Taking a Sociotechnical Perspective on Self-Sovereign Identity – A Systematic Literature Review

Research Paper

Lukas Florian Bossler[1], Teresa Huber[1], and Julia Kroenung[1]

[1] University of Hagen, Faculty of Business Administration and Economics, Hagen, Germany
{lukas.bossler,teresa.huber,julia.kroenung}@fernuni-hagen.de

Abstract. With the increasing use of the Internet, individuals must manage countless accounts across multiple platforms, making it difficult for users to track who is using their data. Self-sovereign identity (SSI), supported by regulations such as GDPR and eIDAS, promises to put control of their data back into the hands of the users. Governments need to understand the sociotechnical challenges of SSI. We conduct a systematic literature review, identifying security and privacy as the most prevalent concerns in the academic literature while social challenges are largely overlooked. Further, we find that the academic literature mostly treats SSI in general rather than focusing on specific application domains.

Keywords: self-sovereign identity, decentralized identity, blockchain

1 Introduction

The widespread use of the Internet has become integral to everyday life, offering services such as online shopping, banking, and streaming (Cabinakova et al., 2019). Engaging with these services requires users to disclose personal data, contributing to the rapid expansion of their digital footprint (Kölbel et al., 2022).

Digital identity management often relies on service-specific user accounts, necessitating repeated registration processes due to limited data portability (Sedlmeir et al., 2021). The resulting growth in the number of accounts makes it difficult for users to track who uses their data (Lacity & Carmel, 2022). Multinational corporations like Google, Microsoft, and Meta collect and control vast amounts of interconnected user data, enabling insights into individual behavior, purchases, interests, locations, and health data (Kölbel et al., 2022). Users generally lack control over the extent to which their personal data is misused or shared with third parties (Kulabukhova et al., 2019).

In light of growing data security and privacy concerns (Liu et al., 2021; Schardong et al., 2022), rising skepticism toward large tech companies (Weigl et al., 2022), the General Data Protection Regulation (GDPR), and proposed changes to the electronic IDentification, Authentication and trust Services (eIDAS) regulation (Guggenberger et al., 2023), self-sovereign identity (SSI) is proposed as an approach that enables end

20th International Conference on Wirtschaftsinformatik,
September 2025, Münster, Germany

users to control their personal data disclosure without relying on external, centralized authorities (Johnson Jeyakumar et al., 2022).

Especially in light of the evolving eIDAS 2.0 regulation, SSI presents itself as a way for governments to take control of identity management away from large multinational corporations and put control of personal data back into the hands of individuals (Degen & Teubner, 2024). The success of current government eID initiatives differs greatly across countries. Whereas Nordic countries have an adoption rate of more than 80% (Schneider et al., 2019), only 7% of German citizens have used the German eID (Guggenberger et al., 2023). Furthermore, although considerable research on organizational platform governance and the individual aspects of SSI exists, there is still limited research on how SSI integrates with public digital identity infrastructures and the role of governments in this context (Degen & Teubner, 2024). To facilitate a connection between government institutions and private businesses through a shared solution in a public-private ecosystem, it is important to identify overarching success factors and challenges, both of technical and social nature. Different application contexts may face different challenges. We therefore ask the following research questions:

RQ1: What are sociotechnical challenges to the implementation and adoption of self-sovereign identity?

RQ2: How do these challenges impact different areas of application of self-sovereign identity?

This article makes three major contributions. First, it highlights the sociotechnical challenges of SSI implementation and adoption. Second, it emphasizes the importance of social factors such as user acceptance, trust, and usability. Third, it underscores the need for more domain-specific research.

2 Conceptual Background

A person's identity encompasses personal data and consists of multiple partial identities. Partial identities contain various attributes (e.g., name, address) and are used in different contexts (e.g., work, leisure) (Just, 2011; Sedlmeir et al., 2021). A digital identity is used for identification in digital environments (Schardong & Custodio, 2022).

Identity management systems (IMS) provide tools for handling partial identities across online contexts. They ensure reliable attribute assignment to individuals, enabling authentication (Clauß & Köhntopp, 2001). IMS typically involve three actors: the user, an Identity Provider (IdP), and a Service Provider (SP). The IdP stores users' partial identities, while the SP offers services (Ferdous et al., 2019).

SSI enables users to gain sovereignty over their digital identities (Feulner et al., 2022; Kuperberg, 2019), allowing them to decide with whom they share their data (Schardong & Custodio, 2022). SSI involves three primary actors: (1) the user, who acts as their own IdP (Kulabukhova et al., 2019), (2) issuers, who provide verified credentials that attest to the user's attributes (Cucko et al., 2022; Ehrlich et al., 2021), and (3) parties relying on the provided credentials. Identity holders can present their credentials as verifiable presentations, which include only the necessary identity components for a context, ensuring data minimization (Mühle et al., 2018).

A successful widespread implementation and use of SSI is not only dependent on technical factors, such as security and interoperability. The adoption and use, particularly by end users, is also dependent on social factors, including trust and usability (Sedlmeir, Barbereau, et al., 2022; Weigl et al., 2022). SSI challenges traditional ways of trust in identities, which is usually provided by central authorities (Guggenberger et al., 2023). Users, including organizations and end users, must form new trust relationships, redefining what imbues an entity with trust (Degen & Teubner, 2024). Regulatory frameworks must account for these new forms of trust, allowing them to gain widespread recognition (Kubach et al., 2020). Because of the dual emphasis on technical and social factors, the sociotechnical perspective (Sarker et al., 2019) is well-suited for investigating SSI, whose widespread implementation and adoption depends on technology, individuals, and surrounding structures. The sociotechnical perspective stands at the core of information systems (IS) research and distinguishes the IS discipline from more technically oriented disciplines such as computer science and from more socially oriented disciplines such as management and psychology (Sarker et al., 2019).

3 Research Method

We conducted a systematic literature review following Webster and Watson (2002) and the Preferred Items for Systematic Literature Reviews and Meta-Analysis (PRISMA) guidelines (Page et al., 2021). To ensure a broad coverage of high-quality and relevant IS research, we included all journals and conferences of the VHB Publication Media Ranking area rating "Information Systems", ranked A+ to C, in our data collection.

Our search strategy used the following search terms to identify relevant articles: "self-sovereign identity", "self-sovereignty", and "decentralized identity". Because SSI is often mentioned in conjunction with or implemented using – and thus closely linked to – blockchain technology (Guggenberger et al., 2023), we also used the search terms "blockchain identity" and "blockchain-based identity". In order to identify all articles, we conducted a full-text search and did not set temporal limitations. To allow for traceability and to ensure a rigorous approach to our literature search and analysis, we applied the PRISMA guidelines (Page et al., 2021). Our keyword search resulted in 241 records. After removing duplicates and excluding irrelevant articles based on titles, abstracts, and keywords (150 articles), 91 articles underwent full-text review. A review of the full texts led to the exclusion of 13 articles, leaving 78 articles for analysis.

We analyzed the articles in our final data set to compile a concept matrix following Webster and Watson (2002). For each article, we recorded descriptive information, including the outlet in which the article was published, the research methods applied, and the research questions of the article – if explicitly stated. Furthermore, to determine whether a geographic center for SSI research exists, we recorded the country of the first author and the location of data collection for articles based on empirical data.

To investigate our two research questions, concerned with sociotechnical challenges to the implementation and adoption of SSI and common application areas, respectively, we employed thematic analysis to identify repeating patterns and themes in the articles of our final data set (Braun & Clarke, 2006). Employing inductive analysis, we aimed

to capture all aspects of our articles that relate to influences of sociotechnical nature, adhering to the sociotechnical continuum presented in Sarker et al. (2019), as well as the application scenarios in which SSI has been applied.

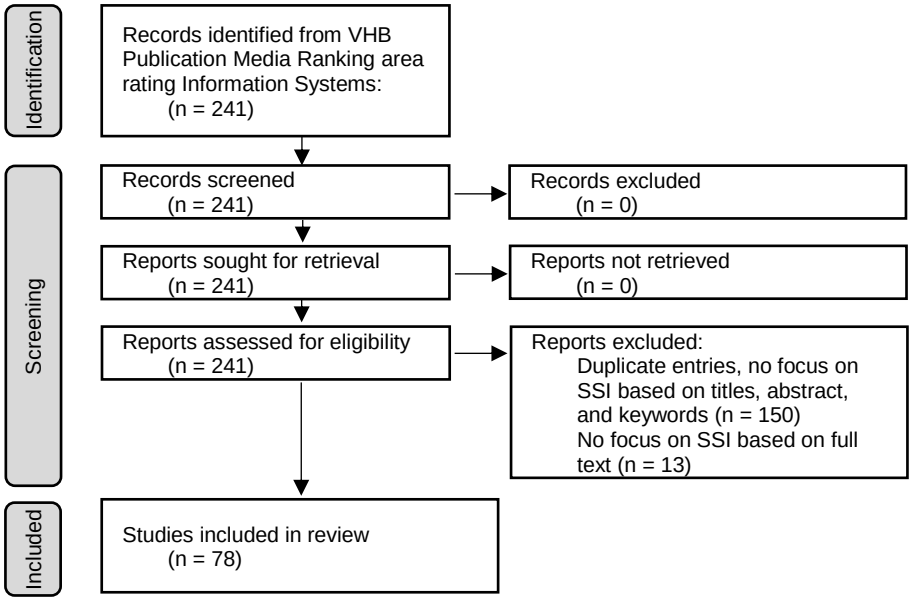

Figure 1. Preferred Items for Systematic Literature Reviews and Meta-Analysis (PRISMA) Flow Diagram

First, we carefully analyzed the articles in our final sample. We identified and recorded all text passages pertaining to social and technical aspects that may influence the implementation and adoption of SSI. This allowed us to generate initial codes. Second, we reviewed the codes, searching for common themes. We discarded themes that only occurred once or twice and combined themes that were conceptually close (e.g., locating GDPR within privacy). Third, we reread the articles and captured where they fit with themes that had been overlooked during the first reading.

Because the challenges can be viewed from different perspectives, this classification of themes is not meant to be exhaustive, but rather a systematic overview. In an effort to support open science and due to space limitations, we have made the concept matrix available at https://osf.io/83px7/?view_only=2a916a17b7c04a45a44d562f7a389fa0.

4 Results

We analyzed the 78 articles in our sample regarding the research methods applied, the geographical locations of the authors and data collection, and the research questions asked. First, regarding research methods, we found that nearly half of the articles featured some kind of design or implementation (n=38). However, only 8 articles utilize theory-informed design science methods, whereas the remaining 30 articles focus on

purely technical designs, such as algorithms and models. A significant number of articles (n=25) are conceptual in nature. 19 articles feature empirical data collection: 13 articles used expert interviews, 4 articles conducted case studies, 3 articles conducted surveys, and 3 articles employed experiments. 8 articles conducted literature reviews. Second, regarding geographical location, the majority of articles are first-authored by researchers with a European (n=54), Asian (n=12), or North American (n=7) affiliation. The most common countries are Germany (n=26), China (n=9), and the USA (n=7). Among the 19 empirical articles, only a few explicitly state the country of data collection. Data collection was conducted European countries, with a focus on Germany, Finland, Sweden and the UK; North America; Australia; and Taiwan. Third, only 15 articles explicitly stated research questions, primarily examining antecedents, challenges, facilitating conditions, outcomes, and advantages of SSI deployment.

4.1 Sociotechnical Requirements and Challenges

To answer research question 1, we applied a sociotechnical lens (Sarker et al., 2019) to identify requirements and challenges that influence the implementation and adoption of SSI. Common themes included security, privacy, acceptance, standardization, and efficiency. Figure 2 shows the identified themes along the social-technical continuum.

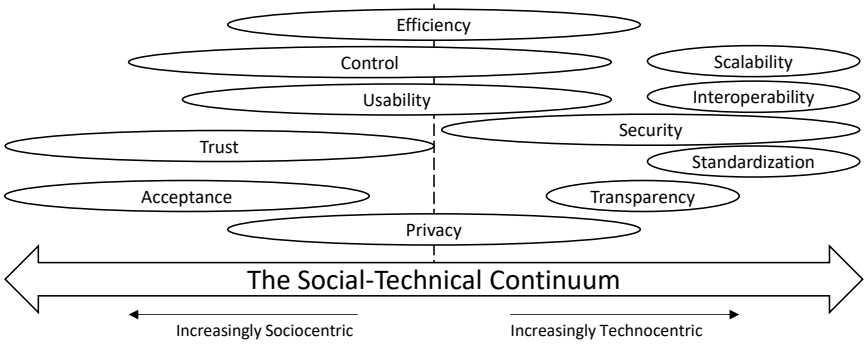

Figure 2. Identified Sociotechnical Challenges along the Social-Technical Continuum

Security

Security is a central requirement, covered in 66 of 78 articles of the final data set. Because many (n=68) SSI implementations rely on blockchain technology (Schlatt et al., 2022; Sedlmeir, Barbereau, et al., 2022), the inherent benefits and shortcomings of blockchain technology must also be considered. Whereas the inherent immutability and tamper-resistant nature of blockchain technology have advantages (Schlatt et al., 2022), helping, for example, to mitigate identity fraud (Nokhbeh Zaeem & Barber, 2020), the decentralized replication of data across blockchain nodes also increases the risk of data sharing with untrusted nodes (Dong et al., 2020; Sedlmeir, Lautenschlager, et al., 2022).

For users, SSI may entail additional responsibilities, making them responsible for the entire life cycle of their data, including the management of cryptographic keys (Kubach et al., 2020). Although this enables users to choose between data backup and recovery mechanisms (Jakubeit et al., 2020), it also requires considerable knowledge.

Privacy

Privacy (n=51) is a vital concern for SSI. Especially in light of data protection laws, such as GDPR, use and processing of personal data needs to be considered (Chomczyk Penedo, 2021). Privacy requirements for SSI are primarily concerned with data minimization and granular control for users (Sedlmeir, Barbereau, et al., 2022). Blockchain technology's immutability conflicts with GDPR's requirements, especially the right to be forgotten (Abraham et al., 2020), a clear identification of entities responsible for data processing, and the potential for users to exercise legal action in case of data misuse (Chomczyk Penedo, 2021; Mahmud et al., 2022), making it difficult for governments and organizations to deploy compliant SSI infrastructures. Potential solutions include off-chain storage, with blockchain storing encrypted hashes and signatures only (Mahmud et al., 2022). However, routing data through centralized servers challenges blockchain's core principle of decentralization (Halpin, 2020) and hinders the manipulation-resistant execution of smart contracts. Other solutions include private and consortia blockchains. However, they also decrease decentralization and may pose interoperability challenges (Kuperberg, 2019; Sedlmeir, Lautenschlager, et al., 2022).

Transparency

Transparency, although less frequently mentioned (n=30), is closely linked to privacy, with all but four articles addressing transparency also mentioning privacy. Although transparency can enable users to exercise control over their data (Ostern & Cabinakova, 2019), the transparency of many public blockchains is a large concern with regard to privacy (Abraham et al., 2020). This tension is exacerbated when immutable records reveal more data than necessary and when the replication across the decentralized network leads to data exposure (Dong et al., 2020; Sedlmeir et al., 2021). Off-chain storage may mitigate this problem, but comes with its own disadvantages, including hindering smart contract execution. As an alternative, Alboaie and Cosovan (2017) propose "Executable Choreographies", with nodes coordinating and executing predefined processes without involving the blockchain, adhering to "privacy by design".

Standardization

Standardization (n=23) is a critical prerequisite for the implementation and adoption of SSI across government institutions and businesses (Johnson Jeyakumar et al., 2022; Schwalm et al., 2022). The current lack of technical standards leads to a dependence on individual platforms (Martinez Jurado et al., 2021; Sedlmeir, Barbereau, et al., 2022) and hinders compatibility between existing, isolated SSI solutions. The current lack of standards may be attributed to the ever-evolving landscape of SSI technologies (Kubach et al., 2020; Laatikainen et al., 2021), challenging developers.

From a legal perspective, the eIDAS regulation may facilitate standardization (Bastian et al., 2022; Martinez Jurado et al., 2021). Although SSI is not integrated in eIDAS 1.0, it is planned for eIDAS 2.0, integrating SSI within a European legal framework (Weigl et al., 2022).

Interoperability

Interoperability (n=34) encompasses the ability of different systems to interact and exchange credentials across different platforms and domains, reducing vendor lock-in (Martinez Jurado et al., 2021; Sedlmeir, Barbereau, et al., 2022). A critical problem is the lack of compatibility with established encryption and authentication standards (Kuperberg, 2019) such as X.509 certificates that enable Decentralized Identifiers and Verifiable Credentials (Martinez Jurado et al., 2021) to comply with existing digital security infrastructures, making SSI unfeasible for highly sensible data. Options for combining these approaches have been proposed by design-oriented research (Bastian et al., 2022). Interoperability is also needed as many organizations already feature established identity management systems. Thus, a complete switch to SSI is both impractical and unlikely. It is therefore necessary to integrate SSI with established identity infrastructures and management systems (Bazarhanova et al., 2019; Kuperberg, 2019).

Scalability

Scalability (n=19) is a crucial success factor for broad adoption among users, government institutions, and organizations (Kubach & Roßnagel, 2021). Economic factors, including transaction costs, need to be considered (Dubovitskaya et al., 2020). Specifically related to blockchain technology, which is often used to implement SSI, two factors need to be considered: (1) data storage and replication and (2) consensus mechanisms. First, blockchain technology's inherent replication across all participating nodes leads to high demands in data storage for maintainers of an SSI implementation. A more scalable data storage could be achieved by storing data off-chain, which, due to faster write and read access, could also improve throughput, and by sharding, which partitions blockchain networks into separate ledgers (Dong et al., 2020; Heiss et al., 2022; Liu et al., 2020; Zhang et al., 2022). Second, depending on the consensus mechanism, a blockchain-based implementation may be resource-intensive (Schanzenbach et al., 2021), resulting in a low transaction volume, negatively influencing user experience and overall system utilization. Transaction efficiency can be improved by various measures: (1) private blockchains, which are faster but sacrifice some degree of decentralization (Fdhila et al., 2021; Nuss et al., 2018), (2) bilateral exchanges between SSI participants, realizing off-chain exchange (Schlatt et al., 2022), and (3) sharding (Zhang et al., 2022).

Acceptance

Acceptance (n=21) of SSI may be inhibited by unfamiliarity and a lack of knowledge about its functionality and advantages in both organizations and individual users (Bazarhanova & Smolander, 2020; Laatikainen et al., 2021; Panait et al., 2020; Weigl et al., 2022). A primary indicator of acceptance is the number of services and users that have adopted SSI (Kubach et al., 2020). Acceptance can be fostered – among others – through (1) training and education, (2) trust-building measures, and (3) institutional support.

First, education and training on the purpose, tasks, and scope of SSI can foster user comprehension (Laatikainen et al., 2021; Ostern & Cabinakova, 2019; Sartor et al., 2022). Providing accessible explanations, especially regarding the privacy and security

features, both of the SSI platform as well as the connected applications, can reduce user concerns (Kubach & Sellung, 2021; Ostern & Cabinakova, 2019).

Second, trust-building measures go further than simple education, shaping and incorporating individual users' skills, beliefs, resources (Laatikainen et al., 2021), emotions, attitudes, and preferences (Sartor et al., 2022). Country and culture level aspects, such as cultural norms may also shape SSI perception (Laatikainen et al., 2021; Weigl et al., 2022). For example, in developing countries, SSI solutions offer significant potential for digital and financial inclusion but face obstacles such as limited smartphone access (Laatikainen et al., 2021).

Third, institutional factors affect SSI adoption. Political initiatives, for example those of the European Commission (Weigl et al., 2022), have been found to help clarify public understanding of SSI. Further, company-specific factors such as automation levels, data sensitivity, and leadership incentives (Laatikainen et al., 2021) as well as interorganizational factors, such as infrastructure integration, strategic aspects and liability considerations may also affect SSI adoption (Bazarhanova & Smolander, 2020).

Usability

Similar to how usability (n=22) plays a central role in the individual acceptance of other information systems (Dubovitskaya et al., 2020), it is also important for decentralized identity management systems (Cabinakova et al., 2019). Generally speaking, pragmatic features (Ostern & Cabinakova, 2019), such as interoperability (Feulner et al., 2022), an intuitive (Jørgensen & Beck, 2022; Sedlmeir, Barbereau, et al., 2022) and straightforward interface (Dubovitskaya et al., 2020; Ostern & Cabinakova, 2019), and a responsive design (Schlatt et al., 2022), are valued more highly than feature-rich, overly functional or administratively oriented designs (Sartor et al., 2022).

Studies on existing SSI wallets show that additional features, such as visual representations of verifiable credentials (VCs), quick access features, folder systems, filters (Sartor et al., 2022), and management of multiple identities on the same platform and across multiple devices (Bazarhanova & Smolander, 2020; Kuperberg, 2019) are highly valued. Finally, it is important for developers to maintain an appropriate balance between user convenience and privacy protection requirements (Kubach et al., 2020).

Trust

Trust (n=62) is a fundamental requirement for SSI, both for managing and relying on credentials (Johnson Jeyakumar et al., 2022; Kubach & Roßnagel, 2021) as well as for overall scaling of identity management systems (Bazarhanova & Smolander, 2020). Ensuring that a public key is issued by the claimed institution is crucial (Kubach et al., 2020). Trust may be established through (the combination of) multiple measures: (1) a secure technical design (Johnson Jeyakumar et al., 2022), (2) institutional trust through regulatory frameworks such as eIDAS (Kubach & Roßnagel, 2021; Kubach et al., 2020), (3) trust anchors and/or intermediaries, which establish trust but contradict SSI's core principle of independence (Schwalm et al., 2022), and (4) organically through reputable actors gaining recognition in the market (Kubach & Sellung, 2021).

Specific approaches aimed to further trust are, for examples, the SSI-eIDAS-Bridge, which can confirm an issuer's identity and VC assignment using electronic signatures

or seals (Kubach & Roßnagel, 2021; Martinez Jurado et al., 2021), and the Trust-Management-Infrastructure (TRAIN), designed to create a transparent and reliable system for identifying trustworthy issuers or trusted decision-making bodies (Johnson Jeyakumar et al., 2022; Kubach & Roßnagel, 2021; Martinez Jurado et al., 2021).

Control

Control (n=47) describes how individuals – indicated by "self-sovereign" – are able to enact exclusive authority in disclosing their own personal information (Bazarhanova et al., 2019; Sedlmeir, Barbereau, et al., 2022). Such control, without the dependence on a third party, comes with a considerable amount of responsibility for the end user, who has to manage secure key storage as well as backups (Bazarhanova & Smolander, 2020; Sedlmeir, Barbereau, et al., 2022). Sufficient knowledge on the side of the user as well as transparency on the side of technology (Ostern & Cabinakova, 2019), for example through open-source publication of SSI component source code (Kulabukhova et al., 2019), is required. Perceived control over disclosed digital data strongly influences perceived transparency and willingness to share information (Cabinakova et al., 2019). Despite formal and perceived control, users may still be coerced to give up more data than they want to, with services restricting access unless specific data is provided (Kuperberg, 2019; Ostern & Cabinakova, 2019).

Efficiency

Efficiency (n=32) encompasses both economic viability and operational effectiveness. On the one hand, establishing and operating SSI-compatible services require financially sustainable business models for maintainers and organizations in light of initial investments, transaction costs, and verification expenses (Dubovitskaya et al., 2020; Laatikainen et al., 2021; Lacity & Carmel, 2022). On the other hand, end users will only consider SSI if it offers a comparable or superior functionality while maintaining acceptable switching costs (Kuperberg, 2019). Although data ownership, control, and transparency have their value (Cabinakova et al., 2019; Ostern & Cabinakova, 2019), other factors, such as transaction fees (Kölbel et al., 2022), time savings (Lacity & Carmel, 2022), perceived usability (Cabinakova et al., 2019), and process effectiveness (Weigl et al., 2022) still play a large role.

Effective SSI solutions must account not only for end user needs but also for SSI service providers (Kubach & Roßnagel, 2021). The interdependent relationship between end users and service providers presents itself as a "chicken or egg" problem. While SSI services are needed to attract users, service providers require a large enough user base (Kubach & Sellung, 2021), highlighting the importance of strategic market development (Schlatt et al., 2022).

4.2 Areas of Application

Addressing research question 2, half of the analyzed articles (n=39) examined SSI in a cross-industry context without focusing on specific application domains. Among the remaining articles (n=39), the most common application domains were e-government,

finance, healthcare, e-commerce, and the internet of things (IoT). In the following sections, we will describe application scenarios in these application domains.

E-Government

E-government (n=6) is a prime area for SSI application, especially to provide common ecosystems for public institutions and private enterprises (Degen & Teubner, 2024). Public authorities and institutions can use blockchain-based SSI systems to improve administrative efficiency in public service delivery (Sung & Park, 2021). Furthermore, SSI can also help address identity verification challenges for refugees or individuals without legal identification by creating verifiable digital identities (Kubach & Sellung, 2021; Laatikainen et al., 2021; Lim et al., 2022; Sedlmeir, Lautenschlager et al., 2022).

Finance

The finance (n=6) sector is a principal area for blockchain technology adoption, particularly in payments and transactions (Sedlmeir, Lautenschlager, et al., 2022). Primary application scenarios for SSI are (1) loan and credit issuance, where SSI has been proposed to (a) provide authentication during security verification processes, and (b) improve credit assessment and accelerate loan approval processes (Liu et al., 2021); (2) compliance with regulatory requirements such as Know Your Customer and Anti-Money Laundering processes (Damgård et al., 2021; Schlatt et al., 2022); (3) transaction access and freezing of funds for law enforcement (Damgård et al., 2021), and (4) open banking, which enables third-party providers to access consumers' account and financial information without sharing personal data (Dong et al., 2020).

Healthcare

In the healthcare (n=7) sector, key application scenarios of SSI include (1) document verification for health insurance, vaccination certificates, and medical prescriptions (Kubach & Sellung, 2021; Sartor et al., 2022; Schwalm et al., 2022), (2) digital immunity passports and reliable attestations, which emerged during the COVID-19 pandemic (Fdhila et al., 2021; Halpin, 2020), (3) cross-border use of health insurance cards while maintaining security (Martinez Jurado et al., 2021), (4) telemedicine services (Alam et al., 2022), (5) exchange of medical data between institutions such as doctors and hospitals (Kshetri, 2017), and (6) data management of health data collected by wearables and IoT devices (Liang et al., 2018; Sousa et al., 2020).

E-Commerce

In e-commerce (n=6), key application scenarios of SSI include (1) event ticket issuance and verification processes to reduce fraud and ticket scalping, enabling privacy-focused revocation mechanisms to reduce risks on secondary markets (Feulner et al., 2022), (2) age verification in online commerce without disclosing exact birthdates (Alber et al., 2021; Kesim et al., 2022), (3) enhancing the authenticity and trustworthiness of online reviews (Yu et al., 2020), (4) privacy-preserving online payment (Schanzenbach et al., 2021), and (5) supply chain tracking (Duan & Patel, 2018).

Internet of Things (IoT)
SSI can also be used to assign credentials to physical objects, digital assets, or logical entities (Lacity & Carmel, 2022). In the IoT sector (n=11), key application scenarios of SSI include (1) the life cycle management of IoT devices (Kulabukhova et al., 2019; Loupos et al., 2022), (2) privacy-preserving authentication for electric vehicle charging (Parameswarath et al., 2022), (3) secure car sharing (Naghmouchi et al., 2022), (4) anonymous vehicle-to-vehicle communication (Wu et al., 2022), and (5) enhancing data security in smart grids (Guo et al., 2021).

Other Application Areas
Other application areas of SSI include, for example, social media, where SSI has potential for identity verification in online communication platforms (Pinter et al., 2019) and to combat misinformation by social bots and fake accounts (Guerar & Migliardi, 2022). SSI may also be used to verify academic credentials, diplomas, and certificates (Dubovitskaya et al., 2020; Krause et al., 2022; Kulabukhova et al., 2019; Terzi et al., 2022).

5 Discussion

This article set out to critically reflect on the challenges and requirements for the implementation and adoption of SSI across multiple application domains, adopting a sociotechnical lens. In doing so, it makes three contributions.

First, the literature review identified and summarized key sociotechnical requirements and challenges for the successful implementation and adoption of SSI and positioned them along the social-technical continuum (Sarker et al., 2019). Security and privacy emerged as central concerns due to SSI's focus on sensitive private data. Compliance with data protection regulations like the GDPR is crucial. Transparency is also essential in blockchain-based SSI solutions to maintain control over user data. Scalability is another important factor for expanding SSI solutions across industries and user groups. The analysis showed that most articles associate SSI with blockchain technology, which, ironically, is not well suited to accommodate the needs for privacy and scalability, relying instead on extensions, such as off-chain storage (Mahmud et al., 2022) and bilateral exchange (Schlatt et al., 2022). Such extensions, which often compromise on blockchain's promises of decentralization and transparency, may serve as an indicator of a potential mismatch between SSI and blockchain technology as basis for implementation. Especially for widespread implementation in potential government contexts, which do not only need to follow regulations such as GDPR and eIDAS but should stand out as flagship projects, other technological approaches might be better suited. Despite the need for other approaches, only few studies have examined SSI solutions without blockchain. Future research ought to identify other technological approaches, potentially better suited for SSI implementation.

Second, the literature review shows that social factors, such as user acceptance, usability, trust, control, and efficiency are crucial for SSI's success. Given that SSI's success depends heavily on user adoption, improving user experience is essential

(Dubovitskaya et al., 2020; Kölbel et al., 2022). Continuous user feedback loops are necessary to refine solutions like digital wallets for end user convenience (Sartor et al., 2022). SSI development requires balancing technical, social, and political factors (Sedlmeir, Barbereau, et al., 2022), with interconnected requirements and challenges influencing one another. Despite their importance, these predominantly social factors are less frequently addressed in the literature, indicating a need for further research.

Third, the literature review shows that over half of the examined articles focus on SSI in general rather than focusing on specific application domains. This demonstrates the potential adaptability of SSI across different application domains. However, different contexts have different requirements. Research in the domains of e-government, finance, and healthcare appears to emphasize security and privacy considerations more, likely due to the sensitive data these fields handle. E-government literature, in particular, has a more noticeable focus on interoperability, standardization, control, and efficiency, which can be attributed to the large number of potential users and its central role in society. Trust was considered important in all domains. Usability was mentioned less frequently, which is partially explainable by the large number of articles with a technical focus (e.g., algorithm or model) across domains. New unexplored implementation contexts could always pose new challenges, emphasizing the need for SSI research to focus on specific application areas. Examining SSI in specific contexts (Guggenberger et al., 2023) with theory-informed design-oriented research methods (Hevner et al., 2004; Peffers et al., 2007) could provide additional insights.

6 Conclusion

Digital identity management is often handled by large tech companies, such as Google, Microsoft, and Meta. Growing concerns about data security and privacy, as well as multinational regulations such as GDPR and eIDAS, make SSI emerge as an approach that empowers end users to control their own personal data. We conducted a systematic literature review to identify sociotechnical requirements and challenges across multiple application contexts for SSI, including e-government, finance, healthcare, e-commerce, and IoT. Our study shows that security and privacy are the primary concerns, whereas social factors, such as user acceptance and usability, are underrepresented. Furthermore, most of the literature addresses SSI in a general way, suggesting the need for more design-oriented research in specific domains. The practical implications of our study highlight that in addition to providing a secure and interoperable infrastructure, trust and usability in SSI solutions need to be fostered. Standardization through supportive regulatory frameworks can build trust and facilitate SSI development and adoption (Weigl et al., 2022). Future research can expand on our findings, limited to the IS field and investigated solely through a sociomaterial lens, by (1) considering other research disciplines, such as computer science, public administration, and law, as well as grey literature, such as whitepapers on established SSI solutions like Sovrin, uPort, and Civic (Kulabukhova et al., 2019) and (2) employing other theoretical lenses, such as institutional theory (Orlikowski & Barley, 2001), to draw additional conclusions from the source material.

References

Abraham, A., Hörandner, F., Omolola, O., & Ramacher, S. (2020). *Privacy-Preserving eID Derivation for Self-Sovereign Identity Systems* Information and Communications Security. ICICS 2019. Lecture Notes in Computer Science, Beijing, China.

Alam, N., Liang, X., & Sultana, T. (2022). *Impact of Blockchain-based Digital Identity on Privacy Concern and Privacy Protective Behavior* PACIS 2022 Proceedings, Virtual Conference.

Alber, L., More, S., Mödersheim, S., & Schlichtkrull, A. (2021). Adapting the TPL Trust Policy Language for a Self-Sovereign Identity World. Open Identity Summit 2021, Lyngby, Denmark.

Alboaie, S., & Cosovan, D. (2017). Private Data System Enabling Self-Sovereign Storage Managed by Executable Choreographies. In L. Y. Chen & H. P. Reiser, *Distributed Applications and Interoperable Systems* Neuchâtel, Switzerland.

Bastian, P., Stöcker, C., & Schwalm, S. (2022). Combination of x509 and DID/VC for inheritance properties of trust in digital identities. Open Identity Summit 2022, Lyngby, Denmark.

Bazarhanova, A., Magnusson, J., Lindman, J., Chou, E., & Nilsson, A. (2019). *Blockchain-based Electronic Identification: Cross-Country Comparison of Six Design Choices* Proceedings of the 27th European Conference on Information Systems (ECIS), Stockholm & Uppsala, Sweden.

Bazarhanova, A., & Smolander, K. (2020). *The Review of Non-Technical Assumptions in Digital Identity Architectures* Proceedings of the 53rd Hawaii International Conference on System Sciences, Maui, Hawaii, USA.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77-101. https://doi.org/10.1191/1478088706qp063oa

Cabinakova, J., Ostern, N. K., & Kroenung, J. (2019). *Understanding Preprototype User Acceptance of Centralised and Decentralised Identity Management Systems* Proceedings of the 27th European Conference on Information Systems (ECIS), Stockholm & Uppsala, Sweden.

Chomczyk Penedo, A. (2021). Self-sovereign identity systems and European data protection regulations: an analysis of roles and responsibilities. Open Identity Summit 2021, Lyngby, Denmark.

Clauß, S., & Köhntopp, M. (2001). Identity management and its support of multilateral security. *Computer Networks*, *37*(2), 205-219. https://doi.org/10.1016/s1389-1286(01)00217-1

Cucko, S., Becirovic, S., Kamisalic, A., Mrdovic, S., & Turkanovic, M. (2022). Towards the Classification of Self-Sovereign Identity Properties. *IEEE Access*, *10*, 88306-88329. https://doi.org/10.1109/access.2022.3199414

Damgård, I., Ganesh, C., Khoshakhlagh, H., Orlandi, C., & Siniscalchi, L. (2021). Balancing Privacy and Accountability in Blockchain Identity Management. In K. G. Paterson, *Topics in Cryptology – CT-RSA 2021* Virtual Conference.

Degen, K., & Teubner, T. (2024). Wallet wars or digital public infrastructure? Orchestrating a digital identity data ecosystem from a government perspective. *Electronic Markets*, *34*(1). https://doi.org/10.1007/s12525-024-00731-1

Dong, C., Wang, Z., Chen, S., & Xiang, Y. (2020). BBM: A Blockchain-Based Model for Open Banking via Self-sovereign Identity. In Z. Chen, L. Cui, B. Palanisamy, & L.-J. Zhang, *Blockchain – ICBC 2020* Honolulu, HI, USA.

Duan, J., & Patel, M. (2018). Blockchain in Global Trade. In S. Chen, H. Wang, & L.-J. Zhang, *Blockchain – ICBC 2018* Seattle, WA, USA.

Dubovitskaya, A., Mazzola, L., & Denzler, A. (2020). Towards a Trusted Support Platform for the Job Placement Task. In U. Schwardmann, C. Boehme, D. B. Heras, V. Cardellini, E. Jeannot, A. Salis, C. Schifanella, R. R. Manumachu, D. Schwamborn, L. Ricci, O. Sangyoon, T. Gruber, L. Antonelli, & S. L. Scott, *Euro-Par 2019: Parallel Processing Workshops* Göttingen, Germany.

Ehrlich, T., Richter, D., Meisel, M., & Anke, J. (2021). Self-Sovereign Identity als Grundlage für universell einsetzbare digitale Identitäten. *HMD Praxis der Wirtschaftsinformatik*, *58*(2), 247-270. https://doi.org/10.1365/s40702-021-00711-5

Fdhila, W., Stifter, N., Kostal, K., Saglam, C., & Sabadello, M. (2021). Methods for Decentralized Identities: Evaluation and Insights. In J. González Enríquez, S. Debois, P. Fettke, P. Plebani, I. van de Weerd, & I. Weber, *Business Process Management: Blockchain and Robotic Process Automation Forum* Rome, Italy.

Ferdous, M. S., Chowdhury, F., & Alassafi, M. O. (2019). In Search of Self-Sovereign Identity Leveraging Blockchain Technology. *IEEE Access*, *7*, 103059-103079. https://doi.org/10.1109/access.2019.2931173

Feulner, S., Sedlmeir, J., Schlatt, V., & Urbach, N. (2022). Exploring the use of self-sovereign identity for event ticketing systems. *Electronic Markets*, *32*(3), 1759-1777. https://doi.org/10.1007/s12525-022-00573-9

Guerar, M., & Migliardi, M. (2022). TruthSeekers Chain: Leveraging Invisible CAPPCHA, SSI and Blockchain to Combat Disinformation on Social Media. In O. Gervasi, B. Murgante, S. Misra, A. M. A. C. Rocha, & C. Garau, *Computational Science and Its Applications – ICCSA 2022 Workshops* Malaga, Spain.

Guggenberger, T., Kühne, D., Schlatt, V., & Urbach, N. (2023). Designing a cross-organizational identity management system: Utilizing SSI for the certification of retailer attributes. *Electronic Markets*, *33*(1). https://doi.org/10.1007/s12525-023-00620-z

Guo, Y., Chen, X., Tian, S., Yang, L., Liang, X., Lian, J., Jin, D., Balabontsev, A., & Zhang, Z. (2021). Blockchain Based Trusted Identity Authentication in Ubiquitous Power Internet of Things. In D.-S. Huang, K.-H. Jo, J. Li, V. Gribova, & A. Hussain, *Intelligent Computing Theories and Application* Shenzhen, China.

Halpin, H. (2020). Vision: A Critique of Immunity Passports and W3C Decentralized Identifiers. In T. van der Merwe, C. Mitchell, & M. Mehrnezhad, *Security Standardisation Research* London, UK.

Heiss, J., Muth, R., Pallas, F., & Tai, S. (2022). Non-disclosing Credential On-chaining for Blockchain-Based Decentralized Applications. In J. Troya, B. Medjahed, M. Piattini, L. Yao, P. Fernández, & A. Ruiz-Cortés, *Service-Oriented Computing* Seville, Spain.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS quarterly*, *28*(1). https://doi.org/10.2307/25148625

Jakubeit, P., Dercksen, A., & Peter, A. (2020). SSI-AWARE: Self-sovereign Identity Authenticated Backup with Auditing by Remote Entities. In M. Laurent & T. Giannetsos, *Information Security Theory and Practice* Paris, France.

Johnson Jeyakumar, I. H., Chadwick, D. W., Kubach, M., Roßnagel, H., Schunck, C. H., & Mödersheim, S. (2022). *A novel approach to establish trust in verifiable credential issuers in Self-sovereign identity ecosystems using TRAIN* Open Identity Summit 2022, Lecture Notes in Informatics (LNI) - Proceedings, Volume P-305, Copenhagen, Denmark. https://dl.gi.de/server/api/core/bitstreams/d91fcb27-0129-499f-871d-c3b8ac336b63/content

Jørgensen, K. P., & Beck, R. (2022). Universal Wallets. *Business & Information Systems Engineering*, *64*(1), 115-125. https://doi.org/10.1007/s12599-021-00736-6

Just, M. (2011). Identity Management. In H. C. A. van Tilborg & S. Jajodia (Eds.), *Encyclopedia of Cryptography and Security* (pp. 586-587). Springer US. https://doi.org/10.1007/978-1-4419-5906-5_78

Kesim, Ö., Grothoff, C., Dold, F., & Schanzenbach, M. (2022). Zero-Knowledge Age Restriction for GNU Taler. In V. Atluri, R. Di Pietro, C. D. Jensen, & W. Meng, *Computer Security – ESORICS 2022* Copenhagen, Denmark.

Kölbel, T., Gawlitza, T., & Weinhardt, C. (2022). *Shaping Governance in Self-Sovereign Identity Ecosystems: Towards a Cooperative Business Model* Wirtschaftsinformatik 2022 Proceedings, Nürnberg, Germany.

Krause, T., Gösling, H., Digel, S., Biel, C., Kolvenbach, S., & Thomas, O. (2022). Adaptive Cross-Platform Learning for Teachers in Adult and Continuing Education. In M. M. Rodrigo, N. Matsuda, A. I. Cristea, & V. Dimitrova, *Artificial Intelligence in Education. Posters and Late Breaking Results, Workshops and Tutorials, Industry and Innovation Tracks, Practitioners' and Doctoral Consortium* Durham, UK.

Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications Policy*, *41*(10), 1027-1038. https://doi.org/10.1016/j.telpol.2017.09.003

Kubach, M., & Roßnagel, H. (2021). A lightweight trust management infrastructure for self-sovereign identity. Open Identity Summit 2021, Lyngby, Denmark.

Kubach, M., Schunck, C. H., Sellung, R., & Roßnagel, H. (2020). Self-sovereign and Decentralized identity as the future of identity management? Open Identity Summit 2020, Copenhagen, Denmark.

Kubach, M., & Sellung, R. (2021). On the Market for Self-Sovereign Identity: Structure and Stakeholders. Open Identity Summit 2021, Lyngby, Denmark.

Kulabukhova, N., Ivashchenko, A., Tipikin, I., & Minin, I. (2019). Self-Sovereign Identity for IoT Devices. In S. Misra, O. Gervasi, B. Murgante, E. Stankova, V. Korkhov, C. Torre, A. M. A. C. Rocha, D. Taniar, B. O. Apduhan, & E. Tarantino, *Computational Science and Its Applications – ICCSA 2019* Saint Petersburg, Russia.

Kuperberg, M. (2019). Blockchain-Based Identity Management: A Survey From the Enterprise and Ecosystem Perspective. *IEEE Transactions on Engineering Management*, *67*(4), 1008-1027. https://doi.org/10.1109/tem.2019.2926471

Laatikainen, G., Kolehmainen, T., Li, M., Hautala, M., Kettunen, A., & Abrahamsson, P. (2021). *Towards a Trustful Digital World: Exploring Self-Sovereign Identity Ecosystems* PACIS 2021 Proceedings, Dubai, UAE.

Lacity, M., & Carmel, E. (2022). Self-Sovereign Identity and Verifiable Credentials in Your Digital Wallet. *MIS Quarterly Executive*, 241-251. https://doi.org/10.17705/2msqe.00068

Liang, X., Shetty, S., Zhao, J., Bowden, D., Li, D., & Liu, J. (2018). Towards Decentralized Accountability and Self-sovereignty in Healthcare Systems. In S. Qing, C. Mitchell, L. Chen, & D. Liu, *Information and Communications Security* Beijing, China.

Liu, J., Liu, P., Ou, Z., Zhang, G., & Song, M. (2021). An Inclusive Finance Consortium Blockchain Platform for Secure Data Storage and Value Analysis for Small and Medium-Sized Enterprises. In Q. Zu, Y. Tang, & V. Mladenović, *Human Centered Computing* Virtual Conference.

Liu, Y., Lu, Q., Paik, H.-Y., Xu, X., Chen, S., & Zhu, L. (2020). Design Pattern as a Service for Blockchain-Based Self-Sovereign Identity. *IEEE Software*, *37*(5), 30-36. https://doi.org/10.1109/ms.2020.2992783

Loupos, K., Kalogirou, C., Niavis, H., Skarmeta, A., Torroglosa-Garcia, E., Palomares, A., Song, H., Brun, P.-E., Giampaolo, F., Van Landuyt, D., Michiels, S., Podgorelec, B., Xenakis, C., Bampatsikos, M., & Krilakis, K. (2022). A Holistic Approach for IoT Networks' Identity and Trust Management – The ERATOSTHENES Project. In A. González-Vidal, A. Mohamed Abdelgawad, E. Sabir, S. Ziegler, & L. Ladid, *Internet of Things* Dublin, Ireland.

Mahmud, H., Islam, A. K. M. N., Naqvi, B., & Mäntymäki, M. (2022). Toward a GDPR Compliant Blockchain Governance Framework. In S. Papagiannidis, E. Alamanos, S. Gupta, Y. K. Dwivedi, M. Mäntymäki, & I. O. Pappas, *The Role of Digital Technologies in Shaping the Post-Pandemic World* Newcastle upon Tyne, UK.

Martinez Jurado, V., Vila, X., Kubach, M., Henderson Johnson Jeyakumar, I., Solana, A., & Marangoni, M. (2021). Applying assurance levels when issuing and verifying credentials using Trust Frameworks. Open Identity Summit 2021, Lyngby, Denmark.

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

Naghmouchi, M., Ayed, H. K. B., & Laurent, M. (2022). An Automatized Identity and Access Management System for IoT Combining Self-Sovereign Identity and Smart Contracts. In E. Aïmeur, M. Laurent, R. Yaich, B. Dupont, & J. Garcia-Alfaro, *Foundations and Practice of Security* Paris, France.

Nokhbeh Zaeem, R., & Barber, K. S. (2020). How Much Identity Management with Blockchain Would Have Saved Us? A Longitudinal Study of Identity Theft. In W. Abramowicz & G. Klein, *Business Information Systems Workshops* Colorado Springs, CO, USA.

Nuss, M., Puchta, A., & Kunz, M. (2018). Towards Blockchain-Based Identity and Access Management for Internet of Things in Enterprises. In S. Furnell, H. Mouratidis, & G. Pernul, *Trust, Privacy and Security in Digital Business* Regensburg, Germany.

Orlikowski, W. J., & Barley, S. R. (2001). Technology and Institutions: What Can Research on Information Technology and Research on Organizations Learn from Each Other? *MIS quarterly*, *25*(2). https://doi.org/10.2307/3250927

Ostern, N. K., & Cabinakova, J. (2019). *Pre-Prototype Testing: Empirical Insights on the Expected Usefulness of Decentralized Identity Management Systems* Proceedings of the 52nd Hawaii International Conference on System Sciences, Maui, HI, USA.

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hrobjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., . . . Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *Int J Surg*, *88*, 105906. https://doi.org/10.1016/j.ijsu.2021.105906

Panait, A.-E., Olimid, R. F., & Stefanescu, A. (2020). Analysis of uPort Open, an Identity Management Blockchain-Based Solution. In S. Gritzalis, E. R. Weippl, G. Kotsis, A. M. Tjoa, & I. Khalil, *Trust, Privacy and Security in Digital Business* Bratislava, Slovakia.

Parameswarath, R. P., Gope, P., & Sikdar, B. (2022). User-empowered Privacy-preserving Authentication Protocol for Electric Vehicle Charging Based on Decentralized Identity and Verifiable Credential. *ACM Transactions on Management Information Systems*, *13*(4), 1-21. https://doi.org/10.1145/3532869

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, *24*(3), 45-77. https://doi.org/10.2753/mis0742-1222240302

Pinter, K., Schmelz, D., Lamber, R., Strobl, S., & Grechenig, T. (2019). Towards a Multi-party, Blockchain-Based Identity Verification Solution to Implement Clear Name Laws for Online Media Platforms. In C. Di Ciccio, R. Gabryelczyk, L. García-Bañuelos, T. Hernaus, R. Hull, M. Indihar Štemberger, A. Kő, & M. Staples, *Business Process Management: Blockchain and Central and Eastern Europe Forum* Vienna, Austria.

Sarker, S., Chatterjee, S., Xiao, X., & Elbanna, A. (2019). The Sociotechnical Axis of Cohesion for the IS Discipline: Its Historical Legacy and its Continued Relevance. *MIS quarterly*, *43*(3), 695-719. https://doi.org/10.25300/misq/2019/13747

Sartor, S., Sedlmeir, J., Rieger, A., & Roth, T. (2022). *Love at First Sight? A User Experience Study of Self-Sovereign Identity Wallets* ECIS 2022 Research Papers, Timisoara, Romania.

Schanzenbach, M., Grothoff, C., Wenger, H., & Kaul, M. (2021). Decentralized Identities for Self-sovereign End-users (DISSENS). Open Identity Summit 2021, Lyngby, Denmark.

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

Schardong, F., Custódio, R., Pioli, L., & Meyer, J. (2022). Matching Metadata on Blockchain for Self-Sovereign Identity. In A. Marrella & B. Weber, *Business Process Management Workshops* Rome, Italy.

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

Schneider, D., Klumpe, J., Adam, M., & Benlian, A. (2019). Nudging users into digital service solutions. *Electronic Markets*, *30*(4), 863-881. https://doi.org/10.1007/s12525-019-00373-8

Schwalm, S., Albrecht, D., & Alamillo, I. (2022). eIDAS 2.0: Challenges, perspectives and proposals to avoid contradictions between eIDAS 2.0 and SSI. Open Identity Summit 2022, Lyngby, Denmark.

Sedlmeir, J., Barbereau, T., Huber, J., Weigl, L., & Roth, T. (2022). *Transition Pathways towards Design Principles of Self-Sovereign Identity* ICIS 2022 Proceedings, Copenhagen, Denmark.

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

Sedlmeir, J., Smethurst, R., Rieger, A., & Fridgen, G. (2021). Digital Identities and Verifiable Credentials. *Business & Information Systems Engineering*, *63*(5), 603-613. https://doi.org/10.1007/s12599-021-00722-y

Sousa, P. R., Resende, J. S., Martins, R., & Antunes, L. (2020). The case for blockchain in IoT identity management. *Journal of Enterprise Information Management*, *35*(6), 1477-1505. https://doi.org/10.1108/jeim-07-2018-0148

Terzi, S., Ioannis, S., Votis, K., & Tsiatsos, T. (2022). A Life-Long Learning Education Passport Powered by Blockchain Technology and Verifiable Digital Credentials: The BlockAdemiC Project. In A. Cerone, M. Autili, A. Bucaioni, C. Gomes, P. Graziani, M. Palmieri, M. Temperini, & G. Venture, *Software Engineering and Formal Methods. SEFM 2021 Collocated Workshops* Virtual Conference.

Webster, J., & Watson, R. T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MIS quarterly*, *26*(2), 11.

Weigl, L., Barbereau, T., Rieger, A., & Fridgen, G. (2022). *The Social Construction of Self-Sovereign Identity: An Extended Model of Interpretive Flexibility* Proceedings of the 55th Hawaii International Conference on System Sciences, Virtual Conference.

Wu, H., Feng, X., Kan, G., & Jiang, X. (2022). BIPP: Blockchain-Based Identity Privacy Protection Scheme in Internet of Vehicles for Remote Anonymous Communication. In Y. Lai, T. Wang, M. Jiang, G. Xu, W. Liang, & A. Castiglione, *Algorithms and Architectures for Parallel Processing* Virtual Event.

Yu, X., Ge, R., & Li, F. (2020). Research on Blockchain-Based Identity Authentication Scheme in Social Networks. In X. Chen, H. Yan, Q. Yan, & X. Zhang, *Machine Learning for Cyber Security* Guangzhou, China.

Zhang, Y., Li, P., Cong, P., Zou, H., Wang, X., & He, X. (2022). Web 3.0: Developments and Directions of the Future Internet Architecture? In Y. Zhang & L.-J. Zhang, *Web Services – ICWS 2022* Honolulu, HI, USA.