electronic prescription management by offering patients control over their data by design, a sufficient level of 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; double-spending; healthcare; token; privacy; self-sovereign identity