The Convergence of Emerging Digital Technologies – Examining the Interplay of the Internet of Things and Distributed Ledger Technology

Dissertation

zur Erlangung des Grades eines Doktors der Wirtschaftswissenschaft

der Rechts- und Wirtschaftswissenschaftlichen Fakultät

der Universität Bayreuth

Vorgelegt

von

Jannik Lockl

aus

Fürth

Dekan:	Prof. Dr. Jörg Schlüchtermann
Erstberichterstatter:	Prof. Dr. Maximilian Röglinger
Zweitberichterstatter:	Prof. Dr. Jens Strüker
Tag der mündlichen Prüfung:	29.04.2021

"The advance of technology is based on making it fit in
so that you don't really even notice it,
so it's part of everyday life."

Bill Gates

I wish to thank my family and friends for your continuous support throughout my life, for this great journey, and for all these memories. You gave me the strength and support to pursue my passion. I shall forever be grateful.

Further, I would like to express my sincere gratitude to my supervisor, Maximilian. You gave me the tools, guidance, and freedom to reach my goals. You have been a great supervisor and an even better mentor. Thank you for signposting the path of your so-called free radical.

Abstract

Digitalization is driven by the fast emergence and adoption of digital technologies (DTs), the questioning of societal conventions and the adjustment of organizational routines. DTs play a visible role in our daily lives, both on an organizational and indeed on an individual level. Despite extensive efforts in research and industry, questions remain unanswered, be they about theoretical underpinnings or their respective influence on practical use. This lack of a thorough understanding limits the scientific discourse and denies practical users the full value of DTs. To fill in this research gap, the cumulative doctoral thesis contains within these pages comprises five research articles which examine the two DTs that are the Internet of Things (IoT) and distributed ledger technology (DLT). Upon examining each of these technologies in their own right, the subsequent sections of this dissertation will shed light on the convergence of these DTs, their implementation, and their adoption. The thesis covers questions of research as well as challenges in practice. It is thus relevant to researchers and practitioners alike.

The IoT connects physical objects with the digital world through sensors, networking capabilities, and digital logic. To a large extent, the IoT builds on smart things, the term ‘smart’ commonly being used to describe the features and capabilities of such things. However, a clear *understanding* of smartness as one of the key concepts of the IoT has not been defined as of yet. The subsequent thesis addresses this knowledge gap by proposing the concept of a ‘smart action’ and deriving from it a general definition of smartness (research article #1). DLTs are distributed and physically decentralized databases which store information in a tamper-resistant way. For a decade, research on DLT was technology-driven, but nowadays it faces the challenge that technological progress was largely unaware of regulatory boundaries. After all, *establishing* rules and conventions of compliance is essential for the practical use of DLT. That is why this thesis conceptualizes how DLT could be designed to comply with the GDPR (research article #2). The IoT, much like DLT, are DTs that affect systems at the data layer. With a firmer grasp of the mutual influence of these DTs, DLT could serve as a storage for data generated by smart things of the IoT. The effects and interdependencies resulting from such a *convergence* of both DTs are, however, still unknown. To resolve this problem, research article #3 is an attempt to identify certain design principles for the development of a DLT-based IoT system. Although the convergence in question offers multiple opportunities for a variety of organizations, many of them have to date struggled to gain value from digitalization and successfully embed DTs in their processes. With regard to the *implementation* of DTs, research article #4 then provides a success model for process digitalization projects by highlighting factors that drive the success of such implementation projects. Throwing a glance at the users reveals that products and services based on DTs are often hard to comprehend and suffer from lacking adoption. As such a novel technological concept at the intersection of the IoT and DLT, a self-sovereign identity enables users to manage their digital identities in a privacy-preserving manner. To explain and predict its use, research article #5 investigates the effect of information privacy on the *adoption* of a self-sovereign identity.

Table of Contents

I. Introduction[1]

Digitalization is driven by the fast emergence and adoption of digital technologies (DTs), the questioning of societal conventions and the adjustment of organizational routines (Vial 2019). DTs drive the structural change of society and challenge established organizational processes, products, and services (Benbya et al. 2020; Denner et al. 2018). The result is a hyper-connected and opportunity-rich environment for organizations (Beverungen et al. 2020). In practice, this means access to new data sources, fusion of the digital and the physical world, pervasive connectivity, and interactions among individuals, organizations, and real-world objects (Benbya et al. 2020). DTs also provide a connective and indeed a communicative link with other objects and individuals. As such, they form webs of sociotechnical relations and thus build a digital infrastructure (Benbya et al. 2020; Reuver et al. 2018). According to a more general definition, DTs are "combinations of information, computing, communication, and connectivity" (Bharadwaj et al. 2013, p. 471). The potential benefit of DTs for organizations rests on three main factors (Kerpedzhiev et al. 2020; Porter and Heppelmann 2015; Zarkadakis et al. 2016). First, DTs remove temporal and spatial constraints, enabling collaboration in the business-to-consumer and business-to-business domains. Second, DTs facilitate continuous customer-company interactions via smart devices as they predict customer needs through advanced data analytics. Third, DTs provide an opportunity for novel forms of human-computer interaction and automation in the physical and the digital world. It is worth noting that some DTs – such as digital platforms or digital agents – exist only in the digital world (Runde and Faulkner 2019; Vial 2019). Although these DTs may have some form of physical representation, they are specified by a passive form of usage in which the DT remains largely invisible for users and has no direct impact on its physical environment (Berger et al. 2018). DTs range from well-established to emergent. They are often summarized in the form of acronyms, such as the well-known SMACIT: social media, mobile, analytics, cloud-based, and Internet of Things (Vial 2019). Another familiar acronym is DARQ: distributed ledgers, artificial intelligence, extended reality, and quantum computing (Daugherty 2020; Gartner 2020). Today, DTs are the basis of countless applications, and new DTs continue to emerge from them (Arthur 2009). DTs play a visible role in our daily lives, both on an organizational and on an individual level. Since they are among the most studied and practically applied, the *Internet of Things (IoT)* and *distributed ledger technology (DLT)* are both considered to be DTs that will hold disruptive potential across various industries (Beck et al. 2017; Chanson et al.

[1] This thesis is partly comprised of content taken from the research articles included in this thesis. To improve the readability of the text, I omit the standard labeling of these citations.

2019; Li et al. 2015). Applications of the IoT are diverse and by now they occur in almost every area of society (Gubbi et al. 2013), ranging across 30 billion connected devices in 2021 and predicted to extend as far as 75 billion in 2025 (Mostarda et al. 2021). At the same time, DLT has gained serious attention for being "expected to revolutionize industry and commerce and drive economic change on a global scale" (Underwood 2016, p. 15).

The *IoT* connects physical objects with the digital world through "sensors and actuators to the Internet via data communication technology" (Oberländer et al. 2018, p. 488). The resulting network of smart interconnected objects reflects the IoT (Borgia 2014; Fleisch et al. 2009), predominantly understood as a paradigm as well as a DT (Athanasopoulou et al. 2018; Huber et al. 2019; Oberländer et al. 2018). The IoT is of use both in private and business contexts, among humans as well as among machines. 'Smart objects, 'smart devices' or 'smart things' thus bridge the gap between the physical and the digital world (Beverungen et al. 2019; Oberländer et al. 2018). As for its technical arrangement, the IoT is typically organized in a layered technology stack consisting of three layers (Wortmann and Flüchter 2015). At the core lies the device layer which includes the object's hardware, sensors, and all embedded software running on the hardware devices. The connectivity layer in the center is where network communication protocols enable devices for communication. At the top, an IoT cloud layer offers functions such as device management, analytics, and data management, as well as general IoT application software (Wortmann and Flüchter 2015).

In recent years, certain features of the IoT have led to a wide range of different applications (Püschel et al. 2020). For example, today's homes can be equipped with smart things capable of managing core household items such as refrigerators (Borgia 2014; Solaimani et al. 2013). What is more, applications of the IoT extend beyond individual benefits to organizational levels, where the IoT provides countless solutions for service and manufacturing industries (Porter and Heppelmann 2014; Rosemann 2013). Smart factories can flexibly adapt production processes in response to changing conditions in the production environment, and they can do so by reacting in real-time to context-specific problems (Fay and Kazantsev 2018; Häckel et al. 2017). Smart things and systems are now able to carry out actions, functions, or services of which only humans were previously capable (Fleisch and Thiesse 2007; Huber et al. 2019). This technological development provides a foundation for new services and business models, and further academic inquiry is required to explore its full potential, as said potential is far from fully utilized (Brem et al. 2020; Noura et al. 2019). IS research focuses chiefly on smartness to differentiate smart things from common physical objects (Fernando et al. 2016; Warkentin et al. 2017; Weber 2017). A smart thing is capable of observing its environment and connecting

to other actors (e.g., DTs) and service systems, thus forming systems of systems. It is also capable of acting upon others (Novales et al. 2016; Porter and Heppelmann 2014). Hence, the IoT builds on smart things while the terminus 'smart' is commonly used to describe the features and capabilities of such things. Yet, in the wake of recent technological developments and the inflationary use of the term, it remains unclear what exactly is meant by 'smart' or 'smartness' (Alter 2019), and a clear *understanding* of smartness as a theoretical underpinning of the IoT is yet to be established.

DLTs, of which blockchains are probably the most popular subset, describe distributed databases that serve as a physically decentralized but logically centralized source of truth for information (Alt 2020; Rossi et al. 2019). The concept of blockchain first emerged as the technology supporting the cryptocurrency Bitcoin in 2008 (Nakamoto 2008). Blockchain works by storing transactions grouped in blocks in a way that is transparent, chronological, and tamper-resistant (Porru et al. 2017). The data structure and thus the technology itself are often mistakenly heralded as being immutable. This is false, as attackers could theoretically change the state of a blockchain. Such a change could be performed, for example, through a 51%-attack. The data structure is replicated on all nodes participating in a peer-to-peer network (Glaser 2017). The individual blocks are linked cryptographically by referencing the hash value of the previous valid block (Tschorsch and Scheuermann 2016). The verifiability and consistency of the system are thus dependent on all previous blocks (Glaser 2017). The nodes in the network regularly add blocks to the blockchain by way of a consensus mechanism (Christidis and Devetsikiotis 2016), which ensures that data is consistent and validated across the network (Glaser 2017). Different consensus mechanisms exist for distinct types of DLTs. Bitcoin, for example, performs the proof-of-work consensus algorithm, called mining, which usually involves computationally expensive calculations. These days there is a variety of alternative consensus mechanisms (Fernández-Caramés and Fraga-Lamas 2018; Tschorsch and Scheuermann 2016; Zheng et al. 2017), such as proof-of-stake or proof-of-authority (Andoni et al. 2019). The protocol is the key element of a DLT and ensures that all of the stored data is backward tamper-resistant. The protocol also safeguards a high availability as it is stored on multiple consistent nodes in the network (Rossi et al. 2019). Due to these characteristics, the consensus among experts is that DLTs have the potential to replace intermediaries and fundamentally challenge existing business structures (Cong and He 2019; Nakamoto 2008; Schweizer et al. 2017). It is worth noting, however, that certain DLT-based systems exhibit consensus algorithms (e.g., the proof-of-authority), which are not tamper-resistant in the manner described above. Also, DLTs can differ in terms of their data structure or their method

of storing data. Due to this multitude of design options, and indeed due to this ease of reading, the term DLT will from hereon in be used on the understanding that it generally denotes its subset blockchain (e.g., for generalizing statements on tamper-resistance, which many DLTs are not but a blockchain is).

Since DLT was first implemented in relation to Bitcoin, a wide range of applications has developed in quick succession. This has resulted in extended functionalities and enhanced privacy (e.g., Monero) to address the requirements of organizational use (e.g., Hyperledger Fabric). Many of those applications use DLT as their infrastructure yet embed processes and business logic with arbitrary logic – so-called smart contracts (e.g., Ethereum) which can be defined as scripts stored on the DLT (Christidis and Devetsikiotis 2016). When invoked, these scripts are executed by the nodes using a virtual machine (Glaser 2017). In the meanwhile, light-client protocols emerged which allow devices with lower processing capabilities (e.g., smart things within the IoT) to participate in DLT networks by storing hashes of blocks instead of the complete blocks (Glaser 2017). Able to draw on these capabilities and features, various incumbent organizations, and more recent startups, have by now explored DLT in a multitude of use cases (Lacity 2018). The research community has made further headway in examining a wide range of applications, ranging from energy markets (Andoni et al. 2019) to medical supply chain management (Mattke et al. 2019) and social finance (Schweizer et al. 2017). For the first decade research on DLT was largely technology-driven, but as DLT projects move beyond the proof-of-concept stage, they begin to push against regulations and legal barriers. Foremost among these is the General Data Protection Regulation (GDPR) of the European Union. While the GDPR is a European regulation, global platforms, and cross-border firms also adhere to its requirements. The GDPR protects a 'natural person' from unregulated processing of their personal data (Council of the European Union and European Parliament 2016), and this is where the GDPR comes into conflict with DLT. For instance, DLT does not envisage the data being erased at a later point. Hence, *establishing* rules and conventions to comply with regulatory boundaries is essential for the practical use of DLT.

DT	Definition	Key characteristics
IoT	It connects physical objects through sensors and networking capabilities, whereof a network of smart, interconnected objects results.	• Connects the physical and the digital world. • Collects information for actions of smart things.
DLT	A distributed, tamper-resistant database that spans a network committing to one verifiable and consistent state of information without relying on an institutional intermediary.	• The tamper-resistant history of transactions allows for auditability and trust in the system. • Replaces intermediaries through trust in technology instead of an institution.

Table 1: Definitions and Key Characteristics of the IoT and DLT.

Both DTs, of which rough definitions and essential characteristics are outlined in Table 1, have an essential aspect in common: they are infrastructural DTs the application of which most users do not fully realize. An opposite example is a DT like extended reality (Berger et al. 2018). The IoT, on the one hand, is a DT that describes a world of smartphones, smart homes, and smart factories – a world with an increasing number of sensors wherever more humans are connecting with smart things and smart systems. DLT stores the data generated by smart things in a secure and tamper-resistant manner. Current architectures for the IoT typically rely on transmitting device data to centralized cloud servers for processing (Kshetri 2017). In this scenario, the use of cloud services is supposed to enhance the IoT in terms of storage, computation, and communication capability (Botta et al. 2014). However, this approach typically generates isolated data silos and requires trust in the third parties who operate the cloud servers (Shafagh et al. 2017), and who in doing so represent single points of failure (Taylor et al. 2019). What is more, centralized cloud-based applications lack transparency and thus allow for undetected manipulation and concealment of IoT data (Kshetri 2017). This is especially problematic in applications where data integrity and availability are important, such as in monitoring sensor data in food supply chains (Cong and He 2019) or industrial applications (Bahga and Madisetti 2016). DLT has been discussed as an option that might replace centralized cloud structures as the back-end in the IoT (Fernández-Caramés and Fraga-Lamas 2018; Kshetri 2017; Makhdoom et al. 2019). Their convergence is supposed to solve the problems of current IoT architectures with regard to data integrity and availability (Liu et al. 2017; Reyna et al. 2018). Extending the use of DLT to the IoT facilitates a traceable, verifiable, and thus trustworthy network (Lao et al. 2020). Against this background, the potential of the *convergence* of the IoT and DLT becomes apparent, as does the fact that the convergence of the DTs can accelerate the promises held by each DT per se (Dietzmann et al. 2020; Lee and Lim 2018). The power of convergence can, indeed, unlock tremendous potential if the DTs are united (Arthur 2009; Lee and Trimi 2021). However, research on practical implementations as well as theoretical and managerial implications of this remain scarce (Chanson et al. 2019; Rossi et al. 2019). While a literature review by Conoscenti et al. (2016) identifies tamper-resistant logging of data collected by devices and related events as one particularly promising use case for DLT in the IoT, the focus of most research to date focuses on issues such as access control and device identity management (Lin et al. 2018) or distributed firmware updates (Roy and Kumar 2019). It is worth noting, then, that the convergence of the IoT and DLT brings about multiple opportunities but requires further examination.

Despite this promising convergence of DTs, organizations struggle to derive value from DTs (Davenport and Westerman 2018), as they do not fully understand how to use DTs (Denner et al. 2018). Going beyond the DT-enabled transformation of products into smart things (Beverungen et al. 2019; Huber et al. 2019), organizations must embed DTs into their business processes in order to capitalize on the opportunities of digitalization (Denner et al. 2018). Once this is done, they can implement DTs to improve and innovate existing or novel processes (Mendling et al. 2020). For example, DTs support advanced process automation, adaptive process execution, and process data analytics (Kerpedzhiev et al. 2020). While the literature includes methods and tools which assist practitioners in the identification of process digitalization ideas and related projects (Denner et al. 2018; Rosemann 2020), guidance on the successful *implementation* of DTs within processes is not yet readily available. This circumstance presents organizations with substantial challenges, as the failure may entail huge sunk costs and even jeopardize their competitiveness (McLean and Antony 2014). For their internal purposes, some organizations have successfully leveraged DTs in order to raise process efficiency or effectiveness.

While investigating the implementation within processes from an organizational perspective, DT-enhanced products and services[2] must be investigated from an individual perspective. To derive value from DTs embedded in products/services, an individual must actually use the respective product/service (Karahanna et al. 1999; Venkatesh et al. 2016). Although required for the later success, knowledge on user *adoption* of DT-enhanced products/services is scarce (Bélanger and Crossler 2011; Crossler and Posey 2017; Seltsikas and O'Keefe 2010). A self-sovereign identity (SSI) is such a DT-enhanced product/service, one which converges IoT and DLT. An SSI enables users to limit the disclosure of their personal information and control their digital identity without losing access to digital services (Hesse and Teubner 2020; Mühle et al. 2018; Stokkink and Pouwelse 2018). SSI is an alternative to existing IdM systems like login via e-mail and password. The concept of SSIs is based on three core principles – the security, controllability, and portability of identities (Allen 2016; Tobin and Reed 2016). An SSI supports verifiable claims and anonymous digital credentials (Camenisch and Lysyanskaya 2001) which do not necessarily rely on intermediating certificate authorities but can, instead, build on DLT-based public registries which provide information on credential issuers (Stokkink and Pouwelse 2018). In contrast to a system based on intermediating central authorities, changes in data are transparent when DLT is used, and the transaction history cannot be

[2] Due to the blurring of products and services when enhanced by DTs, for the ease of reading, the generalization ‘products/services’ is used representing both digital products and digital services.

tampered with (Dunphy and Petitcolas 2018). The IoT is the connecting layer based on which SSIs identify and communicate with the SSI of another participant or smart thing (Fedrecheski et al. 2020). These smart things – extended with wallet apps for their practical use – store the components (i.e., the keys and verifiable credentials) of the SSI in most parts (Mühle et al. 2018). A smartphone can be such a smart thing, as can a Raspberry Pi which provides a wallet for a robot or a car. While the technological progress of SSI is rapid, studies involving users of SSI remain scarce. Unfortunately, user-agnostic progress leads to unforeseen behavior, such as UK citizens refusing identity cards due to a lack of protection of private data (Landau and Moore 2012), although they use the single sign-on mechanism of Facebook and in doing so share excessive data with the service provider (Krasnova et al. 2014; Landau and Moore 2012). Further knowledge on the successful implementation and adoption of DTs would thus allow for greater value to be derived from DTs.

Highlighting and examining the convergence of the IoT and DLT, the cumulative doctoral thesis at hand consists of five research articles (RA) about the IoT, DLT, their convergence, and studies on the successful implementation and usage of DTs. Figure 1 depicts an overview of how these research articles contribute to a larger examination of the convergence of DTs that focus on the IoT and DLT. The thesis as a whole, then, does not only cover questions of research but also those of practice, and in doing so it guides organizations in their attempts to capitalize on DTs. It is, therefore, relevant to researchers and practitioners alike.

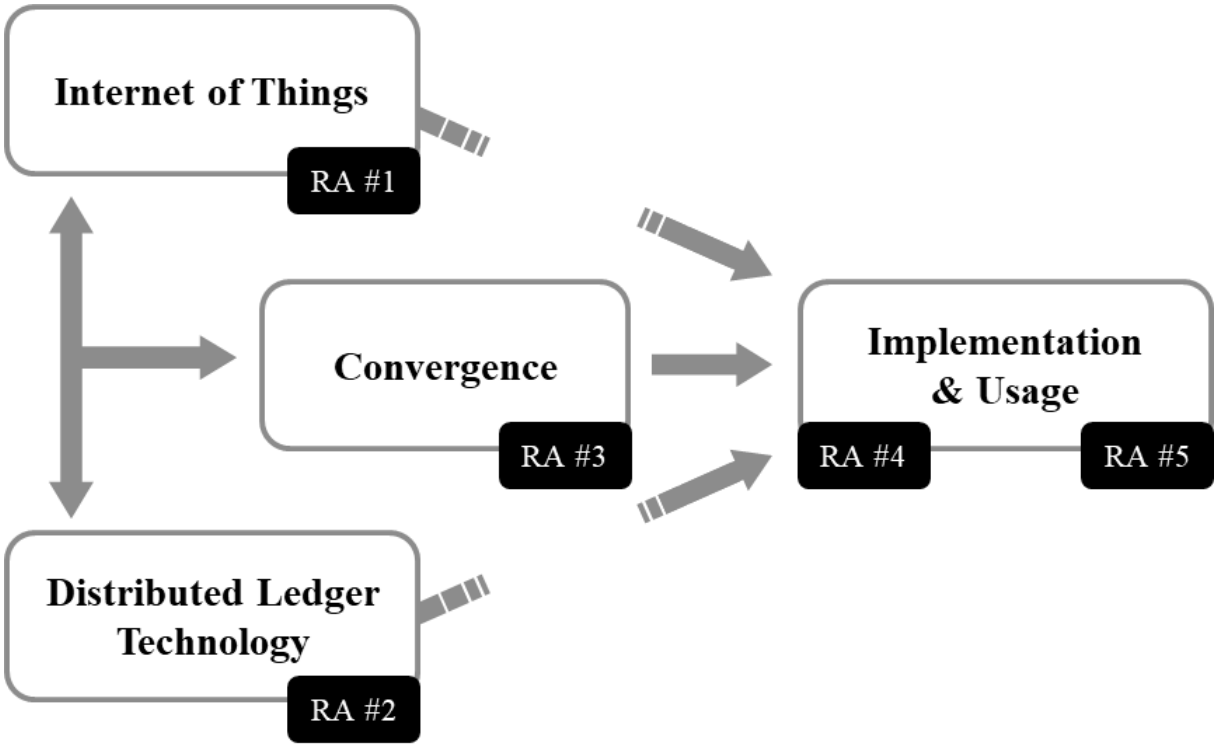

Figure 1: The Convergence of Emerging Digital Technologies.

Figure 1 depicts the structure of this thesis. After examining the IoT and DLT, their convergence is followed by their respective implementation and adoption. To further the *understanding* of the theoretical underpinnings of the IoT, the thesis examines the IoT's technological backbone: smart things (Section II.1). In IS research, the term 'smartness' has become ever more popular and important (Huber et al. 2019; Weber 2017). Although IS publications on smart and smartness have vastly grown in number (Cheng and Liang 2018; Lim and Maglio 2018), understandings and descriptions of smart things, smart services, and smart systems vary significantly (Alter 2019). There is no rigorous understanding of exactly what is meant by the term 'smartness', even though it would be invaluable for research to build on well-defined foundations and for practice to capitalize on an increased *understanding* of the nature of smart devices. For this reason, the thesis at hand examines this lack of foundational knowledge by proposing the concept of a 'smart action' and developing a general definition of smartness (research article #1).

DLT on the other hand – driven by research on the DT per se – faces the dual challenge that the regulatory body has not kept up with the rapid technological progress, and the technological progress has largely been unaware of regulatory boundaries. However, DLT use cases must comply with existing laws and regulations (Lacity 2018). The GDPR is the regulatory boundary with the greatest influence on DLT (Truong et al. 2020). It poses challenges to most potential use cases of DLTs, since they regularly involve technological features that claim to safeguard the immutability of data written on the respective DLT. The GDPR, in contrast, stipulates that personal data must – if required – be erasable. Therefore, Section II.1 of this thesis conceptualizes how a DLT could be designed to comply with the GDPR (research article #2). To be of such practical use, this section provides three recommendations for the management of GDPR requirements and the design of GDPR-compliant DLT solutions. *Establishing* such conventions and rules is an important prerequisite when it comes to implementing a DT and ensuring its convergence with other DTs.

Building on an enhanced *understanding* of its theoretical foundations and a deeper knowledge of *establishing* a DT in line with regulatory boundaries, the interplay of DTs raises questions about their *convergence* and how they would affect each other (Section II.2). The IoT could be the data generator for DLT, while the latter can store the data, again, for the smart things of the IoT. These smart things can finally execute operations based on reliable and trusted data. DLT could thus replace structures relying on centralized cloud services. Research article #3 of this thesis will examine the *convergence* of the IoT and DLT by developing and evaluating a DLT-based IoT sensor data logging and monitoring system. The analysis of this system will show

that converging these DTs increases data integrity and availability. The interplay of these DTs is context-agnostic and therefore highly valuable for future research.

Questions about the *implementation* of DTs within organizations and their subsequent *adoption* by users will then be examined in Section II.3. Although digitalization offers multiple opportunities, organizations have in the past struggled to derive value from DTs as they have lacked the understanding and ability to embed DTs within their processes. Accordingly, research article #4 will explore the *implementation* of DTs by providing a successful model of a process digitalization project. The 38 multi-faceted success factors of this model will outline such a successful implementation, but they do not cover an individual perspective on the later use of DTs. Thus, the model extends current knowledge on business process management (BPM) and serves as a foundation for future research on process digitalization.

To derive substantial value from DTs within products/services, user adoption is crucial (Karahanna et al. 1999). However, the effects leading to the adoption of DT-enhanced products/services have not yet been studied to a sufficient extent. To support the use of products/services enhanced by the convergence of DTs, research article #5 will investigate the *adoption* of SSIs, which is to say of a technological concept for digital identities at the intersection of the IoT and DLT. The empirical study on how information privacy influences the adoption of SSIs indicates that perceived control over the information disclosure through SSIs positively affects the perception of privacy, while perceived privacy does not affect the acceptance of SSIs.

Finally, Section III will offer a look ahead at future research. Section IV will provide the publication bibliography, and Section V (i.e., the Appendix) will give a reference guide in the shape of an index of all five of the research articles that form part of this doctoral thesis (Section V.1), my contributions (Section V.2), and the complete research articles (Section V.3 - 7).

II. Overview and Context of the Research Articles

1 Understanding and Establishing the Internet of Things and Distributed Ledger Technology

1.1 Understanding the Internet of Things

The term ‘smart’ is used widely in the academic literature on the IoT and related application domains (e.g., smart home, smart city, and smart factory) (Porter and Heppelmann 2015; Wiener et al. 2020). Yet, in the wake of recent technological developments and the inflationary use of the term, the actual meaning ‘smart’ or ‘smartness’ is unclear (Alter 2019). The terms also appear in other contexts and domains, often used as part of a technological, economic, and social vocabulary (Gaztambide-Fernández and Rivière 2019; Paukstadt and Becker 2019; Thakor 2015). In IS research, in particular, the term has become increasingly popular and important (Huber et al. 2019; Weber 2017), But although IS publications on smart and smartness have vastly increased in number (Cheng and Liang 2018; Lim and Maglio 2018), understandings and descriptions of smart things, smart services, and smart systems vary significantly (Alter 2019). For example, Beverungen et al. (2019) define smart things as boundary objects, which is to say objects that interact between customers and service providers, whereas Oberländer et al. (2018) define smart things as physical objects equipped with their own agency and with human-like cognitive characteristics. Most definitions of smartness are either highly domain-specific or very general. Yet, while IS research is rich in explorations of smart things and their application domains, it offers no clear understanding of the concept of smartness. To date, there is no well-grounded understanding of smartness in the context of its formation, its manifestations, and its actors. So far, no study has examined the state of research on smartness and its application fields in different domains. This lack of knowledge hampers not only scientific progress but also clear-headed decision-making in industry.

To address this problem, research paper #1 aims to expand the *understanding* of ‘smart’ with the concept of smartness (Huber et al.). This is encountered in many areas of IS literature and described in diverse ways, although it repeatedly involves the same types of actors (i.e., individuals, smart things) and components (i.e., physical objects, technologies, tools). These actors and components are featured in publications relating to smart technologies (Ojo et al. 2014; Warkentin et al. 2017), smart systems (Busquets 2010; Vervest et al. 2004), and smart systems of systems, such as smart cities (Corbett and Mellouli 2017; Petercsak et al. 2016; Porter and Heppelmann 2014). The literature consistently suggests that smartness becomes

manifest in this reproducible set of actors and components and in how they interact. In order to describe how such smartness appears in IS research, the concept of the inner nature of smartness – a 'smart action' – was developed. Figure 2 presents a visualization of how the corresponding elements lead to smart actions. The following section offers an overview of the concept of a smart action, the sub-concepts of which are explained in detail.

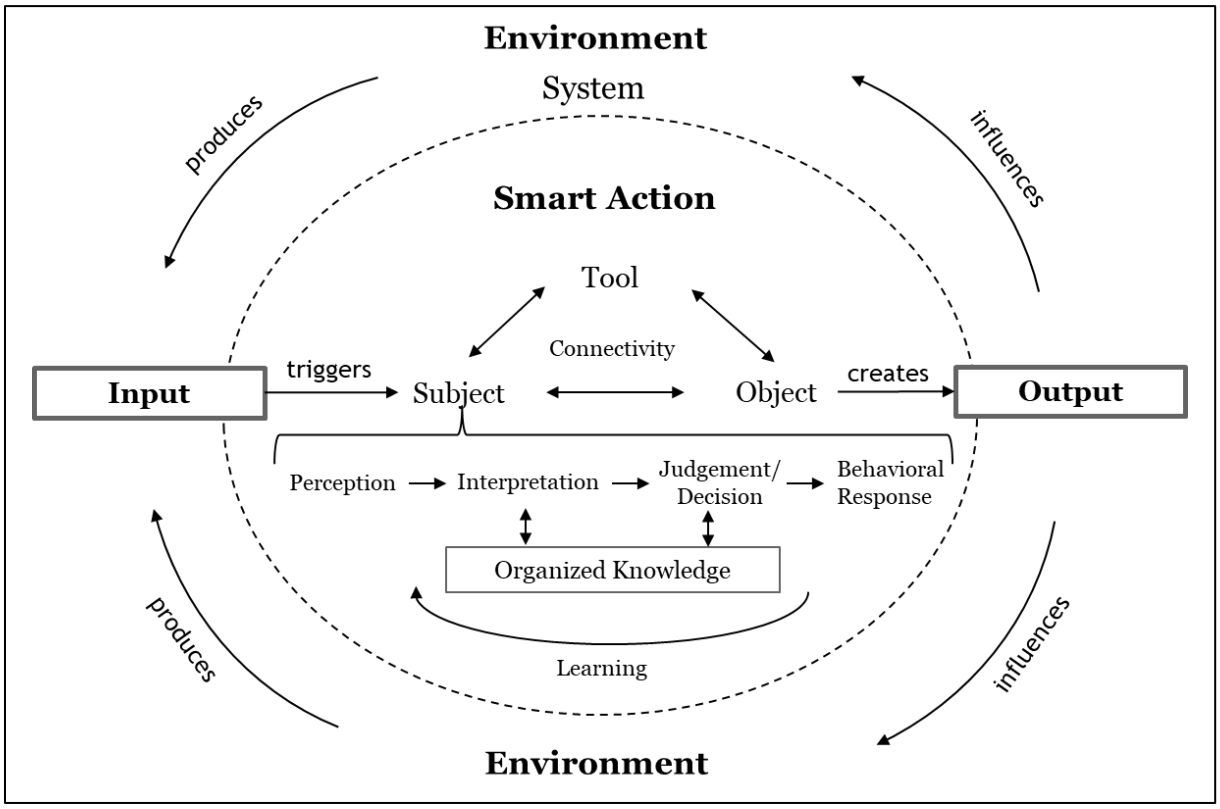

Figure 2: The Concept of Smartness

Represented by the arrows in Figure 2, interactions among actors build the core of smart actions. Actors participating in interactions can be distinguished into two categories: those carrying out actions independently (subjects) and those acted upon (objects) (Benbunan-Fich 2019). Subjects can either be individuals (i.e., human beings) or smart things. When a subject is triggered by an input it acts upon an object either directly, or indirectly by using a tool. Thus, a sequence of information is processed within the subject from perception to interpretation to judgment/decision to behavioral response (Fischer et al. 2020; Song et al. 2019). After the behavioral response, the subject analyzes the output, evaluates the result of the action, and incorporates the evaluation in its organized knowledge to optimize subsequent actions. As the smart action is not carried out in isolation, the surrounding environment predefines the possible input. The output again influences the surrounding environment. Finally, if the output of the smart action is perceived as smart by an external observer, smartness becomes manifest. At this point, an action becomes smart in that the interpretation is not trivial. Of course, the

understanding of whether an interpretation is trivial is dynamic and dependent on the observer. Indeed, emerging from an age of trivial logic, contemporary smart actions could soon be perceived to be as trivial as computing power, which is to say that the expectations of observers will most likely further increase.

To approach the conceptualization of smartness with research article #1, a structured literature review was conducted which identifies and connects concepts that are linked to smartness and repeatedly appear in IS research. Following an approach proposed by Wolfswinkel et al. (2013), a combination of Grounded Theory techniques based on a structured literature review was used to conceptualize smartness and its manifestations. The same approach has been applied in peer-reviewed publications in leading domain-specific journals for inducing theory (Boell and Cecez-Kecmanovic 2015). To follow their approach Wolfswinkel et al. (2013) propose five steps of defining, searching, selecting, analyzing, and presenting. In the "define" step, inclusion and exclusion criteria were defined before identifying the research domains, the appropriate sources of evidence, and the search terms. The 'search' step involved applying the search term along with the inclusion and exclusion criteria to data sources. This resulted in 316 papers. In the 'selection' step, the sample was refined and the number of papers due an in-depth analysis was hence reduced to 180. During 'analysis' open, axial, and selective coding was applied to the point of theoretical saturation (Corbin and Strauss 1990). This procedure identified 16 sub-concepts, which were summarized in three higher-order concepts. Finally, in the 'present' step the results found a representation in the concept of a smart action (Wolfswinkel et al. 2013).

Comparing the theoretical findings with existing theories from (non-) IS-specific domains extended and embedded the primary conceptualization in a larger theoretical discourse. The concepts identified in IS literature appeared to stem from three existing theories which researchers have already applied in the IS context. These theories – Activity Theory (Engeström 1987), General Systems Theory (van Bertalanffy 1968), and Cognitive Information Processing Theory (Greifeneder et al. 2017) – allowed to situate the inferred concept of smartness and its smart action on a stable foundation of knowledge and interpret the findings in a broader context.

To conclude, this thesis investigates smartness in the IS literature and conceptualizes how this concept becomes manifest. While research on the IoT and its smart things is attracting ever more attention, and the term smart is now widely used in both research and practice, a clear understanding of its meaning is not yet available. By using Grounded Theory techniques based on a literature review (Wolfswinkel et al. 2013), a concept was developed to describe smartness in IS. The concept of a smart action involves constructs that take part in the action and their

interrelations. Further, it emphasizes that smartness only becomes manifest and perceivable through smart actions. The insights gained in this section of the thesis are thus of relevance to the theoretical discourse of smartness per se, but they also extend to a broader view of how smartness becomes manifest, including the actors and components involved as well as their interactions, which in turn reveals how these smart actions are initiated and which outcomes they generate. With research article #1, then, this thesis contributes to an increased *understanding* of smartness, smart things, and the IoT. With such an increased understanding, the applicability of smartness advanced what ultimately allows a greater number of users to derive value from the IoT.

1.2 Establishing Distributed Ledger Technology

While a sophisticated understanding makes it possible to apply DTs, the *establishing* of conventions on how to design DTs in practice is a prerequisite for their actual implementation in real-world scenarios (Abu-Elkheir et al. 2013; Lohmann 2013). Before the implementation of a DT, conventions and principles must be established to comply with regulatory boundaries. In the case of DLT, the GDPR is among the regulatory boundaries with the greatest influence on the realization of a DT (Truong et al. 2020). The GDPR regulates the processing of all information relating to an identified or identifiable natural person (i.e., an individual human being) and protects this person from any unregulated processing of personal data. The GDPR also establishes rules governing the free movement of personal data. It stipulates clear responsibilities for compliance with its regulation and prohibits the processing of personal data without a lawful basis, such as the granting of explicit consent or the ruling on whether the action is required to fulfill obligations under law or contract. Moreover, it codifies essential rights of natural persons, such as the right to have inaccurate personal data rectified, or completed if it is incomplete, and to have personal data erased, for instance, upon certain requests or after certain legal time limits. DLT, however, is tamper-resistant by design. GDPR requirements appear to conflict with the basic properties of DLT, and even beyond the contested 'right-to-erasure' the decentralized nature of DLT networks seems to prevent the designation of clear responsibilities. What is perhaps more noteworthy still is the fact that the need to obtain a lawful basis for processing personal data at each node appears daunting. However, DLT offers an innovative path through the challenges that beset existing IT solutions in the public sector. In federal systems, most data is stored in fragmented databases and IT infrastructures differ between agencies, and yet processes mostly require cross-organizational collaboration and the

exchange of data. The DT could foster collaboration and communication between governmental agencies, facilitate federalism, and strengthen democracy.

A research team within the context of the German Federal Office for Migration and Refugees (in short: BAMF) has recently addressed the challenges arising from regulatory boundaries. Research article #2 (Rieger et al. 2019), depicts the resulting GDPR-compliant DLT architecture for cross-organizational process management. It also identifies which rules and principles were *established* prior to the implementation of the system. In Germany, asylum procedures involve close collaboration between various authorities at municipal, state, and federal levels, with the BAMF playing a pivotal role by virtue of the fact that it manages and issues decisions on asylum applications. State-level migration authorities are responsible for the initial registration of asylum seekers. Security agencies are involved in background checks, municipal governments generally handle accommodation, and health authorities provide medical care. Federal separation of competencies prevents the delegation of workflow governance to a central authority. The separation also leads to a significant degree of variation between workflows and complicates the implementation of a conventional workflow management system. Figure 3 depicts a high-level overview of the German asylum procedure.

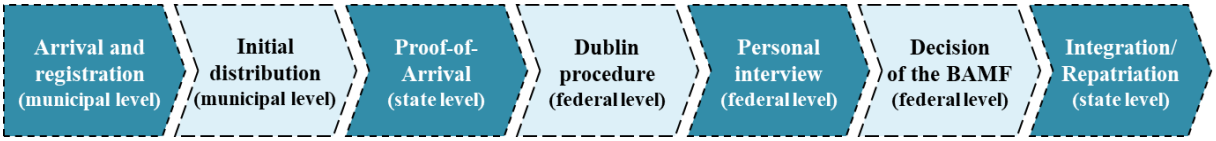

Figure 3: Steps in the German Asylum Procedure.

The shortcomings encouraged BAMF to explore decentralized alternatives for cross-organizational workflow coordination, which would not require the delegation of workflow governance to a single authority. The DLT project was started in January 2018 with a proof-of-concept intended to show that a DLT solution could offer the functionality required to coordinate the workflow of the German asylum procedure. The prototype used a DLT to log and propagate the completion of essential steps in the procedure. BAMF decided to avoid the creation of a central authority. Accordingly, they used a pseudonymization approach with so-called privacy services to ensure is the GDPR-compliance of the DLT solution. With the said solution, each participant runs an off-chain service that maps pseudonymous identifiers on the DLT to the IDs used by the participant and does so in a privacy-compliant, erasable and rectifiable manner. Without the mapping, BAMF (and other authorities involved in the DLT solution) cannot attribute the data on the DLT to a natural person. To enable the sharing of meaningful information, the privacy services can exchange mapping information through

secure communication channels. Such a DLT solution can comply with the right to erasure by eliminating the additional information.

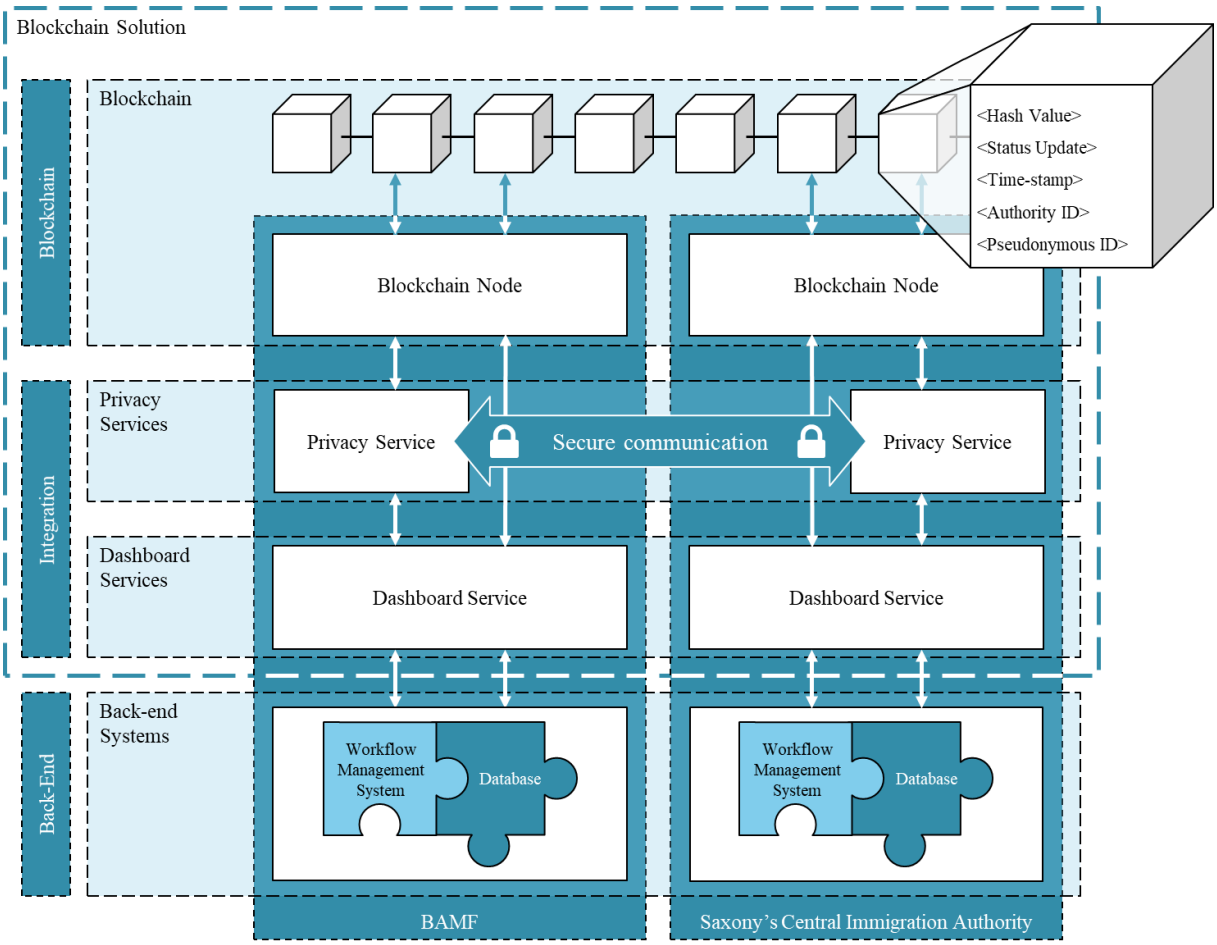

Figure 4: Three-Level Architecture of the GDPR-Compliant DLT solution.

In terms of technical measures, BAMF implemented a DLT architecture with three layers (cf., Figure 4). Layer 1 (back-end systems) hosts the existing workflow management systems and data repositories of the authorities involved. The other two layers do not need to be integrated with these back-end systems. They can be loosely coupled through a set of application interfaces. Layer 2 hosts privacy services that map the pseudonymous DLT IDs with the specific IDs used in the back-end systems. It further hosts dashboard services, which create the event logs and can display data to users from both the back-end systems and the DLT (Layer 3). The design of Layers 1 and 2 can vary between the authorities involved in the DLT solution; only the DLT layer is standardized across all authorities. The DLT layer propagates pseudonymized event logs, with each entry consisting of four elements – a status update, a timestamp, the ID of the authority that created the status update, and a pseudonymous ID. From a functional perspective, these elements reflect the smallest amount of data required for effective use. From a GDPR perspective, they are sufficiently non-specific to limit the risk of inadvertent attribution – for example, through the analysis of the trail of event logs (Montjoye

et al. 2013). The risk of inadvertent attribution from data points with both location and time attributes is high because even a few data points can be sufficient to uniquely identify a person (linkability risk). On the privacy layer (one part of the integration layer), a network of authority-specific privacy services was created, with each authority hosting a standalone privacy service. The privacy services support role-based access procedures for different user groups within authorities and can exchange mapping information. Such an exchange is important for the handover of an asylum application to another authority. With dashboard services (the other part of the integration layer), BAMF made it possible to send event logs to the DLT, display data from both the DLT and back-end systems, and receive alerts when data was pushed through by other participants. Importantly, a user can only view information for which the authority and the user have clearance and legal permission. As outlined above, the erasure of personal data from a DLT may become necessary due to simple errors in entering data or the expiry of legal permission. The erasure procedure implemented in the solution's architecture is triggered when an authority issues a command to its privacy service, which then deletes the respective mapping and submits a so-called 'erasure event log' to the DLT. An erasure event log on the DLT invalidates the pseudonymous DLT ID and prevents further use of this ID by all authorities in the DLT network. Moreover, the log informs other authorities of the erasure.

The GDPR-compliant DLT solution for processing asylum applications was developed by a joint research team within the context of BAMF. Accordingly, an action research approach was deployed (Baskerville and Myers 2004), with three of the co-authors providing scientific advisory services to the DLT project from January 2018 onward. These three co-authors familiarized the employees of the agency team with DLT and organized an ongoing cycle of cross-team reflections which continued throughout the project (Avison et al. 1999). One co-author, for instance, guided the agency's architectural board and worked closely with the IT vendor hired by BAMF to implement the DLT solution. Two other co-authors were not involved with the project team's operations but functioned as external observers. The combination of three collaborating and two observing researchers allowed the research team to maintain high standards of evidence gathering and academic rigor. During the project, four different sources of evidence were gathered. The research team conducted workshops, observed technical meetings of developers, recorded, transcribed, and coded 15 semi-structured interviews with DLT experts, and reviewed all internal and external project-related documents.

As a result of this multi-faceted research, three design principles were derived. DLT solutions should be designed in such a way that it is not necessary to store personal data on the DLT. When the solution that processes personal data requires two or more participants to share

additional information for attribution, establishing a private and permitted DLT network is strongly recommended. For cross-organizational workflows identifier mapping (i.e., separate mapping databases for each participant) provides the best trade-off between value and security.

In summary, a GDPR-compliant DLT application has been developed within the context of BAMF. The application for asylum procedures demonstrates that DLT and the GDPR are not incompatible and that organizations should continue to explore and develop DLT solutions that will involve the processing of personal data. Because DLT solutions emphasize decentralized governance, they could be a particularly promising alternative in cross-organizational settings which prevent the delegation of workflow governance to a central authority. In research article #2, this thesis *establishes* a set of principles in accordance with which to design DLT solutions that comply with the regulatory boundaries of the GDPR. A next essential step for the widespread deployment of GDPR-compliant DLT applications will be to establish standards and reference architectures which ensure the interoperability of various DLTs and solutions.

2 Convergence of the Internet of Things and Distributed Ledger Technology

Building on the increased *understanding* and *established* conventions of Section II.1, the interplay of the IoT and DLT raises questions about the *convergence* of both DTs. The IoT, on the one hand, collects data and connects physical objects to the Internet (Al-Fuqaha et al. 2015). DLT, on the other hand, stores data in a secure and decentralized manner with high data availability (Cong and He 2019; Fthi Abadi et al. 2018). As outlined in Section I, IoT architectures face challenges of data integrity and availability if they rely on centralized cloud servers for storing and processing data (Kshetri 2017), thus promoting isolated data silos operated by a trusted yet nontransparent intermediary, i.e., a single-point-of-failure (Shafagh et al. 2017; Taylor et al. 2019). Nontransparent intermediaries require blind faith since they could manipulate and conceal IoT data undetected (Chanson et al. 2019; Lao et al. 2020). DLT, once established in line with regulatory boundaries (cf., Section II.1), could replace centralized cloud structures as the backend in the IoT (Fernández-Caramés and Fraga-Lamas 2018; Kshetri 2017; Makhdoom et al. 2019). However, the focus of most research to date has focused on specific problems (e.g., access control management). The limited research efforts that have gone into IoT data logging applications recommend solutions which are still somehow reliant on centralized cloud services (Bocek et al. 2017; Samaniego and Deters 2016; Taylor et al. 2019). To tackle these shortcomings, the development of prototypes could assist in evaluating the

applicability of DLT in new domains (Lindman et al. 2017). More specifically, Makhdoom et al. (2019) argue that designing and developing a DLT-based IoT system could meet the requirements of a future world of autonomous smart things. To achieve this, generic design principles for these systems are important (Gregor and Hevner 2013; Nærland et al. 2017).

To this end, research article #3 addresses the lack of DLT-based implementations in ongoing attempts to replace the centralized cloud system with a design science project. Examining the interplay of the IoT and DLT, a DLT-based IoT sensor data logging and monitoring system was developed and evaluated (Lockl et al. 2020). Section II.2 of this thesis generates knowledge on the *convergence* of both DTs through an exploration of their mutual influence. It further proposes an architecture of a DLT-based IoT system as can be found in Figure 5 and derives three generic design principles on how to design systems which offer data integrity and availability (cf., Table 2).

The system's development was based on well-defined design objectives and followed a test-driven approach. The definition of the objectives was predicated on design principles from prior studies from both the IoT (Chatterjee et al. 2018; Hermann et al. 2016) and DLT (Nærland et al. 2017). From an IoT perspective, the prototype was designed to 1) provide information transparency as well as 2) allow for interoperability and interconnectivity. Furthermore, the solution should 3) feature decentralized decisions, 4) be a socio-technical system and provide technical assistance to humans, and 5) maintain a simple design. From a DLT perspective, the artifact was further intended to 6) comprise a digitized process and 7) provide tamper-resistant storage. The artifact was also supposed to 8) be accessible to a wide range of users, and 9) provide user authentication for all users of the artifact. A test-driven approach was taken throughout the software development process. At a preliminary stage, DLTs were evaluated in terms of their suitability to serve as the desired backend for the system. An Ethereum network was chosen for the prototype because of the wide dissemination of Ethereum, the ability to run smart contracts on it, and existing applications for communicating with the DLT system (e.g., through webservers). To date, Ethereum is the most prominent DLT that provides a consensus protocol to allow for the execution of smart contracts on its network. While the main Ethereum network is public (i.e., anyone can participate), private networks can also be implemented on the Ethereum protocol (Fernández-Caramés and Fraga-Lamas 2018). To avoid the smart contract execution costs when operating on the main network, a private network instance was implemented. Upon set-up, a network protocol was chosen similar to that of the Ethereum main network, including a proof-of-work consensus algorithm.

	Objective	Relevance for DLT-based IoT systems
IoT-specific Objectives	[O1] Information transparency (Hermann et al. 2016)	To add value to the link between the virtual and physical world and allow for the analysis of information from both realms, transparency of information for all stakeholders in the IoT is required so as to enable appropriate decision-making (Hermann et al. 2016).
	[O2] Inter-operability (Chatterjee et al. 2018) and inter-connection (Hermann et al. 2016)	Individual components of the system must function together to fulfill a specified goal (Chatterjee et al. 2018; Hermann et al. 2016). In the identified scenario, this refers to providing high sensor data availability and integrity.
	[O3] Decentral decision-making (Hermann et al. 2016)	Due to the various stakeholders with interest in transparency and data availability in IoT settings and their complex interactions, decisions should be made by autonomous actors on different levels (Hermann et al. 2016).
	[O4] Socio-technical system (Chatterjee et al. 2018) and technical assistance (Hermann et al. 2016)	Especially in sensor data monitoring, humans must be able to make informed decisions based on the data they receive from the system (Chatterjee et al. 2018). Therefore, the respective systems must be designed to support humans in their tasks.
	[O5] Simplistic design (Chatterjee et al. 2018)	To increase users' acceptance of an IoT system and facilitate easy maintenance of its components and interfaces, a simple system design is desirable.
DLT-specific Objectives	[O6] Digitization of underlying processes (Nærland et al. 2017)	Using digitized information at all steps in the data monitoring process ensures faster information exchange and higher cost-efficiency (Nærland et al. 2017).
	[O7] Tamper-resistance (Nærland et al. 2017)	The system must prohibit manipulation by superseding an intermediary (Risius and Spohrer 2017), such as a cloud operator. It must also prohibit undetected manipulation of data. "High-risk" applications, such as monitoring sensor data in the supply chain for sensitive and precious goods, are especially relevant to this objective.
	[O8] System accessibility (Nærland et al. 2017)	Users of IoT systems for sensor data monitoring have different technical abilities, which is why simple access to the system must be provided.
	[O9] User authentication (Nærland et al. 2017)	Especially in the rapidly growing IoT, individual devices and users must be uniquely identifiable (Khan and Salah 2018) and authenticate their corresponding actions in the system.

Table 2: Design objectives for the prototype of a DLT-based IoT system

The conceptualized system consists of three major components, each providing individual functionality (cf., Figure 5). The IoT sensor data logger component (1) is responsible for reading temperature and humidity data with a sensor board. The Raspberry Pi used for communication serves as a light-client node for the underlying DLT (i.e., an Ethereum network). The DLT and the smart contracts deployed serve as a data storage and information processing infrastructure (2). Smart contracts store the Ethereum addresses of the IoT devices and log information when certain predefined conditions are met (e.g., temperature threshold violations). The monitoring dashboard component (3) displays the sensor data to a user through a web application with accessibility independent from the operating system. It communicates with the contracts and acts as a mining node adding blocks to the DLT and generating Ether.

Light-clients cannot mine and do not store the complete ledger but root hashes of blocks, which makes it possible to verify the integrity of their content (Glaser 2017).

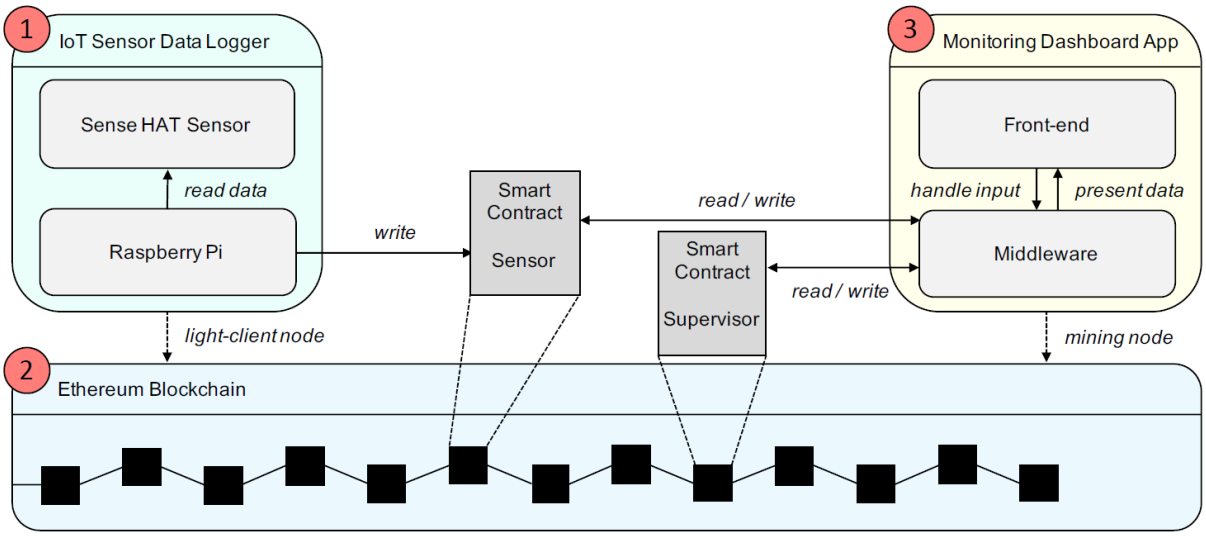

Figure 5: High-Level Architecture of the Sensor Data Logging and Monitoring System

The user interface of the web application is a single-page dashboard that facilitates a convenient and quick overview of the monitored devices. The dashboard is one of the first academic artifacts to make content from a DLT accessible. Figure 6 depicts the final interface.

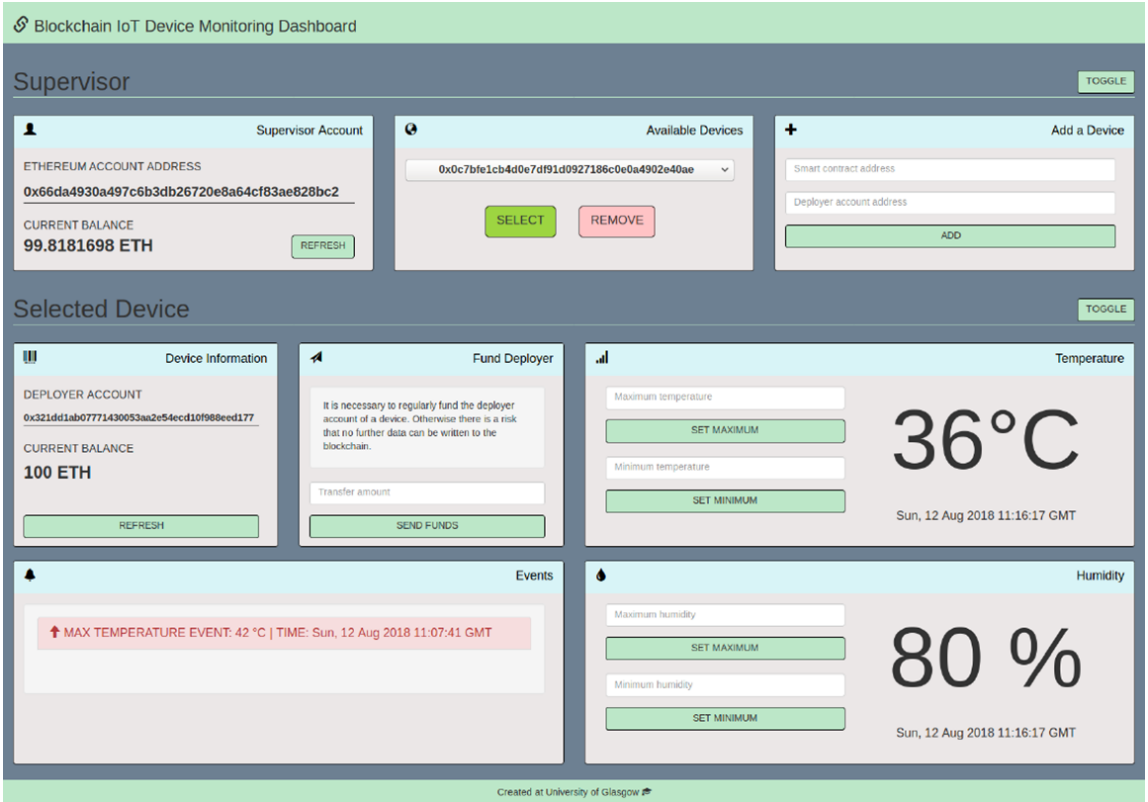

Figure 6: The Dashboard User Interface of the Sensor Data Monitoring Web Application.

To plug the knowledge gap when it comes to the implementation of DLT-based IoT systems, it made sense to make the development and evaluation of the DLT-based IoT prototype follow a

design science approach (March and Smith 1995; March and Storey 2008; Walls et al. 1992). Design science research involves building, applying, and evaluating an artifact while creating and extending generalizable knowledge, as well as understanding a problem domain and its solution (Hevner et al. 2004). This project followed the iterative design science approach proposed by Peffers et al. (2007). Accordingly, a problem of practical relevance was identified (i.e., isolated silos, trust in an intermediary, lacking transparency, and single-point-of-failure). Design objectives were derived from principles developed in the seminal literature on the IoT and DLT. This made it possible to infer the necessary actions to build a DLT-based IoT system with high data availability and integrity. Within the system, a hardware device measures environmental data which is stored and processed directly on a DLT network that serves as a data layer. A web application provides the information accessible with a dashboard user interface. The technical viability of the system was established by means of thorough software testing approaches and by repeatedly executing the key functions to demonstrate the specified functionality. The system was evaluated with logical reasoning as well as evaluation criteria, technical evaluation tools (e.g., the Ganache simulation tool[3]), eight structured expert interviews to assess the prototype quantitatively, and seven semi-structured expert interviews to enhance and confirm the findings. Prioritizing expert interviews as the main evaluation method made it possible to draw generalizable findings, especially concerning novel artifacts (Gregor and Hevner 2013; Nærland et al. 2017). Publishing this work in the form of research article #3 is the last step in communicating the resultant generic design principles of DLT-based IoT systems.

Design Principle	IoT	DLT	DLT-based IoT system
Information transparency (Hermann et al. 2016)	X		X
Interoperability (Chatterjee et al. 2018) and interconnection (Hermann et al. 2016)	X		X
Decentral decision-making (Chatterjee et al. 2018)	X		X
Socio-technical system (Chatterjee et al. 2018) and technical assistance (Hermann et al. 2016)	X		X
Simplistic Design (Chatterjee et al. 2018)	X		X
Digitization of underlying processes (Nærland et al. 2017)		X	X
Tamper-resistance (Nærland et al. 2017)		X	X
System accessibility (Nærland et al. 2017)		X	X
User authentication (Nærland et al. 2017)		X	X
Modularity			X
Data parsimony			X
Availability			X

Table 3: Design principles for DLT-based IoT systems

[3] https://www.trufflesuite.com/ganache

By developing and evaluating a prototype as the output of the design science research (March and Smith 1995), the goal was to derive design knowledge in order to support the future development of artifacts in the field of the IoT and comparable contexts (Gregor and Hevner 2013). The findings from this evaluation offer general clues on how to design and implement systems built upon DLT and the IoT. In addition to existing design principles, the findings are therefore relevant for each of the two DTs and their convergence. The three design principles derived are modularity, data parsimony, and availability (cf., Table 3).

The interviewed practitioners emphasized that designing for Modularity is vital at the technological evolution stage of the IoT and DLT. To adopt new features quickly and integrate them into existing systems, modular design is necessary. Organizations must be able to implement multiple different DLTs suitable for the systems and sensors of the IoT used by their customers. The second design principle refers to designing a proper architecture and data storage concept. Data Parsimony is of great relevance in DLT-based IoT systems. In particular, the performance of current public DLTs supporting smart contracts is not sufficient to handle a large amount of data, as typically generated in the IoT. The execution of code stored in a contract is triggered by sending a transaction to an address (Christidis and Devetsikiotis 2016; Glaser 2017). To avoid spam (e.g., through the execution of infinite loops) (Glaser 2017), all operations imply pre-defined costs (Wood 2018). Substantial amounts of data stored in smart contracts and operations processed through them cause excessive costs on public proof-of-work DLTs. What is more, organizations should consider the data transparency aspect in public DLTs and only push data they are willing to publish. This aspect is concomitant with privacy issues discussed and recommendations given in Section II.1. Cost-driven Data Parsimony would thus align with the concept of privacy-driven Data Parsimony, and this ties in with the third design principle: Availability. The high degree of system availability is obligatory to achieve a reliable exchange and agreement of information. DLTs store data to the point of redundancy within a distributed network. The remaining components of the system must satisfy the same availability standards, including fault tolerance, high device uptime, and a reliable network connection.

Summing up the results of Section II on the *convergence* of the IoT and DLT, the mutual influence of the IoT and DLT was hypothesized, a respective system was implemented and evaluated, and generalizable insights were taken to set the scene for further research and practice. First, generic design principles for implementing DLT-based IoT solutions were derived from the evaluation of the prototype. Second, managerial and technical insights were highlighted by extrapolating implications for practitioners on how to implement a DLT-based IoT system successfully. Thus, research article #3 provides generic knowledge on the mutual

value of the IoT and DLT, on the principles for the design of converging systems, and on the practical decisions required of managers when developing DLT-based applications in the IoT, rather than proposing a complete and productive technical system.

3 Implementation and Adoption of Digital Technologies

Before converging DTs, this thesis advanced the *understanding* of the IoT through conceptualizing smartness. It also *established* principles on how to design DLT-based systems that comply with the regulatory boundaries of the GDPR. Section II.2 then sheds light on the *convergence* of the IoT and DLT through the analysis of a prototype system built on both DTs. With these valuable findings and implications in mind, organizations could start capitalizing on these and similar DTs contextualized in processes and products/services. However, the successful *implementation* of DTs within internal processes, and the *adoption* of products/services enhanced by DT, are still adversely affected by rudimentary knowledge of research and practice.

3.1 Implementing Digital Technologies within Processes

DTs have the potential to improve processes and products/services, but organizations still struggle to capitalize on DTs (Davenport and Westerman 2018; Mendling et al. 2020). Embedding DTs in products/services facilitates novel value propositions (Beverungen et al. 2019; Huber et al. 2019), while organizations implement DTs internally to improve and innovate their processes (Denner et al. 2018; Mendling et al. 2020). From a BPM perspective, process improvement and innovation are considered to produce the greatest value increase within the BPM lifecycle (Denner et al. 2018; Rosemann and Vom Brocke 2015). Projects such as this leverage DTs by improving processes in terms of their effectiveness and efficiency, and they can therefore be referred to as process digitalization projects (PDPs). Efficiency and effectiveness are commonly used success criteria (Beer et al. 2013; Drucker 2007; Schmiedel et al. 2020). Embedding DTs in processes is thus of crucial importance if one is to capitalize on the opportunities afforded by DTs, especially now that knowledge on how to implement DTs successfully within processes is still scarce. How to be successful in the related fields of BPM, project management, and digitalization per se has already been studied (Al-Mashari and Zairi 1999; Soluk and Kammerlander 2021; Trkman 2010). These studies demonstrate that there are isolated pockets of understanding scattered throughout numerous works. An integrated view on factors that drive PDP success, however, is yet to be explored.

Research article #4 fills this knowledge gap on the factors at work in the success of PDPs (Baier et al.). Taking a success factors (SFs) perspective (Bullen and Rockart 1981), research article #4 makes a significant contribution in form of the PDP Success Model outlined in Figure 7. This model links the candidate SFs with relevant PDP success criteria and proposes preliminary success rationales. It includes 38 candidate SFs of which 28 are already backed by the literature, whereas 10 emerged in the course of explorative interviews. The PDP Success Model extends the existing knowledge on BPM and serves as a foundation for future research on process digitalization, which will advance knowledge on the *implementation* of DTs. Further, it guides PDP managers and their teams both when planning and when performing PDPs.

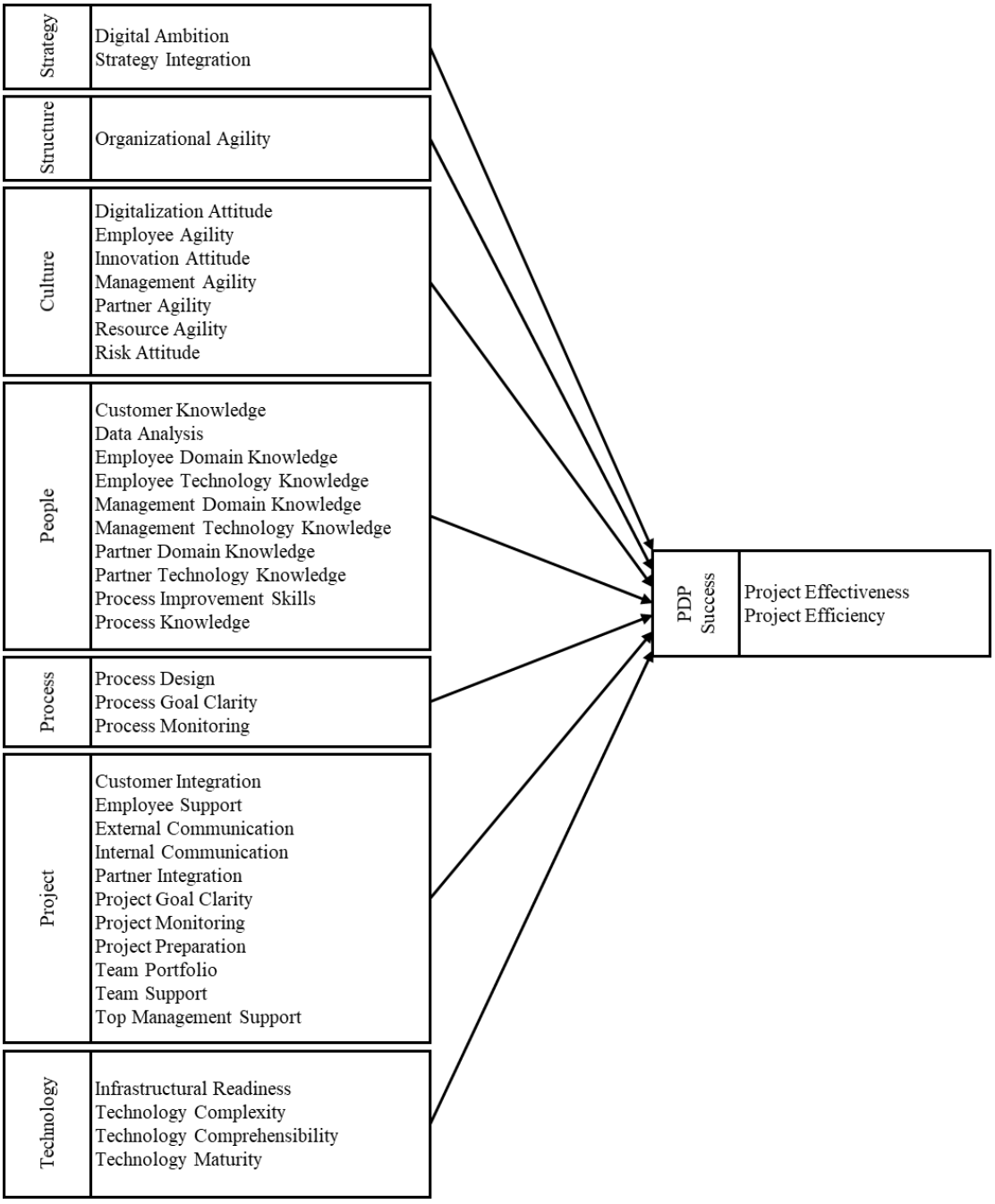

Figure 7: The PDP Success Model

After the initial extraction from literature and grouping of the candidate PDP SFs, it became evident that no seminal IS success model covers the PDP context. Accordingly, frameworks were reviewed in related fields such as work systems theory, BPM, and PM, all of which fit the interdisciplinary and socio-technical nature of the study (i.e., Aladwani 2002; Alter 2013; Petter et al. 2013; Rosemann and Vom Brocke 2015). As the categories were overlapping, they were grouped. The strategy category (2 SFs; 7%) includes factors that relate to the clarity of goals and the integration of departmental digitalization strategies. Structure (2 SFs, 7%) relies on infrastructural and organizational agility, while culture (5 SFs, 16%) comprises factors about the working environment as well as the attitudes of different roles and individuals. The people category (7 SFs, 23%) covers factors that impact human knowledge and skills in various areas relevant to PDPs. The process category (2 SFs, 7%) includes selected activities from the BPM lifecycle, which were found to positively affect PDP success, while the project category (10 SFs, 33%) emphasizes the influence of communication and selected PM activities. The technology category (2 SFs, 7%) accounts for SF candidates that depend on the DTs employed.

While conducting interviews, seven new candidate SFs were identified, and two candidate SFs known from literature refined into three new ones updated to the context of PDPs. Moreover, data from the interviews supports the influence of 19 candidate SFs from the ex-ante list. Interestingly, nine candidate SFs identified from the literature were not supported by empirical data. Based on the refinement and validation of the ex-ante list, the new SFs that were supported by empirical data were included in the ex-post list, as indeed were the SF candidates without empirical support, if only due to the exploratory nature of the research.

As the study set out to explore PDP SFs, a structured literature review was conducted to identify candidate SFs in the BPM, PM, and digitalization literature. This review of 645 studies (101 in-depth) resulted in 1029 codes of SFs, before open and axial coding brought an ex-ante list which included 30 candidate SFs from a broad spectrum of socio-technical topics. Through selective coding, the SFs merged into seven SF categories. With Burton-Jones et al. (2018) and Kerpedzhiev et al. (2020) arguing that digitalization raises fundamental questions about IS theories and BPM assumptions alike, SFs retrieved from the literature most likely do not fully account for the peculiarities of PDPs – an assumption that has since been confirmed by the results of the study. Moreover, owing to the fast-moving nature of digitalization, first-hand experiences often need to be documented academically. Therefore, as a second step, semi-structured interviews with 21 participants of PDPs were performed in German manufacturing companies. These interviews validated, refined, and extended the ex-post list of candidate PDP SFs. The PDPs performed were largely introductions to IoT platforms. After 21 interviews with

experts from seven PDPs conducted in four companies, the support and refinement of candidate SFs met with consistent results. Linking the SF candidates from the ex-post list with relevant PDP success criteria – the former as independent variables, the latter as dependent variables – finally led to the PDP Success Model. In summary, the research method included the following steps: structured database search, code extraction from the literature and building of the ex-ante list of candidate SFs, semi-structured expert interviews, code extraction from the interviews and building of the ex-post list of candidate SFs, and compilation of the PDP Success Model.

The resultant PDP Success Model includes 38 candidate SFs distributed across seven literature-backed categories: strategy, structure, culture, people, process, project, and technology. Preliminary success rationales extracted from the literature for all candidate SFs offer further, tentative explanations of how the SFs take effect. Research article #4 was the first to link the three research fields BPM, PM, and digitalization, and the first to investigate SFs specifically for PDPs as an important approach for organizations to capitalize on DTs. The PDP Success Model implies that the SFs currently discussed in the BPM, PM, and wider digitalization literature requires more work to cover the particularities of PDPs. This implication is in line with Kerpedzhiev et al. (2020) who state that BPM in the digital age calls for different capabilities. Research article #4 shows that capabilities on the project level, as part of a PDP, change as well. From a managerial point of view, PDP teams can use the model as a tool for fit/gap analyses and assess the extent to which certain candidate SFs can be influenced in their specific context. They can then sensibly allocate scarce team resources and steer the management's attention. Since ten new candidate SFs emerged during the exploratory part of research article #4, PDP teams should not blindly trust in what they learned in the past but pay particular attention to the newly identified candidate SFs.

By way of consolidating research article #4, Section II.3 advances the knowledge on BPM and indicates promising paths for future research on business process digitalization. The PDP Success Model guides organizations on how to successfully *implement* DTs within their processes by means of PDPs. The study was motivated by the lack of knowledge on how organizations can leverage DTs to improve and innovate processes. The PDP Success Model consists of 38 candidate SFs distributed across seven literature-backed categories (strategy, structure, culture, people, process, project, technology). After analyzing the DTs in charge about their understanding, establishing, and convergence, organizations can now rely on the PDP Success Model to implement DTs successfully.

3.2 User Adoption of Self-Sovereign Identities

When implementing DTs within processes, organizations can also capitalize on DTs to improve their products/services. Integrating features of DTs within such products/services is concomitant with the disclosure of sensitive data by users, and sharing personal information is fundamental to their use (Forsythe et al. 2006). Users must balance the risks of sharing sensitive information with the benefits of products/services (Dinev and Hart 2006). However, due to the privacy paradox, users often willingly disclose personal information despite expressing significant privacy concerns (Smith et al. 2011). Recent examples – such as the scandal of Facebook sharing user data with the analytics company Cambridge Analytica – illustrate the impact that information disclosure can have on citizens. They also highlight the need for new privacy-preserving DTs (Isaak and Hanna 2018). As outlined in Sections II.1 and II.2, the two DTs both highlight the importance of privacy-preserving measures when integrating the IoT and DLT. What is more, the two DTs also provide the basis for SSIs. As a privacy-preserving concept, an SSI enables users to limit the disclosure of their personal information and control their digital identity without losing access to products/services (Dunphy and Petitcolas 2018; Mühle et al. 2018). Privacy is theorized to be a substantial reason for the user adoption of digital identities (Hansen et al. 2004). Features of SSIs may provide a solution to privacy concerns by reinstating a user's control over identity and personal information while enabling them to benefit from other products/services (Acquisti 2008; Mühle et al. 2018). However, research on SSI and the larger field of identity management (IdM) does not yet extend to the interplay between digital identities and DTs, nor does it answer the question why users adopt such IdM systems (Crossler and Posey 2017; Halperin 2006; Kjærgaard and Gal 2009).

To answer this question, research article #5 describes an empirical examination of the effects that would lead to the *adoption* of an SSI from a user perspective (Lockl et al.). To this end, existing theories of technology acceptance and research on information privacy were combined in the new context of SSIs. Coming from both research streams, determinants of 'behavioral intention to use an SSI' and 'perceived information privacy' were used to develop a research model which defines and hypothesizes the relationships between the variables examined. The hypotheses were operationalized based on renowned studies in these fields (e.g., Dinev et al. 2013; Krasnova et al. 2010; Pavlou and Fygenson 2006). They were then tested empirically through a survey with 495 respondents. Figure 8 depicts the results of this survey in form of the structural model and its path coefficients, t-values, and significance levels. Remarkably, the findings of research article #5 indicate that Perceived Privacy does not have a significant impact on the Behavioral Intention to Use SSI, indicating a privacy paradox. Further, Perceived Benefit

has a positive effect on Perceived Privacy, which supports the theory of the privacy calculus that users weigh up benefits and risks when making decisions about their privacy. Lastly, the study did not detect an effect of Regulatory Expectations on Perceived Privacy. This finding substantiates the need for privacy-by-design solutions as examined in Section II.1 and II.2 since users do not seem to care about regulations when it comes to the privacy trade-off.

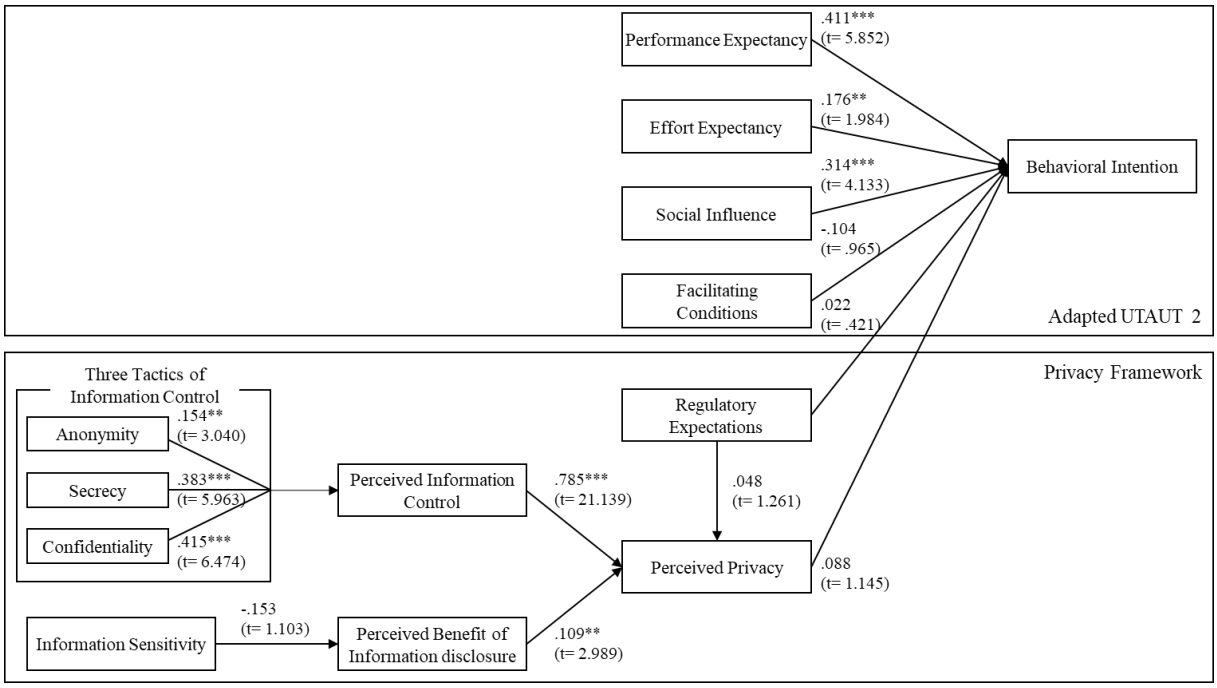

Figure 8: The Adoption Model of IdM Systems

A structural equation model was developed to investigate the relationships in the research model (Benitez et al. 2020; Urbach and Ahlemann 2010). The model was tested with partial least squares structural equation modeling (PLS-SEM) using Smart PLS 3.0 (Hair et al. 2017; Urbach and Ahlemann 2010). Therefore, two different theories were used to explore the influence of information privacy on the adoption of SSIs. The model is thus based on the UTAUT2 of Venkatesh et al. (2012) and the privacy framework of Dinev et al. (2013). Certain components were eliminated from the UTAUT2 since these constructs require an established technology and previous experience of its use (Venkatesh et al. 2012). Constructs from the privacy framework were altered to fit the context. To test the research hypotheses, a survey was developed. The questionnaire was pre-tested with 40 respondents (Kim et al. 2009) and trimmed down following Hair et al. (2017). The model was validated empirically through 495 respondents of which 354 were complete and 240 valid after being filtered through a set of control questions. All items were adapted to the context of digital identities, constructed as reflective indicators, and measured using 7-point Likert scales. Leveraging the explanatory power of the model, it was assessed in terms of reliability as well as convergent and discriminant

validity. Composite reliability was used to examine internal consistency reliability (Urbach and Ahlemann 2010). All of the constructs displayed desirable values and indicators, which is why the constructs were accepted (Hair et al. 2017).

No.	Hypothesis	Result
H1	Performance Expectancy positively affects Behavioral Intention.	Accepted
H2	Effort Expectancy positively affects Behavioral Intention.	Accepted
H3	Social Influence positively affects the Behavioral Intention to use an SSI.	Accepted
H4	Facilitating Conditions positively affects Behavioral Intention.	Rejected
H5	Perceived Privacy positively affects Behavioral Intention.	Rejected
H6	Perceived Information Control positively affects Perceived Privacy.	Accepted
H7	Anonymity positively affects Perceived Information Control.	Accepted
H8	Secrecy positively affects Perceived Information Control.	Accepted
H9	Confidentiality positively affects Perceived Information Control.	Accepted
H10	Perceived Risk negatively affects Perceived Privacy.	Not examined
H11	Perceived Benefits of Information Disclosure negatively affects Perceived Risk.	Not examined
H12	Perceived Benefits of Information Disclosure positively affects Perceived Privacy.	Accepted
H13	Information Sensitivity negatively affects Perceived Benefits of Information Disclosure.	Rejected
H14	Information Sensitivity positively affects Perceived Risk.	Not examined
H15	Importance of Information Transparency positively affects Perceived Risk.	Not examined
H16	Regulatory Expectations positively affects Perceived Privacy.	Rejected
H17	Regulatory Expectations negatively affects Behavioral Intention.	Rejected

Table 4: Summary of the Hypotheses Testing

When evaluating the survey, multiple constructs known from former studies were confirmed, while three interesting effects were found to be discussed separately. An overview of the hypotheses and their acceptance or rejection after the survey can be found in Table 5. Based on the privacy-related constructs from the privacy framework by Dinev et al. (2013), the influence of Perceived Control on Perceived Privacy was hypothesized. Data for Perceived Control indicates that SSI enables users to perceive control over their information, which has a significant positive effect on Perceived Privacy. Analyzing the survey further showed that Anonymity, Secrecy, and Confidentiality significantly affect Perceived Control. The constructs borrowed from UTAUT2 are Performance Expectancy, Effort Expectancy, and Social Influence. These significantly affect Behavioral Intention, which is in line with former research (e.g., Bélanger and Crossler 2011; Pavlou 2011). However, when it came to analyzing the influence of Facilitating Conditions, the results contradicted the outcomes of previous empirical studies. This may be due to the novelty of SSI and the underlying concepts of the IoT and DLT. Hence, users may struggle to determine the available support and the compatibility of these new DTs (Weinhard et al. 2017).

The most remarkable finding of this study is that the effect of Perceived Privacy on Behavioral Intention was not shown to be in any way significant, although extant literature theorized this relationship to be of critical importance to the success of IdM systems (e.g., Hansen et al. 2004; Roßnagel et al. 2014). On the base of this theorized relationship, extensive efforts were made in developing and using privacy-preserving DTs (Mühle et al. 2018), from the infrastructure layer (cf., the GDPR-compliant DLT architecture of Section II.1 or the design principle Data Parsimony of Section II.2) to products/services like SSI. The results presented in this thesis, however, do not confirm this relationship. This may explain a lack of practical use of solutions that build upon this assumption and, in turn, explain the success of single sign-on mechanisms whose value proposition is based on convenience and security, rather than on privacy, such as those of Facebook and Google. For instance, Bauer et al. (2013), as well as Pitkänen and Tuunainen (2012), showed that users of these single sign-on mechanisms – and social networks in general – were unaware of the underlying privacy practices despite consent information that pretends to inform the user about these practices prior to use. The results of the study are in line with studies that investigated the privacy paradox. After all, the likes of Spiekermann et al. (2001) investigated self-reported privacy preferences and the corresponding actual behavior of e-commerce customers. They found that privacy-preserving approaches may be ineffective due to discrepancies between the stated and actual behavior of customers. Users often express privacy concerns regarding the disclosure of personal information but reveal low inhibition thresholds when asked to share their information to benefit from a product/service (Dinev and Hart 2006). Despite the privacy paradox, and despite the fact that SSI enhances perceived control, privacy does not seem to be a factor influencing the adoption of privacy-preserving IdM systems such as SSIs. This conclusion is further supported by Dhamija and Dusseault (2008) who found that IdM, and thus the management of private information, is not a primary goal of consumers. SSI shifts the ownership – and with it the responsibility for their privacy – to users and asks them to actively manage their privacy settings (Der et al. 2017). The findings of the study presented here are therefore of relevance to examine and advance theoretical assumptions that form the basis of the technological progress of SSI.

Beneath the privacy paradox, research article #5 also affirms the privacy calculus. This was originally theorized in a study by Laufer and Wolfe (1977) as a calculus of behavior. Dinev and Hart (2006) found that users calculate whether or not the benefits of an information disclosure outweigh the associated risks. Therefore, the impact of Perceived Benefit on Perceived Privacy was theorized (Kehr et al. 2015). In research article #5, Perceived Benefit was shown to have a positive effect on Perceived Privacy, which supports the underlying theory of the privacy

calculus – users evaluate risks and benefits to assess their state of privacy. If users overlook these risks, the importance of additional factors influencing the success of IdMs (e.g., usability) increases. Kehr et al. (2015) outline that highly beneficial products/services are often associated with the highest privacy risk for users. Consequently, Information Sensitivity was included in the study as it was revealed to be the origin of paradoxical privacy-related behavior. The sensitivity of information multiplies risks and reduces the perceived benefits of information disclosure (Malhotra et al. 2004; Mothersbaugh et al. 2012). Hence, Information Sensitivity was theorized to negatively affect Perceived Benefit. Throughout this study, however, this relationship was not found to be significant.

The final examination presented in these pages is about the effects of Regulatory Expectations on Perceived Privacy and Behavior Intention. Although Perceived Control has a positive impact on Perceived Privacy, the study did not detect a similar effect for Regulatory Expectations on Perceived Privacy. The hypothesis was based on the theory that regulations would empower users to exercise proxy control over their privacy (Lwin et al. 2007; Xu et al. 2012), while an SSI would be a market-based alternative that enables the user to exercise actual instead of proxy control. What is more, no significant effect of Regulatory Expectations on Behavioral Intention could be determined. Hence, from a privacy point of view, proper privacy regulations could make an SSI redundant and negatively affect Behavioral Intention. Two explanations are possible here. First, based on the difference between control agency of proxy control approaches (e.g., privacy regulations) and the real control of individual self-protection through privacy-enhancing technologies (e.g., SSI), Xu et al. (2012) found that the latter affords a greater sense of control and has a stronger impact on a user's perceived information control. Second, self-control mechanisms diminish the need for regulatory expectations, even substituting the expectations to some extent (Xu et al. 2012). These findings substantiate and underline the results from Sections II.1 and II.2, which highlight that DT-enabled systems must be of a privacy-preserving design due to regulatory boundaries (i.e., GDPR). Since users tend to neglect their privacy in favor of benefits associated with the use of a product/service, Organizations have an even greater responsibility to implement privacy-by-design solutions so as not to put users at risk.

Research article #5 offers these findings about the *adoption* of a DT-enhanced product/service at the conclusion of Section II, where it provides an end-to-end view of the understanding, establishing, convergence, implementation, and adoption of DTs. The goal of research article #5 is to examine the adoption of a DT at the intersection of the IoT and DLT by empirically investigating the impact of perceived privacy on the adoption of SSI. A substantial

theoretical body already exists on the influence of such factors as information privacy on the adoption of non-DLT-based IdM systems (Hansen et al. 2004; Seltsikas and O'Keefe 2010), yet to date, empirical results from a behavioral perspective have been scarce in IdM literature, and few studies have investigated the potential of DLT from individual and behavioral perspectives (Mendoza-Tello et al. 2018). Mindful of this crucial lack of knowledge, the study presented here takes an individual perspective to investigate the impact of information privacy-related theories (namely, the privacy paradox and privacy calculus) on the acceptance of SSIs. The research model consists of established constructs from technology acceptance and privacy research. However, given the novelty of the research context described in Section II.3, research article #5 reveals unexpected findings. Analogous to the privacy paradox, the study does not lend empirical support to the claim that perceived privacy has an impact on the adoption of an SSI. On the contrary, these findings contradict the prevailing view of privacy as a key factor for IdM systems and advance knowledge on the *adoption* of DTs.

III. Summary and Future Research

1 Summary

This cumulative doctoral thesis consists of five research articles examining DTs, with spotlights focused on the IoT and DLT. DTs play a visible role in our daily lives, both on an organizational and on an individual level. The *IoT* and *DLT* are among DTs with the potential to disrupt industries and change the rules of the game. The IoT is a concept according to which physical objects with identifying, sensing, networking, and processing capabilities are connected to the Internet. DLT is a distributed database that facilitates the storage of transactions in blocks, and it does so in a transparent, chronological, and tamper-resistant way. Both are infrastructural DTs that affect how data is collected and stored, while they connect humans with smart things, thereby, blurring the lines between the physical and the digital world. Despite vast efforts in research and practice, successful implementations and documented use cases are scarce. Before the DTs can reach large-scale application, further knowledge is required with regard to the theoretical concepts of the DTs, their interplay, and their practical use. Accordingly, this thesis consists of five research articles that examine the IoT and DLT, first by studying each technology as an entity unto itself, then by shedding light on their convergence, their implementation, and their adoption. The thesis as a whole contributes to the body of knowledge with concepts, design principles, and models for the foundations and indeed the applications of DTs. It is thus relevant to research and practice alike.

To date, research efforts have been especially poor in understanding, establishing, converging, implementing, and adopting DTs. Section II.1, therefore, starts with the pre-implementation work of understanding and establishing DTs. The thesis aims to offer an *understanding* of the theoretical underpinnings of the IoT by first providing a conceptualization of ‘smartness’. The term is used for smart things, the backbone of the IoT. Research article #1 theorizes that smartness becomes manifest within smart actions which involve a reproducible set of actors and components as well as a template for how they interact. To constitute a smart action, it must be perceived by an observer. The understanding of smartness changes over time, since whether or not an interpretation is trivial or smart lies in the eye of the beholder, which always depends on the contingencies of when and where said action is performed and witnessed. In Section II.1, this thesis further *establishes* a set of principles on how to design DLT-based systems in compliance with the regulatory boundaries of the GDPR. At first glance, the GDPR imposes boundaries on DLTs. For example, the right-to-erasure conflicts with the so-called immutability of DLT. Research article #2 establishes three design principles for the construction of systems

that comply with the GDPR. First, solutions should not store personal data on the DLT. Second, solutions should build upon private and permitted DLT networks. Third, solutions should leverage cross-organizational workflow identifier mapping. In accordance with these three principles, a GDPR-compliant architecture for such a DLT-based solution was designed.

Section II.2 merged the two DTs examining the *convergence* of the IoT and DLT. IoT architectures face challenges if they rely on centralized cloud servers for the storing and processing of data. These centralized structures promote isolated data silos, require trust in an intermediary, lack transparency, and run the risk associated with a single-point-of-failure. DLT could replace centralized cloud structures as the backend in the IoT. Since practical implementations of an integrated system were unavailable, a DLT-based IoT sensor data logging and monitoring system was developed and evaluated. Research article #3, then, reveals knowledge on the mutual value of the IoT and DLT. It also depicts an architecture of a DLT-based IoT system and highlights three generic design principles on how to design such converging systems while safeguarding data integrity and availability. At the same time, a modular design is necessary in order to react to the rapid technological development of the two DTs. Data parsimony requires a proper architecture and data storage concept to ensure privacy and cost-efficiency. Availability is obligatory to achieve a reliable exchange and agreement of information. Furthermore, practical implications are given for managers to account for the development of DLT-based IoT systems.

Section II.3 examines the implementation and adoption of DTs. Organizations still struggle to derive value from digitalization for the simple reason that they cannot yet rely on readily available knowledge of the successful *implementation* of DTs within their processes. This thesis seeks to resolve this issue by providing the PDP Success Model. PDPs are referred to as projects that implement DTs to improve processes in terms of their effectiveness and efficiency. Research article #4 presents the PDP Success Model which links candidate SFs with relevant PDP success criteria and proposes preliminary success rationales. The model includes 38 candidate SFs distributed across seven literature-backed categories: strategy, structure, culture, people, process, project, and technology. These PDP SFs guide PDP managers and their teams when planning and performing PDPs. Having addressed the implementation within processes from an organizational perspective, DT-enhanced products/services must then be investigated from an individual perspective. Despite vast efforts in research and practice, products/services are frequently not adopted by users. It is with this in mind that research article #5 was dedicated to the effects which would lead to the *adoption* of an SSI as a DT based on the convergence of the IoT and DLT. The most remarkable finding, however, is that Perceived Privacy does not

have a significant impact on the Behavioral Intention to Use SSI, which runs counter to theoretical assumptions of privacy-preserving DTs. Furthermore, Perceived Benefit has a positive effect on Perceived Privacy, which supports the theory of the privacy calculus. Finally, the study did not detect an effect of Regulatory Expectations on Perceived Privacy, which substantiates the need for privacy-by-design solutions as examined in Sections II.1 and II.2.

2 Future Research

This doctoral thesis advances knowledge on the IoT and DLT, their convergence, and their application. Beyond that, the findings point the way toward promising future research. As with all research, this doctoral thesis is subject to certain limitations, and these – along with the many potential avenues for future research – can be found in the following pages.

The IoT and DLT are DTs with significant disruptive potential, but so far they have not been treated with a sophisticated understanding nor is there a set of established principles to govern their use. The IoT builds upon smart things which in themselves are attracting ever more attention. While the term smart is widely used in research and practice, Section II.1 emphasizes the lack of a clear *understanding* of smartness. Research article #1 thus investigates the concept of smartness in IS research, proposes a conceptualization of smartness, and demonstrates that the concept manifests itself in smart actions. This concept can be used as a theoretical lens in future IS research, yet for now, the interpretation and use of the concept of smartness are restricted by the parameters of the research field, the search terms, and the literature sample of the study. The concept should therefore be further developed for use in domains other than IS. Regarding the methodology, future research should consider applying other types of theory to the concept of smartness. Research article #1 provides a theory for description and analysis that is a solid foundation for researchers applying more advanced, complex, and detailed theories (Gregor 2006). Building upon said foundation, theories for explanation promise a deeper understanding of a so-called smart action and its underlying concepts. Meanwhile, theories for design and action can guide managers and practitioners in building and designing smart things. Furthermore, the study has shown that different forms of smartness exist and could be classified hierarchically from very basic to very advanced, and this hierarchy may well change over time. Examining these questions further increases the understanding of the DT, for in order to leverage DTs in real use cases and implement them in accordance with regulatory boundaries, the *establishing* of conventions is a prerequisite. The GDRP, itself perhaps the most significant regulatory boundary, poses challenges to the use of DLT for the storage of personal data.

Research article #2 thus investigates how to design a GDPR-compliant DLT architecture and which rules must be followed for a compliant implementation. The study provides such an architecture and establishes principles for a GDPR-compliant design of DLT-based systems. Since the research project was conducted in a single context, and as an action research project, the study is limited in how far and wide its findings may be extrapolated. Elements of the architecture have yet to demonstrate their suitability for large-scale deployment beyond the authorities involved in the study's setting. Therefore, research and practice should continue to explore and develop DLT solutions that involve the processing of personal data. The next essential step ought to be a consensus on standards and reference architectures in order to ensure the interoperability of various DLTs and solutions. These standards would allow for the widespread deployment of GDPR-compliant DLT applications.

Building on an advanced understanding and established conventions, the *convergence* of the IoT and DLT bears great potential. Section II.2 addresses the problem of knowledge scarcity when it comes to converging implementations in which DLT replaces the centralized cloud structures used in typical IoT systems. In research article #3 a DLT-based IoT sensor data logging and monitoring system is developed. As the main contribution, three generic design principles are derived, but the study faces limitations. It focuses on specific technological frameworks, such as the Ethereum protocol. Future research efforts should, therefore, compare the use of different available technological frameworks and their impact on IoT sensor data integrity and availability, rather than focus on one technology alone. As the design science project revolves around a prototype, the evaluation offered here is mainly theoretical. Deploying and shaping the system in a real-world environment, for example by using Action Design Research (Sein et al. 2011), could lead to fruitful practical knowledge in future research endeavors. Meanwhile, this thesis has focused on increasing data integrity and availability, thus transferring the major functionality of the sensor data monitoring system into a DLT layer. The implications of this architectural approach should be compared to those of other approaches, such as just storing hash references on a DLT layer (Shafagh et al. 2017). Accordingly, data integrity and availability could further leverage the convergence of both DTs.

Finally, Section II.3 deals with the implementation and adoption of DTs. DTs have the potential to improve processes and products/services, but organizations still struggle to capitalize on DTs. To resolve this problem, research article #4 explores the factors which drive the success of PDPs, which are projects during which DTs are implemented within processes. The PDP Success Model consists of 38 candidate SFs distributed across seven literature-backed categories. The SFs were treated as independent, and they were not ranked, since neither the

literature nor the interviews allow to infer that some SFs are more important than others. The explorative nature of this methodology also means that one cannot exclude a positive effect of the SFs when it is not supported in the interviews, which in turn means that a high number of SFs must be considered. As the research focused on the exploration of SFs, the explanatory power of the PDP Success Model has yet to be investigated through confirmatory research. To that end, future research should account for potential interactions among the SFs within the same category as well as across categories, since it is important to understand these interactions to fully understand PDP success (Petter et al. 2013). To account for the diverse domains in which PDPs are performed, context should be included as a moderating variable. Finally, the PDPs covered during these interviews were limited to the business-to-business domain. While searching related BPM, PM, and digitalization literature without restrictions, the study was focused on the manufacturing domain in order to limit the complexity different contexts would induce. Although this was a deliberate methodological decision, interviews in other domains, such as business-to-consumer, may well allow future researchers to identify new candidate SFs. Future research should, therefore, challenge the PDP Success Model by conducting interviews in other domains. Related findings may provide useful clues for a subsequent contextualization of the PDP Success Model in different domains. For the same reason, the individual perspective requires future research. After all, DT-enhanced products/services are frequently not adopted by users. One such ground-breaking DT at the intersection of the IoT and DLT is an SSI that enables users to fully own and manage their digital identities in a way that preserves their privacy. Although the technological concept of SSI has matured and is ready to use, research has not yet fully investigated the factors leading to the wide adoption of SSIs. To fill this research gap, article #5 outlines a structural equation model validated by means of a survey. Remarkably, the study does not empirically support the claim that perceived privacy has an impact on the adoption of SSIs. The study must be interpreted in light of their conceptual and empirical limitations. Conceptually, a forward-facing approach was taken, seeing as respondents were asked to consider their intention, rather than their actual use of SSI. Future research could examine actual Use Behavior instead of Behavioral Intention since SSI was implemented and respondents have become familiar with the concept. Such research would improve the comparability of the results and eliminate the risk of participants misunderstanding underlying concepts (Arnold and Feldman 1981). To date, users have been struggling to assess the facilitating conditions of SSI. An SSI is DLT-based and to be used within the IoT, but users might be unaware of the features underpinning an SSI. Accordingly, future research could further examine the impact of facilitating conditions on privacy and trust among various actors

of such an environment capitalizing on the IoT and DLT. From a design science perspective, further research should examine how applications capitalizing on SSI should be designed in order to comply with regulatory boundaries (cf., Section II.1), and how different designs affect the use of an SSI as well as its privacy-preserving nature. With such knowledge about the DTs at hand, research could again focus on behavioral questions, such as whether and how users change their behavior in the presence of fully trusted privacy-preserving IdM systems.

This doctoral thesis stimulates future research of the IoT, DLT, and their convergence. To name but one concrete subject for future research, data privacy is a recurrent issue restricting as well as motivating use cases of the IoT and DLT. Both DTs affect systems at the data layer. Data privacy boundaries limit, for instance, the design of each of the DTs along with their convergence and application. This limits the opportunities afforded by the use of the two DTs. Future research might, therefore, address this challenge by promoting practical implementations and technological progress, which could lead to an increase in the opportunities provided by the DTs. Meanwhile, the drawbacks of both DTs could be mitigated, for example, by advancing the practicability of zero-knowledge-proofs, which might lead to an increase of opportunities in other fields. Future researchers should further study the role of the user in data privacy research and regulation. The privacy paradox confirmed in this thesis stresses a potential discrepancy between regulatory bodies and the will of the people (i.e., the users). Accordingly, future studies could shape the concept of personal data for practical use within DLT systems and improve how users value their privacy when acting within the IoT. As yet another broader field of future research, the convergence of the IoT and DLT with other DTs is an interesting starting point, for instance when investigating the interplay with AI, in which case data stemming from the IoT could be used for AI algorithms. These can optimize the decision-making of smart things and support efforts to improve DLT-based reputation systems by distinguishing fact from fiction. DLT, finally, provides the integrity and traceability of data required to implement trusted AI applications. Such a convergence could improve the reliability, security, and applicability of a system. This thesis, then, has shown that combining their features frequently allows one to resolve challenges that DTs face in and of themselves. Future researchers should, therefore, not only focus on the features and challenges one DT exhibits when examined in isolation but also respect the fact that DTs affect one another and the system as a whole. Only a comprehensive approach can reveal the full potential and effects of DTs and in doing so set the scene for further technological and societal progress.

IV. Publication Bibliography

Abu-Elkheir, M., Hayajneh, M., and Ali, N. A. 2013. "Data management for the internet of things: design primitives and solution," *Sensors* (13:11), pp. 15582-15612 (doi: 10.3390/s131115582).

Acquisti, A. 2008. "Identity Management, Privacy, and Price Discrimination," *IEEE Security & Privacy Magazine* (6:2), pp. 46-50 (doi: 10.1109/MSP.2008.35).

Aladwani, A. M. 2002. "An Integrated Performance Model Information Systems Projects," *Journal of Management Information Systems* (19:1), pp. 185-210 (doi: 10.1080/07421222.2002.11045709).

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., and Ayyash, M. 2015. "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys & Tutorials* (17:4), pp. 2347-2376.

Allen, C. 2016. *The Path to Self-Sovereign Identity*. http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html. Accessed March 30th, 2021.

Al-Mashari, M., and Zairi, M. 1999. "BPR implementation process: An analysis of key success and failure factors," *Business Process Management Journal* (5:1), pp. 87-112 (doi: 10.1108/14637159910249108).

Alt, R. 2020. "Electronic Markets on blockchain markets," *Electronic Markets* (30:2), pp. 181-188 (doi: 10.1007/s12525-020-00428-1).

Alter, S. 2013. "Work system theory: Overview of core concepts, extensions, and challenges for the future," *Journal of the Association for Information Systems* (14:2), p. 72.

Alter, S. 2019. "Making Sense of Smartness in the Context of Smart Devices and Smart Systems," *Information Systems Frontiers* (14:22), pp. 381-393 (doi: 10.1007/s10796-019-09919-9).

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

Arnold, H. J., and Feldman, D. C. 1981. "Social Desirability Response Bias in Self-Report Choice Situations," *Academy of Management Journal* (24:2), pp. 377-385 (doi: 10.5465/255848).

Arthur, W. B. 2009. *The nature of technology*: *What it is and how it evolves*, New York: Free Press.

Athanasopoulou, A., Haaker, T., and Reuver, M. de 2018. "Tooling for internet-of-things business model exploration: A design science research approach," in *Proceedings of the 26th European Conference on Information Systems*, Portsmouth, UK. 23-28 June, pp. 1-11.

Avison, D. E., Lau, F., Myers, M. D., and Nielsen, P. A. 1999. "Action research," *Communications of the ACM* (42:1), pp. 94-97 (doi: 10.1145/291469.291479).

Bahga, A., and Madisetti, V. K. 2016. "Blockchain platform for industrial internet of things," *Journal of Software Engineering and Applications* (9:10), p. 533.

Baier, M.-S., Lockl, J., Röglinger, M., and Weidlich, R. “An Exploration into Success Factors for Process Digitalization Projects,” *Schmalenbach Journal of Business Research* (under review), pp. 1-29.

Baskerville, and Myers 2004. “Special Issue on Action Research in Information Systems: Making IS Research Relevant to Practice: Foreword,” *MIS Quarterly* (28:3), p. 329 (doi: 10.2307/25148642).

Bauer, L., Bravo-Lillo, C., Fragkaki, E., and Melicher, W. 2013. “A comparison of users' perceptions of and willingness to use Google, Facebook, and Google+ single-sign-on functionality,” in *Proceedings of the 2013 ACM workshop on Digital identity management - DIM '13*, T. Groß and M. Hansen (eds.), Berlin, Germany. 08.11.2013 - 08.11.2013, New York, New York, USA: ACM Press, pp. 25-36.

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

Beer, M., Fridgen, G., Mueller, H.-V., and Wolf, T. 2013. “Benefits Quantification in IT Projects,” *Wirtschaftsinformatik Proceedings 2013* (45), pp. 707-720.

Bélanger, F., and Crossler, R. E. 2011. “Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems,” *MIS Quarterly* (35:4), pp. 1017-1041 (doi: 10.2307/41409971).

Benbunan-Fich, R. 2019. “An affordance lens for wearable information systems,” *European Journal of Information Systems* (28:3), pp. 256-271 (doi: 10.1080/0960085X.2018.1512945).

Benbya, H., Nan, N., Tanriverdi, H., and Yoo, Y. 2020. “Complexity and Information Systems Research in the Emerging Digital World,” *MIS Quarterly* (44:1), pp. 1-17.

Benitez, J., Henseler, J., Castillo, A., and Schuberth, F. 2020. “How to perform and report an impactful analysis using partial least squares: Guidelines for confirmatory and explanatory IS research,” *Information & management* (57:2), pp. 103-168 (doi: 10.1016/j.im.2019.05.003).

Berger, S., Denner M-S., and Röglinger, M. 2018. “The Nature of Digital Technologies: Development of a Multi-layer Taxonomy,” in *Proceedings of the 26th European Conference on Information Systems*, Portsmouth, UK. 23-28 June, pp. 1-18.

Beverungen, D., Buijs, J. C. A. M., Becker, J., Di Ciccio, C., van der Aalst, W. M. P., Bartelheimer, C., Vom Brocke, J., Comuzzi, M., Kraume, K., Leopold, H., Matzner, M., Mendling, J., Ogonek, N., Post, T., Resinas, M., Revoredo, K., del-Río-Ortega, A., La Rosa, M., Santoro, F. M., Solti, A., Song, M., Stein, A., Stierle, M., and Wolf, V. 2020. “Seven Paradoxes of Business Process Management in a Hyper-Connected World,” *Business & Information Systems Engineering* (18:2), p. 279 (doi: 10.1007/s12599-020-00646-z).

Beverungen, D., Müller, O., Matzner, M., Mendling, J., and Vom Brocke, J. 2019. “Conceptualizing smart service systems,” *Electronic Markets* (29:1), pp. 7-18 (doi: 10.1007/s12525-017-0270-5).

Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., and Venkatraman, N. 2013. “Digital Business Strategy: Toward a Next Generation of Insights,” *MIS Quarterly* (37:2), pp. 471-482 (doi: 10.25300/MISQ/2013/37:2.3).

Bocek, T., Rodrigues, B. B., Strasser, T., and Stiller, B. 2017. “Blockchains everywhere-a use-case of blockchains in the pharma supply-chain,” in *Integrated Network and Service Management (IM), 2017 IFIP/IEEE Symposium on*, pp. 772-777.

Boell, S. K., and Cecez-Kecmanovic, D. 2015. "On being 'Systematic' in Literature Reviews in IS," *Journal of Information Technology* (30:2), pp. 161-173 (doi: 10.1057/jit.2014.26).

Borgia, E. 2014. "The Internet of Things vision: Key features, applications and open issues," *Computer Communications* (54), pp. 1-31 (doi: 10.1016/j.comcom.2014.09.008).

Botta, A., Donato, W. de, Persico, V., and Pescapé, A. 2014. "On the integration of cloud computing and internet of things," in *Future internet of things and cloud (FiCloud), 2014 international conference on*, pp. 23-30.

Brem, A., Viardot, E., and Nylund, P. A. 2020. "Implications of the Coronavirus (COVID-19) outbreak for innovation: Which technologies will improve our lives?" *Technological Forecasting and Social Change*, p. 120451 (doi: 10.1016/j.techfore.2020.120451).

Bullen, C. V., and Rockart, J. F. 1981. "A primer on critical success factors,"

Burton-Jones, A., Butler, B., Scott, S., and Xin Xu, S. 2018. "Call for Papers: Next-Generation Information Systems Theories," (42:2), pp. 695-696.

Busquets, J. 2010. "Orchestrating Smart Business Network dynamics for innovation," *European Journal of Information Systems* (19:4), pp. 481-493 (doi: 10.1057/ejis.2010.19).

Camenisch, J., and Lysyanskaya, A. 2001. "An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation," in *Advances in cryptology*, B. Pfitzmann (ed.), Springer, Berlin, Heidelberg, pp. 93-118.

Chanson, M., Bogner, A., Bilgeri, D., Fleisch, E., and Wortmann, F. 2019. "Blockchain for the IoT: Privacy-Preserving Protection of Sensor Data," *Journal of the Association for Information Systems*, pp. 1272-1307 (doi: 10.17705/1jais.00567).

Chatterjee, S., Byun, J., Dutta, K., Pedersen, R. U., Pottathil, A., and Xie, H. 2018. "Designing an Internet-of-Things (IoT) and sensor-based in-home monitoring system for assisting diabetes patients: iterative learning from two case studies," *European Journal of Information Systems* (27:6), pp. 670-685.

Cheng, H. K., and Liang, T.-P. 2018. *Call for Papers: Special Issue of Journal of the Association for Information Systems*: *Smart Service, Smart Business, Smart Research*. https://aisel.aisnet.org/jais/jais_cfp_smart.pdf. Accessed 14 February 2020.

Christidis, K., and Devetsikiotis, M. 2016. "Blockchains and smart contracts for the internet of things," *Ieee Access* (4), pp. 2292-2303.

Cong, L. W., and He, Z. 2019. "Blockchain Disruption and Smart Contracts," *The Review of Financial Studies* (32:5), pp. 1754-1797 (doi: 10.1093/rfs/hhz007).

Conoscenti, M., Vetro, A., and Martin, J. C. de 2016. "Blockchain for the Internet of Things: A systematic literature review," in *Computer Systems and Applications (AICCSA), 2016 IEEE/ACS 13th International Conference of*, pp. 1-6.

Corbett, J., and Mellouli, S. 2017. "Winning the SDG battle in cities: how an integrated information ecosystem can contribute to the achievement of the 2030 sustainable development goals," *Information Systems Journal* (27:4), pp. 427-461 (doi: 10.1111/isj.12138).

Corbin, J. M., and Strauss, A. L. 1990. "Grounded theory research: Procedures, canons, and evaluative criteria," *Qualitative Sociology* (13:1), pp. 3-21 (doi: 10.1007/BF00988593).

Council of the European Union, and European Parliament 2016. *European Union (EU) General Data Protection Regulation*: *GDPR*.

Crossler, R., and Posey, C. 2017. "Robbing Peter to Pay Paul: Surrendering Privacy for Security's Sake in an Identity Ecosystem," *Journal of the Association for Information Systems* (18:7), pp. 487-515 (doi: 10.17705/1jais.00463).

Daugherty, P. 2020. "Managing Technology for the Post-Digital Era," *MIT sloan management review*.

Davenport, T. H., and Westerman, G. 2018. "Why so many high-profile digital transformations fail," *Harvard Business Review*.

Denner, M.-S., Püschel, L., and Roeglinger, M. 2018. "How to Exploit the Digitalization Potential of Business Processes," *Business & Information Systems Engineering* (60:4), pp. 331-349 (doi: 10.1007/s12599-017-0509-x).

Der, U., Jähnichen, S., and Sürmeli, J. 2017. "Self-sovereign Identity - Opportunities and Challenges for the Digital Revolution," *ArXiv* (abs/1712.01767).

Dhamija, R., and Dusseault, L. 2008. "The Seven Flaws of Identity Management: Usability and Security Challenges," *IEEE Security & Privacy Magazine* (6:2), pp. 24-29 (doi: 10.1109/MSP.2008.49).

Dietzmann, C., Heines, R., and Alt, R. 2020. "The Convergence of Distributed Ledger Technology and Artificial Intelligence: An End-to-End Reference Lending Process for Financial Services," in *Proceedings of the 28th European Conference on Information Systems (ECIS)*: *An Online AIS Conference*. 15.06.2020-17.06.2020.

Dinev, T., and Hart, P. 2006. "An Extended Privacy Calculus Model for E-Commerce Transactions," *Information systems research* (17:1), pp. 61-80 (doi: 10.1287/isre.1060.0080).

Dinev, T., Xu, H., Smith, J. H., and Hart, P. 2013. "Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts," *European Journal of Information Systems* (22:3), pp. 295-316 (doi: 10.1057/ejis.2012.23).

Drucker, P. F. 2007. *People and performance*: *The best of Peter Drucker on management*, Boston, Mass: Harvard Business School Press.

Dunphy, P., and Petitcolas, F. A. 2018. "A First Look at Identity Management Schemes on the Blockchain," *IEEE Security & Privacy Magazine* (16:4), pp. 20-29 (doi: 10.1109/MSP.2018.3111247).

Engeström, Y. 1987. *Learning by expanding*: *An activity-theoretical approach to developmental research*, Helsinki: Orienta.

Fay, M., and Kazantsev, N. 2018. "When Smart Gets Smarter: How Big Data Analytics Creates Business Value in Smart Manufacturing," in *Proceedings of the 39th International Conference on Information Systems*. ICIS 2018 Proceedings, San Francisco, USA. 13-16 December, pp. 384-392.

Fedrecheski, G., Rabaey, J. M., Costa, L. C. P., Calcina Ccori, P. C., Pereira, W. T., and Zuffo, M. K. 2020. "Self-Sovereign Identity for IoT environments: A Perspective," in *2020 IEEE Global Internet of Things Summit (GIoTS) proceedings*, Dublin, Ireland. 6/3/2020 - 6/3/2020, Piscataway, NJ: IEEE, pp. 1-6.

Fernández-Caramés, T. M., and Fraga-Lamas, P. 2018. "A Review on the Use of Blockchain for the Internet of Things," *Ieee Access*.

Fernando, N., Ter Chian Felix Tan, Vasa, R., Mouzakis, K., and Aitken, I. 2016. "Examining Digital Assisted Living: towards a Case Study of Smart Homes for the Elderly," in

Proceedings of the 24th European Conference on Information Systems: *Istanbul, Turkey, 12-15 June*.

Fischer, M., Heim, D., Hofmann, A., Janiesch, C., Klima, C., and Winkelmann, A. 2020. "A taxonomy and archetypes of smart services for smart living," *Electronic Markets* (30:1), pp. 131-149 (doi: 10.1007/s12525-019-00384-5).

Fleisch, E., Sarma, S., and Thiesse, F. 2009. "Preface to the focus theme section: 'Internet of things'," *Electronic Markets* (19:2), pp. 99-102 (doi: 10.1007/s12525-009-0016-0).

Fleisch, E., and Thiesse, F. 2007. "On the Management Implications of Ubiquitous Computing: An IS Perspective," in *Proceedings of the 15th European Conference on Information Systems, St. Gallen, Switzerland, 7-9 June*, St. Gallen, Switzerland. 7-9 June, pp. 1929-1940.

Forsythe, S., Liu, C., Shannon, D., and Gardner, L. C. 2006. "Development of a scale to measure the perceived benefits and risks of online shopping," *Journal of Interactive Marketing* (20:2), pp. 55-75 (doi: 10.1002/dir.20061).

Fthi Abadi, Joshua Ellul, and George Azzopardi 2018. "The Blockchain of Things, Beyond Bitcoin: A Systematic Review," in *The 1st International Workshop on Blockchain for the Internet of Things 2018 - 2018 IEEE Blockchain - BIoT*, IEEE.

Gartner 2020. *Hype Cycle for Emerging Technologies*: *2020*, Stamford, CT: Gartner, Inc.

Gaztambide-Fernández, R. A., and Rivière, D. 2019. "A Positive, Safe Environment: Urban Arts High Schools and the Safety Mystique," *Harvard Educational Review* (89:3), pp. 397-420 (doi: 10.17763/1943-5045-89.3.397).

Glaser, F. 2017. "Pervasive Decentralisation of Digital Infrastructures: A Framework for Blockchain-enabled System and Use Case Analysis," in *Proceedings of the 50th Hawaii International Conference on System Sciences*.

Gregor, S. 2006. "The Nature of Theory in Information Systems," *MIS Quarterly* (30:3), pp. 611-642 (doi: 10.2307/25148742).

Gregor, S., and Hevner, A. R. 2013. "Positioning and presenting design science research for maximum impact," *MIS Quarterly* (37:2).

Greifeneder, R., Bless, H., and Fiedler, K. 2017. *Social cognition*: *How individuals construct social reality*, London, New York: Routledge Taylor & Francis Group.

Gubbi, J., Buyya, R., Marusic, S., and Palaniswami, M. 2013. "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems* (29:7), pp. 1645-1660.

Häckel, B., Miehle, D., Pfosser, S., and Übelhör, J. 2017. "Development of Dynamic Key Figures for the Identification of Critical Components in Smart Factory Information Networks," in *Proceedings of the 25th European Conference on Information Systems, Guimarães, Portugal, 5-10 June*, Guimarães, Portugal. 5-10 June, pp. 2767-2776.

Hair, J. F., Hult, G. T. M., Ringle, C. M., and Sarstedt, M. 2017. *A primer on partial least squares structural equation modeling (PLS-SEM)*, Los Angeles, London, New Delhi, Singapore, Washington DC, Melbourne: SAGE.

Halperin, R. 2006. "Identity as an emerging field of study," *Datenschutz und Datensicherheit - DuD* (30:9), pp. 533-537 (doi: 10.1007/s11623-006-0137-y).

Hansen, M., Berlich, P., Camenisch, J., Clauß, S., Pfitzmann, A., and Waidner, M. 2004. "Privacy-enhancing identity management," *Information Security Technical Report* (9:1), pp. 35-44 (doi: 10.1016/S1363-4127(04)00014-7).

Hermann, M., Pentek, T., and Otto, B. 2016. "Design principles for industrie 4.0 scenarios," in *System Sciences (HICSS), 2016 49th Hawaii International Conference on*, pp. 3928-3937.

Hesse, M., and Teubner, T. 2020. "Reputation portability – quo vadis?" *Electronic Markets* (30:2), pp. 331-349 (doi: 10.1007/s12525-019-00367-6).

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

Huber, R., Lockl, J., Röglinger, M., and Weidlich, R. "Conceptualizing Smartness - Results from Analyzing Leading Information Systems Literature," *Schmalenbach Journal of Business Research* (under review), pp. 1-28.

Huber, R. X. R., Püschel, L. C., and Röglinger, M. 2019. "Capturing smart service systems: Development of a domain-specific modeling language," *Information Systems Journal* (29:6), pp. 1207-1255 (doi: 10.1111/isj.12269).

Isaak, J., and Hanna, M. J. 2018. "User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection," *Computer* (51:8), pp. 56-59 (doi: 10.1109/MC.2018.3191268).

Karahanna, E., Straub, D. W., and Chervany, N. L. 1999. "Information Technology Adoption Across Time: A Cross-Sectional Comparison of Pre-Adoption and Post-Adoption Beliefs," *MIS Quarterly* (23:2), pp. 183-206 (doi: 10.2307/249751).

Kehr, F., Kowatsch, T., Wentzel, D., and Fleisch, E. 2015. "Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus," *Information Systems Journal* (25:6), pp. 607-635 (doi: 10.1111/isj.12062).

Kerpedzhiev, G. D., König, U. M., Röglinger, M., and Rosemann, M. 2020. "An Exploration into Future Business Process Management Capabilities in View of Digitalization," *Business & Information Systems Engineering* (14), p. 33 (doi: 10.1007/s12599-020-00637-0).

Khan, M. A., and Salah, K. 2018. "IoT security: Review, blockchain solutions, and open challenges," *Future Generation Computer Systems* (82), pp. 395-411.

Kim, G., Shin, B., and Lee, H. G. 2009. "Understanding dynamics between initial trust and usage intentions of mobile banking," *Information Systems Journal* (19:3), pp. 283-311 (doi: 10.1111/j.1365-2575.2007.00269.x).

Kjærgaard, A., and Gal, U. 2009. "Identity in information systems," in *Proceedings of the 17th European Conference on Information Systems*, Verona, Italy, pp. 1999-2011.

Krasnova, H., Eling, N., Abramova, O., and Buxmann, P. 2014. "Dangers of Facebook Login for Mobile Apps: Is There a Price Tag for Social Information?" in *Proceedings of the 35th International Conference on Information Systems*. ICIS 2014 Proceedings, Auckland, New Zealand.

Krasnova, H., Spiekermann, S., Koroleva, K., and Hildebrand, T. 2010. "Online Social Networks: Why We Disclose," *Journal of Information Technology* (25:2), pp. 109-125 (doi: 10.1057/jit.2010.6).

Kshetri, N. 2017. "Can blockchain strengthen the internet of things?" *IT Professional* (19:4), pp. 68-72.

Lacity, M. C. 2018. "Addressing Key Challenges to Making Enterprise Blockchain Applications a Reality," *MIS Quarterly Executive* (17:3), pp. 201-222.

Landau, S., and Moore, T. 2012. “Economic tussles in federated identity management,” *First Monday* (17:10), pp. 1-29 (doi: 10.5210/fm.v17i10.4254).

Lao, L., Li, Z., Hou, S., Xiao, B., Guo, S., and Yang, Y. 2020. “A Survey of IoT Applications in Blockchain Systems,” *ACM Computing Surveys* (53:1), pp. 1-32 (doi: 10.1145/3372136).

Laufer, R. S., and Wolfe, M. 1977. “Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory,” *Journal of Social Issues* (33:3), pp. 22-42 (doi: 10.1111/j.1540-4560.1977.tb01880.x).

Lee, S. M., and Lim, S. 2018. *Living innovation: from value creation to the greater good*, Emerald Group Publishing.

Lee, S. M., and Trimi, S. 2021. “Convergence innovation in the digital age and in the COVID-19 pandemic crisis,” *Journal of Business Research* (123), pp. 14-22 (doi: 10.1016/j.jbusres.2020.09.041).

Li, S., Da Xu, L., and Zhao, S. 2015. “The internet of things: a survey,” *Information Systems Frontiers* (17:2), pp. 243-259 (doi: 10.1007/s10796-014-9492-7).

Lim, C., and Maglio, P. P. 2018. “Data-Driven Understanding of Smart Service Systems Through Text Mining,” *Service Science* (10:2), pp. 154-180 (doi: 10.1287/serv.2018.0208).

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,” *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 in Payments-A Research Agenda,” in *Proceedings of the 50th Hawaii International Conference on System Sciences*.

Liu, B., Yu, X. L., Chen, S., Xu, X., and Zhu, L. 2017. “Blockchain based data integrity service framework for IoT data,” in *Web Services (ICWS), 2017 IEEE International Conference on*, pp. 468-475.

Lockl, J., Röglinger, M., and Thanner, N. “The Paradoxical Impact of Information Privacy on Privacy-Preserving Technology: The Case of Self-Sovereign Identities,” *Information Systems Frontiers* (under review), pp. 1-44.

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

Lohmann, N. 2013. “Compliance by design for artifact-centric business processes,” *Information Systems* (38:4), pp. 606-618 (doi: 10.1016/j.is.2012.07.003).

Lwin, M., Wirtz, J., and Williams, J. D. 2007. “Consumer online privacy concerns and responses: a power–responsibility equilibrium perspective,” *Journal of the Academy of Marketing Science* (35:4), pp. 572-585 (doi: 10.1007/s11747-006-0003-3).

Makhdoom, I., Abolhasan, M., Abbas, H., and Ni, W. 2019. “Blockchain's adoption in IoT: The challenges, and a way forward,” *Journal of network and computer applications* (125), pp. 251-279.

Malhotra, N. K., Kim, S. S., and Agarwal, J. 2004. “Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model,” *Information systems research* (15:4), pp. 336-355 (doi: 10.1287/isre.1040.0032).

March, S. T., and Smith, G. F. 1995. “Design and natural science research on information technology,” *Decision support systems* (15:4), pp. 251-266.

March, S. T., and Storey, V. C. 2008. “Design science in the information systems discipline: an introduction to the special issue on design science research,” *MIS Quarterly*, pp. 725-730.

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

McLean, R., and Antony, J. 2014. “Why continuous improvement initiatives fail in manufacturing environments?: A systematic review of the evidence,” *International Journal of Productivity and Performance Management* (63:3), pp. 370-376 (doi: 10.1108/IJPPM-07-2013-0124).

Mendling, J., Pentland, B., and Recker, J. 2020. “Building a Complementary Agenda for Business Process Management and Digital Innovation,” *European Journal of Information Systems*, pp. 1-25 (doi: 10.1080/0960085X.2020.1755207).

Mendoza-Tello, J. C., Mora, H., Pujol-Lopez, F. A., and Lytras, M. D. 2018. “Social Commerce as a Driver to Enhance Trust and Intention to Use Cryptocurrencies for Electronic Payments,” *Ieee Access* (6), pp. 50737-50751 (doi: 10.1109/ACCESS.2018.2869359).

Montjoye, Y.-A. de, Hidalgo, C. A., Verleysen, M., and Blondel, V. D. 2013. “Unique in the Crowd: The privacy bounds of human mobility,” *Scientific Reports* (3:1), p. 1376 (doi: 10.1038/srep01376).

Mostarda, L., Navarra, A., and Nobili, F. 2021. “Fast File Transfers from IoT Devices by Using Multiple Interfaces,” *Sensors* (21:1), pp. 1-24 (doi: 10.3390/s21010036).

Mothersbaugh, D. L., Foxx, W. K., Beatty, S. E., and Wang, S. 2012. “Disclosure Antecedents in an Online Service Context,” *Journal of Service Research* (15:1), pp. 76-98 (doi: 10.1177/1094670511424924).

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

Nærland, K., Müller-Bloch, C., Beck, R., and Palmund, S. 2017. “Blockchain to Rule the Waves - Nascent Design Principles for Reducing Risk and Uncertainty in Decentralized Environments,” in *Proceedings of the 38th International Conference on Information Systems*. ICIS 2017 Proceedings, Seoul, South Korea.

Nakamoto, S. 2008. *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://bitcoin.org/bitcoin.pdf. Accessed 31 July 2018.

Noura, M., Atiquzzaman, M., and Gaedke, M. 2019. “Interoperability in Internet of Things: Taxonomies and Open Challenges,” *Mobile Networks and Applications* (24:3), pp. 796-809 (doi: 10.1007/s11036-018-1089-9).

Novales, A., Mocker, M., and Simonovich, D. 2016. “IT-enriched "Digitized" Products: Building Blocks and Challenges,” in *Proceedings of the 22nd Americas Conference on Information Systems, San Diego, USA, 11-14 August*, pp. 1595-1604.

Oberländer, A. M., Röglinger, M., Rosemann, M., and Kees, A. 2018. “Conceptualizing Business-to-Thing Interactions – A Sociomaterial Perspective on the Internet of Things,” *European Journal of Information Systems* (27:4), pp. 486-502 (doi: 10.1080/0960085X.2017.1387714).

Ojo, A., Curry, E., and Janowski, T. 2014. "Designing next generation smart city initiatives-harnessing findings and lessons from a study of ten smart city programs," in *22nd European Conference on Information Systems, Tel Aviv, Israel, 9-11 June*, pp. 1-14.

Paukstadt, U., and Becker, J. 2019. "Uncovering the business value of the internet of things in the energy domain – a review of smart energy business models," *Electronic Markets* (19:3), pp. 359-375 (doi: 10.1007/s12525-019-00381-8).

Pavlou, P. 2011. "State of the Information Privacy Literature: Where are We Now And Where Should We Go?" *MIS Quarterly* (35:4), pp. 977-988 (doi: 10.2307/41409969).

Pavlou, P., and Fygenson, M. 2006. "Understanding and Predicting Electronic Commerce Adoption: An Extension of the Theory of Planned Behavior," *MIS Quarterly* (30:1), pp. 115-143 (doi: 10.2307/25148720).

Peffers, K., Tuunanen, T., Rothenberger, M. A., and Chatterjee, S. 2007. "A design science research methodology for information systems research," *Journal of Management Information Systems* (24:3), pp. 45-77.

Petercsak, R., Maccani, G., Donellan, B., Helfert, M., and Connolly, N. 2016. "Enabling Factors for Smart Cities: A Case Study," in *Proceedings of the 37th International Conference on Information Systems*. ICIS 2016 Proceedings, Dublin, Ireland. 11-14 December, pp. 1628-1637.

Petter, S., DeLone, W., and McLean, E. R. 2013. "Information systems success: The quest for the independent variables," *Journal of Management Information Systems* (29:4), pp. 7-62.

Pitkänen, O., and Tuunainen, V. K. 2012. "Disclosing Personal Data Socially — An Empirical Study on Facebook Users' Privacy Awareness," *Journal of Information Privacy and Security* (8:1), pp. 3-29 (doi: 10.1080/15536548.2012.11082759).

Porru, S., Pinna, A., Marchesi, M., and Tonelli, R. 2017. "Blockchain-oriented software engineering: challenges and new directions," in *Proceedings of the 39th International Conference on Software Engineering Companion*, pp. 169-171.

Porter, M. E., and Heppelmann, J. E. 2014. "Spotlight on managing the Internet of Things," *Harvard Business Review* (92:11), pp. 64-88.

Porter, M. E., and Heppelmann, J. E. 2015. "How Smart, Connected Products Are Transforming Companies," *Harvard Business Review* (93:10), pp. 96-114.

Püschel, L., Röglinger, M., and Brandt, R. 2020. "Unblackboxing Smart Things: A Multi-Layer Taxonomy and Clusters of Non-Technical Smart Thing Characteristics," *IEEE Transactions on Engineering Management*.

Reuver, M. de, Sørensen, C., and Basole, R. C. 2018. "The Digital Platform: A Research Agenda," *Journal of Information Technology* (33:2), pp. 124-135 (doi: 10.1057/s41265-016-0033-3).

Reyna, A., Martin, C., Chen, J., Soler, E., and Diaz, M. 2018. "On blockchain and its integration with IoT. Challenges and opportunities," *Future Generation Computer Systems* (88), pp. 173-190.

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

Risius, M., and Spohrer, K. 2017. "A blockchain research framework," *Business & Information Systems Engineering* (59:6), pp. 385-409.

Rosemann, M. 2013. “The Internet of Things: new digital capital in the hands of customers,” *Business Transformation Journal* (9:1), pp. 6-15.

Rosemann, M. 2020. “Explorative Process Design Patterns,” in *Business Process Management*, D. Fahland, C. Ghidini, J. Becker and M. Dumas (eds.), Cham: Springer International Publishing, pp. 349-367.

Rosemann, M., and Vom Brocke, J. 2015. “The Six Core Elements of Business Process Management,” in *Handbook on Business Process Management 1*: *Introduction, Methods, and Information Systems*, J. Vom Brocke and M. Rosemann (eds.), Berlin, Heidelberg, s.l.: Springer Berlin Heidelberg, pp. 105-122.

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",” *Journal of the Association for Information Systems* (20:9), pp. 1388-1403 (doi: 10.17705/1jais.00571).

Roßnagel, H., Zibuschka, J., Hinz, O., and Muntermann, J. 2014. “Users' willingness to pay for web identity management systems,” *European Journal of Information Systems* (23:1), pp. 36-50 (doi: 10.1057/ejis.2013.33).

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.

Runde, J., and Faulkner, P. 2019. “Theorizing the digital object,” *MIS Quarterly* (43:4), pp. 1279-1302 (doi: 10.25300/MISQ/2019/13136).

Samaniego, M., and Deters, R. 2016. “Blockchain as a Service for IoT,” in *2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pp. 433-436.

Schmiedel, T., Recker, J., and Vom Brocke, J. 2020. “The relation between BPM culture, BPM methods, and process performance: Evidence from quantitative field studies,” *Information & management* (57:2), p. 103175 (doi: 10.1016/j.im.2019.103175).

Schweizer, A., Schlatt, V., Urbach, N., and Fridgen, G. 2017. “Unchaining Social Businesses – Blockchain as the Basic Technology of a Crowdlending Platform,” in *Proceedings of the International Conference on Information Systems (ICIS) 2017,* Seoul. 10.12-13.12.

Sein, M. K., Henfridsson, O., Purao, S., Rossi, M., and Lindgren, R. 2011. “Action Design Research,” *Management Information Systems Quarterly* (35:1), pp. 37-56.

Seltsikas, P., and O'Keefe, R. M. 2010. “Expectations and outcomes in electronic identity management: the role of trust and public value,” *European Journal of Information Systems* (19:1), pp. 93-103 (doi: 10.1057/ejis.2009.51).

Shafagh, H., Burkhalter, L., Hithnawi, A., and Duquennoy, S. 2017. “Towards blockchain-based auditable storage and sharing of iot data,” in *Proceedings of the 2017 on Cloud Computing Security Workshop*, pp. 45-50.

Smith, H. J., Dinev, T., and Xu, H. 2011. “Information Privacy Research: An Interdisciplinary Review,” *MIS Quarterly* (35:4), pp. 989-1015 (doi: 10.2307/41409970).

Solaimani, S., Bouwman, H., and Secomandi, F. 2013. “Critical design issues for the development of Smart Home technologies,” *Journal of Design Research* (11:1), pp. 72-90 (doi: 10.1504/JDR.2013.054067).

Soluk, J., and Kammerlander, N. 2021. “Digital transformation in family-owned Mittelstand firms: A dynamic capabilities perspective,” *European Journal of Information Systems* (16:2), pp. 1-36 (doi: 10.1080/0960085X.2020.1857666).

Song, Z., Sun, Y., Wan, J., Huang, L., and Zhu, J. 2019. “Smart e-commerce systems: current status and research challenges,” *Electronic Markets* (29:2), pp. 221-238 (doi: 10.1007/s12525-017-0272-3).

Spiekermann, S., Grossklags, J., and Berendt, B. 2001. “E-privacy in 2nd generation E-commerce,” in *Proceedings of the 3rd ACM conference on Electronic Commerce - EC '01*, M. P. Wellman and Y. Shoham (eds.), Tampa, Florida, USA. 14.10.2001 - 17.10.2001, New York, New York, USA: ACM Press, pp. 38-47.

Stokkink, Q., and Pouwelse, J. 2018. “Deployment of a Blockchain-Based Self-Sovereign Identity,” in *IEEE International Conference on Internet of Things, IEEE Green Computing and Communications, IEEE Cyber, Physical and Social Computing, and IEEE Smart Data*, Halifax, NS, Canada, IEEE, pp. 1336-1342.

Taylor, P. J., Dargahi, T., Dehghantanha, A., Parizi, R. M., and Choo, K.-K. R. 2019. “A systematic literature review of blockchain cyber security,” *Digital Communications and Networks*, pp. 1-10 (doi: 10.1016/j.dcan.2019.01.005).

Thakor, A. 2015. “Lending Booms, Smart Bankers, and Financial Crises,” *American Economic Review* (105:5), pp. 305-309 (doi: 10.1257/aer.p20151090).

Tobin, A., and Reed, D. 2016. *The Inevitable Rise of Self-Sovereign Identity*: *A white paper from the Sovrin Foundation*. https://sovrin.org/wp-content/uploads/2018/03/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf. Accessed 9 June 2020.

Trkman, P. 2010. “The critical success factors of business process management,” *International Journal of Information Management* (30:2), pp. 125-134 (doi: 10.1016/j.ijinfomgt.2009.07.003).

Truong, N. B., Sun, K., Lee, G. M., and Guo, Y. 2020. “GDPR-Compliant Personal Data Management: A Blockchain-Based Solution,” *IEEE Transactions on Information Forensics and Security* (15), pp. 1746-1761 (doi: 10.1109/tifs.2019.2948287).

Tschorsch, F., and Scheuermann, B. 2016. “Bitcoin and beyond: A technical survey on decentralized digital currencies,” *IEEE Communications Surveys & Tutorials* (18:3), pp. 2084-2123.

Underwood, S. 2016. “Blockchain beyond bitcoin,” *Communications of the ACM* (59:11), pp. 15-17.

Urbach, N., and Ahlemann, F. 2010. “Structural equation modeling in information systems research using Partial Least Squares,” *Journal of Information Technology Theory and Application* (11), pp. 5-40.

van Bertalanffy, L. 1968. *General system theory*: *Foundations, development, applications*, New York: Braziller.

Venkatesh, V., Thong, J. Y., and Xu, X. 2012. “Consumer Acceptance and Use of Information Technology: Extending the Unified Theory of Acceptance and Use of Technology,” *MIS Quarterly* (36:1), pp. 157-178 (doi: 10.2307/41410412).

Venkatesh, V., Thong, J. Y., and Xu, X. 2016. *Unified Theory of Acceptance and Use of Technology: A Synthesis and the Road Ahead*.

Vervest, P., Preiss, K., van Heck, E., and Pau, L.-F. 2004. “The emergence of smart business networks,” *Journal of Information Technology* (19:4), pp. 228-233 (doi: 10.1057/palgrave.jit.2000024).

Vial, G. 2019. “Understanding digital transformation: A review and a research agenda,” *The Journal of Strategic Information Systems* (28:2), pp. 118-144 (doi: 10.1016/j.jsis.2019.01.003).

Walls, J. G., Widmeyer, G. R., and El Sawy, O. A. 1992. “Building an information system design theory for vigilant EIS,” *Information systems research* (3:1), pp. 36-59.

Warkentin, M., Goel, S., and Menard, P. 2017. “Shared Benefits and Information Privacy: What Determines Smart Meter Technology Adoption?” *Journal of the Association for Information Systems* (18:11), pp. 758-786.

Weber, T. A. 2017. “Smart Products for Sharing,” *Journal of Management Information Systems* (34:2), pp. 341-368 (doi: 10.1080/07421222.2017.1334466).

Weinhard, A., Hauser, M., and Thiesse, F. 2017. “Explaining Adoption of Pervasive Retail Systems with a Model based on UTAUT2 and the Extended Privacy Calculus,” in *Proceedings of the 21st Pacific-Asia Conference on Information Systems*.

Wiener, M., Saunders, C., and Marabelli, M. 2020. “Big-data business models: A critical literature review and multiperspective research framework,” *Journal of Information Technology* (35:1), pp. 66-91 (doi: 10.1177/0268396219896811).

Wolfswinkel, J. F., Furtmueller, E., and Wilderom, C. P. M. 2013. “Using grounded theory as a method for rigorously reviewing literature,” *European Journal of Information Systems* (22:1), pp. 45-55 (doi: 10.1057/ejis.2011.51).

Wood, G. 2018. *Ethereum: A Secure Decentralised Generalised Transaction Ledger Byzantium Version*. https://ethereum.github.io/yellowpaper/paper.pdf. Accessed 9 August 2018.

Wortmann, F., and Flüchter, K. 2015. “Internet of things,” *Business & Information Systems Engineering* (57:3), pp. 221-224.

Xu, H., Teo, H.-H., Tan, B. C. Y., and Agarwal, R. 2012. “Research Note —Effects of Individual Self-Protection, Industry Self-Regulation, and Government Regulation on Privacy Concerns: A Study of Location-Based Services,” *23 (4)* (4), pp. 1342-1363 (doi: 10.1287/isre.1120.0416).

Zarkadakis, G., Jesuthasan, R., and Malcolm, T. 2016. *The 3 Ways Work Can Be Automated*. https://hbr.org/2016/10/the-3-ways-work-can-be-automated. Accessed 25 November 2020.

Zheng, Z., Xie, S., Dai, H., Chen, X., and Wang, H. 2017. “An overview of blockchain technology: Architecture, consensus, and future trends,” in *Big Data (BigData Congress), 2017 IEEE International Congress on*, pp. 557-564.

V. Appendix

1 Index of Research Articles

Research Article #1, Section II.1: Conceptualizing Smartness – Results from Analyzing Leading Information Systems Literature

Huber R., Lockl J., Röglinger M., Weidlich R. Conceptualizing Smartness – Results from Analyzing Leading Information Systems Literature. Submitted to (1st revision): *Schmalenbach Journal of Business Research*.

(VHB-JOURQUAL 3: Category B)

Research Article #2, Section II.1: Building a Blockchain Application that Complies with the EU General Data Protection Regulation

Rieger A., Guggenmos F., Lockl J., Fridgen G., 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.

(VHB-JOURQUAL 3: Category B)

Research Article #3, Section II.2: Toward Trust in Internet of Things Ecosystems: Design Principles for Blockchain-Based IoT Applications

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

(VHB-JOURQUAL 3: Category B)

Research Article #4, Section II.3: An Exploration into Success Factors for Process Digitalization Projects

Baier M.-S., Lockl J., Röglinger M., and Weidlich R. An Exploration into Success Factors for Process Digitalization Projects. Submitted to (1st revision): *Business Process Management Journal*.

(VHB-JOURQUAL 3: Category C)

Research Article #5, Section II.3: The Paradoxical Impact of Information Privacy on Privacy-Preserving Technology: The Case of Self-Sovereign Identities

Lockl J., Thanner N., and Röglinger M. The Paradoxical Impact of Information Privacy on Privacy-Preserving Technology: The Case of Self-Sovereign Identities. Submitted to: *Information Technology and Management*.

(VHB-JOURQUAL 3: Category C)

2 Individual Contribution to the Included Research Papers

This thesis is cumulative consisting of five research articles that comprise the main body of work. All articles were developed in teams with multiple authors. Thus, this section details the respective research settings and highlights my individual contributions to each research article.

Research article #1 (Huber et al.) was developed in a team of four authors. All co-authors jointly developed the article's basic concept and created the content. Specifically, I was responsible for guiding one co-author who was in an early stage of his academic career, deriving parts of the conceptual model, and embedding our model within existing theory. During the literature review, I was part of the organizing, analyzing, and coding. Overall, the authors made equal contributions to the content of the research article, and I was involved in each part of the project.

Research article #2 (Rieger et al. 2019) was developed in a team of five authors. I was involved in each step of the project and was responsible for our methodological approach and investigation as well as data collection within the organization. I acquired and conducted expert interviews, observed the project team members, and built the technological framework. Although one co-author took a leading role throughout the project, the other three co-authors and I engaged in each part of the project and helped to discuss and advance our contribution.

Research article #3 (Lockl et al. 2020) was developed in a team of five authors. All co-authors jointly developed the article's basic concept and created the content. Two co-authors developed the prototype in Scotland. I was involved in refining the research project from the beginning, since I was responsible for determining, shaping, and writing the methodological approach. One co-author and I conceptualized the key outcomes of the study. One co-author quitted the research team after the initial submission. During the three revisions, I was the lead of one revision, wrote the change sheet, and incorporated the feedback of the reviewers. Overall, the authors made equal contributions to the content of the research article, and I was involved in each part of the project.

Research article #4 (Baier et al.) was developed in a team of four authors. Three of the co-authors jointly developed the article's basic concept and created the content. As the paper was written in the early stages of my doctoral study, I drove the whole research project. After the joint development of the paper's main idea, I was primarily responsible for the collection of relevant literature, the formulation of the research question, the identification of a comprehensive research approach, and the development of the results (a model of success factors for process digitalization projects). Regarding the latter, I conducted expert interviews to explore process digitalization projects in a real-world scenario and ensure recentness of our

findings. During the whole research process, the paper significantly benefited from the feedback of the experienced co-authors. Together with one co-author, we conducted the further re-submissions, while one co-author stepped back and one new came in. Overall, each author substantially contributed to the research article, and I was involved in each part of the project.

Research article #5 (Lockl et al.) was developed with two co-authors while I was the lead author and established the research setting. I was responsible for the establishment of the research project, shaping the theoretical lens and research model, guiding data collection, drafting the article together with one co-author, and preparing as well as finishing for submission. I assured the quality of the paper and to fit the requirements of the targeted outlet. Although the research article traces back, to a substantial extent, to my leading role, the two co-authors engaged in each part of the project and helped to discuss and advance our contribution.

3 Research Article #1: Conceptualizing Smartness – Results from Analyzing Leading Information Systems Literature

Authors: Huber, R., Lockl J., Röglinger M., and Weidlich R.

Title: Conceptualizing Smartness – Results from Analyzing Leading Information Systems Literature

Submitted to: *Schmalenbach Journal of Business Research* (1st revision)

Extended Abstract: In recent years, the term 'smartness' has entered widespread use in research and in daily life. It has emerged with various applications of the Internet of Things, such as smart homes and smart factories (Wiener et al. 2020). In information systems (IS) research, in particular, the term has become increasingly popular and important (Huber et al. 2019).

However, rapid technological development and inflationary use of the term mean that, in IS research, a common understanding of smartness has not yet been established (Alter 2019). For example, Beverungen et al. (2019) define smart things as boundary objects, interacting between customers and service providers, whereas Oberländer et al. (2018) define smart things as physical objects equipped with own agency and with human-like cognitive characteristics. Hence, most definitions of smartness-in-the-context-of-smart-things that IS research currently offers are either highly domain-specific or very general. And while it is recognized that smartness encompasses more than the use of impressive information technology applications, a unified conceptualization of what smartness is and how it is created remains lacking. This lack of knowledge hampers scientific progress as well as clear-headed decision-making in industry. Our study intends to fill this gap by answering the following research question: *What is smartness and how does it manifest in IS research?*

To address this research gap, we aim to conceptualize smartness to the extent of understanding the actions that take place when something is perceived as smart. To this end, we conducted a structured literature review identifying and connecting concepts linked to smartness that repeatedly appear in IS research. We followed an approach, proposed by

Wolfswinkel et al. (2013), to conceptualize smartness and its manifestations by using and combining techniques from Grounded Theory to analyze data from the structured literature review. Thereby, we aim to develop a thorough and well-grounded analysis of smartness which would reveal connections between related concepts and develop a clear concept of smartness itself.

In our study, we found that smartness occurs through actions, in which smart things and individuals interact, process information, and make data-based decisions that are perceived as smart. Building on these findings, we propose the concept of a 'smart action' and derive a general definition of smartness. The concept is in line with the general systems theory, activity theory, and information processing theory, which are theories that have already been applied in IS research.

Our findings augment knowledge about how smartness is formed, offering a new perspective on smartness, and providing a type I theory to describe and analyze interactions that take place in a smart action (Gregor 2006). The concept of a smart action will unify and increase understanding of 'smartness' in IS research. It will support future research by providing a concept for describing, analyzing, and designing smart actions, smart devices, and smart services.

Keywords: Smartness; smart action; smart thing; internet of things; digital technologies; literature review; grounded theory

References

Alter, Steven. 2019. Making Sense of Smartness in the Context of Smart Devices and Smart Systems. Information Systems Frontiers 14 (22): 381–393. doi: 10.1007/s10796-019-09919-9.

Beverungen, Daniel, Oliver Müller, Martin Matzner, Jan Mendling, and Jan Vom Brocke. 2017. Conceptualizing smart service systems. Electronic Markets 83 (10): 7–18. doi: 10.1007/s12525-017-0270-5.

Gregor, S. 2006. The Nature of Theory in Information Systems. MIS Quarterly 30 (3): 611–642. doi: 10.2307/25148742.

Huber, Rocco X. R., Louis C. Püschel, and Maximilian Röglinger. 2019. Capturing smart service systems: Development of a domain-specific modelling language. Information Systems Journal 29 (6): 1207–1255. doi: 10.1111/isj.12269.

Oberländer, Anna M., Maximilian Röglinger, Michael Rosemann, and Alexandra Kees. 2018. Conceptualizing business-to-thing interactions – A sociomaterial perspective on the Internet of Things. European Journal of Information Systems 27 (4): 486–502. doi: 10.1080/0960085X.2017.1387714.

Wiener, Martin, Carol Saunders, and Marco Marabelli. 2020. Big-data business models: A critical literature review and multiperspective research framework. Journal of Information Technology 35 (1): 66–91. doi: 10.1177/0268396219896811.

Wolfswinkel, Joost F., Elfi Furtmueller, and Celeste P. M. Wilderom. 2013. Using grounded theory as a method for rigorously reviewing literature. European Journal of Information Systems 22 (1): 45–55. doi: 10.1057/ejis.2011.51.

4 Research Article #2: Building a Blockchain Application that Complies with the EU General Data Protection Regulation

Authors: Rieger A., Guggenmos F., Lockl J., Fridgen G., and Urbach N.

Title: Building a Blockchain Application that Complies with the EU General Data Protection Regulation

Published in: *MIS Quarterly Executive* (2019)

Abstract: Compliance with Europe's General Data Protection Regulation (GDPR) is a significant challenge for many blockchain projects. Essential for meeting this challenge are the establishment of clear responsibilities for compliance, the securing of lawful bases for data processing, and the observance of the right to erasure and rectification. Here, we describe how Germany's Federal Office for Migration and Refugees managed these challenges and reconciled its blockchain solution for cross-organizational workflow coordination with the GDPR. Moreover, we provide three recommendations for the management of GDPR requirements and the design of GDPR-compliant blockchain solutions.

Keywords: Blockchain; cross-organizational workflow coordination; data privacy; GDPR; refugee management

5 Research Article #3: Toward Trust in Internet of Things Ecosystems: Design Principles for Blockchain-Based IoT Applications

Authors: Lockl J., Schlatt V., Schweizer A., Urbach N., and Harth N.

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

Published in: *IEEE Transactions on Engineering Management* (2020)

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 points 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 (DSR) approach. 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 like high operating costs through smart contract computation fees. Further, semi-structured 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; IoT; internet of things; design principle; ecosystem; cloud computing

6 Research Article #4: An Exploration into Success Factors for Process Digitalization Projects

Authors: Baier, M.-S., Lockl J., Röglinger M., and Weidlich R.

Title: An Exploration into Success Factors for Process Digitalization Projects

Submitted to: *Business Process Management Journal* (1st revision)

Extended Abstract: Digitalization substantially impacts organizations, which increasingly use digital technologies (DTs) to improve and innovate their business processes. DTs range from established technologies (e.g., social, mobile, analytic, and cloud) (Fitzgerald et al. 2014) to emerging ones (e.g., distributed ledger, artificial intelligence, extended reality, and quantum computing) (Daugherty 2020).

Although digitalization brings about manifold opportunities, organizations struggle with deriving value from DTs (Davenport and Westerman 2018), as they do not fully understand how to use DTs. To capitalize on the opportunities of digitalization, organizations must embed DTs into existing or novel processes (Denner et al. 2018), which commonly happens through projects. In our study, we refer to projects that leverage DTs for improving business processes in terms of their effectiveness and efficiency as process digitalization projects (PDPs). While there are methods and tools for identifying process digitalization ideas and for defining related projects, guidance on the implementation of PDPs is missing. In line with the importance of successful PDPs, our research question is as follows: *Which factors drive PDP success?*

To answer this question, we followed an exploratory approach. As a first step, we extracted candidate SFs from the business process management, project management, and digitalization literature via a structured literature review. Screening selected databases brought initial 645 studies, whereof 101 studies were analyzed in-depth, which resulted in a final set of 38 studies that gave valuable insights through 1029 success codes. Through axial coding, we built an ex-ante list, which included 30 candidate SFs covering a broad spectrum of socio-technical topics. In the next step, selective coding helped us to develop categories for grouping

the SF candidates included in the ex-ante list (Wolfswinkel et al. 2013). The seven categories are namely strategy, structure, culture, people, process, project, and technology. We then validated, refined, and extended these intermediate results through interviews with 21 members of diverse PDP teams in the German manufacturing industry. This step helped us to gain access to first-hand experience which may not yet have found their way into the academic literature and resulted in the ex-post list of candidate PDP success factors (Lange et al. 2016).

The key contribution of our study is in the PDP Success Model, which links the identified candidate SFs with relevant PDP success criteria and proposed preliminary success rationales. The model addresses the lack of knowledge on how organizations can leverage DTs to improve and innovate business processes. The PDP Success Model covers 38 candidate PDP success factors, whereof 30 are already backed by the literature and eight have emerged during the interviews. Furthermore, the success factors are structured according to seven categories from the literature.

Our work is the first to systematically explore PDP success factors. The findings show that PDPs require a unique set of success factors, which combine established as well as hitherto underrepresented knowledge. The PDP Success Model extends the knowledge on business process management and serves as foundation for future research on process digitalization and the successful implementation of PDPs.

Keywords: Business process management; digitalization; success factors; literature review; exploratory interviews

References

Daugherty, Paul. 2020. Managing Technology for the Post-Digital Era. *MIT sloan management review*. 2020. https://sloanreview.mit.edu/article/managing-technology-for-the-post-digital-era/. Accessed Retrieved 16 April 2020.

Davenport, Thomas H., and George Westerman. 2018. Why so many high-profile digital transformations fail. *Harvard Business Review*. 2018. https://hbr.org/2018/03/why-so-many-high-profile-digital-transformations-fail. Accessed Retrieved at 16 April, 2020.

Denner, Marie-Sophie, Louis Püschel, and Maximilian Roeglinger. 2018. How to Exploit the Digitalization Potential of Business Processes. *Business & Information Systems Engineering* 60 (4): 331–349. doi: 10.1007/s12599-017-0509-x.

Lange, M., Mendling, J. and Recker, J. (2016), "An empirical analysis of the factors and measures of Enterprise Architecture Management success", *European Journal of Information Systems*, Vol. 25 No. 5, pp. 411–431.

Fitzgerald, Michael, Nina Kruschwitz, Didier Bonnet, and Michael Welch. 2014. Embracing digital technology: A new strategic imperative. *MIT sloan management review* 55 (2): 1.

Wolfswinkel, Joost F., Elfi Furtmueller, and Celeste P. M. Wilderom. 2013. Using grounded theory as a method for rigorously reviewing literature. *European Journal of Information Systems* 22 (1): 45–55. doi: 10.1057/ejis.2011.51.

7 Research Article #5: The Paradoxical Impact of Information Privacy on Privacy-Preserving Technology: The Case of Self-Sovereign Identities

Authors: Lockl J., Thanner N., and Röglinger M.

Title: The Paradoxical Impact of Information Privacy on Privacy-Preserving Technology: The Case of Self-Sovereign Identities

Submitted to: *Information Technology and Management*

Extended Abstract: Advance of digital technologies brings great benefits but also takes users at risk of the dark sides of the internet. Users must balance the risks of sharing sensitive information with the benefits of digital services (Dinev and Hart 2006). They thereby often willingly disclose personal information despite expressing significant privacy concerns (Smith et al. 2011). Recent examples – such as the scandal of Facebook sharing user data to the analytics company Cambridge Analytica – illustrate the impact that information disclosure can have on nations, society, and citizens. Preventive mechanisms and privacy-preserving solutions could overcome this challenge (Isaak and Hanna 2018). As such, a self-sovereign identity (SSI) is a privacy-preserving technology that enables users to limit the disclosure of their personal information and control their digital identity without losing access to digital services (Mühle et al. 2018).

However, studies involving prospective users of privacy-preserving technologies, such as an SSI, remain scarce. This scarcity has led to calls for more behavioral research in the identity management domain (Crossler and Posey 2017). Current research lacks an empirical examination of users' perceptions of privacy in the context of the adoption of identity management systems.

Addressing these shortcomings, we combined and adapted existing theories of technology acceptance and information privacy research to fit the identity management context, and specifically, the novel context of SSIs. We derived our hypotheses from both research streams. To validate them empirically, we operationalized each construct with reflective

measurement indicators derived from renowned studies in the information privacy and technology acceptance literature (e.g., Dinev et al. 2013), and pre-tested the resulting questionnaire with multiple respondents. We developed a structural equation model and used the Partial-Least-Square approach to investigate the relationships in our research model (Benitez et al. 2020). Lastly, we analyzed the data with SmartPLS 3 and determined the theoretical and managerial implications of our study.

The study (i) provides empirical and behavioral insights for the adoption of identity management- and blockchain-based systems, (ii) improves the understanding of the interplay of privacy and technology acceptance by combining existing theories from these two domains, and (iii) examines the importance of information privacy from a user perspective against the background of privacy-preserving technologies.

The results contradict existing theory that privacy is critical to the success of identity management systems. Analogous to the privacy paradox, the study does not lend empirical support that perceived privacy has an impact on the adoption of an SSI. On the contrary, these findings contradict the prevailing view of privacy as a key factor for identity management systems and contribute to knowledge on privacy and adoption behavior.

Keywords: Blockchain; identity management; information privacy; self-sovereign identity; structural equation model; technology acceptance research

References

Benitez, J., Henseler, J., Castillo, A., & Schuberth, F. (2020). How to perform and report an impactful analysis using partial least squares: Guidelines for confirmatory and explanatory IS research. Information & Management, 57, 103–168. doi:10.1016/j.im.2019.05.003.

Crossler, R., & Posey, C. (2017). Robbing Peter to Pay Paul: Surrendering Privacy for Security's Sake in an Identity Ecosystem. Journal of the Association for Information Systems, 18, 487–515. doi:10.17705/1jais.00463.

Dinev, T., & Hart, P. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions. Information Systems Research, 17, 61–80. doi:10.1287/isre.1060.0080.

Dinev, T., Xu, H., Smith, J. H., & Hart, P. (2013). Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. European Journal of Information Systems, 22, 295–316. doi:10.1057/ejis.2012.23.

Isaak, J., & Hanna, M. J. (2018). User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. Computer, 51, 56–59. doi:10.1109/MC.2018.3191268.

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

Smith, H. J., Dinev, T., & Xu, H. (2011). Information Privacy Research: An Interdisciplinary Review. MIS Quarterly, 35, 989–1015. doi:10.2307/41409970.