Is blockchain necessary for Self-Sovereign Identity?

Panagiotis-Christos Kyrmpatsos
Research Methodology Course for MSc in Computer Science
Athens University of Economics and Business
pankyrbatsos@aueb.gr

Abstract

Digital identity is currently a pressing issue, being patched by efforts of individual companies and yet, still, remaining highly centralized. By placing a user in the center and leveraging decentralization, Self-Sovereign Identity (SSI) implementations aspire to provide the long-awaited Identity layer to our digital lives. Many of them utilize blockchain technology to achieve this. In this paper, we will look at three different implementations of SSI systems. We shall also explore which criteria SSI solutions need to meet and furthermore, propose a 12-point system for evaluation purposes. Lastly, we will score those solutions against our evaluation criteria to understand whether blockchain technology is a prerequisite for building SSI systems. We conclude that blockchain can be advantageous but not necessary to SSI systems.

Index Terms

Digital Identity, Distributed Ledger, Self Sovereign Identity, Zero-Knowledge Proof

1 Introduction

SSI has become a trend within the digital identity circles. Since the concept first appeared in 2016 [1], plenty of implementations have been proposed to re-imagine the way we manage our Digital Identity. Overall, SSI attempts to solve identity without relying on central authority [15]. For that reason, many SSI systems use DLT to promote decentralization. The append-only nature of blockchain, also, guarantees persistence, with transparency also being a plus. In an SSI system users should be able to decide which attributes they want to tie to their digital identity and also exchange claims about those attributes with third parties.

The current literature mainly focuses on individual SSI solutions. Only a few research papers deal with the comparison and evaluation of already proposed systems. Our goal is to explore three SSI solutions and rate them against a comprehensive list of criteria. Through this evaluation, we hope to be able to answer the following question: Is blockchain a necessary block for implementing an SSI solution? To answer that the following issues shall be investigated first:

- What are the necessary attributes of an SSI solution ?
- How can each proposed system be evaluated?
- How do certain implementations score against our criteria?

In the following sections we will attempt to provide answers to the questions above by reviewing the current literature, proposing a 12-point evaluation scheme and analyzing three SSI solutions.

2 Preliminaries

To facilitate the issues discussed forward, we provide some definitions and abbreviations explained in more detail:

Distributed Ledger Technology (DLT): The technological infrastructure and protocols that allow simultaneous access, validation, and record updating in an immutable manner across a network that's spread across multiple entities or locations.

GNU Name System (GNS): A decentralized and censorship-resistant domain name resolution protocol that provides a privacy-enhancing alternative to the Domain Name System (DNS) protocols [14].

Interplanetary File System (IPFS): IPFS is a peer-to-peer (p2p) distributed storage network.

Namecoin: A key/value pair registration and transfer system based on the Bitcoin technology.

Public Key Infrastructure (PKI): A combination of policies, procedures and technology needed to manage digital certificates in a public key cryptography scheme [4].

Zero-Knowledge Proof (ZKP): A method by which one party (the prover) can prove to another party (the verifier) that a given statement is true while the prover avoids conveying any additional information apart from the fact that the statement is indeed true [5].

3 Related Work

In this section, we will discuss some of the considerations regarding Identity Management and examine some evaluation criteria that have already been proposed. A more in-depth analysis of the evaluation criteria will be presented in section 4. K. Cameron (2005), in his seminal work *The Laws of Identity* [9] underlines the challenges we need to face from an Identity Management perspective because the Internet was built without an identity layer. By exploring the dynamics that determine the success of various systems, he proposes seven laws that should form the basis of any successful identity implementation. While K. Cameron does not directly comment on SSI requirements, his laws, nonetheless, are fully applicable to every SSI system implementation. Cameron's seven laws are as follows:

- **User Control and Consent**: Information that identifies the user should only be revealed with the user's consent. Note that a distinction exists between the two. This distinction is underlined by the proposition of two separate laws [1]. Thus, implementations may exist where only one property is satisfied but not the other.
- **Minimal Disclosure for a Constrained Use**: Information regarding our digital Identity should always be revealed on a "need-to-know" basis. The information exchanged should also be disclosed in such a way that renders it unfeasible to identify an individual across different contexts.
- **Justifiable Parties**: Digital identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship.
- **Directed Idenity**: A universal identity system must support both "omni-directional" identifiers for use by public entities and "unidirectional" identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles. Observe that from the first three laws, individuals are private first, and public only to the degree they wish to be in different circumstances.
- **Pluralism of Operators and Technologies**: A universal identity system must channel and enable the interworking of multiple identity technologies run by multiple identity providers. In other words, identity solutions should support interoperability.
- **Human Integration**: This law stresses the importance of UX and UI in any implementation. As Dhamija (2008) explains: "identity management is not a primary goal" [2].
- **Consistent Experience Across Contexts**: The unifying identity metasystem must guarantee its users a simple, consistent experience while enabling the separation of contexts through multiple operators and technologies. In simpler terms, individuals should be able to manage multiple identities for different contexts (e.g. browsing, personal, professional, citizen, etc.)

In 2016, C. Allen created a comprehensive list of ten properties [1] that SSI solutions should adhere to.C. Allen builds upon K. Cameron's laws, expands and distills them into more comprehensive properties specifically fit to SSI.

In 2018, Q. Stokkink and J. Pouwelse introduced an extra property of SSI systems, requiring claims to be provable [15]. In *Deployment of a Blockchain-Based Self-Sovereign Identity*, they argue that, individual blockchain storage for each user, combined with the use of ZKP to exchange claims, would result in a system that satisfies all 11 properties.

A comparative evaluation between different identity management schemes is provided in *A First Look at Identity Management Schemes on the Blockchain* [3]. By using K. Cameron's laws as evaluation criteria three different Identity management schemes are examined. Two SSI solutions - Sovrin, uPort [1], and a digital identity system- shoCard [2]. It is concluded that DLT "is not a silver bullet solution for Identity Management", while more attention should be placed on usability and privacy aspects.

The same conclusion regarding the usefulness of DLT in implementing SSI is reached in *With Blockchain or not? Opportunities and challenges of self-sovereign identity implementation in public administration* [10]. Since they focus on evaluating the Belgian e-identity scheme, which leverages SSI principles, Mahula et al. (2021) propose two extra evaluation criteria on top of using Allen's rules. These include the *usability* principle—the SSI solution must be hassle-free and easy to operate— and the *costless* principle— the user should not be burdened with extra costs when interacting with public sector organizations. Since we are not solely analyzing public sector-focused schemes we do not include the *costless* principle in our evaluation criteria. However, the *usability* principle shall be included in our criteria. This principle is also explicitly included as "Human Integration" in K. Cameron's laws.

A similar approach for assessing different SSI solutions is utilized in *Self-Sovereign Identity systems, Evaluation Framework* [12] where A. Satybaldy et al. (2020) utilize the *usability* principle in conjunction with K. Cameron's laws to present a systematic analytical study of a few SSI systems.

4 Evaluation Framework

To date, there exist no definitive evaluation criteria for SSI systems. Most attempts focus on the laws of K. Cameron or C. Allen and append extra properties depending on the context of the analysis. We shall pursue the same path by utilizing C. Allen's 10 laws [1] as our basis. We shall also add the *usability* principle to our analysis since easy-of-use remains Achille's heel regarding several SSI proposals. It is worth noting that usability is inherently difficult to formally prove. Correspondingly, it will be evaluated on a personal preference basis. Lastly, we use the proposal of Q. Stokkink and J. Pouwelse [15] which requires claims to be provable. The ten laws are quoted from [15].

The evaluation criteria are as follows:

1. **Existence.** Users must have an independent existence.
2. **Control.** Users must control their identities.
3. **Access.** Users must have access to their own data.
4. **Transparency.** Systems and algorithms must be transparent.
5. **Persistence.** Identities must be long-lived.
6. **Portability.** Information and services about identity must be transportable.
7. **Interoperability.** Identities should be as widely usable as possible.

[1] uPort has split into two projects Serto and Veramo

[2] shoCard is now part of PingIdentity

8. **Consent.** Users must agree to the use of their identity.
9. **Minimalization.** Disclosure of claims must be minimized.
10. **Protection.** The rights of users must be protected.
11. **Provable.** Claims must be shown to hold true.
12. **Usability.** User experience is straightforward and consistent with the user's needs and expectations.

5 Evaluation

Three solutions will be examined. Sovrin, reclaimID and a modified did:self system that we suggest as a potential SSI solution. Sovrin is blockchain-based while reclaimID can be based on blockchain depending on the implementation. Lastly, the did:self system does not utilize blockchain but rests on IPFS. The selection of the particular systems was dictated by the need to evaluate systems covering the whole range of blockchain utilization.

5.1 Sovrin

Sovrin is based on a public permissioned distributed ledger (Hyperledger) [18]. The core of the Sovrin network rests upon *Stewards*—trusted institutions responsible for maintaining Hyperledger nodes. The project is characterised by a combination of both decentralisation (Hyperledger) and centralisation (*Stewards* must be approved by the Sovrin Foundation) to tackle trust issues when dealing with SSI.

Transparency is achieved through the open-source nature and development of Plenum [11] and Hyperledger. The solution also fulfills the *minimalization* principle by enabling selective disclosure of claims through ZKPs. Users' *control*, *consent*, and *access* over their own data is also guaranteed through the use of *consent receipts* and the capability of maintaining multiple identifiers for each context. *Persistence* is attained by using blockchain technology and separating the identity from its claims [1]—a user that enters the system does not have any attribute tied to their identity.

Through the use of system-independent data formats like JSON-LD [12], [17], the *interoperability* and *portability* criteria are being met. Moreover, contrary to [16] we firmly hold that claims are provable in Sovrin through the use of ZKPs [17]. This holds despite the fact that no Proof-of-Work algorithm is used to reach consensus [11].

Protection of users' rights is not explicitly assured since no attestation is present regarding the correct functioning of each node in the network [8]. Lastly, there is no guarantee regarding the *usability* aspects of this solution. Sovrin states that new solutions will be introduced as more individuals and organizations join them [18].

5.2 reclaimID

reclaimID is an architecture that utilizes a name system to store and retrieve data which could potentially be implemented using blockchain [13]. Since certain characteristics are contingent upon implementation details we will examine the cases of using GNS and Namecoin.

reclaimID enables the creation of a digital identity *(existence)* alongside the self-attestation of attributes related to that identity without the need for a centralized service provider [13]. Users can add, delete and update their attributes and "selectively authorize and revoke access of requesting parties to subsets of their attributes" [13]. Therefore the *access*, *control* and *consent* criteria are satisfied. Furthermore, the identity and the accompanying attributes aside from being stored locally , are also disseminated in a decentralised maner both in the GNS and in the Namecoin case. Thus, the danger of a third party exercising coercive power over users is mitigated, hence, satisfying the *protection* requirement.

Access of a third party to the attributes that the user has disclosed and encrypted is possible either through the chosen namesystem or via an out-of-band exchange (e.g. by using a web-based authentication protocol) [13] providing the necessary *portability* to the implementation.

Since the reclaimID architecture is open-source, *transparency* is achieved in every component of the system when open-source name systems, like Namecoin and GNS, are used. By harnessing a well-established blockchain solution for the name system component of the system, *persistence* is present. It is underlined that this property is dependent upon the particular name system choice. Identities and their attributes are also *portable* in this architecture [13].

The attributes are user-defined so they could be used in any context for authentication thus satisfying the *interoperability* criterion. Moreover, ZKPs can be used to *minimize* the disclosure of claims [13]. However, attributes are self-signed in reclaimID hence the claims made are provable, to the extent that we trust the user. We need to highlight that implementation where third-party verification of claims is enabled [13] is entirely possible. The decentralized and open-source nature of the reclaimID architecture enables a multitude of implementations to take place. However, currently, usability is a definite hurdle for adoption.

5.3 did:self and IPFS

The last proposal we will explore was presented in *Enabling self-verifiable mutable content items in IPFS using Decentralized Identifiers* [7] and although it was not originally intended as an SSI implementation we feel that it combines several characteristics that make it favorable to such usage.

By leveraging the did:self method [6] each user can create and sign attributes for oneself in a similar fashion that reclaimID proposes. Since users are responsible for the creation of the metadata and the signing of the DID document in addition to the documents' storage, *control*, *access*, and *consent* are satisfied. *Transparency* is also present due to the open-source nature of the did:self method and IPFS's protocols. Claims that are disseminated through IPFS remain valid for the period defined in the `expires` property inside the proof section of the self-verifiable content item, thereby, achieving *persistence* and *portability*.

The *minimalization* criterion is met by creating and dissem-

Table 1: A summary of analysis based on SSI principles

Evaluation criteria	Sovrin	GNS	NC	did:self
1. Existence	✓	✓	✓	✓
2. Control	✓	✓	✓	✓
3. Access	✓	✓	✓	✓
4. Transparency	✓	✓	✓	✓
5. Persistence	✓	✗	✓	✓
6. Portability	✓	✓	✓	✓
7. Interoperability	✓	✓	✓	✓
8. Consent	✓	✓	✓	✓
9. Minimalization	✓	✓	✓	✓
10. Protection	✗	✓	✓	✓
11. Provable	✓	✓	✓	✓
12. Usability	✗	✗	✗	✗

A table cell with ✓ indicates that we found evidence that a system complies with a specific requirement, and a cell with ✗ indicates that a system does not fully comply with a specific requirement. reclaimID with GNS is marked on the GNS column. reclaimID with Namecoin is marked on the NC column.

inating a separate did:self for each claim that a user would make. This might look cumbersome, however, it is remarkable that one could minimize the disclosure of claims without the need for ZKPs.

Protection and *interoperability* are given due to the decentralized nature of both IPFS and the sovereignty present in the process of creating a claim. What's more, claims are provable owing to the self-verifiable nature of the did:self method [7]. *Usability*, however, is a thorny issue since a certain degree of technical comprehension is required to fully utilize the capabilities of this solution.

6 Conclusion

Our paper inquires into whether blockchain technology is necessary for SSI implementations. By reviewing three systems we conclude that blockchain can be helpful in meeting specific SSI criteria, however, it is not necessary. In particular, *persistence*, *access*, and *transparency* are likely guaranteed through the use of a well-established blockchain. We also gather that through the use of the did:self method [7] disclosure of claims is minimized without using ZKPs. In addition, we hold that the 12-point system of evaluation we proposed encapsulates all necessary attributes that an SSI solution must satisfy.

It is worth mentioning that adequate usability is absent in all implementations. This proves that even though there may exist solutions that fulfill the SSI criteria from a technical standpoint, nonetheless, they fail to provide value because of a lack of attention to user experience. These findings are consistent with [3] who also emphasizes the need for more intuitive implementations.

Future research, among other things, could explore ways to allow third-party entities to sign claims regarding reclaimID and did:self systems. We also hold that, from a usability standpoint, seamless smartphone integration and wide usage of QR codes should serve as a building block for a satisfactory user experience. In the end, if a system isn't usable, it isn't secure.

References

[1] Allen, C. The path to self-sovereign identity. *Life with Alacrity* (2016).

[2] Dhamija, R., and Dusseault, L. The seven flaws of identity management: Usability and security challenges. *IEEE Security Privacy 6*, 2 (2008), 24–29.

[3] Dunphy, P., and Petitcolas, F. A. A first look at identity management schemes on the blockchain. *IEEE Security and Privacy 16*, 4 (2018), 20–29.

[4] ENISA. Glossary: Pubic key infrastructure. https://www.enisa.europa.eu/topics/incident-response/glossary/public-key-infrastructure-pki, 2022.

[5] Feige, U., Fiat, A., and Shamir, A. Zero-knowledge proofs of identity. *Journal of cryptology 1*, 2 (1988), 77–94.

[6] Fotiou, N. did:self method specification. https://github.com/excid-io/did-self, 2021.

[7] Fotiou, N., Siris, V. A., and Polyzos, G. C. Enabling self-verifiable mutable content items in IPFS using Decentralized Identifiers. *2021 IFIP Networking Conference, IFIP Networking 2021* (2021).

[8] Joosten, R. A conceptual analysis on sovrin. Tech. Rep. R10161, TNO, The Hague, Netherlands, 01 2018.

[9] Kameron, C. The laws of identity. https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf.

[10] Mahula, S., Tan, E., and Crompvoets, J. With blockchain or not? Opportunities and challenges of self-sovereign identity implementation in public administration: Lessons from the Belgian case. *ACM International Conference Proceeding Series* (2021), 495–504.

[11] Reed, D., Law, J., and Hardman, D. The technical foundation of sovrin:a white paper from the sovrin foundation. https://www.evernym.com/wp-content/uploads/2017/07/The-Technical-Foundations-of-Sovrin.pdf.

[12] Satybaldy, A., Nowostawski, M., and Ellingsen, J. *Self-Sovereign Identity Systems: Evaluation Framework.* 03 2020, pp. 447–461.

[13] Schanzenbach, M., Bramm, G., and Schutte, J. ReclaimID: Secure, Self-Sovereign Identities Using Name Systems and Attribute-Based Encryption. *Proceedings - 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE 2018* (2018), 946–957.

[14] Schanzenbach, M., Grothoff, C., and Fix, B. The gnu name system, 2020.

[15] Stokkink, Q., and Pouwelse, J. Deployment of a Blockchain-Based Self-Sovereign Identity. *Proceedings - IEEE 2018 International Congress on Cybermatics: 2018 IEEE Conferences on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, iThings/Gree* (2018), 1336–1342.

[16] van Bokkem, D., Hageman, R., Koning, G., Nguyen, L., and Zarin, N. Self-Sovereign Identity Solutions: The Necessity of Blockchain Technology. 1–8.

[17] Windley, P. J. How sovrin works: A technical guide from the sovrin foundation. https://sovrin.org/wp-content/uploads/2018/03/How-Sovrin-Works.pdf.

[18] Windley, P. J. The inevitable rise of self-sovereign identity:a white paper from the sovrin foundation. https://sovrin.org/wp-content/uploads/2018/03/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf.