International Journal of Innovation and Technology Management
Vol. 20, No. 4 (2023) 2350025 (39 pages)
© World Scientific Publishing Company
DOI: 10.1142/S0219877023500256

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

Jannik Lockl[*,†,§], Nico Thanner[*], Manuel Utz[*] and Maximilian Röglinger[*,‡]

[*]*University of Bayreuth*
Universitätsstr. 30, 95447 Bayreuth, Germany

[†]*UCL Centre for Blockchain Technologies*
Malet Place, London WC1E 6BT, UK

[‡]*Branch Business & Information Systems Engineering of the Fraunhofer*
FIT and FIM Research Center
Wittelsbacherring 10, 95444 Bayreuth, Germany
[§]*jannik.lockl@gmail.com*

Received 27 February 2022
Revised 17 December 2022
Accepted 28 December 2022
Published 14 March 2023

Advance of digital technologies brings great benefits but takes users at risk of the dark sides of the internet. Preventive mechanisms and privacy-preserving solutions could overcome this challenge. As such, self-sovereign identities (SSIs) provide users with increased control over personal information. However, users neglect their privacy in favor of the most convenient solution. In this paper, we empirically examine how information privacy influences adoption of SSIs. Our results contradict the existing theory that privacy is critical to the success of identity management (IdM) 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 IdM 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.

1. Introduction

The disclosure of personal information is fundamental to the use of digital services [Forsythe *et al.*, (2006)], yet increases concerns over loss of privacy and identity theft [Hille *et al.* (2015)]. Users must balance the risks of sharing sensitive information with the benefits of digital services [Dinev and Hart (2006)], but they 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. These cases highlight

[§]Corresponding author.

the need for solving the problems related to nature of the internet [Lee (2015)], for instance, through new privacy-preserving technologies and policy laws [Isaak and Hanna (2018)]. 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); Stokkink and Pouwelse (2018); Hesse and Teubner (2020)]. In other words, an SSI is an identity management (IdM) system that enables users to fully own and manage their digital identities [Dunphy and Petitcolas (2018); Mühle *et al.* (2018)]. Features of SSIs may provide a solution to privacy concerns by returning users' control over identity and personal information while enabling them to benefit from digital services [Mühle *et al.* (2018); Acquisti (2008)]. Thus, an SSI can enable users to experience "the convenience and freedom of expression [of anonymity]" [Lee (2015, S. iii)], while benefiting from digital services. SSI might, therefore, even present a solution to counteract anonymous fraud and crime as key challenges of the Bright Internet [Lee (2015); Lee *et al.* (2020)]. To leverage its full potential, a critical number of users and service providers must implement and use an IdM system that builds on an SSI. Such an IdM must cover multiple digital services from different providers so that the system is convenient for users. Unfortunately, only a small number of IdM systems — for example, Facebook's single sign-on (SSO) — have, so far, achieved widespread adoption across multiple digital services [Hansen *et al.* (2004); Jensen (2011)].

Blockchain regularly is a central technological component of an SSI. Since Nakamoto introduced the peer-to-peer (P2P) electronic cash system [Nakamoto (2008)], Bitcoin, blockchain technology has emerged into the public consciousness igniting interests in research [Lee *et al.* (2020)] and practice [Chong *et al.* (2019)]. Blockchains are distributed databases that serve as a physically decentralized but logically centralized source of truth for information [Alt (2020); Rossi *et al.* (2019)]. Multiple studies ascribe substantial potential to blockchain in different use cases [Constantinides *et al.* (2018); Du *et al.* (2019)]. One application domain that aims to capitalize on the features of blockchain is that of IdM and decentralized identities. The importance of digital identities is increasing due to the growing importance of the Internet in our daily lives [Crossler and Posey (2017); Hille *et al.* (2015); Whitley *et al.* (2014)]. Yet, individuals must rely on an intermediating registration authority to use digital services, but they could instead trust a blockchain-based system. Therein, changes in data are transparent, and the transaction history cannot be tampered [Dunphy and Petitcolas (2018); Hawlitschek *et al.* (2018)]. Blockchain then pairs identification and authentication and ensures consensus, transparency, and integrity [Mühle *et al.* (2018); Rieger *et al.* (2021)], comparable to the preventive cybersecurity measures of the Bright Internet initiative, in which blockchain can serve as an audit trail to prevent misuse of personal data [Lee *et al.* (2020); De Filippi *et al.* (2020)].

The increasing importance of digital identities means that users must, in turn, spend increasing effort managing their identities, for example, administering different account information and passwords for various digital services. These efforts are to the detriment of the value proposition of digital services [Hansen *et al.* (2004)].

IdM systems can support users in managing their digital identities and facilitate the use of digital services, and are, thus, an emerging field for practice and research. However, the field of IdM still lacks knowledge about the interplay between identity and technologies, and the factors affecting user adoption of IdM systems [Kjærgaard and Gal (2009); Halperin (2006); Alkhalifah and D'Ambra (2015)]. Privacy is one factor thought to influence adoption. For example, Hansen *et al.* [2004] claimed that privacy is the key factor determining the acceptance of IdM systems. In the United Kingdom, for example, users refused to adopt identity cards due to a lack of protection of private data [Landau and Moore (2012)]. On the other hand, Facebook's SSO mechanism contradicts these observations and has become the most popular IdM system, despite the fact that the system shares excessive user data with the digital service to which users sign up [Landau and Moore (2012); Buxmann *et al.* (2014)]. This discrepancy highlights the need for advance in knowledge on IdM. Research must investigate the impact of privacy and privacy concerns through the assessment of individuals' privacy perceptions [Crossler and Posey (2017); Hansen *et al.* (2008); Mueller *et al.* (2006)].

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 IdM domain and studies about these systems from a user perspective [Alkhalifah and D'Ambra (2015); Bélanger and Crossler (2011); Crossler and Posey (2017); Seltsikas and O'Keefe (2010)]. Current research lacks an empirical examination of users' perceptions of privacy in the context of the adoption of IdM systems. Given these considerations, this study aims at understanding the effect of information privacy on the intention to adopt a system for SSIs. Thereby the specific goals of this paper are (i) to present empirical and behavioral insights for the adoption of IdM- and blockchain-based systems, (ii) to understand the interplay of privacy and technology acceptance by combining existing theories from these two domains, and (iii) to examine the importance of information privacy from a user perspective against the background of privacy-preserving technologies.

In this study, we combine and adapt existing theories of technology acceptance and information privacy research to fit the IdM context — specifically, the novel context of SSIs. We deduce determinants of behavioral intention to use an SSI system, since consumers yet cannot use an SSI-system breadthways as well as perceived information privacy to develop a research model defining and hypothesizing the relationships between the variables examined. To validate our hypotheses 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); Krasnova *et al.* (2010); Pavlou and Fygenson (2006)], and pre-tested the resulting questionnaire with multiple respondents [Kim *et al.* (2009)]. We developed a structural equation model (SEM) and used the Partial-Least-Square (PLS) approach to investigate the relationships in our research model [Benitez *et al.* (2020); Urbach and Ahlemann (2010)]. Lastly, we analyzed the data with SmartPLS 3 and determined the theoretical and managerial implications of our study.

The remainder of this study is structured as follows: First, we outline the theoretical foundations of information privacy, IdM, blockchain and SSI, as well as technology acceptance research. Next, we present our research model and our hypotheses. In Sec. 4, we clarify our research method before presenting the results of our survey. In Sec. 6, we discuss the hypotheses, our theoretical contribution, and the managerial implications. Finally, we shed light on each of the limitations of our work as well as fruitful paths for future research and conclude the study.

2. Theoretical Foundations

2.1. *Information privacy*

The internet enables the collection, storage, processing, and utilization of personal information by multiple parties [Smith *et al.* (2011)]. As companies often misuse personal information, consumers' privacy has become an important topic of the information age [Pavlou and Fygenson (2006); Smith *et al.* (2011); Spiekermann *et al.* (2001)], and information privacy has become an important subject of research [Bélanger and Crossler (2011); Li (2012); Pavlou (2011)].

Despite the significance of privacy in current research, several discipline-specific definitions and conceptualizations of privacy exist [Smith *et al.* (2011)]. In the field of law, privacy is seen as a right [Clarke (1999); Warren and Brandeis (1890)]. Social science and information systems (ISs), in contrast, highlight control of one's information as an integral part of privacy [Altman (1975); Westin (1967); Schoeman (1984)]. As a result, some researchers equate privacy with control [Smith *et al.* (2011)]. Other researchers define privacy as a state of restricted access [Schoeman (1984)]. To resolve confusion regarding definitions of privacy, Smith *et al.* [2011] classified different approaches in value-based and cognate-based definitions. According to the value-based definition, privacy is a human right and part of society's norms and values. In contrast, the cognate-based definition sees privacy as an individual's mind, perceptions, and cognition. A significant stream within the latter category highlights the role of control in the context of privacy. According to definitions by Westin [1967] and Altman [1975], control of transactions in order to reduce privacy risks is central to privacy [Margulis (1977)]. Control becomes particularly relevant in contexts with a high risk of opportunistic behavior and a breach of social contracts [Malhotra *et al.* (2004)]. Consequently, control plays a major role in information privacy as consumers often disclose highly sensitive personal data when conducting transactions on the internet [Malhotra *et al.* (2004)]. Furthermore, control is a crucial factor for decreasing privacy concerns and perceived privacy invasions [e.g. Culnan and Armstrong (1999); Dinev and Hart (2004)]. We ground our understanding of privacy on the cognate-based conceptualization, which has emerged as the dominant stream in IS and so provides a suitable lens for our study [Smith *et al.* (2011)]. Following research practice [Smith *et al.* (2011); Karwatzki *et al.* (2017)], we use the term "privacy" to refer to "information privacy", even though information privacy is only one element of the larger concept [Bélanger and Crossler (2011)].

Analogous to the definition of privacy, measuring privacy in behavioral research is similarly complex [Smith *et al.* (2011)]. The most common proxies for privacy are information privacy concerns and perceived information privacy [Dinev *et al.* (2006, 2013); Xu *et al.* (2011)]. Researchers often combine these privacy constructs with other privacy-related theories [Smith *et al.* (2011)]. The most common theory is the privacy calculus [Li (2012)]. Rational individuals perform a risk-benefit analysis (i.e. privacy calculus) to decide whether to disclose personal information [Culnan and Armstrong (1999); Acquisti and Grossklags (2005); Simon (1959)]. Consumers disclose information if they perceive that the overall benefits balance or exceed the perceived risk of disclosure [Dinev and Hart (2006)]. Disclosure incentives for customers can be economic benefits [e.g. Culnan and Armstrong (1999); Xu *et al.* (2009)], the personalization or increased convenience of services [e.g. Chellappa and Sin (2005); Hann *et al.* (2007)], or social or relational benefits [e.g. Culnan and Armstrong (1999); Lu *et al.* (2004)]. Nevertheless, studies show that the fundamental assumption that individuals make rational choices is flawed, and that individuals tend to decide irrationally [Dinev *et al.* (2015)]. Consequently, the privacy decisions of individuals often seem paradoxical. Users may, for example, state that they have serious concerns about privacy but readily submit their personal information [Smith *et al.* (2011)]. This phenomenon is called the "privacy paradox", which describes a dichotomy between attitudes to privacy and actual behaviors [Spiekermann *et al.* (2001); Norberg *et al.* (2007); Bélanger and Crossler (2011)]. These opposing reactions can be explained by limited rationality in the decision-making process [Acquisti (2004); Acquisti and Grossklags (2005)], individuals' tendency to discount future benefits and risk [O'Donoghue and Rabin (2001, 2000)], or situational factors (e.g. factors related to a specific website or online company) that override privacy concerns [Li *et al.* (2011)].

2.2. *Foundations of identity management*

An identity answers question such as "who am I?" and "what am I like?" [Chatman *et al.* (2005)]. Although there is no consistent definition of identity in academic literature, definitions tend to share three fundamental characteristics [Weick (1995)]. The first is that identities represent or are associated with entities (e.g. individuals or organizations) [Camp (2004); Jøsang and Pope (2005)]. In keeping with the first, the second is that identities cannot be related to more than one entity, although an individual might have several identities that emerge in different social contexts, which are referred to as "partial identities" [Jøsang and Pope (2005); Hansen *et al.* (2004); Talamo and Ligorio (2001)]. The third characteristic is that identities consist of a set of temporary or permanent individual attributes [Camp (2004)].

IS research focuses on identities in digital contexts [Whitley *et al.* (2014)]. These digital identities consist of "a set of claims made by one digital subject about itself or another digital subject" [Cameron (2005, S. 11)] and enable digital subjects to prove that they are who they claim to be and to distinguish between different entities [Mühle *et al.* (2018)]. As identities are fundamental to participation in online transactions [Mühle *et al.* (2018); Whitley *et al.* (2014)], the management of identities is subject to significant attention. IdM enables identity holders to authenticate, identify, and authorize within an identity domain. As the importance of digital services grows, a manual IdM can limit access to the benefits of online transactions [Hansen *et al.* (2004); Jøsang and Pope (2005)]. IdM systems, therefore, facilitate the management of identities [Dhamija and Dusseault (2008)]. These technologies or programs establish the collection and connection of identifiers with identity attributes, enable a digital service to trust in the identity of a user, and allow the user to engage these services [Dhamija and Dusseault (2008); Dunphy and Petitcolas (2018); Hansen *et al.* (2004)]. IdM systems enable seamless transactions, combat fraud, connect information on multiple devices, and enable the development and use of innovative services [Hansen *et al.* (2008)].

Several different IdM systems exist, and these have evolved in recent years [Hansen *et al.* (2004); Allen (2016)]. Centralized IdM models are closed systems in which a single exclusive authority acts as a provider of identifiers and credentials [Dhamija and Dusseault (2008); Jøsang and Pope (2005)]. As a single authority controls and manages identities, users can raise concerns about privacy, security, and trust [Allen (2016); Hansen *et al.* (2004)]. In contrast, federated identity management (FIM) systems distribute an identity and enable authentication across domains [Landau and Moore (2012); Maler and Reed (2008)]. FIM systems try to reduce the number of identifiers and credentials a user has to manage and to enhance the usability and user experience of digital services [Jøsang and Pope (2005)]. As identity providers need to share the personal information of users within the federated domain, these systems are often a source of significant user concern regarding privacy [Maler and Reed (2008)]. User-Centric IdM systems go one step further by enabling clients to use and control their identity across multiple digital services. These systems selectively disclose personal data and credentials for authentication on digital services [Allen (2016); Hansen *et al.* (2004)]. Since User-Centric IdM systems focus on authentication, users must be able to manage their identifiers and credentials effectively, which requires a high level of usability [Jøsang and Pope (2005)]. As an alternative to IdM systems that still rely mostly on central entities, decentralized IdM systems have emerged. They do not rely on a central identity provider but distribute identities across multiple local user repositories [Reed *et al.* (2018); Ahn *et al.* (2004); Dhamija and Dusseault (2008)].

2.3. *Blockchain and self-sovereign identities*

Blockchains can serve as underlying technology for decentralized IdM systems [Mühle *et al.* (2018)]. The idea behind blockchain is based on the concept of Distributed-Ledger-Technologies (DLT). DLTs avoid centralized data storage by using P2P networks to distribute data across nodes of a network [Amend *et al.* (2021); Cho *et al.* (2021)]. These nodes commonly make decisions about the actualization of stored data. Each node maintains a local copy of all data and can distribute new data across the network [Ziolkowski *et al.* (2020)]. Blockchains are databases that store transactions on decentralized nodes [Glaser (2017)]. Transactions are validated in the network and combined to form blocks. New blocks are cryptographically chained to their predecessor, which generates a chronological, tamper-resistant order of all transactions: a chain of blocks [Du *et al.* (2019); Chong *et al.* (2019)]. Central to the functioning of blockchains are the hashing and linking of transactions, which produce validated and retrospectively tamper-resistant transactions that reduce risks for users [Glaser (2017); Beck *et al.* (2018); Zhang *et al.* (2019)]. Blockchains use consensus mechanisms like Proof-of-Work and Proof-of-Stake to determine the database's consistency [Beck *et al.* (2018); Lock *et al.* (2020)]. Newer generations of DLTs, such as Ethereum, also facilitate executable programs in forms of so-called smart contracts. These are protocols triggered by an external event that runs on every node of the network [Glaser (2017); Guggenberger *et al.* (2021); Lock *et al.* (2020)].

One alternative to user-centric IdMs are decentralized IdM systems, which distribute identifiers across multiple user repositories [Ahn *et al.* (2004); Dhamija and Dusseault (2008); Reed *et al.* (2018)]. Blockchains serve as a technological infrastructure in decentralized IdM systems, extended by the concept of Decentralized Identifiers (DIDs). A DID represents an entity within such systems, which is persistent and not governed by a central authority. DIDs support authentication via cryptographic proofs (e.g. digital signatures) [W3C (2019a); Reed *et al.* (2018)], and serve as identifiers for verifiable claims (VCs), which are claims verified through the digital signature of an identity provider [Mühle *et al.* (2018)]. The World Wide Web Consortium (W3C) conceptualized DIDs following privacy by design requirements. Hence, VCs capitalize on DIDs to enhance the security and privacy of a person's identity [W3C (2019a)].

An SSI is such a concept for IdM and is regularly based on blockchain, though approaches exist that do not necessarily require a blockchain for SSI [Hoess *et al.* (2022); Sedlmeir *et al.* (2021)]. An SSI enables users to fully own and manage their digital identities [Dunphy and Petitcolas (2018); Mühle *et al.* (2018)]. An SSI is based on three core principles — the security, controllability, and portability of identities [Allen (2016); Tobin and Reed (2016)] — which are achieved and maintained using blockchain. The technology replaces the registration authority, pairing identification and authentication based on a public key infrastructure (PKI) where the public key is stored as a value of the identifier on the blockchain [Mühle *et al.* (2018)]. Blockchain assures consensus, transparency, and integrity when it comes to transactions, and thus, provides elements essential for IdM systems [Dunphy and Petitcolas (2018)]. Identity information can be referenced on the blockchain without being owned by a single authority. Furthermore, changes in data are made transparent, and historical activity cannot be tampered with. Blockchain also increases the inclusivity of humans restricted in their access to digital services and can reduce costs. Lastly, users gain increased control over their digital identifiers and can minimize the disclosure of personal data [Dunphy and Petitcolas (2018)]. An SSI uses zero-knowledge-proofs (ZKPs), which enable cryptographic tools to prove, statistically, that an assertion is valid without revealing additional information [Goldreich *et al.* (1991); Sedlmeir *et al.* (2021)]. ZKPs provide three features in the context of digital identities [W3C (2019b)]. Firstly, they combine multiple VCs from several issuers to form a single, verifiable presentation without revealing VCs or identifiers to the verifier. Secondly, they allow users to minimize data disclosure while retaining full control over their own identity [Sovrin (2018); Mühle *et al.* (2018)]. Lastly, they increase the flexibility of VCs, as VCs issued previously can be adapted to the requirements of the verifier and so do not need to be reissued [W3C (2019b)]. Thus, the critical components of an SSI that enhance the technology's privacy-preserving character are blockchains, DIDs, VCs, PKI, and ZKPs. Figure 1 provides an overview of the interplay of these components.

As noted earlier, blockchain acts as a tamper-resistant registration authority [Mühle *et al.* (2018)]. Due to the privacy-risks of the blockchain, users store their private information in local storage. They can use this information to make an identity claim that needs to be verified by an issuer. Furthermore, each user manages an indefinite number of DIDs stored in a personal wallet [W3C (2019a)]. Based on PKI, the user can verify the ownership of a specific DID using the corresponding secret key. To verify a specific claim, the user presents a DID and the claim to an issuer. As an approved authority with a public identifier, the issuer does not necessarily require several DIDs. A user can now present the VC-DID combination to a verifier (e.g. to gain access to a digital service). To prevent the verifier and the issuer

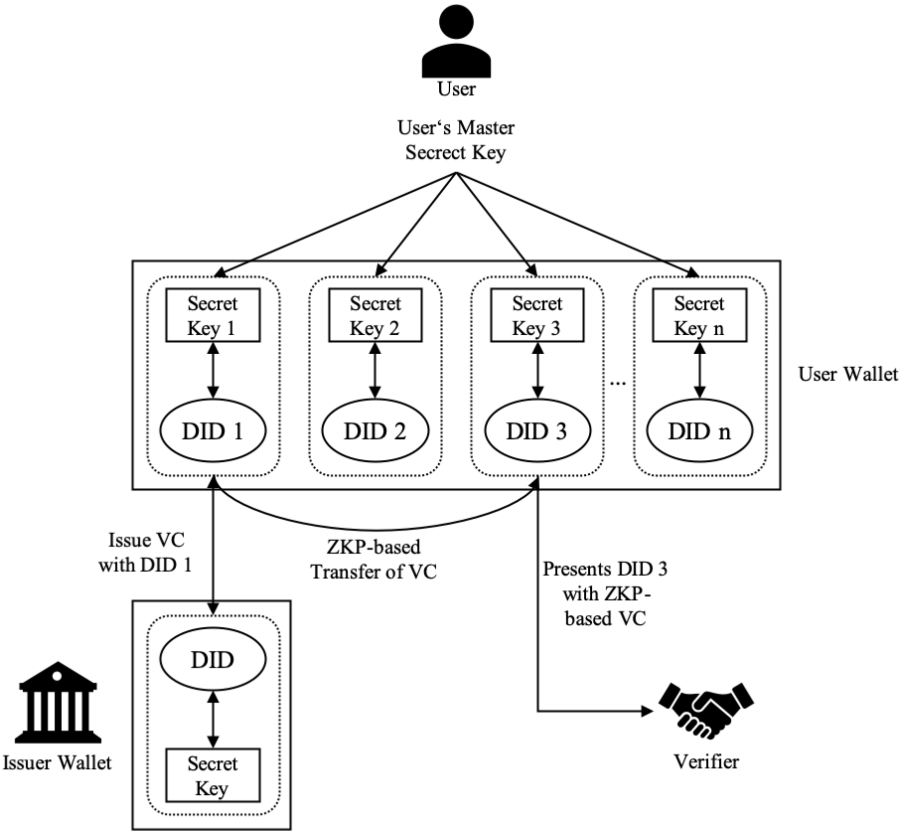

Fig. 1. Interplay of DID, VC, and ZKPs in an SSI.

from correlating a user's DIDs [W3C (2019b)], which would pose a significant risk to the privacy and security of identities, the user transfers the VC from the original DID to another DID in the wallet, using a ZKP. This procedure is called pairwise DID and decreases the privacy risk of users while enabling them to reuse a VC [W3C (2019b)]. Pairwise DIDs enable users to remain anonymous, which representing one extreme on the SSI's spectrum of privacy with 'totally identifiable' at the other extreme. The necessity for a broad spectrum of privacy, which SSIs would facilitate, reflects the varying degrees of privacy required by users in different situations [W3C (2019a)].

2.4. *Technology acceptance research*

A major area within IS research examines factors that influence individuals' decisions to adopt particular innovations [Rogers (1983)]. These factors need to be considered at various stages of the technology and product life cycle [Mathieson (1991)]. Therefore, researchers developed so-called Technology Acceptance Models (TAM) [Venkatesh *et al.* (2003)]. Based on Fishbein's Theory of Reasoned Action [Fishbein and Ajzen (1975)], Davis [1985] proposed one of the first models, the so-called TAM. The TAM investigates individuals' decision-making to explain the later success of IS. Using the TAM, [Davis (1985)] identified *Perceived Usefulness* and *Perceived Ease of Use* as factors affecting *Attitude toward Using*, which is embedded in a complex relationship between external variables and potential system usage [Marangunić and Granić (2015)]. Due to the prominence of this research field, researchers developed several other frameworks including different constructs to explain a user's intention to adopt a technology. Venkatesh *et al.* [2003] reviewed eight of these models and unified them into one comprehensive theory of the acceptance and use of technology (i.e. UTAUT). Thanks to the relevance of these models — particularly UTAUT — these frameworks were extended and integrated into new contexts and researchers developed enhanced versions of the TAM and UTAUT [Venkatesh *et al.* (2012)].

3. Research Model and Hypotheses

3.1. *Research model*

To recognize different influencing factors of SSI, we combined and adapted two different theories that build on research models suitable for exploring the influence of information privacy on the adoption of a system for SSIs. To this aim, technology acceptance as well as privacy are the two central theories that underly our study. Our model, thus based on UTAUT2 and the privacy framework of Dinev *et al.* [2013], can be used to determine *Perceived Privacy* via a control-risk calculus. UTAUT2 is a popular framework examining technology acceptance by users in different domains [Venkatesh *et al.* (2012)]. The key elements of UTAUT2 are Performance Expectancy, Effort Expectancy, Social Influence, Facilitating Conditions, Habit, Hedonic Motivation, and Price Value, Use Behavior and Behavioral Intention. We excluded *Use Behavior* on the basis that *Behavioral Intention* serves to explain more of the variance of a model and customers cannot yet use an SSI-based IdM [Venkatesh *et al.* (2012); Weinhard *et al.* (2017)]. We eliminated *Habit*, *Hedonic Motivation*, and *Price Value*, as these constructs require an established technology and previous experience of its use [Salinas Segura and Thiesse (2015)]. As the privacy perspective cannot yet be entirely validated by using UTAUT2, we integrated that perspective into our model by applying the model proposed by Dinev *et al.* [2013], determining *Perceived Privacy* through a control-risk calculus. Dinev *et al.* [2013] strongly recommend future research to clarify, enhance, and develop this model. Thus, we adopted additional relationships for *Perceived Benefits* and *Information Sensitivity* [Kehr *et al.* (2015)] and altered the role of *Regulatory Expectations*. Regulation is a proxy control mechanism ensuring the user's privacy [Xu *et al.* (2012)]. Hence, we added a relationship between *Regulatory Expectations* and *Perceived Privacy*. Altering the role of *Regulatory Expectations* enables the comparison of a market-based approach, protecting customers' privacy, with a regulatory approach [Berg *et al.* (2017)]. We also examined the effect that regulatory expectations have on the acceptance of an SSI.

3.2. *Hypotheses*

Performance Expectancy

Performance Expectancy is the strongest predictor of *Behavioral Intention* and refers to users' gains from the use of a new technology [Venkatesh *et al.* (2003)]. So far, passwords are the dominant authentication method used on the internet, but they are inconvenient and can lead to security problems [Neumann (1994); Recordon and Reed (2006); Roßnagel *et al.* (2014)]. An SSI can increase the performance of a user by providing a single-sign-on mechanism that enables easier access to digital services while securing the user's privacy [Dunphy and Petitcolas (2018)]. If users expect a higher performance gain from an SSI, they are more willing to adopt the IdM system [Venkatesh *et al.* (2003)].

H1: *Performance Expectancy positively affects Behavioral Intention.*

Effort Expectancy

Effort Expectancy reflects the "degree of ease associated with the use of the system" [Venkatesh *et al.* (2003, p. 450)] and is especially important in the early stages of a technology [Venkatesh *et al.* (2003)]. Due to complex privacy and security requirements, designing easy-to-use IdM systems is challenging [Roßnagel *et al.* (2014)]. However, usability is a critical factor for the success of such systems [Jøsang *et al.* (2007); Dhamija and Dusseault (2008)], and SSI providers need to align usability with privacy and security requirements to achieve adoption.

H2: *Effort Expectancy positively affects Behavioral Intention.*

Social Influence

Social Influence includes the perceived impact of a user's social surroundings on their *Behavioral Intention* [Venkatesh *et al.* (2003)]. The effect of the social environment is especially significant for new technologies [Venkatesh *et al.* (2003)]. Research also shows that the social environment influences the privacy decisions of individuals [Laufer and Wolfe (1977)]. As an SSI is a new concept based on emerging technology that aims to secure a user's privacy (i.e. blockchain), social influence can have a positive effect on a user's decision to adopt an SSI.

H3: *Social Influence positively affects Behavioral Intention.*

Facilitating Conditions

The perceived availability of support in the use of a new technology varies significantly in different consumer settings [Venkatesh *et al.* (2003, 2012)]. An SSI is based on blockchain and sophisticated cryptographic techniques [Mühle *et al.* (2018)]. Thus, providers of an SSI cannot expect every customer to have a deep understanding of these concepts. This means that providers need to offer facilitation to their customers. Consumers with access to assistive resources are more likely to intend to use a technology [Venkatesh *et al.* (2012)].

H4: *Facilitating Conditions positively affects Behavioral Intention.*

Perceived Privacy

Perceived Privacy implies a cognitive calculus resulting in a perceived state of privacy in a specific situation [Kehr *et al.* (2015); Schoeman (1984)]. Research shows that privacy concerns and the privacy calculus can influence the adoption of technologies [e.g. Angst and Agarwal (2009); Li *et al.* (2016); Dinev *et al.* (2006)]. Since privacy is the key factor determining the acceptance of IdM systems, these systems need to acknowledge the users' privacy and enable users to control their information disclosure [Hansen *et al.* (2004)]. The conceptualization of SSIs follows privacy by design and information minimization principles, and enables users to control their information privacy [Sovrin (2018); Berg *et al.* (2017)]. Consequently, individuals expecting an SSI to increase their level of privacy are more willing to use the technology.

H5: *Perceived Privacy positively affects Behavioral Intention.*

Perceived Information Control

The perceived ability of individuals to control their information disclosure can be supported by privacy-preserving technologies, such as SSIs. Dinev *et al.* [2013] distinguish between control over information disclosure and control over shared information. An SSI enables control over the disclosure of information by allowing users to share their information selectively [Mühle *et al.* (2018)]. The combined use of ZKPs, and VCs enables control over shared information based on the two concepts of "Zero-Knowledge-Set-Membership (ZKSM)" [Ma *et al.* (2022)] and "Zero-Knowledge-Range-Proofs (ZKRP)" [Günsay *et al.* (2021)]. In ZKSM, information within a VC is present in an unordered fashion (e.g. the list of students enrolled in a university) while in ZKRP, information must necessarily be present in an ordered fashion (e.g. the minimum age of individuals to attend events) [Morais *et al.* (2019)].

The proofs in both ZKSM and ZKRP can now be integer- or binary-based [Morais *et al.* (2019)]. In the integer-based proof, all elements of the (mostly unordered) data within the VC are signed. The verifier's knowledge of this signature (or a sum resulting from the signatures) is now sufficient for proof. In binary-based proof, so-called secrets are used instead of signatures. These are split into individual bits and must be supplied by the verifier to provide the proof. As a result, users do not need to share actual personal data but only a DID and a VC proving that the actual requirement is fulfilled. Thus, users do not have to fear the misuse of disclosed personal information as the information is anonymized, pseudonymized, and untraceable. Hence, we assume an SSI to increase users' perception [Culnan and Armstrong (1999); Dinev *et al.* (2013); Sheehan and Hoy (2000)].

H6: *Perceived Information Control positively affects Perceived Privacy.*

Tactics of Information Control

Customers use three tactics to control the amount and accuracy of disclosed information: anonymity, secrecy, and confidentiality [Zwick and Dholakia (2004)]. Anonymity (and pseudonymity) enables users to conceal their true identity by creating various identity representations to hide their identity and prevent tracking [Zwick and Dholakia (2004); Turkle (1997)]. An SSI follows a comparable approach and enables the customer to create several minimized identities. Furthermore, it uses pairwise DIDs to avoid tractability while guaranteeing the validity of the identity claim [W3C (2019a, 2019b)]. Secrecy is defined as the concealment of personal information to prevent a digital representation of an individual [Tefft (1980); Zwick and Dholakia (2004)]. An SSI obtains Secrecy using pairwise DIDs and ZKPs. For instance, users can state that they are eligible to buy restricted products without sharing their real age. Lastly, Confidentiality is the externalization of limited but highly accurate personal information, and includes the unauthorized access of third parties to this information [Zwick and Dholakia (2004); Camp (1999)]. Service providers store information in databases, which can be attacked by hackers [Hille *et al.* (2015)]. Hence, consumers need to trust the organization to securely store information in a provider's database [Camp (1999); Dinev *et al.* (2013)]. With an SSI, consumers do not need to rely on trust, since users share DIDs solely with the service provider and determine access to their personal data [Sovrin (2019)]. In the event of a data breach in which information storing resources (e.g. user wallets) are affected, they make their DIDs unusable for third parties [Sovrin (2018)]. These three tactics of IdM are essential for users to limit the disclosure of their information. Thus, we conclude that:

H7: *Anonymity positively affects Perceived Information Control.*
H8: *Secrecy positively affects Perceived Information Control.*
H9: *Confidentiality positively affects Perceived Information Control.*

Perceived Risk

Perceived Risk is the fear of negative outcomes as a result of information disclosure, and implies a loss of control over personal information [Dinev and Hart (2006);

Dinev *et al.* (2013)]. Risk is provoked by uncertainty, discomfort, or anxiety [Dowling and Staelin (1994)] as a result of potential opportunistic behavior on the part of organizations, such as unauthorized access, theft [Rindfleisch (1997)], and the sharing or sale of personal information [Budnitz (1997)]. Studies show that risk determines users' information and identity disclosure, perceived privacy, and privacy concerns [Dinev and Hart (2004); Dinev *et al.* (2013); Krasnova *et al.* (2009)].

H10: *Perceived Risk negatively affects Perceived Privacy.*

Perceived Benefits of Information Disclosure

Perceived Benefits of Information Disclosure is based on the notion of the privacy calculus and represents the perception of a positive net outcome of the assessment of risks and benefits of the information disclosure [Culnan and Bies (2003); Dinev *et al.* (2013)]. In return for disclosing information on digital services, consumers receive monetary or social benefits, personalized services, or increased convenience [Forsythe *et al.*, (2006); Hann *et al.* (2007); Lu *et al.* (2004)]. These benefits can exceed the negative consequences of information disclosure and lead to an enhanced perceived state of privacy in a given situation [Smith *et al.* (2011); Kehr *et al.* (2015)]. Chellappa and Sin [2005] even demonstrated that the benefits of personalization are almost twice as significant as consumers' privacy concerns. Thus, an individual's perceived benefits also impede the perception of risks associated with information disclosure [Kehr *et al.* (2015)].

H11: *Perceived Benefits of Information Disclosure negatively affects Perceived Risk.*

H12: *Perceived Benefits of Information Disclosure positively affects Perceived Privacy.*

Information Sensitivity

The general disclosure of information does not necessarily raise privacy concerns. Rather, it may be the sensitivity of information that determines a user's privacy concerns and leads to paradoxical privacy-related behavior [Mothersbaugh *et al.* (2012)]. *Information Sensitivity* involves a cognitive and rational assessment and depends on personal characteristics, cultural backgrounds, legislative settings, and the specific context [Bansal *et al.* (2010); Bellman *et al.* (2004); Kehr *et al.* (2015)]. Hence, a user's perception of the sensitivity of a piece of information determines the impact on perceived privacy, privacy concerns, or the disclosure of private data [Kam and Chismar (2006); Malhotra *et al.* (2004)]. Empirical studies show that higher sensitivity of personal information intensifies *Perceived Risk* and reduces the *Perceived Benefit of Information Disclosure* [Malhotra *et al.* (2004); Mothersbaugh *et al.* (2012)].

H13: *Information Sensitivity negatively affects Perceived Benefits of Information Disclosure.*

H14: *Information Sensitivity positively affects Perceived Risk.*

Importance of Information Transparency

From a user perspective, organizational approaches to handling sensitive information regularly lack transparency. Consequently, individuals emphasize being informed by organizations about the collection and processing of their personal information [Dinev *et al.* (2013); Waldo (2007)]. Organizations can increase their transparency and enable customers to assess their privacy risk by publishing privacy policy statements that aggregate the organization's privacy practices [Awad (2006)]. Opaque privacy practices increase the perceived risks and individuals' fear of adverse consequences [Pitkänen and Tuunainen (2012)]. They also reduce the willingness of customers with high demand for transparency to disclose their personal information [Awad (2006); Karwatzki *et al.* (2017)].

H15: *Importance of Information Transparency positively affects Perceived Risk.*

Regulatory Expectations

Researchers distinguish three approaches to protecting information privacy: individual self-protection, industry self-regulation, and government legislation [Culnan and Bies (2003); Tang *et al.* (2008); Xu *et al.* (2009)]. An SSI is a market-based approach to individual self-protection, offering an alternative to privacy regulations [Zheng *et al.* (2018)]. Regulatory approaches, such as the General Data Protection Regulation (GDPR) in the European Union, can similarly realize the fundamental principles of SSIs, namely privacy by design, minimization, and portability [Allen (2016)], and enable individuals to exercise proxy control, and diminish privacy concerns and perceived risks [Berg *et al.* (2017); Dinev *et al.* (2013); Xu (2007)]. Individuals tend to demand more rigorous privacy regulations if they perceive that alternative approaches alone do not preserve their privacy [Smith *et al.* (2011)]. However, their limited resources mean that users often struggle to evaluate their protection [Lwin *et al.* (2007)]. In contrast, regulators have the required resources, meaning they are most able to protect individuals' privacy. This is particularly apparent in their ability to punish those responsible for privacy breaches [Spiro and Houghteling (1981)]. Thus, effective privacy regulations are an alternative to an SSI and would decrease the willingness to adopt SSI systems.

H16: *Regulatory Expectations positively affects Perceived Privacy.*
H17: *Regulatory Expectations negatively affects Behavioral Intention.*

4. Research Methodology

4.1. *Measurement development*

To validate our research hypotheses, we developed a survey, in English, using constructs and items from the privacy and technology acceptance literature. We adapted all items to our specific research context of digital identities, and modified items of control-related constructs and *Perceived Privacy* to support the use of an SSI. All items were built as reflective indicators and measured using 7-point Likert scales ranging from totally disagree (1) to totally agree (7). We incorporated multiple additional indicators for most of our constructs to improve reliability.

The introduction provided respondents with basic knowledge, briefly explaining identity attributes, the difference between centralized and decentralized identity, SSI, and the increased control of personal data enabled by an SSI. All respondents were asked to reflect the use of SSI from a mandatory perspective. We also added three control questions to verify that our respondents correctly understood these descriptions. Respondents who answered one of these questions incorrectly were excluded from the data analysis to minimize differing perceptions of our constructs. Lastly, to compare descriptive statistics, we added questions collecting demographic data from our respondents.

Following Kim *et al.* [2009] and Urbach and Ahlemann [2010], we conducted a pre-test to validate our reflective measurement model in terms of reliability and validity. In total, we collected 40 complete responses, of which 30 respondents answered the control questions correctly. We used SmartPLS 3 to evaluate our pre-test and followed the procedure recommended by Hair *et al.* [2017] to trim down our questionnaire. As a result, we eliminated selected indicators as well as the constructs *Importance of Information Transparency* and *Perceived Risk* and their corresponding hypotheses as we could not ensure validity and reliability without neglecting content validity. Appendix A provides a table with all constructs, their corresponding items (those excluded are marked gray) as well as the source of these items. Figure 2 illustrates our final research model with the remaining hypotheses.

4.2. *Data collection*

To gather a diverse sample of respondents, we distributed our survey on several social networks, internal mailing lists, chats, forums of blockchain communities, and

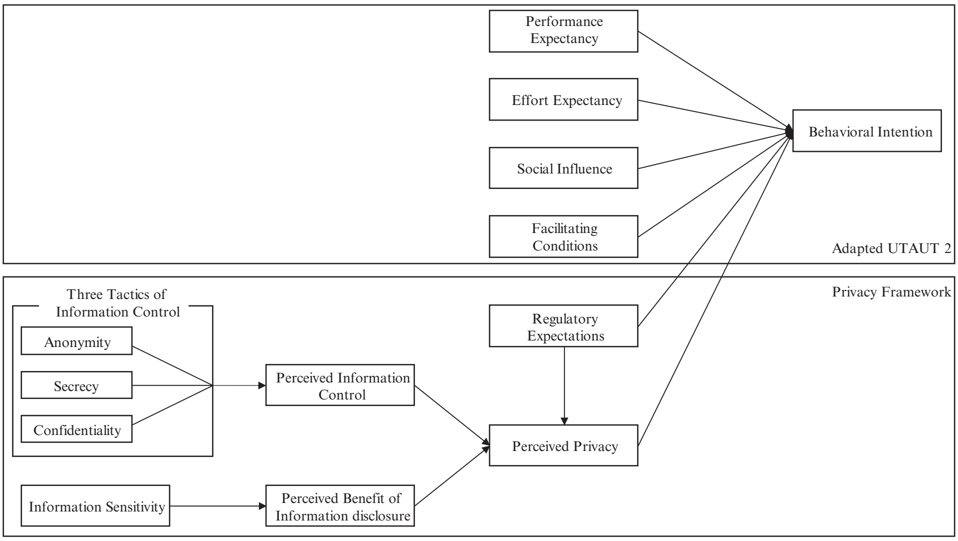

Fig. 2. Final research model.

survey exchange platforms, as well as Amazon Mechanical Turk. In total, we collected 495 responses, of which 354 were complete. We eliminated data points where respondents did not answer our control questions correctly. In the end, we amassed 240 valid responses. Of our respondents, 56.20% were male, and 43.30% were female. Their average age was 30.42 years. Nearly half held a bachelor's degree or higher, with 38.8% of current students, and 45% full-time employees (cf. Table 1).

There is little consensus among researchers as to the required sample size for conducting SEM-PLS. In general, PLS is favored by many researchers as it does not require a large sample, and because the sample size is independent of the model's complexity [Hair *et al.* (2017); Cassel *et al.* (1999)]. A minimum of $n = 130$ responses for a survey with six constructs determining a dependent variable and a significance level of $p = 0.050$ and an R^2 of 0.250 is required [Hair *et al.* (2017)]. Other researchers recommend conducting a G*Power analysis to determine the required sample size [Faul *et al.* (2009)]. The *a priori* G*Power analysis (effect size $f^2 = 0.111$, alpha $= 0.050$, Power $= 0.800$, 12 predictors) reports a required sample size of $n = 167$. Other researchers state that the requirements for SEM-PLS are comparable to those of covariance-based approaches ($n > 150$) and recommend using bootstrapping to assess the significance levels of the sample and the standard errors [Urbach and Ahlemann (2010)]. Hence, we fulfill the recommendations for the required sample size for SEM-PLS.

Table 1. Descriptive statistics.

Demographic variables	Category	Value
Age	Minimum	15
	Maximum	77
	Mean	30.42
	Median	27
	Standard deviation	10.07
Gender	Male	56.30%
	Female	43.30%
	Other	0.40%
Education	No schooling completed	1.30%
	High school graduate	26.70%
	Bachelor's degree	49.20%
	Master's degree	20.00%
	Doctorate degree	2.90%
Employment	Employed full time	45.00%
	Employed part time	11.30%
	Unemployed looking for work	2.10%
	Unemployed not looking for work	1.30%
	Retired	1.30%
	Student	38.80%
	Disabled	0.40%

5. Data Analysis

5.1. *Measurement model*

To maximize the explanatory power of our model, we evaluated our data in terms of reliability as well as convergent and discriminant validity. We primarily followed the general recommendations of Hair *et al.* [2017] and Benitez *et al.* [2020], supported by the guidelines of Urbach and Ahlemann [2010] for IS specifics.

To examine internal consistency reliability, we used composite reliability [Urbach and Ahlemann (2010)]. All our constructs displayed a desirable CR between 0.700 and 0.950 (cf. Table 2) [Nunnally and Bernstein (2008)]. Next, we assessed convergent reliability on the indicator and construct levels. We investigated the indicators' outer loadings to examine internal reliability. Outer loadings higher than 0.708 are favorable; indicators with outer loadings between 0.400 and 0.700 may be retained [Hair *et al.* (2017)]. Our data showed that all values were higher than 0.400. *Perceived Benefit*, *Social Influence*, and *Information Sensitivity* had at least one indicator between 0.600 and 0.700, with indicator 3 (IS3) of *Information Sensitivity* having the lowest value of 0.495. Nevertheless, we concluded that indicator reliability was given. We used average variance extracted (AVE) with a threshold of 0.500 to evaluate convergent reliability on a construct level [Fornell and Larcker (1981); Urbach and Ahlemann (2010)]. Our constructs displayed an AVE between 0.517 and 0.811, indicating convergent reliability. Thus, all of our indicators and constructs imply convergent reliability.

To examine the degree of difference between the constructs, we assessed discriminant validity using the Fornell–Larcker criterion, which requires a latent variable (LV) to share more variance with its assigned indicators than with any other LV [Urbach and Ahlemann (2010); Fornell and Larcker (1981)]. Remarkably, discriminant validity was not established for *Perceived Control* with *Confidentiality* and *Perceived Privacy*. Thus, we examined the inter-item correlation to identify highly correlating indicators. Subsequently, we eliminated the indicators PCTL1

Table 2. Reliability and validity.

Construct	Cronbach's alpha	Composite reliability	Average variance extracted (AVE)
ANYT	0.888	0.923	0.749
BEN	0.833	0.890	0.671
BI	0.895	0.929	0.769
CFDT	0.859	0.905	0.703
EE	0.846	0.895	0.681
FC	0.718	0.841	0.640
IS	0.752	0.749	0.517
LAW	0.838	0.903	0.756
PCTL	0.916	0.937	0.748
PE	0.923	0.940	0.723
PRIV	0.883	0.928	0.811
SCRT	0.864	0.908	0.711
SI	0.840	0.889	0.620

Table 3. Fornell–Larcker criterion.

	ANYT	BEN	BI	CFDT	EE	FC	IS	LAW	PCTL	PE	PRIV	SCRT	SI
ANYT	0.865												
BEN	0.444	0.819											
BI	0.453	0.314	0.877										
CFDT	0.736	0.402	0.516	0.839									
EE	0.424	0.372	0.563	0.530	0.825								
FC	0.340	0.342	0.490	0.463	0.785	0.800							
IS	0.099	−0.153	0.091	0.097	0.065	0.022	0.719						
LAW	0.070	−0.005	0.221	0.225	0.324	0.309	0.249	0.869					
PCTL	0.722	0.406	0.565	0.825	0.568	0.495	0.163	0.223	0.865				
PE	0.583	0.444	0.690	0.615	0.581	0.536	0.204	0.202	0.630	0.850			
PRIV	0.727	0.427	0.545	0.831	0.556	0.495	0.057	0.223	0.840	0.589	0.900		
SCRT	0.685	0.312	0.565	0.773	0.518	0.454	0.179	0.264	0.810	0.556	0.837	0.843	
SI	0.422	0.441	0.633	0.492	0.557	0.591	0.047	0.231	0.492	0.565	0.525	0.515	0.788

and PCTL2 of *Perceived Control*, establishing discriminant validity for all constructs (cf. Table 3).

5.2. *Structural model*

We applied partial least squares structural equation modeling (PLS-SEM) to test our research model using Smart PLS 3.0 [Hair *et al.* (2017); Urbach and Ahlemann (2010)]. PLS is a popular statistical approach within the IS discipline as it does not require a relatively large sample size or normal-distributed data to test SEMs with a substantial number of constructs, especially for theory development [Urbach and Ahlemann (2010)]. Figure 3 displays the results of our structural model.

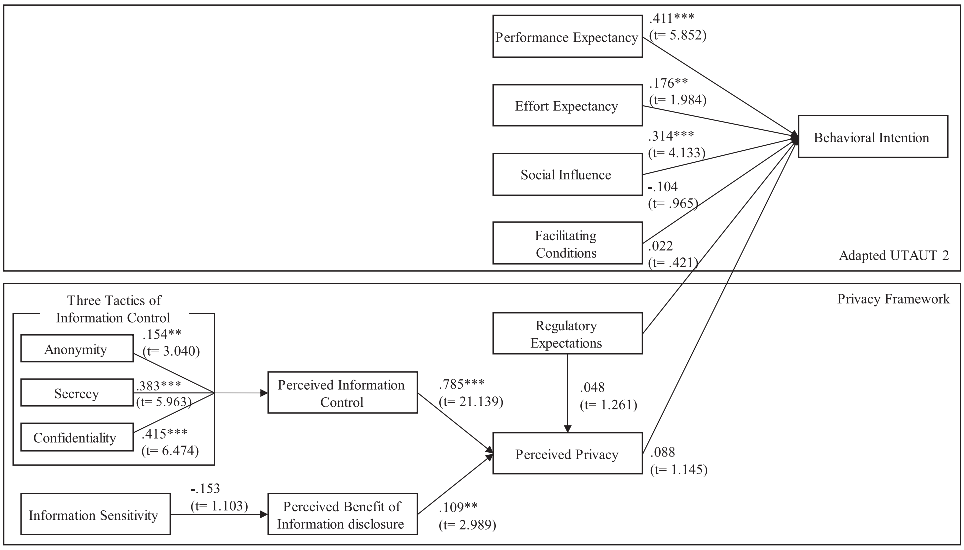

Fig. 3. Research model with path coefficients, t values, and significance levels.

We first investigated the collinearity using VIF values with a threshold of 5.000 [Hair *et al.* (2017)]. *Confidentiality* has the highest VIF value (3.106) indicating no critical degree of collinearity. As seen in Fig. 3, the impact of each of the three tactics of information control on *Perceived Control* is highly significant. *Information Sensitivity* has no significant relationship with *Perceived Benefit. Perceived Benefit* and *Perceived Control* have a strong and highly significant impact on *Perceived Privacy.* On the contrary, *Regulatory Expectations* do not appear to share a significant relationship with *Perceived Privacy.* Furthermore, the construct does not imply a significant relationship with *Behavioral Intention. Performance Expectancy*, *Effort Expectancy*, and *Social Influence* have a significant positive impact on Behavioral Intention. However, the influence of *Facilitating Conditions* on *Behavioral Intention* is not significant. Overall, the model explains $R^2 = 0.583$ of the variance in the dependent variable *Behavioral Intention.* Furthermore, it seems that *Perceived Benefit* has little explanatory power ($R^2 = 0.023$) whereas *Perceived Privacy* ($R^2 = 0.764$) and *Perceived Control* ($R^2 = 0.716$) hold substantial explanatory power.

We used Cohen's f^2 to evaluate the effect size of the paths in our research model [Urbach and Ahlemann (2010); Hair *et al.* (2017); Cohen (2013)]. *Facilitating Conditions* (0.009), *Regulatory Expectations* (0.001), and *Perceived Privacy* (0.010) appear to have little effect. Furthermore, *Regulatory Expectations* (0.001) shows little impact on *Perceived Privacy. Effort Expectancy* (0.024), *Information Sensitivity* (0.024), *Social Influence* (0.127), *Anonymity* (0.042), and *Perceived Benefit* (0.035) evince an average effect. Lastly, *Performance Expectancy* (0.209), *Confidentiality* (0.235), *Secrecy* (0.232), and *Perceived Control* (1.702) are shown to have a significant effect on their dependent variables.

Lastly, we examined the Stone–Geisser criterion's Q^2-values, based on a blindfolding procedure with an omission distance of $D = 7$ [Hair *et al.* (2017)]. The results show that *Perceived Benefit* has little predictive power ($Q^2 = 0.013$). The other LVs indicate high predictive power (*Behavioral Intention*: $Q^2 = 0.415$, *Perceived Privacy*: $Q^2 = 0.541$, *Perceived Control*: $Q^2 = 0.541$).

6. Discussion

6.1. *Hypotheses*

To account for the behavioral perspective in our research model, we borrowed four constructs from UTAUT2 to examine *Behavioral Intention.* The results confirm that *Performance Expectancy* (*H*1), *Effort Expectancy* (*H*2), and *Social Influence* (*H*3) significantly affect *Behavioral Intention*, which is in line with former research [e.g. Bélanger and Crossler (2011); Pavlou (2011)]. Our results for the influence of *Facilitating Conditions* (*H*4), however, contradict the outcomes of prior empirical studies. At no point did our data provide evidence that *Facilitating Conditions* have a positive effect on *Behavioral Intention.* We assume that the novelty of an SSI and the underlying concept of blockchain influenced this result. Hence, users may struggle to determine the available support and the compatibility of these new technologies [Weinhard *et al.* (2017)].

Based on the privacy-related constructs from the privacy framework of Dinev *et al.* [2013], we first stated the influence of *Perceived Privacy* on Behavioral Intention (*H*5). In our sample, we cannot find evidence for this hypothesis. Hence, *Perceived Privacy* does not statistically significantly affect the Behavorial Intention of a user to adopt an SSI-based IdM system. Nevertheless, our data confirm the hypothesis *H*6. *Perceived Control* indicates that an SSI enables users to perceive control over their information, which has a significant positive effect on *Perceived Privacy*. These results confirm the findings of existing privacy literature and the close relationship between control and privacy. Their close relationship, again, could lead to discriminant validity and collinearity concerns within our study. To counteract these concerns, some researchers equate control with privacy [e.g. Smith *et al.* (2011)], while others define control as an important determinant of privacy concerns [Malhotra *et al.* (2004)]. Consequently, we confirm the proximity, but also maintain the separation of these constructs. We further demonstrated and confirmed that *Anonymity*, *Secrecy*, and *Confidentiality* significantly affect *Perceived Control* (*H*7–*H*9). The results confirm the importance of the three tactics of IdM in enabling users to control the disclosure of their information.

In relation to the privacy calculus described by Dinev and Hart [2006] and originally theorized in a study by Laufer and Wolfe [1977] as a calculus of behavior, we studied the impact of *Perceived Benefit* on *Perceived Privacy* (*H*12) [Kehr *et al.* (2015)]. *Perceived Benefit* was shown to have a positive effect on *Perceived Privacy*, which confirms hypothesis *H*12 and supports the underlying theory of the privacy calculus: that 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 services are often associated with the highest privacy risk for users. Consequently, we included *Information Sensitivity* in our study as it has been revealed as 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, we theorized that *Information Sensitivity* negatively affects *Perceived Benefit* (*H*13). Throughout our study, however, this relationship was not found to be significant. Lastly, we rejected both hypotheses related to *Regulatory Expectations*, which examined the effects on *Perceived Privacy* (*H*16) and *Behavior Intention* (*H*17). Table 4 provides an overview of the results of our proposed hypotheses, including the four hypotheses that were excluded from the testing due to statistical considerations.

6.2. *Theoretical contribution*

The goal of our study was to provide empirical insights into the impact of privacy perception on the adoption of IdM systems. These we examined within the emerging context of blockchain for a blockchain-based IdM system called an SSI. Blockchain is particularly interesting as most previous studies in this field have examined the potential of the technology or its technological foundations [e.g. Beck *et al.* (2018); Glaser (2017)], and few have investigated the potential of blockchain from individual

Table 4. Summary of hypothesis testing.

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

and behavioral perspectives [Mendoza-Tello *et al.* (2018)]. Similarly, empirical results from a behavioral perspective remain scarce in IdM literature, although an extensive body of theory exists on the influence of factors such as information privacy on the adoption of non-blockchain-based IdM systems [Hansen *et al.* (2004); Seltsikas and O'Keefe (2010)]. Mindful of this lack of knowledge within the IdM and blockchain literature, we conducted our study from an individual perspective to investigate the impact of information privacy-related theories (namely, the privacy paradox and privacy calculus) on the acceptance of an SSI system. Our research model consisted of established constructs from technology acceptance and privacy research. However, given the novelty of our research context, our study disclosed some unexpected findings. Analogous to the privacy paradox, our research does not empirically support the claim that perceived privacy affects the acceptance of an SSI. These findings contradict the prevailing view of privacy as a key factor for IdM systems.

Despite the effect that *Perceived Control* has on *Perceived Privacy*, we did not find a significant relationship between *Perceived Privacy* and *Behavioral Intention*, 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)]. Our results 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 SSO 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 SSO 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. At the same time, Bauer *et al.* [2013] also showed that, although they continued their use of SSOs, users expressed significant privacy concerns about such mechanisms.

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 digital 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. Additionally, these findings have implications for initiatives seeking to balance privacy with cybersecurity. By identifying themselves, users can be trusted by digital services and therefore benefit from such a service. Besides situations, in which users disclose information voluntarily to benefit from a digital service, cybersecurity could also be a reason to reduce privacy. In line with the concept of the bright internet, in some cases, a user's information privacy is not predominant in favor of legitimate preventive cybersecurity mechanisms [Lee *et al.* (2020)]. Our findings support these considerations.

Remarkably, although *Perceived Control* has a positive impact on *Perceived Privacy,* we did not detect a similar effect for *Regulatory Expectations* on *Perceived Privacy.* Our hypothesis was based on the theory that regulations would empower users to exercise proxy control over their privacy [Xu *et al.* (2012)], while an SSI would be a market-based alternative, which enables the user to exercise actual instead of proxy control. Therefore, we hypothesized that appropriate privacy regulations could make an SSI redundant from a privacy point of view and, hence, negatively affect *Behavioral Intention.* The results of our study are in contrast to studies by Xu *et al.* [2011] and Lwin *et al.* [2007]. Additionally, we did not detect a significant effect of *Regulatory Expectations* on *Behavioral Intention.*

Although we could not find significant effects for the abovementioned relationships within our study, the results do not necessarily mean that the underlying assumptions were wrong as the results are, indeed, in line with previous research. In a study of the role of privacy control and privacy assurance approaches in location-based services — namely, individual self-protection, industry self-regulation, and government legislation — Xu *et al.* [2011] investigated the interplay of these three approaches to identify the extent to which they can substitute one another. The authors present two explanations of particular importance in which the results of our study can be embedded. 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), the latter affords a greater sense of control and has a stronger impact on users' perceived information control [Xu *et al.* (2012)]. Second, self-control mechanisms diminish the need for regulatory expectations and can even substitute them to some extent [Xu *et al.* (2012)]. This previous research provides a tentative explanation for the results of our study. An SSI, as a means of individual self-protection, provokes a greater perception of control than *Regulatory Expectations* and diminishes the proxy-control-effect of *Regulatory Expectations* on *Perceived Privacy*. Consequently, the effect of *Regulatory Expectations* on *Behavioral Intention* also decreases. Therefore, Xu *et al.* [2012] conclude that approaches to individual self-protection must be promoted as an appropriate substitute for other privacy protection approaches, especially due to their feature to overcome "international, regulatory, and business boundaries" [Xu *et al.* (2012, S. 1360)]. This feature is a big advantage of blockchain-based IdM systems and must be heralded to support the adoption of respective systems [Rieger *et al.* (2019)].

6.3. *Managerial implications*

The findings in this study lead to several important practical implications for users, IdM system providers and digital service providers. In light of the privacy paradox, users must be aware that control over their identity does not necessary result in a higher privacy. Therefore, users must calculate the risks and benefits of the information disclosure against the background of the privacy paradox. Additionally, the use of an SSI-based IdM system increases control but demands that users take responsibility and ownership over their information privacy [Der *et al.* (2017)]. For instance, users must define with the help of an SSI-based IdM system what and how much personal information they want to share with a specific digital service. As a result, the efforts in using these digital services increase for respective users.

SSI providers must address these use-related factors (e.g. higher efforts on the user side) to deliver accepted and successful solutions. Although privacy and control are central to the value proposition of SSI-based IdM systems, managers in charge for the implementation of SSI solutions must focus on interoperability, usability, and security, as summarized by Roßnagel *et al.* [2014], to achieve widespread adoption. For instance, interoperability is especially critical from an economic and a network effects perspective. The more users and correspondingly digital services rely on an SSI, the higher will be the benefit from an SSI for these actors [Katz and Shapiro (1994)]. Only the interplay of these factors will ensure the success of such an IdM system, and consequently, of an SSI [Dunphy and Petitcolas (2018)].

Additionally, managers of digital services must set up application programming interfaces within their own organization for capitalizing on an SSI. The organization and their digital services must be prepared to connect to these identity domains and provide a seamless experience to their users. Hence, important questions such as the role of the own organization in the IdM system (e.g. issuer, verifier) must be answered upfront.

6.4. *Limitations and future research*

Our results 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. If an SSI was implemented and respondents became familiar with the concept, research could examine actual *Use Behavior* instead of *Behavioral Intention*. Such research would improve the comparability of the results and eliminate the risk of participants misunderstanding underlying concepts [Arnold and Feldman (1981)]. Furthermore, when consolidating our research model, statistical considerations led us to eliminate constructs of potential relevance. We excluded *Perceived Risk* because we could not ensure validity and reliability without neglecting content validity. However, Dinev *et al.* [2013] found that *Perceived Risk* is an essential antecedent of *Perceived Privacy*. Additionally, privacy protection approaches, such as an SSI, diminish individuals' perceived risk and affect their decision making [Adjerid *et al.* (2018)]. Hence, excluding *Perceived Risk* from our study may have reduced our explanatory power, which may have distorted results. Future studies could attempt to include *Perceived Risk* to increase the explanatory power of the research model.

Empirically, there may be various sources of errors in a study that distort results [Hair *et al.* (2017)]. Although we distributed our survey across multiple channels to reach a wide range of respondents, the representativeness of our study is still limited for at least three reasons. Firstly, we distributed our survey exclusively via selected online channels. This was because our research aimed to examine the digital identities and information privacy of actual online users. Nevertheless, we did not reach users of online services other than those we selected. Secondly, a wide range of personal and cultural factors influence perceptions of privacy [Smith *et al.* (2011)]. However, our descriptive statistics indicate that the sample had a relatively low average age as well as an above-average educational background, which might lead to statistical distortions. Thirdly, we cannot rule out the possibility that linguistic and semantic barriers affected our results. In the survey, we presented a hypothetical setting to our respondents in English. An SSI is a new technology which we briefly explained within our survey. SSIs do not have reached mainstream adoption yet, and we expect that not every respondent was familiar with the underlying technological concepts. As most of our respondents were non-native speakers, we must assume that not every respondent fully understood the concept of an SSI even though we tested their understanding with control questions.

The above-mentioned limitations present useful opportunities for future research. First, studies should examine the effect that additional factors have on the acceptance of an SSI. Our research indicates that users are struggling to assess the facilitating conditions of a blockchain-based privacy-preserving IdM that is an SSI. Hence, the communication of values proposed by blockchain must be effective. Blockchain, which is often implemented as underlying and invisible infrastructure, regularly stays under the radar of users. For instance, blockchain creates trust between parties based on the use of technology rather than trust based on the reputation of institutional intermediaries [Chanson *et al.*, (2019)]. Thanks to the technological features of blockchains, users can trust the tamper-resistance of a document stored on a blockchain [Beck *et al.* (2018); Chanson *et al.* (2019); Rossi *et al.* (2019)]. Yet users may remain unaware that they can trust their counterparts based on the tamper-resistance of blockchain. As a result, blockchain-based service providers should communicate the advantages of their technology-based intermediation, including, for example, increased transparency and reduced transaction costs [Rieger *et al.* (2019); Lock *et al.* (2020)]. Consequently, future research could further examine the impact of facilitating conditions on privacy and trust among various actors of a blockchain network.

Second, usability represents another interesting research opportunity, particularly from a design science perspective. Security and privacy requirements often present complex challenges for the usability of IdM systems [Roßnagel *et al.* (2014)]. Researches could examine how an SSI, with its underlying cryptographic technologies such as ZKP or DIDs, should be designed and how different designs affect the use of an SSI, as well as its privacy-preserving nature [Bélanger and Crossler (2011); Pavlou (2011)]. Research could, therefore, theoretically develop adequate design science artifacts and evaluate these in practice [Hevner and Park (2004)], or even follow an action design research approach and ensure relevance by involving practitioners from the early stages of the project. With such knowledge on the design at hand, research could again focus on behavioral questions, such as, for example, whether and how users change their behavior in the presence of fully trusted privacy-preserving IdM systems.

6.5. *Conclusion*

Blockchain is an innovative technology with significant potential that allows for use-cases such as an SSI. Yet, aside from Bitcoin, blockchain applications have not reached mainstream adoption. This study provides empirical knowledge on the acceptance of a privacy-preserving IdM system that is an SSI. We combined theories of technology acceptance and information privacy to investigate factors influencing the acceptance of an SSI. The results of our study augment knowledge in the aforementioned domains and, in particular, about IdM as a superordinate concept of an SSI. We contribute to the theoretical differentiation of control and privacy and shed light on the privacy paradox in the acceptance of these systems with our empirical finding that privacy is not a critical factor in the acceptance of IdM systems from a behavioral perspective. These results contradict existing literature on the impact of privacy as a critical factor in the success of IdM systems. An SSI allows users perceived control over their digital identities, which positively affects users' perceived privacy. But paradoxically, perceived privacy is not a critical factor in the acceptance of an SSI-based IdM system. Our findings suggest the need for future research on factors that affect the acceptance of IdM systems and blockchain use-cases. We propose that future research should investigate the impact of blockchain's technological features and respective value propositions, which could lead to the acceptance of these use-cases. Here, the focus should be on the individual technological components of an SSI and the selection of a user group with different technology literacy. Future studies should further investigate differences of use behavior within SSI-based IdM systems that rely on capabilities of blockchain technology and within those that do not. These studies would contribute to a more comprehensive understanding of factors critical to the acceptance of blockchain, SSI, and privacy-preserving solutions in general.

Appendix A

Construct	No.	Item	Source
Anonymity	ANYT1	I believe I can hide my true identity on digital services when I would use an SSI.	Dinev *et al.* [2013]
	ANYT2	I believe I can stay anonymous and do everything I want on digital services when I would use an SSI.	
	ANYT3	I can keep my information anonymous on digital services when I would use an SSI.	
	ANYT4	I feel that digital services cannot trace back how I use their services when I would use an SSI.	Benlian *et al.* [2019], adapted from Pinsonneault and Heppel [1997]
	ANYT5	I feel anonymous when I would use an SSI.	
	ANYT6	I do not feel like the digital service identifies my use of their service when I would use an SSI.	
Perceived Benefit of Information Disclosure	BEN1	Revealing my personal information on digital services will help me obtain information/products/services I want.	Dinev *et al.* [2013]
	BEN2	I need to provide my personal information so I can get exactly what I want from digital services.	
	BEN3	I believe that because of my personal information disclosure, I will benefit from a better, customized service and/or better information and products.	
	BEN4	I think my benefits gained from the use of digital services can offset the risks of my information disclosure.	Xu *et al.* [2011]
	BEN5	The value I gain from use of digital services is worth the information I give away.	
	BEN6	I think the risks of my information disclosure will be greater than the benefits gained from digital services.	
	BEN7	Overall, I feel that using digital services is beneficial.	
Behavioral Intention	BI1	I intend to use SSI in the next months.	Gupta *et al.* [2008], adapted from [Fishbein and Ajzen, 1975]
	BI2	I predict I would use SSI in the months.	
	BI3	I plan to use SSI in the next months.	
	BI4	I am curious about SSI.	Oliveira *et al.* [2014], adapted from Kim *et al.* [2009]
	BI5	I intend to manage my accounts using an SSI.	
	BI6	I want to know more about SSI.	
Confidentiality	CFDT1	When I would use an SSI, I believe my personal information provided to digital services remains confidential.	Dinev *et al.* [2013]

(*Continued*)

Construct	No.	Item	Source
	CFDT2	I believe an SSI would prevent unauthorized people from accessing my personal information in databases of digital services.	
	CFDT3	When I would use an SSI, I believe my personal information is accessible only to those authorized to have access.	
	CFDT4	When I would use an SSI, I expect my personal information to be confidential when I use digital services.	Pavlou and Fygenson [2006], adapted from Cheung and Lee [2001] and Salisbury *et al.* [2001]
	CFDT5	An adequate protection of my personal information would make it (much more difficult/easier) for me to use a digital service.	
	CFDT6	When I would use an SSI, I feel secure that my personal information is kept confidential when I use digital services.	
	CFDT7	Feeling secure that personal information is kept private would make it (much more difficult/ easier) for me to use a digital service.	
Effort Expectancy	EE1	I would find it easy to use an SSI to access digital services.	Chan *et al.* [2010], adapted from Venkatesh *et al.* [2003]
	EE2	Learning to use an SSI to access digital services would be easy for me.	
	EE3	It would be easy for me to become skillful at using an SSI to access digital services.	
	EE4	My interaction with SSI would be clear and understandable.	Martins *et al.* [2014], adapted from Venkatesh *et al.* [2003]
Facilitating Conditions	FC1	I expect to have the resources necessary to use an SSI to access digital services.	Chan *et al.* [2010], adapted from Venkatesh *et al.* [2003]
	FC2	I expect to have the knowledge necessary to use an SSI to access digital services.	
	FC3	I expect that a specific person or group would be available for assistance with difficulties using an SSI to access digital services.	
Information Sensitivity	IS1	I do not feel comfortable with the type of information digital services request from me.	Dinev *et al.* [2013]
	IS2	I feel that digital services gather highly personal information about me.	
	IS3	The information I provide to digital services is very sensitive to me.	
Regulatory Expectations	LAW1	I believe that the law should protect me from the misuse of my personal data by online companies providing digital services.	Dinev *et al.* [2013]
	LAW2	I believe that the law should govern and interpret the practice of how digital services collect, use, and protect my private information.	
	LAW3	I believe that the law should be able to address violation of the information I provided to digital services.	

(*Continued*)

Construct	No.	Item	Source
	LAW4	The existing laws in my country are sufficient to protect consumers' online privacy.	Lwin *et al.* [2007]
	LAW5	There are stringent international laws to protect personal information of individuals on the Internet.	
	LAW6	The government is doing enough to ensure that consumers are protected against online privacy violations by digital services.	
	LAW7	The best way to protect personal privacy would be through strong laws.	Milberg *et al.* [2000]
Perceived Information Control	PCTL1	I think I have control over what personal information is released by digital service when I would use an SSI.	Dinev *et al.* [2013]
	PCTL2	I believe I have control over how personal information is used by digital services when I would use an SSI.	
	PCTL3	I believe I have control over what personal information is collected by digital services when I would use an SSI.	
	PCTL4	I believe I can control my personal information provided to these digital services when I would use an SSI.	
	PCTL5	I feel in control over information I provide to digital services when I would use an SSI.	Krasnova *et al.* [2010]
	PCTL6	An SSI would allow me to have full control over the information I provide on digital services.	
	PCTL7	I feel in control of who can view my information on digital services when I would use an SSI.	
Performance Expectancy	PE1	Using an SSI would enable me to access digital services more quickly.	Chan *et al.* [2010], adapted from Venkatesh *et al.* [2003]
	PE2	Using an SSI would make it easier for me to access digital services.	
	PE3	Using an SSI would enhance my effectiveness in accessing digital services.	
	PE4	I think that using an SSI would enable me to conduct tasks more quickly.	Martins *et al.* [2014], adapted from Venkatesh *et al.* [2003]
	PE5	I think that using an SSI would increase my productivity.	
	PE6	I think that using an SSI would improve my performance.	
	PE7	I would find an SSI useful in my job.	[Queiroz and Fosso Wamba (2019)], adapted from Venkatesh *et al.* [2003]
	PE8	I would find an SSI useful in my personal life.	
Perceived Privacy	PRIV1	I feel I have enough privacy when I would use an SSI to access these digital services.	Dinev *et al.* [2013]
	PRIV2	I am comfortable with the amount of privacy I have when I would use an SSI.	
	PRIV3	I think my online privacy is preserved when I would use an SSI to access digital services.	
Perceived Risk	RISK1	In general, it would be risky to give personal information to digital services.	Dinev *et al.* [2013]

(*Continued*)

Construct	No.	Item	Source
	RISK2	There would be high potential for privacy loss associated with giving personal information to digital services.	
	RISK3	Personal information could be inappropriately used by digital services.	
	RISK4	Providing digital services with my personal information would involve many unexpected problems.	
Secrecy	SCRT1	When I would use an SSI, I believe I can hide some information from digital services when I want to.	Dinev *et al.* [2013]
	SCRT2	When I would use an SSI, I feel I can pseudonymize some of my personal information if it is asked for by digital services.	
	SCRT3	When I would use an SSI, I believe I can minimize information I must give to digital services when I think it is too personal.	
	SCRT4	When I would use an SSI, I avoid giving digital services detailed information about myself.	Lwin *et al.* [2007]
	SCRT5	When I would use an SSI, I can have full access and benefits as a registered user without revealing my real identity.	
	SCRT6	When I would use an SSI, I may only fill up data partially to register with digital services.	
Social Influence	SI1	People who influence my behavior would think that I should use an SSI to access digital services.	Chan *et al.* [2010], adapted from Venkatesh *et al.* [2003]
	SI2	People who are important to me would think that I should use an SSI to access digital services.	
	SI3	People who are in my social circle would think that I should use an SSI to access digital services.	
	SI4	I would use an SSI if I needed to.	Shafi and Weerakkody [2009]
	SI5	I would use an SSI if my friends and colleagues used it.	
Importance of Information Transparency	TR1	Please specify the importance of whether digital services will allow me to find out what information about me they keep in their databases.	Dinev *et al.* [2013], adapted from Awad [2006]
	TR2	Please specify the importance of whether digital services tell me how long they will retain information they collect from me.	
	TR3	Please specify the importance of the purpose for which digital services want to collect information from me.	
	TR4	Please specify the importance of whether a digital service is going to use the information they collect from me in a way that will identify me.	Awad [2006]

References

Acquisti, A. (2004). Privacy in electronic commerce and the economics of immediate gratification. In *Proceedings of the 5th ACM Conference on Electronic Commerce*, eds. J. Breese, J. Feigenbaum and M. Seltzer. ACM Press, New York, USA, p. 21.

Acquisti, A. (2008). Identity management, privacy, and price discrimination. *IEEE Security & Privacy*, **6**, 2: 46–50, doi: 10.1109/MSP.2008.35.

Acquisti, A. and Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security & Privacy*, **3**, 1: 26–33, doi: 10.1109/MSP.2005.22.

Adjerid, I., Peer, E. and Acquisti, A. (2018). Beyond the privacy paradox: Objective versus relative risk in privacy decision making. *MIS Quarterly*, **42**, 2: 465–488, doi: 10.25300/MISQ/2018/14316.

Ahn, G.-J., Shin, D. and Hong, S.-P. (2004). Information assurance in federated identity management: Experimentations and issues. In *Web Information Systems — WISE 2004*, eds. D. Hutchison *et al.*, Lecture Notes in Computer Science, Vol. 3306. Springer, Berlin, p. 78–89.

Alkhalifah, A. and D'Ambra, J. (2015). Identity management systems research: Frameworks, emergemce, and future opportunities. University of Münster, Münster, Germany.

Allen, C. (2016). The path to self-sovereign identity. Available at http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html.

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

Altman, I. (1975). *The Environment and Social Behavior. Privacy, Personal Space, Territory, Crowding.* Brooks/Cole Publishing, Monterey, CA.

Amend, J., Kaiser, J., Uhlig, L., Urbach, N. and Völter, F. (2021). What do we really need? A systematic literature review of the requirements for blockchain-based e-government services. *Innovation Through Information Systems*, eds. F. Ahlemann, R. Schütte and S. Stieglitz, Lecture Notes in Information Systems and Organisation, Vol. 46. Springer International Publishing, Cham, pp. 398–412.

Angst, C. M. and Agarwal, R. (2009). Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion. *MIS Quarterly*, **33**, 2: 339–370, doi: 10.2307/20650295.

Arnold, H. J. and Feldman D. C. (1981). Social desirability response bias in self-report choice situations. *Academy of Management Journal*, **24**, 2: 377–385, doi: 10.5465/255848.

Awad, K. (2006). The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly*, **30**, 1: 13–28, doi: 10.2307/25148715.

Bansal, G., Zahedi, F. M. and Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems*, **49**, 2: 138–150, doi: 10.1016/j.dss.2010.01.010.

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*, eds. T. Groß and M. Hansen. ACM Press, New York, USA, pp. 25–36.

Beck, R., Müller-Bloch, C. and King, J. L. (2018). Governance in the blockchain economy: A framework and research agenda. *Journal of the Association for Information Systems*, pp. 1020–1034, doi: 10.17705/1jais.00518.

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: 1017–1041, doi: 10.2307/41409971.

Bellman, S., Johnson, E. J., Kobrin, S. J. and Lohse, G. L. (2004). International differences in information privacy concerns: A global survey of consumers. *The Information Society*, **20**, 5: 313–324, doi: 10.1080/01972240490507956.

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: 103–168, doi: 10.1016/j.im.2019.05.003.

Benlian, A., Klumpe, J. and Hinz, O. (2019). Mitigating the intrusive effects of smart home assistants by using anthropomorphic design features: A multimethod investigation. *Information Systems Journal*, **34**, 4: 112–151. Special Issue — The Digitalization of the Individual: 112–151, doi:10.1111/isj.12243.

Berg, C., Davidson, S. and Potts, J. (2017). The institutional economics of identity. *SSRN Journal*, doi: 10.2139/ssrn.3072823.

Budnitz, M. E. (1997). Privacy protection for consumer transactions in electronic commerce: Why self-regulation is inadequate. *South Carolina Law Review*, **49**: 847–886.

Buxmann, P., Krasnova, H., Eling, N. and Abramova, O. (2014). Dangers of 'Facebook Login' for mobile apps: Is there a price tag for social information? In *International Conference on Information Systems, ICIS* 2014, doi: 10.7892/BORIS.68894.

Cameron, K. (2005). The laws of identity. *Microsoft Corporation*, **12**, 1: 8–11. Available at https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf.

Camp, L. J. (1999). Web security and privacy: An American perspective. *The Information Society*, **15**, 4: 249–256, doi: 10.1080/019722499128411.

Camp, L. J. (2004). Digital identity. *IEEE Technology and Society Magazine*, **23**, 3: 34–41, doi: 10.1109/MTAS.2004.1337889.

Cassel, C., Hackl, P. and Westlund, A. H. (1999). Robustness of partial least-squares method for estimating latent variable quality structures. *Journal of Applied Statistics*, **26**, 4: 435–446, doi: 10.1080/02664769922322.

Chan, F., Thong, J., Venkatesh, V., Brown, S., Hu, P. and Tam, K. (2010). Modeling citizen satisfaction with mandatory adoption of an e-government technology. *Journal of the Association for Information Systems*, **11**, 10: 519–549, doi: 10.17705/1jais.00239.

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*, 1272–1307, doi: 10.17705/1jais.00567.

Chatman, C. M., Eccles, J. and Malanchuk, O. (2005). Identity negotiation in everyday settings. *Navigating the Future: Social Identity, Coping and Life Tasks*, eds. G. Downey, J. S. Eccles and C. M. Chatman, Russell Sage Foundation, New York, pp. 116–139.

Chellappa, R. K. and Sin, R. G. (2005). Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information Technology and Management*, **6**, 2–3: 181–202, doi: 10.1007/s10799-005-5879-y.

Cheung, C. M. and Lee, M. K. (2001). Trust in internet shopping. *Journal of Global Information Management*, **9**, 3: 23–35, doi: 10.4018/jgim.2001070103.

Cho, S., Lee, K., Cheong, A., No, W. G. and Vasarhelyi, M. A. (2021). Chain of values: Examining the economic impacts of blockchain on the value-added tax system. *Journal of Management Information Systems*, **38**, 2: 288–313, doi: 10.1080/07421222.2021.1912912.

Chong, A. Y. L., Lim, E. T. K., Hua, X., Zheng, S. and Tan, C.-W. (2019). Business on chain: A comparative case study of five blockchain-inspired business models. *Journal of the Association for Information Systems*, 1308–1337, doi: 10.17705/1jais.00568.

Clarke, R. (1999). Internet privacy concerns confirm the case for intervention. *Communications of the ACM*, **42**, 2: 60–67, doi: 10.1145/293411.293475.

Cohen, J. (2013). *Statistical Power Analysis for the Behavioral Sciences*, 2nd edn. Taylor and Francis, Hoboken. http://gbv.eblib.com/patron/FullRecord.aspx?p=1192162.

Constantinides, P., Henfridsson, O. and Parker, G. G. (2018). Introduction — platforms and infrastructures in the digital age. *Information Systems Research*, **29**, 2: 381–400, doi: 10.1287/isre.2018.0794.

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: 487–515, doi: 10.17705/1jais.00463.

Culnan, M. J. and Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science*, **10**, 1: 104–115, doi: 10.1287/orsc.10.1.104.

Culnan, M. J. and Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal Social Issues*, **59**, 2: 323–342, doi: 10.1111/1540-4560.00067.

Davis, F. (1985). A technology acceptance model for empirically testing new end-user information systems: Theory and results. Doctoral dissertation, Massachusetts Institute of Technology.

De Filippi, P., Mannan, M. and Reijers, W. (2020). Blockchain as a confidence machine: The problem of trust and challenges of governance. *Technology in Society*, **62**: 101284, doi: 10.1016/j.techsoc.2020.101284.

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*, **6**, 2: 24–29, doi: 10.1109/MSP.2008.49.

Dinev, T. and Hart, P. (2004). Internet privacy concerns and their antecedents — measurement validity and a regression model. *Behaviour & Information Technology*, **23**, 6: 413–422, doi: 10.1080/01449290410001715723.

Dinev, T. and Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, **17**, 1: 61–80, doi: 10.1287/isre.1060.0080.

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I. and Colautti, C. (2006). Privacy calculus model in e-commerce — a study of Italy and the United States. *European Journal of Information Systems*, **15**, 4: 389–402, doi: 10.1057/palgrave.ejis.3000590.

Dinev, T., McConnell, A. R. and Smith, H. J. (2015). Research commentary — informing privacy research through information systems, psychology, and behavioral economics: Thinking outside the "APCO" box. *Information Systems Research*, **26**, 4: 639–655, doi: 10.1287/isre.2015.0600.

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: 295–316, doi: 10.1057/ejis.2012.23.

Dowling, G. R. and Staelin, R. (1994). A model of perceived risk and intended risk-handling activity. *Journal Consumer Research*, **21**, 1: 119–134, doi: 10.1086/209386.

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

Dunphy, P. and Petitcolas, F. A. P. (2018). A first look at identity management schemes on the blockchain. *IEEE Security & Privacy*, **16**, 4: 20–29, doi: 10.1109/MSP.2018.3111247.

Faul, F., Erdfelder, E., Buchner, A. and Lang, A.-G. (2009). Statistical power analyses using G*Power 3.1: Tests for correlation and regression analyses. *Behavior Research Methods*, **41**, 4: 1149–1160, doi: 10.3758/BRM.41.4.1149.

Fishbein, M. and Ajzen, I. (1975). *Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research.* Addison-Wesley, Reading, MA.

Fornell, C. and Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, **18**, 1: 39–50, doi: 10.2307/3151312.

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: 55–75, doi: 10.1002/dir.20061.

Günsay, E., Onur, C. B. and Cenk, M. (2021). An improved range proof with base-3 construction. In *2021 14th International Conference on Security of Information and Networks*, Vol. 1. IEEE, pp. 1–6.

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*. Hawaii, USA, pp. 1543–1552.

Goldreich, O., Micali, S. and Wigderson, A. (1991). Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems. *Journal of the ACM*, **38**, 3: 690–728, doi: 10.1145/116825.116852.

Guggenberger, T., Lockl, J., Röglinger, M., Schlatt, V., Sedlmeir, J., Stoetzer, J.-C., Urbach, N. and Völter, F. (2021). Emerging digital technologies to combat future crises: Learnings from COVID-19 to be prepared for the future. *International Journal of Innovation and Technology Management*, **18**, 4: 2140002, doi: 10.1142/S0219877021400022.

Gupta, B., Dasgupta, S. and Gupta, A. (2008). Adoption of ICT in a government organization in a developing country: An empirical study. *The Journal of Strategic Information Systems*, **17**, 2: 140–154, doi: 10.1016/j.jsis.2007.12.004.

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)*, 2nd edn. SAGE, Melbourne.

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

Hann, I.-H., Hui, K.-L., Lee, S.-Y. T. and Png, I. P. L. (2007). Overcoming online information privacy concerns: An information-processing theory approach. *Journal of Management Information Systems*, **24**, 2: 13–42, doi: 10.2753/MIS0742-1222240202.

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

Hansen, M., Schwartz, A. and Cooper, A. (2008). Privacy and identity management. *IEEE Security & Privacy*, **6**, 2: 38–45, doi: 10.1109/MSP.2008.41.

Hawlitschek, F., Notheisen, B. and Teubner, T. (2018). The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy. *Electronic Commerce Research and Applications*, **29**: 50–63, doi: 10.1016/j.elerap.2018.03.005.

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

Hevner, M. and Park, R. (2004). Design science in information systems research. *MIS Quarterly*, **28**, 1: 75–105, doi: 10.2307/25148625.

Hille, P., Walsh, G. and Cleveland, M. (2015). Consumer fear of online identity theft: Scale development and validation. *Journal of Interactive Marketing*, **30**: 1–19. doi: 10.1016/j.intmar.2014.10.001.

Hoess, A., Roth, T., Sedlmeir, J., Fridgen, G. and Rieger, A. (2022). With or without blockchain? Towards a decentralized, SSI-based eRoaming architecture. In *Proceedings of the 55th Hawaii International Conference on System Sciences (HICSS)*, Kauai, Hawaii, USA, pp. 1–10.

Isaak, J. and Hanna, M. J. (2018). User data privacy: Facebook, Cambridge analytica, and privacy protection. *Computer*, **51**, 8: 56–59, doi: 10.1109/MC.2018.3191268.

Jensen, J. (2011). Benefits of federated identity management — a survey from an integrated operations viewpoint. *Availability, Reliability and Security for Business, Enterprise and Health Information Systems*, eds. D. Hutchison *et al.*, Lecture Notes in Computer Science, No. 6908. Springer, Berlin, pp. 1–12.

Jøsang, A. and Pope, S. (2005). User centric identity management. In *AusCERT Asia Pacific Information Technology Security Conference*. Citeseer, Gold Coast, Australia, pp. 77–89.

Jøsang, A., Al Zomai, M. and Suriadi, S. (2007). Usability and privacy in identity management architectures. In *Proceedings of the Fifth Australasian Symposium on ACSW Frontiers*. Australian Computer Society, Australia, pp. 143–152.

Kam, L. E. and Chismar, W. G. (2006). Online self-disclosure: Model for the use of internet-based technologies in collecting sensitive health information. *International Journal of Healthcare Technology and Management*, **7**, 3/4: 218–232, doi: 10.1504/IJHTM.2006.008433.

Karwatzki, S., Trenz, M., Tuunainen, V. K. and Veit, D. (2017). Adverse consequences of access to individuals' information: An analysis of perceptions and the scope of organisational influence. *European Journal of Information Systems*, **26**, 6: 688–715, doi: 10.1057/s41303-017-0064-z.

Katz, M. L. and Shapiro, C. (1994). Systems competition and network effects. *Journal of Economic Perspectives*, **8**, 2: 93–115, doi: 10.1257/jep.8.2.93.

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: 607–635, doi: 10.1111/isj.12062.

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: 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., Günther, O., Spiekermann, S. and Koroleva, K. (2009). Privacy concerns and identity in online social networks. *Identity in the Information Society*, **2**, 1: 39–63, doi: 10.1007/s12394-009-0019-1.

Krasnova, H., Spiekermann, S., Koroleva, K. and Hildebrand, T. (2010). Online social networks: Why we disclose. *Journal of Information Technology*, **25**, 2: 109–125, doi: 10.1057/jit.2010.6.

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

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: 22–42, doi: 10.1111/j.1540-4560.1977.tb01880.x.

Lee, J. K., Chang, Y., Kwon, H. Y. and Kim, B. (2020). Reconciliation of privacy with preventive cybersecurity: The bright internet approach. *Information Systems Frontiers*, **22**, 1: 45–57, doi: 10.1007/s10796-020-09984-5.

Lee, J. K. (2015). Research framework for AIS grand vision of the bright ICT initiative. *MIS Quarterly*, **39**, 2: iii–xii, Available at https://www.misq.org/misq/downloads/download/editorial/620/.

Li, H., Sarathy, R. and Xu, H. (2011). The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. *Decision Support Systems*, **51**, 3: 434–445, doi: 10.1016/j.dss.2011.01.017.

Li, H., Wu, J., Gao, Y. and Shi, Y. (2016). Examining individuals' adoption of healthcare wearable devices: An empirical study from privacy calculus perspective. *International Journal of Medical Informatics*, **88**: 8–17, doi: 10.1016/j.ijmedinf.2015.12.010.

Li, Y. (2012). Theories in online information privacy research: A critical review and an integrated framework. *Decision Support Systems*, **54**, 1: 471–481, doi: 10.1016/j.dss.2012.06.010.

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*, 1–15, doi: 10.1109/TEM.2020.2978014.

Lu, Y., Tan, B. C. Y. and Hui, K. L. (2004). Inducing customers to disclose personal information to internet businesses with social adjustment benefits. In *Proceedings of the International Conference on Information Systems*, Washington, DC, USA, pp. 571–582.

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 Sciences*, **35**, 4: 572–585, doi: 10.1007/s11747-006-0003-3.

Mühle, A., Grüner, A., Gayvoronskaya, T. and 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.

Ma, X., Zhou, Y., Wang, L. and Miao, M. (2022). Privacy-preserving byzantine-robust federated learning. *Computer Standards & Interfaces*, **80**, C: 103561, doi: 10.1016/j.csi.2021.103561.

Maler, E. and Reed, D. (2008). The venn of identity: Options and issues in federated identity management. *IEEE Security & Privacy*, **6**, 2: 16–23, doi: 10.1109/MSP.2008.50.

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: 336–355, doi: 10.1287/isre.1040.0032.

Marangunić, N. and Granić, A. (2015). Technology acceptance model: A literature review from 1986 to 2013. *Universal Access in the Information Society*, **14**, 1: 81–95, doi: 10.1007/s10209-014-0348-1.

Margulis, S. T. (1977). Conceptions of privacy: Current status and next steps. *Journal of Social Issues*, **33**, 3: 5–21, doi: 10.1111/j.1540-4560.1977.tb01879.x.

Martins, C., Oliveira, T. and Popovič, A. (2014). Understanding the Internet banking adoption: A unified theory of acceptance and use of technology and perceived risk application. *International Journal of Information Management*, **34**, 1: 1–13, doi: 10.1016/j.ijinfomgt.2013.06.002.

Mathieson, K. (1991). Predicting user intentions: Comparing the technology acceptance model with the theory of planned behavior. *Information Systems Research*, **2**, 3: 173–191, doi: 10.1287/isre.2.3.173.

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**: 50737–50751, doi: 10.1109/ACCESS.2018.2869359.

Milberg, S. J., Smith, H. J. and Burke, S. J. (2000). Information privacy: Corporate management and national regulation. *Organization Science*, **11**, 1: 35–57, doi: 10.1287/orsc.11.1.35.12567.

Morais, E., Koens, T., Van Wijk, C. and Koren, A. (2019). A survey on zero knowledge range proofs and applications. *SN Applied Sciences*, **1**, 946: 1–17, doi: 10.1007/s42452-019-0989-z.

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: 76–98, doi: 10.1177/1094670511424924.

Mueller, M. L., Park, Y., Lee, J. and Kim, T.-Y. (2006). Digital identity: How users value the attributes of online identifiers. *Information Economics and Policy*, **18**, 4: 405–422, doi: 10.1016/j.infoecopol.2006.04.002.

Nakamoto, S. (2008): Bitcoin: A peer-to-peer electronic cash system. Available at https://bitcoin.org/bitcoin.pdf.

Neumann, P. G. (1994). Risks of passwords. *Communications of the ACM*, **37**, 4: 126, doi: 10.1145/175276.175289.

Norberg, P. A., Horne, D. R. and Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, **41**, 1: 100–126, doi: 10.1111/j.1745-6606.2006.00070.x.

Nunnally, J. C. and Bernstein, I. H. (2008). *Psychometric Theory*, 3rd edn., McGraw-Hill Series in Psychology. McGraw-Hill, New York.

O'Donoghue, T. and Rabin, M. (2000). The economics of immediate gratification. *Journal of Behavioural Decision Making*, **13**, 2: 233–250, doi: 10.1002/(SICI)1099-0771(200004/06)13:2<233::AID-BDM325>3.0.CO;2-U.

O'Donoghue, T. and Rabin, M. (2001). Choice and procrastination. *The Quarterly Journal of Economics*, **116**, 1: 121–160, doi: 10.1162/003355301556365.

Oliveira, T., Faria, M., Thomas, M. A. and Popovič, A. (2014). Extending the understanding of mobile banking adoption: When UTAUT meets TTF and ITM. *International Journal of Information Management*, **34**, 5: 689–703, doi: 10.1016/j.ijinfomgt.2014.06.004.

Pavlou, P. and Fygenson, M. (2006). Understanding and predicting electronic commerce adoption: An extension of the theory of planned behavior. *MIS Quarterly*, **30**, 1: 115–143, doi: 10.2307/25148720.

Pavlou, P. (2011). State of the information privacy literature: Where are we now and where should we go?*MIS Quarterly*, **35**, 4: 977–988, doi: 10.2307/41409969.

Pinsonneault, A. and Heppel, N. (1997). Anonymity in group support systems research: A new conceptualization, measure, and contingency framework. *Journal of Management Information Systems*, **14**, 3: 89–108, doi: 10.1080/07421222.1997.11518176.

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: 3–29, doi: 10.1080/15536548.2012.11082759.

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

Recordon, D. and Reed, D. (2006). OpenID 2.0. In *Proceedings of the Second ACM Workshop on Digital Identity Management — DIM'06*, eds. A. Juels, M. Winslett and A. Goto, Alexandria, Virginia, USA, 3 November. ACM Press, New York, USA, pp. 11–16.

Reed, D., Sporny, M., Longley, D., Allen, C., Grant, R. and Sabadello, M. (2018). Decentralized identifiers (DIDs): Data model and syntaxes for decentralized identifiers (DIDs). Available at https://w3c-ccg.github.io/did-spec/.

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: 263–279, doi: 10.17705/2msqe.00020.

Rieger, A., Roth, T., Sedlmeir, J. and Fridgen, G. (2021). The privacy challenge in the race for digital vaccination certificates. *Med*, **2**, 6: 633–634, doi: 10.1016/j.medj.2021.04.018.

Rindfleisch, T. C. (1997). Privacy, information technology, and health care. *Communications of the ACM*, **40**, 8: 92–100, doi: 10.1145/257874.257896.

Rogers, E. M. (1983). *Diffusion of Innovations*, 3rd edn. New York, NY: Free Press.

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: 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: 36–50, doi: 10.1057/ejis.2013.33.

Salinas Segura, Alexander and Thiesse, Frédéric, "Extending UTAUT2 to Explore Pervasive Information Systems" (2015). ECIS 2015 Completed Research Papers. Paper 154. ISBN 978-3-00-050284-2.

Salisbury, W. D., Pearson, R. A., Pearson, A. W. and Miller, D. W. (2001). Perceived security and World Wide Web purchase intention. *Industrial Management & Data Systems*, **101**, 4: 165–177, doi: 10.1108/02635570110390071.

Schoeman, F. D. (1984). *Philosophical Dimensions of Privacy. An Anthology.* Cambridge University Press, Cambridge. http://www.loc.gov/catdir/description/cam031/84005898.html.

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

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: 93–103, doi: 10.1057/ejis.2009.51.

Shafi, A. and Weerakkody, V. (2009). Understanding citizens' behavioural intension in the adoption of e-government services in the state of Qatar. In *17th European Conference on Information Systems*, Verona, Italy, pp. 1618–1629.

Sheehan, K. B. and Hoy, M. G. (2000). Dimensions of privacy concern among online consumers. *Journal of Public Policy & Marketing*, **19**, 1: 62–73, doi: 10.1509/jppm.19.1.62.16949.

Simon, H. A. (1959). Theories of decision-making in economics and behavioral science. *The American Economic Review*, **49**, 3: 253–283.

Smith, H. J., Dinev, T. and Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, **35**, 4: 989–1015, doi: 10.2307/41409970.

Sovrin (2018). Sovrin: A protocol and token for self-sovereign identity and decentralized trust. Whitepaper. Sovrin Foundation. https://sovrin.org/wp-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf.

Sovrin (2019). Sovrin governance framework V2. Master Document V1. Sovrin Foundation. Available at https://sovrin.org/wp-content/uploads/Sovrin-Governance-Framework-V2-Master-Document-V1.pdf.

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*, eds. M. P. Wellman and Y. Shoham, Tampa, Florida, USA, 14–17 October. ACM Press, New York, USA, pp. 38–47.

Spiro, W. G. and Houghteling, L. J. (1981). *The Dynamics of Law*. 2nd edn. Harcourt Brace Jovanovich, New York.

Stokkink, Q. and Pouwelse, J. (2018). Deployment of a blockchain-based self-sovereign identity. In *2018 IEEE International Conference on Internet of Things (IEEE iThings), IEEE Green Computing and Communications (IEEE GreenCom), IEEE Cyber, Physical and Social Computing (IEEE CPSCom), and IEEE Smart Data (IEEE SmartData)*. IEEE, Halifax, NS, Canada, pp. 1336–1342.

Talamo, A. and Ligorio, B. (2001). Strategic identities in cyberspace. *Cyberpsychology & Behavior: The Impact of the Internet, Multimedia and Virtual Reality on Behavior and Society*, **4**, 1: 109–122, doi: 10.1089/10949310151088479.

Tang, Z., Hu, Y. and Smith, M. D. (2008). Gaining trust through online privacy protection: Self-regulation, mandatory standards, or caveat emptor. *Journal of Management Information Systems*, **24**, 4: 153–173, doi: 10.2753/MIS0742-1222240406.

Tefft, S. K. (1980). *Secrecy. A Cross-cultural Perspective*. Human Sciences Press, New York.

Tobin, A. and Reed, D. (2016). The inevitable rise of self-sovereign identity. A white paper from the Sovrin Foundation. Available at https://sovrin.org/wp-content/uploads/2018/03/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf.

Turkle, S. (1997). *Life on the Screen. Identity in the Age of the Internet*. Touchstone (A Touchstone book), New York.

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**: 5–40.

Venkatesh, V., Morris, M. G. and Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, **27**, 3: 425–478, doi: 10.2307/30036540.

Venkatesh, V.Thong, J. Y. L. 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: 157–178, doi: 10.2307/41410412.

W3C (2019a). A Primer for Decentralized Identifiers. An introduction to self-administered identifiers for curious people. Available at https://w3c-ccg.github.io/did-primer.

W3C (2019b). Verifiable Credentials Data Model 1.0. Expressing verifiable information on the Web. Available at https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials.

Waldo, J. (2007). *Engaging Privacy and Information Technology in a Digital Age*. National Academies Press, Washington, D.C.

Warren, S. D. and Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, **4**, 5: 193–220, doi: 10.2307/1321160.

Weick, K. E. (1995). *Sensemaking in Organizations*. Sage Publishing, Thousand Oaks, CA.

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*, pp. 1–13.

Westin, A. F. (1967). *Privacy and Freedom*. IG Publishing, New York.

Whitley, E. A., Gal, U. and Kjaergaard, A. (2014). Who do you think you are? A review of the complex interplay between information systems, identification and identity. *European Journal of Information Systems*, **23**, 1: 17–35, doi: 10.1057/ejis.2013.34.

Xu, H., Teo, H.-H., Tan, B. C. Y. and Agarwal, R. (2009). The role of push-pull technology in privacy calculus: The case of location-based services. *Journal of Management Information Systems*, **26**, 3: 135–174, doi: 10.2753/MIS0742-1222260305.

Xu, H., Dinev, T., Smith, J. and Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems*, **12**, 12: 798–824, doi: 10.17705/1jais.00281.

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. *Information Systems Research*, **23**, 4: 1342–1363, doi: 10.1287/isre.1120.0416.

Xu, H. (2007). The effects of self-construal and perceived control on privacy concerns. In *Proceedings of the International Conference on Information Systems*. Montreal (Quebec), Canada, pp. 125–139.

Zhang, H., Wang, J. and Ding, Y. (2019). Blockchain-based decentralized and secure keyless signature scheme for smart grid. *Energy*, **180**: 955–967, doi: 10.1016/j.energy.2019.05.127.

Zheng, Z., Xie, S., Dai, H. N., Chen, X. and Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services*, **14**, 4: 352–375, doi: 10.1504/IJWGS.2018.095647.

Ziolkowski, R., Miscione, G. and Schwabe, G. (2020). Decision problems in blockchain governance: Old wine in new bottles or walking in someone else's shoes? *Journal of Management Information Systems*, **37**, 2: 316–348, doi: 10.1080/07421222.2020.1759974.

Zwick, D. and Dholakia, N. (2004). Whose identity is it anyway? Consumer representation in the age of database marketing. *Journal of Macromarketing*, **24**, 1: 31–43, doi: 10.1177/0276146704263920.

Biography

Jannik Lockl studied Industrial Engineering and Management at the University of Bayreuth. Jannik has been working as a research associate and postdoctoral researcher at the FIM Research Center and Branch Business & Information Systems Engineering of the Fraunhofer FIT since February 2018, while he further holds a position as research associate at UCL CBT. His research on emerging digital technologies has been published in conferences and journals such as the International Conference on Information Systems, ACM Transactions on Management Information Systems, IEEE Transactions on Engineering Management, International Journal of Technology Assessment in Health Care, and MISQ Executive. Jannik worked as a consultant for companies like BMW and IBM and is founder of the AI-driven MedTech startup inContAlert GmbH.

Nico Thanner studied Business Administration (M.Sc.) at the University of Bayreuth. His research focusses on topics in emerging technologies and digital innovation, with a specific focus on an entrepreneurial perspective. He worked in innovation and growth centers of Porsche Digital and N26, and the technology labs of the FIM Research Center and Project Group Business & Information Systems Engineering of the Fraunhofer FIT. Since 2021, Nico works for the Danish InsurTech startup Undo, delivering strategic insights to founders based on data analyses and predictive analytics.

Manuel Utz is a doctoral candidate at the Chair of Information Systems and Digital Energy Management at the University of Bayreuth, Germany. His research focuses on the design and implementation of blockchain-based applications in energy markets. Currently Manuel is also employed at BMW Group as Head of Digital Energy Management.

Maximilian Röglinger holds the chair of Information Systems and Business Process Management at the University of Bayreuth and is Adjunct Professor in the School of Management at Queensland University of Technology. Maximilian also serves as Deputy Academic Director of the Research Center Finance & Information Management (FIM) as well as Deputy Director of Fraunhofer FIT. Maximilian's activities in research and teaching center around business process management, digital innovation, and customer orientation. His work has been published in journals such as Business & Information Systems Engineering, Decision Support Systems, European Journal of Information Systems, Journal of Strategic Information Systems, Information Systems Journal, and Journal of the Association for Information Systems. Maximilian is passionate about joint research with companies. Among others, he has collaborated with Allianz, Deutsche Bahn, Deutsche Bank, Fujitsu Technologies, HILTI, Infineon Technologies, Munich Airport, and ZEISS.