# An Evaluation of Privacy Protection in Blockchain-Based Self-Sovereign Identity

**Remy Duijsens**, **Martijn de Vos**, **Johan Pouwelse**
Delft University of Technology

## Abstract

Digital identity management has been established in a mainly centralized manner. In response to a lack of control in current identity management systems, the concept of Self-Sovereign Identity (SSI) was defined to enable decentralization. Recently, this concept gained traction, and several implementations have been proposed. The decentralized nature of blockchain technology was combined with the concept of SSI. However, no critical review on the privacy protection of this technology in combination with SSI currently exists. This research evaluates current blockchain-based SSI implementations in the lights of privacy protection. It proposes a model for determining the privacy protection that specific solutions can offer based on defined criteria. The technology to be able to satisfy these privacy criteria in blockchain-based SSI is available. However, the evaluation shows that most implementations do not satisfy all privacy criteria, of which some even score poorly on privacy protection.

## 1 Introduction

The internet was invented to be a distributed, and open system for everyone [1]. However, in the 21st century, the decay of its users' privacy is an ongoing problem [2]. This is because machines are the endpoints within the internet and not the users. To track and store users, online services implement the authentication layers themselves, sometimes with the help of an Identity Provider, such as Facebook or Google. As such, they create user profiles that are strongly tied to the online behaviour of the users. That is problematic, as this encourages, for example, massive data mining, which can be valuable to companies, governments, and even malicious parties [3].

By a survey of InnoValor, it became clear that (Dutch) citizens feel a lack of control and a desire to be in more control of their online identities [4]. This is where the notion of a self-sovereign identity is introduced. It gives people back the authority over their own digital identities. This is achieved by only sharing identity information on a need-to-know basis with the use of verifiable credentials. Christopher Allen has proposed ten principles that should be satisfied by this self-sovereign identity (SSI) [5]. Several implementations for SSI have been proposed in academic literature, for example, several blockchain approaches of which one is a solution for Dutch digital passports [6]. However, not many critical reviews on the current SSI technology have been proposed. One of the biggest problems in blockchain-based implementations is guaranteeing privacy to its users [7].

This research aims at finding the technical limitations for privacy protection of the current blockchain-based SSI implementations. It provides an evaluation of privacy protection of several existing solutions based on defined criteria.

Our work focuses on the following overarching research question:

*What are the technical limitations for privacy protection in current blockchain-based SSI implementations?*

The paper will be structured using a bottom-up approach, where the main research question is split up into the following sub-questions:

1. What are the privacy issues that SSI tries to solve?
2. What privacy-preserving methods are currently available for blockchain-based SSI?
3. How do the current blockchain-based SSI implementations preserve privacy?

First, we will describe the problem that this paper addresses in more detail. Then related work will be presented. These works mainly represent overviews and evaluations of identity management systems, SSI, blockchain-based SSI, and privacy protection in identity management. From here, the research will present the necessary definitions and concepts of digital privacy, identity management, and blockchain-based SSI. The following section defines the evaluation criteria for the evaluation. The evaluation will consist of an overview in table form, which assesses the most prominent blockchain-based SSI implementations against the criteria from the previous section. The most notable results of the evaluation will then be discussed. Finally, this work is concluded by stating that the privacy-preserving methods that can enable blockchain-based SSI solutions to satisfy the privacy criteria are already available. However, the evaluation results show that most of the evaluated implementations do not satisfy all privacy criteria. Some solutions score poorly on privacy protection and do not even provide a privacy plan to discuss their reasoning. Future research on the subject can focus on the adoption issues that arise regarding privacy protection.

## 2 Problem Description

In the past decade, there has been a rise in the literature on blockchain technology [8]. The original use case of this technology, Bitcoin, has enabled a way to truly enable decentralized computer networks [9]. The applicability of blockchain is being evaluated in many different application domains such as Healthcare, Banking, and Supply-Chain [10]. One eminent domain is digital identity management. Similar to the financial system, identity management is currently a mainly centralized business. As presented in the introduction of this paper, the motivation to decentralize identity management is clear. Self-sovereign identities provide a conceptual solution to decentralized identity management.

The original article by Christopher Allen provides a technology-independent description of SSI [5]. Several SSI implementations have been proposed in both white papers and academic articles in the years after this publication. The current trend in SSI solutions is based on blockchain technology, a natural catalyst of decentralization. However, blockchain technology also has its shortcomings. A recent survey on blockchain technology regarding privacy shows that there are still problems to be discussed and improved [11].

This problem translates naturally to blockchain-based SSI implementations. A repository of identity-related blockchain applications shows the amount of different initiatives [1]. These initiatives are not bound to a specific type of blockchain technology and use many different solutions in the broad spectrum of blockchain [10]. There is, however, a lack of research on blockchain-based SSI implementations regarding privacy. This paper aims to fill this research gap by providing a thorough evaluation based on clearly defined criteria.

## 3 Related Work

Currently, there is much ongoing research on new identity management solutions. SSI, and in particular blockchain-based SSI, plays a leading role in the novel solutions that are proposed. Aside from these novel solutions, there is a rise in evaluations and reviews about the technology and implementations.

In [11], an extensive survey regarding privacy and blockchain technology is presented. It describes the privacy problem, the shortcomings of blockchain technology concerning privacy, the technical solutions to protect privacy, and specific blockchain applications. However, it does not provide any references or conclusions on identity management.

Another extensive review on privacy-preserving blockchain solutions is provided by [12]. It is comprehensive in its definitions, and it provides excellent criteria for a privacy evaluation. Nevertheless, the focus is on a broad range of application domains. Therefore it only has a small section on blockchain-based identity management.

An analysis that treats identity management using blockchain technology is given in [13]. It provides an overview of SSI and different types of blockchain technology. It then focuses on three specific implementations, namely, uPort, Sovrin and ShoCard. The analysis minimally treats privacy. It is therefore not clear how the implementations perform in terms of privacy.

A similar analysis is done in [14]. This article provides a more extensive survey on identity management systems. It provides a large background section on the subject matter and an evaluation framework with 75 criteria, which they apply on 43 different offerings. Nevertheless, one of the criteria that describes itself as SSI is marked as not a mandatory criterion. Furthermore, privacy aspects are underrepresented in the criteria.

The authors of [15] provide a great starting point for a privacy evaluation on blockchain-based SSI. It features an overview of ten implementations that are analyzed. However, its missing specific criteria and certain properties do not fit in privacy or security.

More specific related work is mentioned in the following sections. Note that the research gap mentioned in the problem description can be observed from the incompleteness of the related work in terms of privacy.

## 4 Background

This section will provide all the necessary background information that is needed for the criteria and evaluation sections. A large part of it contributes to answering sub-question one, ”What are the privacy issues that SSI tries to solve?” stated in the Introduction. The section will start with digital privacy and identity management. We then continue with the identity management approach we consider, namely SSI. From here, blockchain and privacy implications on blockchain technology will be discussed. At last, we consider specific privacy-preserving methods and blockchain-based SSI implementations. This subsection will provide answers to sub-question two, ”What privacy-preserving methods are currently available for blockchain-based SSI?”.

### 4.1 Digital Privacy

In the 21st century, privacy awareness is more present than ever before [16]. Privacy is defined as ”someone's right to keep their personal matters and relationships secret” by Cambridge Dictionary[2]. This is not just limited to this definition. The fact that privacy is a right is part of our legislation, and with the recent addition of the GDPR in Europe, it is present in all digital services. However, privacy protection is still not up to the expectations of many people. This became apparent after a survey by InnoValor, stating that citizens feel a lack of control of their digital identity. [4].

[1] https://github.com/peacekeeper/blockchain-identity

[2] https://dictionary.cambridge.org/dictionary/english/privacy

The current digital environment is mainly maintained in a centralized manner. When an online service is used, digital identity management is implemented either by this service or by a Federated Identity Management (FIM) platform such as Facebook. The digital identity is stored, monitored, and owned by the service. Therefore, much trust is necessary from the user of such a service. Nevertheless, there is often not an alternative. This makes privacy abuse a genuine concern, take, for example, the controversy around Facebook's real-name policy [17].

## 4.2 Decentralized Identities

We need a decentralized solution that returns the control of the identity management to the identity owner. The notion of a Self-Sovereign Identity (SSI) is introduced to make this possible. It defines a solution where the identity owner is in control of his or her own identity. In ”The Path to Self-Sovereign Identity”, Christopher Allen motivates this concept, including ten principles that are still used today as a foundation for SSI technology [5].

The movement to a decentralized solution is not new. One of the most famous examples is the decentralization of money via Bitcoin [9]. This heavily influenced the SSI development by showing the potential that blockchain might also have on the decentralization of identity management. The underlying blockchain technology allows for decentralization by creating a peer-to-peer consensus protocol that no longer needs a centralized intermediary. Already there are many initiatives for blockchain-based SSI solutions [18].

In these solutions, we can differentiate between three parties: the Issuer, the User and the Verifier. The user holds and obtains verifiable claims and credentials that are issued by the Issuing Authority. The claims are stored as attestations on a blockchain. Often these attestations are in the form of identity hashes and verifiable claims. The Verifier can check the attestations and the attestations' signatures on the blockchain to verify that the claim a User makes is valid. In Figure 1 an overview of this design is given.

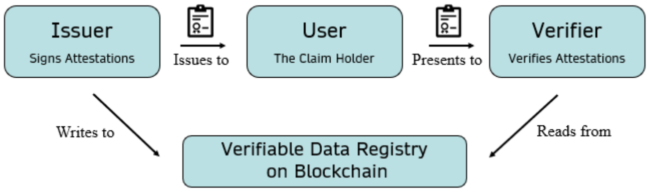

Figure 1: The roles and information flow used in SSI solutions.

Privacy protection is one of the main goals of this technology. It is accounted for in the design of the system described in the previous paragraph. Privacy protection is achieved by only sharing identity information on a need-to-know basis using verifiable credentials. The User is in control and decides whether to share verified claims to a Verifier. The User can also accept or reject claims that an Issuer can pose upon a User.

## 4.3 Blockchain Technology

Blockchain is currently known as a revolutionizing technology that is at the core of a lot of digital innovations [19]. However, not many people are aware of how this technology works. Blockchain is a chain of blocks that consists of transactions or data. This chain is stored in a decentralized fashion where any participating node has a copy of the blockchain. This is sometimes also called Distributed Ledger Technology (DLT). Furthermore, it is maintained in a decentralized way and is cryptographically secured.

By itself, the technology is not new. The first known blockchain started in 1995 and is still being published in the New York Times [20]. The technology took off after the Bitcoin white paper. It has since been seen as the catalyst of decentralization.

Soon after the decentralization of money via cryptocurrencies, other application domains were considered as well [21]. One of these domains is digital identity management, which fits naturally with the notion of SSI. However, SSI has more prerequisites than just decentralization. Privacy protection is the primary concern. Data should only be disclosed to a party when consent is given. Moreover, the right to be forgotten that the European Union enforces should be complied with. This has substantial implications on the underlying technology, and this is where problems start to arise.

## 4.4 Privacy Issues of Blockchain

Traditional blockchain solutions such as Bitcoin can be classified as permissionless blockchains. This means that there is no permission policy in place. All the users of the network can participate in any role they desire. It is based on zero trust, where the underlying technology maintains consensus and security. Anyone can view the data, and once data has been processed into the blockchain, it is there to stay forever unless 51% of the users decide differently.

The open-access and immutable data structure contradict the necessities for SSI. Thus a trade-off between full decentralization and privacy is present. To counter these limitations, different technological privacy-preserving methods are necessary. A prominent technology is Decentralized Identifiers (DIDs) [22]. DIDs are globally unique identifiers designed to function in a decentralized environment. The goals are Decentralization, Control, Privacy, Security, Proof-based, Discoverability, Interoperability, Portability, Simplicity, and Extensibility. Consequently, there is an important overlap between the goals of DIDs and the principles that define SSI. Regarding privacy, it promises to enable entities to control the privacy over their data and related attributes.

Aside from permissionless blockchain, there is also a permissioned variant. It provides extra security by adding an access control layer to the blockchain. Users of the blockchain take on specific roles determined by the authoritative party that regulates the blockchain.

## 4.5 Privacy-Preserving Methods

Privacy and security are inherently coupled. This section will describe several privacy-preserving methods that can be applied to blockchain technology.

**Secure Multiparty Computation**
Secure Multiparty Computation (SMC) is a cryptographic algorithm that is used for increased privacy protection. In SMC, the data is split between $N$ parties using secret sharing. A specific subset of $M$ parties are needed in the computation process. Each party only receives part of the data, and in order to generate the total data output, all involved parties of the subset need to cooperate in a distributed computation. This method is already extensively used in blockchain [23]. SMC is most commonly applied in applications where no trust exists between computing entities while privacy over the data should be guaranteed. Blockchain by itself does not secure the data in the computation process, while SMC secures the input data through the computation process such that the data will not be revealed to other users. However, the computation process is quite complex and inefficient, which makes it impractical for adoption [11].

**Zero-Knowledge Proofs**
A Zero-Knowledge Proof (ZKP) is a cryptographic protocol between two entities that enables them to communicate data in a privacy-preserving manner. A User can use a ZKP to prove to a Verifier that a claim is correct by only revealing information about whether the proof itself is correct or not. ZKPs can significantly improve the privacy of a blockchain. Currently, there are many ZKP implementations, each with its characteristics and use-cases [24]. Each implementation at least shares the three core properties of ZKP:

1. Completeness: If the User's claim is true, then the Verifier will always find it true.
2. Soundness: If the User's claim is false, then a malicious User can only up to a minimal probability convince the Verifier otherwise.
3. Zero-Knowledge: If the User's claim is true, then the Verifier only learns that the statement is true.

**zk-SNARK**
Zero-Knowledge Succinct Non-interactive Argument of Knowledge (zk-SNARK) is the most widely used type of ZKP in blockchain. A one-way communication channel from the Verifier to the User characterizes this type. Moreover, because of the one-way communication, this type of proof can generally be verified very fast. It is used extensively by Zcash, a currency system that is known for its privacy features [25].

**Decentralized Identifiers**
The W3C published a Candidate Recommendation for a new technological standard which is called Decentralized Identifiers (DIDs) [22]. DIDs are a new type of globally unique identifiers that enable decentralized and verifiable digital identities. The technology is designed with the principles of SSI in mind. A DID can be regarded as an URL that associates the DID subject to the data, called the DID Document. In a blockchain, DIDs are primarily used to be able to store data off-chain. This dramatically improves privacy protection since the data is not publicly available on the blockchain itself. Instead, a reference to the data is stored on the blockchain. Furthermore, the data itself can be cryptographically secured, and the link to the DID can be revoked at any time.

**Verifiable Credentials**
The design of a general SSI solution as shown in Figure 1 is based upon the verifiability of claims about the User. The W3C has published a recommendation called Verifiable Credentials Data Model, which attempts to improve digital credentials in a privacy-preserving way [26]. Verifiable Credentials (VCs) can represent all sorts of identity information. Users can generate Verifiable Presentations that can be shared with the Verifier to prove that they have specific VCs. The recommendation explains several privacy-enhancing technologies that can be used to improve the security of VCs. Zero-Knowledge Proofs are also included as privacy-enhancing technology.

**Commitment Schemes**
A Commitment Scheme (CS) is, just like a ZKP, a cryptographic protocol that allows a User to hide a secret value that is associated with an original value while at the same time binding this value to the User [12]. This allows a Verifier to verify if a User tells the truth when the original value is revealed, without revealing the sensitive secret value. A CS can be of two types, either unconditionally binding or unconditionally hiding. The former says that a User cannot open the secret value to a different value than the original value. The latter says that a Verifier cannot guess the secret value a User is committed to.

**Homomorphic Hiding**
Homomorphic Hiding is based on Homomorphic Encryption. It allows users to do computations directly on the encrypted data. This is due to the homomorphic properties, which retains the algebraic structure of the underlying numerical data. Therefore, it is a powerful privacy-preserving method since it is not needed to decrypt the data in order to use it. It is actively used in many Blockchain applications that use cryptography, such as zkSNARK and Bitcoin.

**Ring Signatures**
A Ring Signature is a particular type of signature scheme that uses a ring of entities that can create signatures. It allows a User to sign other ring members messages using the User's private key and the public key of the other members. The strength of this scheme comes from the fact that a Verifier cannot tell who signed a message, only that the signer is a member of the ring. When this scheme is applied to a blockchain, the signature of the transaction can be guaranteed to be anonymous, correct and unforgeable [12].

## 4.6 Blockchain-Based SSI Implementations

The evaluation will be performed on the most popular blockchain-based SSI solutions that are in active development. Popularity will be determined based on references to the specific SSI implementations in recent literature. Activity will be determined by consulting the official website of the

SSI solution and, if present, the source code of the implementation. This section will provide references to the evaluated implementations.

The specific blockchain-based SSI implementations chosen for this evaluation are Sovrin [27][28], ShoCard[29][30], uPort[31][32], Vetri Global[33], Trustchain[34], Everest[35], EverID[36], Spidchain[37], Blockpass[38], Affinidi[39], Dominode[40], ID.ee[41], Evernym Verity[42], LifeID[43], SelfKey[44], Sora[45], and myIDsafe[46]. More implementations are available, but are either inactive or do not provide the information that is necessary to perform this evaluation.

# 5 Criteria

In this section, the evaluation criteria are presented and discussed. The criteria are established by examining the privacy challenges that are present in blockchain technology. Furthermore, it takes into account the privacy needs of self-sovereign identity management.

### Data Minimization

In order to satisfy data minimization in SSI, Zero-Knowledge Proofs (ZKPs) or comparable methods should be used. ZKPs keep the information needed for the User to prove a claim to a Verifier at a bare minimum. When this technology is not applied, the risks that are present in current centralized identity management solutions will also be present in SSI. A Verifier can then store any information that a User provides needed for a proof, thus not satisfying data minimization.

### Usability Privacy

Usability in SSI applications entails, for a large part, the user experience. Therefore, it is essential that users can utilize their SSI application so that they are not confronted with too many technical details. This could lead to users not understanding the privacy risks resulting from careless handling of identity data. As such, we should seek for user-friendly privacy management.

### Privacy-Aware Development

Developers play an essential role in preventing privacy risks. In privacy-aware development, there is a need for a privacy-preserving abstraction layer that developers can use. This creates a developer-friendly environment where the chance to introduce privacy risks is reduced.

### Interoperable Privacy

Interoperability in SSI is the principle that explains that different systems should seemingly work together for the user. However, when different systems are used, identity data is transferred from one system to the other. This can be a considerable privacy risk since the data may need to be converted through different formats in this process. This can lead to exposing sensitive information. To be able to cope with this, we need Interoperable Privacy. This can be achieved by adopting industry standards that any service should comply with. For example, the W3C published articles on Decentralized Identifiers and Verifiable Credentials, which could serve as industry standards and which are already adopted by some implementations.

### Open Source

Software that is used to participate in decentralized identity management should be open source. When software is open source, the risk that malicious code, privacy-sensitive bugs, and missing privacy features go unnoticed is reduced. A main principle of SSI says that the user should be in complete control over their own identity. This can only be the case when the user also has access to the source code of the SSI applications that the user is ought to use.

### Erasable Data

Blockchains are by nature immutable. To cope with non-erasable data and the need for mutable data structures in identity management, the blockchain-based SSI solution should provide means to make data mutable. This is often realized by storing sensitive identity data off-chain. Decentralized Identifiers can be used to create on-chain references to off-chain data that allow for mutability.

### Secure Key Storage

SSI wallet apps should allow for secure key storage. The private keys of a user should be stored using decentralized key management. As such, the user should have the private keys offline in their wallet. Furthermore, the user must be able to be in complete control over their private keys, allowing the user to move or delete the keys at will.

### Backdoor Proof

Permissioned blockchains are also known as privately governed blockchains. Permissioned blockchains can introduce increased data protection since a trusted authority protects against malicious users and other malicious factors. However, this comes at the cost of losing control. The governance of the SSI system can be subordinate to other interests of the body that controls it. This can be a reason to introduce backdoors into the system to comply with legislation and other factors for when an intervention is necessary. These backdoors introduce risks to privacy protection. Thus the choice for a permissioned blockchain is a trade-off between a fully decentralized blockchain-based SSI solution and a solution that protects against malicious users by not allowing them to run the blockchain nodes.

### Quantum Resistance

Quantum Computing has been proven to form a significant risk to current cryptographic algorithms [47]. Cryptography forms the backbone of blockchain technology, and thus this risk applies directly to blockchain and blockchain-based SSI implementations. Therefore, to guarantee privacy in the long run, SSI implementations should be using or ready to adopt quantum-resistant encryption algorithms.

### Privacy Plan

Until now, we only used criteria that can be derived from the white papers and technical specifications of the blockchain-based SSI implementations. It is also essential to see whether the creators envisioned the design of the implementation with privacy in mind. A so-called 'Privacy Plan' can be part of their specifications in which they state how they try to preserve the users' privacy. If this plan is not part of their specification, one should use such an implementation cautiously regarding privacy protection.

## 6 Evaluation

The evaluation will be performed on the blockchain-based SSI implementations that are mentioned in Section 4.6 based on the criteria of Section 5. The criteria will be evaluated using 'Yes' if a criterion is satisfied and 'No' if a criterion is not satisfied. If a criterion cannot be determined for a particular implementation, an 'X' symbol is written. The results are presented in Table 1. Based on the data provided in the table, specific implications on the privacy protection of the implementations can be made. Furthermore, it will provide answers to sub-question three, "How do the current blockchain-based SSI implementations preserve privacy?".

### 6.1 Table Examination

The results in Table 1 show substantial differences in the satisfied criteria for the evaluated implementations. Almost all implementations differ on at least one criterion from each other. Even more remarkable is that not a single implementation scores positively on all criteria. However, there are a few implementations that satisfy eight or more criterion, namely uPort [31][32], Sovrin [27][28], LifeID [43], and SelfKey [44].

Notice that not a single implementation is quantum resistant when we look at the evaluation table per criterion. While there is quantum-resistant cryptography already available, blockchain-based SSI implementations tend not to use it yet. However, this could change soon since some implementations are based on the Ethereum blockchain, such as uPort. Ethereum has quantum-resistant cryptography planned for its Ethereum 2.0 release.

On the other side, most implementations satisfy the Usability Privacy, Erasable Data, and Secure Key Storage criteria. This can be explained by the fact that these are technically relatively easy to implement. Most implementations feature a user-friendly (wallet) application, which is needed for Usability Privacy. The application can be used to manage the private keys stored locally on the device, thus satisfying the Secure Key Storage criterion. Erasable Data is in most cases satisfied because of the European GDPR and other legislation that the implementations need to comply with.

At last, the Privacy Plan criterion can be regarded as a critical component of the evaluation. The privacy plan should describe how the implementation tries to guarantee privacy protection and what it considers as possible privacy risks. In some cases, the privacy plan also reflected its design decisions on legislation. Considering the importance of this criterion, it is astonishing to see that only 6 out of the 17 evaluated implementations have a privacy plan in some form.

### 6.2 Privacy Overview

Overall, the privacy protection in current blockchain-based SSI implementations does generally not meet the expectations and the promises of SSI. Except for a few implementations mentioned in Section 6.1, the current implementations have too many criteria that are not satisfied. Earlier in Section 4.5 we mentioned several privacy-preserving methods that can be used to meet the evaluation criteria. As such, there are, in general, no technical limitations for satisfying the criteria. All the technology and standards are already in existence. Besides the technical methods, some implementations do not satisfy specific criteria because of their commercial and often closed source intent.

## 7 Responsible Research

The importance of responsible research can not be understated. It is fundamental for trustworthy, ethical, and reproducible research. Furthermore, the integrity of the research is at stake if the research is not performed responsibly. In this work, privacy is a central subject of discussion. Privacy is inherently coupled to the principles of responsible research. As such, the research is performed with utmost care. In this section, the related work, the reproducibility, and the privacy aspects are discussed.

The related work and references were carefully selected. First of all, the articles were found with the use of the trusted academic search engine Scopus [48]. The articles were then filtered by influence factor, place of publication, and citation score. Finally, the articles were critically assessed before including them in the literature list of this work. Citations and references are provided where deemed necessary to provide complete information and sufficient argumentation.

In terms of reproducibility, this research can be verified and reproduced using the literature references. It is also presented objectively, purely based on references and easy to follow logical deductions. As such, this work can be typed as a literature study. It does not provide any new practical experiments or implementations that need to be evaluated. For specific reproducibility questions on any mentioned implementation or technology, the reader should seek the provided references.

At last, privacy is an essential aspect of responsible research and plays a vital role in this work. This paper does not contain any methodologies or uses any data that can be considered a privacy issue. It is purely based on publicly available information and specifications. However, in the evaluation, implications are made on the treated blockchain-based SSI implementations regarding privacy protection. It should be noted that these implications are not sufficient in deciding whether to use a particular implementation concerning privacy protection. The reader should be aware that privacy is a complex concept that is not only defined in technical terms. This overview provides a part of the technical answer. Other privacy authorities should be consulted for a complete picture.

## 8 Conclusions and Future Work

This paper evaluated several blockchain-based SSI implementations regarding privacy protection. The evaluation was based on several criteria that define the technical privacy aspects an implementation should adhere to. The criteria table contains the results of the evaluation. Based on these results, we came up with several implications regarding the privacy

| Implementations | Data Minimization | Usability Privacy | Privacy-Aware Development | Interoperable Privacy | Open Source | Erasable Data | Secure Key Storage | Backdoor Proof | Quantum Resistance | Privacy Plan |
|---|---|---|---|---|---|---|---|---|---|---|
| Sovrin | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| ShoCard | No | Yes | No | No | No | No | Yes | Yes | No | Yes |
| uPort | No | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes |
| Vetri Global | Yes | Yes | No | No | No | Yes | Yes | No | No | Yes |
| Trustchain | Yes | No | Yes | No | Yes | Yes | Yes | No | No | No |
| Everest | No | Yes | No | No | No | Yes | Yes | No | No | No |
| EverID | No | Yes | No | No | No | Yes | Yes | No | No | No |
| Spidchain | No | No | No | Yes | Yes | Yes | Yes | Yes | No | No |
| Blockpass | No | Yes | No | Yes | No | Yes | Yes | No | No | No |
| Affinidi | No | Yes | Yes | Yes | No | Yes | Yes | No | No | No |
| Dominode | X | X | X | X | No | X | X | No | X | No |
| ID.ee | No | Yes | Yes | No | No | X | Yes | No | No | No |
| Evernym Verity | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | No |
| LifeID | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes |
| SelfKey | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes |
| Sora | No | Yes | X | Yes | X | Yes | Yes | No | No | No |
| myIDsafe | No | X | Yes | Yes | X | Yes | X | X | X | No |

Table 1: Evaluation results of selected blockchain-based SSI implementations based on defined criteria.

protection of the examined SSI implementations. With this knowledge, we can answer the sub-questions and the overarching research questions. Furthermore, we provide pointers and recommendations for future research.

## 8.1 Conclusions

The notion of SSI came to exist because there is a lack of control concerning identity management. The ten principles provided by Christopher Allen represent the core values of SSI. The currently proposed technical solutions for implementing SSI are often blockchain-based. While blockchain naturally enables many SSI principles, it also brings new privacy problems, as seen in some of the papers in the related work section. These new privacy problems are the main subject of this literature study.

We looked at several privacy-preserving methods that are already used in blockchain-based applications. A list of ten criteria was defined to be able to evaluate seventeen blockchain-based SSI implementations. These criteria are Data Minimization, Usability Privacy, Privacy-Aware Development, Open Source, Erasable Data, Secure Key Storage, Backdoor Proof, Quantum Resistance, and Privacy Plan.

The privacy-preserving methods that enable blockchain-based SSI solutions to satisfy the mentioned privacy criteria are already available. There are no technical limitations that prevent the SSI solutions to comply with all evaluation criteria. However, the evaluation results show that most of the evaluated implementations do not satisfy all privacy criteria. Some solutions score poorly on privacy protection and do not even provide a privacy plan to discuss their reasoning. As such, current SSI implementations should focus on improving privacy protection to meet the privacy expectations for SSI technology.

## 8.2 Future Work

Future research can focus on more practical privacy issues. Usability is an essential aspect of SSI technology that should enable a more friendly user experience without compromising privacy and security. Furthermore, the adoption issues regarding privacy can be expanded considering cultural, social or political factors. One could look at global versus local deployments of the SSI solutions based on these additional factors in terms of privacy. At last, legislation plays a significant role in the data privacy field. The technical solutions could be compared to current legislation to determine whether the solutions or legislation is up to expectations for this upcoming technology.

## References

[1] Preukschat, A., Reed, D. (2021). Self-Sovereign Identity: Decentralized digital identity and verifiable credentials (1st ed.). Manning Publications.

[2] Smit, A. (2020). Identity Reboot: Reimagining Data Privacy for the 21st Century (1st ed.). MintBit Ltd.

[3] Jiang, L., Ren, Y., Wang, J., Xu, L., and Yuan, J. (2014). Information Security in Big Data: Privacy and Data Mining. IEEE Access. 2. 1-28. 10.1109/ACCESS.2014.2362522.

[4] InnoValor. (2016). Persoonlijke data, onder controle?

[5] Allen, C. (2016). The Path to Self-Sovereign Identity.

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

[7] Baars, D. (2016). Towards self-sovereign identity using blockchain technology.

[8] Hellwig. (2020). Build Your Own Blockchain: A Practical Guide to Distributed Ledger Technology (Management for Professionals) (1st ed.). Springer.

[9] Nakamoto, S. (2009). Bitcoin: A Peer-to-Peer Electronic Cash System.

[10] Syed, T. A., Alzahrani, A., Jan, S., Siddiqui, M. S., Nadeem, A., and Alghamdi, T. (2019). A comparative analysis of blockchain architecture and its applications: Problems and recommendations. IEEE acces. 7. 176838-176869.

[11] Wang, D., Wang, Y., and Zhao, J. (2020). A Survey on Privacy Protection of Blockchain: The Technology and Application. IEEE Access. 1-1. 10.1109/ACCESS.2020.2994294.

[12] Bernal Bernabe, J., Canovas Sanchez, J. L., Hernández-Ramos, J., Torres Moreno, R., and Skarmeta, A. (2019). Privacy-Preserving Solutions for Blockchain: Review and Challenges. IEEE Access. 10.1109/ACCESS.2019.2950872.

[13] Haddouti, S. E., and Ech-Cherif El Kettani, M. D. (2019). Analysis of Identity Management Systems Using Blockchain Technology. 2019 International Conference on Advanced Communication Technologies and Networking (CommNet). 1-7. 10.1109/COMMNET.2019.8742375.

[14] Kuperberg, M. (2019). Blockchain-Based Identity Management: A Survey From the Enterprise and Ecosystem Perspective. IEEE Transactions on Engineering Management. 1-20. 10.1109/TEM.2019.2926471.

[15] Panait Drăgnoiu, A., Olimid, R., and Stefanescu, A. (2020). Identity Management on Blockchain - Privacy and Security Aspects. Proceedings of the Romanian Academy - Series A: Mathematics, Physics, Technical Sciences, Information Science. 21. 45-52.

[16] Garfinkel, S. (2000). Database Nation: The Death of Privacy in the 21st Century.

[17] Gunthe, S. (2015). Facebook's "Real Name" Policy: A Violation of the Corporate Responsibility to Respect Human Rights. Columbia University.

[18] Liu, Y., He, D., Obaidat, M., Kumar, N., Khan, K., and Choo, K.R. (2020). Blockchain-based identity management systems: A review. Journal of Network and Computer Applications. 166. 102731. 10.1016/j.jnca.2020.102731.

[19] Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J., and Amaba, B. (2017). Blockchain technology innovations. IEEE Technology Engineering Management Conference (TEMSCON). 137-141. 10.1109/TEMSCON.2017.7998367.

[20] Oberhaus, D. (2018). The World's Oldest Blockchain Has Been Hiding in the New York Times Since 1995. Vice.

[21] Jaoude, J. A., Saade, R. G. (2019). Blockchain Applications – Usage in Different Domains. In IEEE Access, vol. 7, pages 45360-45381

[22] Reed, D., Sporny, M., Longley, D., Allen, C., Grant, R., and Sabadello, M. (2021). DID. W3C.

[23] Zhong, H., Sang, Y., Zhang, Y., and Xi, Z. (2019). Secure multi-party computation on blockchain: an overview. Springer CCIS. 452–460. 10.1007/978.981.15.2767.8.40

[24] Sánchez, D. (2019). Zero-Knowledge Proof-of-Identity: Sybil-Resistant, Anonymous Authentication on Permissionless Blockchains and Incentive Compatible, Strictly Dominant Cryptocurrencies.

[25] Sasson, E.B., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., and Virza, M. (2014). Zerocash: Decentralized anonymous payments from bitcoin. Proc. IEEE Symp. Secur. Privacy. 459–474. 10.1109/SP.2014.36

[26] Sporny, M., Longley, D., and Chadwick, D. (2019). Verifiable Credentials Data Model. W3C.

[27] Reed, D., Law, J., and Hardman., D. (2016). The Technical Foundations of Sovrin.

[28] Law, J., and Hardman., D. (2016). Self-Sovereign Privacy By Design.

[29] SITA. (2016). ShoCard Travel Identity of the Future.

[30] ShoCard. (2021). https://www.shocard.com/.

[31] Lundkvist, C., Heck, R., Torstensson, J., Mitton, Z., and Sena, M. (2016). uPort: a Platform for Self-Sovereign Identity.

[32] uPort. (2021) uPort Developer Portal. https://developer.uport.me/.

[33] Vetri. (2017). Vetri: Value Your Data.

[34] Pouwelse, J. (2018). Trustchain Protocol. https://tools.ietf.org/id/draft-pouwelse-trustchain-01.html

[35] Reid, B., and Witteman, B. (2018). Everest: Whitepaper.

[36] Reid, B., and Witteman, B. (2018). EverID: Whitepaper.

[37] SpidChain. (2017). SpidChain: A distributed digital identity system with a marketplace for verifiable claims.

[38] Blockpass. (2018). Identity for a Connected World: A user centric identity application for regulated industries and the Internet of Everything.

[39] Affinidi. (2020). Affinidi Documentation. https://docs.affinidi.com/.

[40] Dominode. (n.d.). http://www.dominode.com/.

[41] ID.ee. (2003). The Estonian ID Card and Digital Signature Concept: Principles and Solutions.

[42] Evernym. (2021). https://evernym.com.

[43] lifeID. (n.d.). Welcome to lifeID: An open-source, blockchain-based platform for self-sovereign identity.

[44] SelfKey Foundation. (2017). SelfKey: Whitepaper.

[45] Takemiya, M., and Vanieiev, B. (2018). Sora Identity: Secure, Digital Identity on the Blockchain. IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC). 582-587. 10.1109/COMPSAC.2018.10299.

[46] Weinhandl, G. (2019). myIDsafe: Selbst-Souverane Identitaten auf der Blockchain.

[47] Mavroeidis, V., Vishi, K., Zych, M.D., and Jøsang, A. 2018. The impact of quantum computing on present cryptography. arXiv:1804.00200.

[48] Scopus. (n.d.). https://scopus.com.