Self-Sovereign Identity Technology

Subjects: Computer Science, Theory & Methods

Contributor: Abylay Satybaldy , Anushka Subedi , Mariusz Nowostawski

Self-sovereign identity (SSI) is a set of technologies that build on core concepts in identity management, blockchain technology, and cryptography. SSI enables entities to create fraud-proof verifiable credentials and instantly verify the authenticity of a digital credential.

SSI blockchain technology decentralization digital identity self-sovereign identity

1. Introduction

Self-sovereign identity (SSI) is a new model of identity management that builds on core concepts of decentralization, distributed ledger technology and cryptography, and holds the potential to make the existing systems more secure, efficient, interoperable, and user-centric. It is a new paradigm that enables individuals to have complete control over how their personal information and data is stored, shared and used. In essence, SSI allows individuals to manage their own digital documents and credentials. It also allows organizations to define their own business processes and workflows without having to rely on third-parties and central authorities. This makes SSI a powerful tool for organizations looking for self-sovereign solutions in the digital world.

2. Self-Sovereign Identity

SSI is a set of technologies that move the control of digital identity from third parties directly to individuals. In the centralized and federated identity models, the locus of control is with the issuers and verifiers in the network. In the decentralized SSI model, the locus of control shifts to the individual user, who can now interact with everyone else as a full peer [1]. This relation is presented in **Figure 1**.

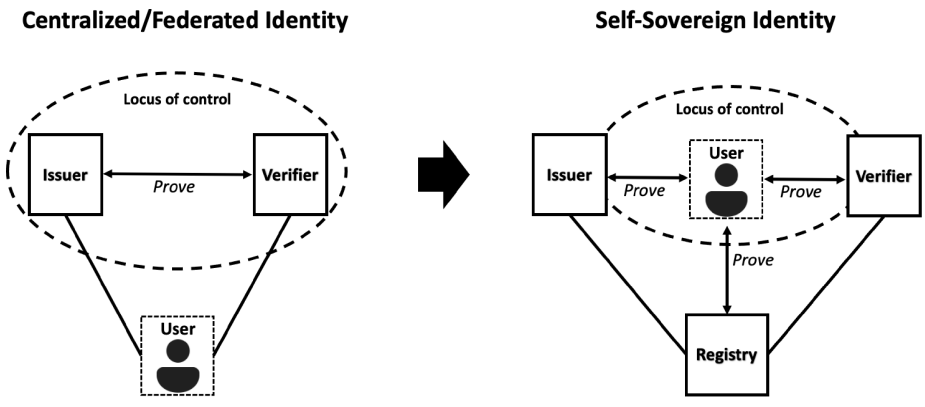

Figure 1. Shift of control with SSI.

SSI holds the potential to address current issues of digital identity in order to make the system secure, trustworthy, easier to use and interoperable. It does this by leveraging blockchain technology and by introducing a decentralized infrastructure to minimize trust in third parties. The sole ownership over the ability to control the user's personal data is handed to the user in SSI. The users can then store their credentials on their devices and provide it for verification and transaction without the need to rely upon the central authority [2]. Trusted third parties thus only act as an issuer of credentials on request by the subject and cannot learn with whom or when subjects share their credentials. The SSI, in theory, thus guarantees data minimization and data control.

In addition, SSI technology is unique in a way that it serves as a digital analog for identification in the physical world. The strength of identification in the physical world is that the credential is always with the owner (such as a driving license) and is legally and practically recognized as a valid proof of identity (signature of the issuer and picture of the owner), and most importantly, it is always shared between the identity owner and the verifier without the knowledge of the issuing party.

The SSI space is growing exponentially and there are different groups and standardization agencies working to develop new standards and protocols which could be the base of the SSI model. These efforts come from agencies such as the Decentralized Identity Foundation (DIF), the European Blockchain Services Infrastructure (EBSI), the Internet Engineering Task Force (IETF), Sovrin, ISO, the OpenID Foundation (ODIF), and the World Wide Web Consortium (W3C) [3]. To date, the two fundamental base standards for self-sovereign identities are decentralized identifiers (DIDs) [4] and verifiable credentials (VCs) [3] by the W3C. The DID and VC standards propose a common data model for unique identifiers and credentials for self-sovereign identity solutions.

3. Decentralized Identifiers

A DID is a new type of identifier that is decentralized, globally unique, resolvable, and cryptographically secure. It differs from other types of identifiers in that it can exist without the involvement of any certificate authorities, third parties, providers, or centralized identity registers.

A DID is expressed as a URI scheme; an example of a DID is "did:example:12345". A DID is made up of three parts that are separated by colons. The "did" part of this DID represents that it is a DID, "example" is the DID method, and "12345" is the method-specific identifier that is used to distinguish this DID from other DIDs with the same method. The DID can be stored as a DID document on a blockchain or other storage system.

The DID document contains all the information required to authenticate, authorize, or interact with the subject of the DID, such as the cryptographic material and public keys. It may also contain service endpoints that describe a mechanism on how the DID subject is reached and establishes trusted communication. A DID document can be serialized in either the JSON or JSON-LD format [5]. The location of where the document is stored depends on the used DID method and may be stored either on-chain, meaning that the document is written to a blockchain, or off-chain, meaning that the document is not written to the blockchain and stored somewhere else.

The DID method describes how to resolve a DID to its associated DID document. It also specifies the operations that could be made to the document, such as how the document can be modified by the DID controller. In simple terms, a DID uses the DID method to resolve a document (DID document) that describes the subject (DID subject) to which the DID refers to and it is controlled by the DID controller. There are many different DID methods currently available, and Fdhila et al. [6] evaluated some of them, including an analysis of their qualities.

4. Verifiable Credentials

The VC data model was adopted as a standard in 2019 by the W3C. It is used to build trust between the involved parties in an SSI ecosystem, which often includes an issuer, holder, verifier, and verifiable data repository. A common procedure among the roles is that the issuer first offers the holder a VC. The credential is used by the issuer of a credential to make claims about a credential subject. A credential can hold many claims about a subject. The issuer is responsible for creating and specifying the credential's content as well as the verification method. The verifiable credential is typically held by the credential subject, who then stores it in a digital wallet and is referred to as the holder of the credential. The credential subject can then present these claims to the verifier upon request to prove something about themselves. Lastly, the verifier then validates that the credential has not been tampered with and was issued by a trustworthy issuer, in addition to its own policy, to determine the credentials validity. The verification process can be carried out without involving the issuer directly.

A VC is made up of three main parts. First, there are the credential metadata, which consist of information that describes the credential such as credential type, who issued the credential, when it was issued, and when it expires, as well as a context property that permits an agreed-upon understanding of the credential and its structure and can be processed by JSON-LD. Second, the credential can contain statements about the credential subject in the form of one or more claims expressed as property–value pairs in the credential. Last but not least, it contains proof(s) that enable(s) the credential to be cryptographically verifiable using digital signatures. A verifiable credential can be serialized in JSON or JSON-LD, with the proof format being JWT or Linked Data.

Verifiable credentials are typically used in conjunction with decentralized identifiers to make attestations about a certain DID subject issued by a trusted DID. When presenting and validating a credential, it may be necessary to demonstrate that the holder is also the credential's subject. Because a DID is bound to a VC via the credential subject attribute, the prover can show possession of the private key corresponding to this DID to a verifier by including verifiable credentials inside a verifiable presentation signed with this key. A device that stores verifiable credentials should also have adequate security features, such as enabling device passwords, pins, biometric data, or multi-factor authentication to protect against unauthorized use.

A verifiable presentation (VP) [7] contains data that can be cryptographically verified and is commonly used to encapsulate one or more VCs. It could also include zero-knowledge proof (ZKP)-derived data and selective disclosure. In addition, the proof on the VP is often used for authenticating the holder.

5. Distributed Ledger Technology

Distributed ledger technology (DLT), often known as “blockchain”, is the technology underpinning decentralized databases that allows users to govern the generation of data across entities via a peer-to-peer network, using consensus techniques to ensure data replication among nodes [8]. SSI was born as a result of blockchain technology providing an exciting new way to establish a decentralized public key infrastructure [1]. In SSI, the blockchain acts as a replacement for the registration authority in classic identity management systems where the pairing of identification and authentication is maintained [9]. In other words, the blockchain acts as an immutable record of data used to store the public DID of the organization who issued the credential. The verifying parties can then utilize the blockchain’s infrastructure to check the authenticity of the attestation and attesting party (such as the government) from which they can determine whether to confirm the proof instead of checking the validity of the actual data in the presented evidence. An example of this could be when a holder presents a proof of their date of birth, instead of checking the accuracy of the date of birth, the verifying party will validate the government’s signature that is issued and attested to the credential. The verifier can then decide whether they trust the government’s assessment of the data’s accuracy. The first blockchain designed specifically to support SSI was created in 2016 by Evernym [10] as an open-source codebase for public permissioned ledger with all nodes controlled by trusted institutions. The codebase was subsequently contributed to the Sovrin Foundation hosted by the Linux Foundation [11], where it became Hyperledger Indy which has transaction and record types that make DID management easy. At present, the majority of SSI systems utilize the blockchain technology including Serto (Ethereum) [12], ION (Bitcoin) [13], Trinsic (Sovrin) [14], and SpruceID (Tezos, Polygon and Ethereum) [15]. From an academic research perspective, blockchain-based SSI systems are also gaining a lot of attention to introduce new solutions for digital identities [16][17][18][19][20].

Other traditional databases, such as DID registries, could also be considered for SSI. However, such databases are neither self-service nor censorship resistant. Furthermore, trust in most of these databases is based on centralized administrators whose interests may differ from those of the people they identify. In addition, when a third-party mediator knows every login or interaction, privacy is questioned. Thus, SSI is still strongly linked with blockchain technology because it requires a neutral platform that provides governance, standards, and essential public information to check the validity of attestations [21].

6. Digital Wallet and Agent

A digital wallet is software or hardware that is responsible for securely storing identity data and cryptographic content. In the context of SSI solutions, this includes storing VCs, DIDs, and the associated cryptographic keys. An SSI digital wallet should implement open standards for portable, self-sovereign VCs and other sensitive private data [1]. This means that the wallet should accept any standardized VC irrespective of the vendors and thus should have the same basic experience no matter what wallet is used. In addition, the user should be able to install the wallet on any device that they use regularly and should be able to back up and move the content to another digital wallet as required. Moreover, an SSI wallet should work with a digital agent to form connections and exchange credentials. An agent acts on behalf of the user and can communicate with other agents to do various actions; it

typically accesses the digital wallet for storing and retrieving information to perform cryptographic operations. Depending on the usage, these actions can be programmed to be executed automatically by the agent or manually by the user. Furthermore, the agent can operate on an edge device or in the cloud.

References

1. Preukschat, A.; Reed, D. Self-Sovereign Identity; Manning Publications: Shelter Island, NY, USA, 2021.
2. Stokkink, Q.; Ishmaev, G.; Epema, D.; Pouwelse, J. A Truly Self-Sovereign Identity System. In Proceedings of the 2021 IEEE 46th Conference on Local Computer Networks (LCN), Edmonton, AB, Canada, 4–7 October 2021; pp. 1–8.
3. The World Wide Web Consortium (W3C). Verifiable Credentials Data Model v1.1. 2022. Available online: https://www.w3.org/TR/vc-data-model/ (accessed on 8 June 2022).
4. W3C Credential Community Group. Decentralized Identifiers. 2022. Available online: https://www.w3.org/TR/did-core/ (accessed on 13 May 2022).
5. The World Wide Web Consortium (W3C). JSON-LD 1.1. 2020. Available online: https://www.w3.org/TR/json-ld11/ (accessed on 28 May 2022).
6. Fdhila, W.; Stifter, N.; Kostal, K.; Saglam, C.; Sabadello, M. Methods for Decentralized Identities: Evaluation and Insights. Int. Conf. Bus. Process. Manag. 2021, 428, 119–135.
7. Decentralized Identity Foundation (DIF). DIF Presentation Exchange. 2022. Available online: https://identity.foundation/presentation-exchange/ (accessed on 18 September 2022).
8. Tykn. Self-Sovereign Identity: The Ultimate Beginners Guide! 2021. Available online: https://tykn.tech/self-sovereign-identity/ (accessed on 20 June 2022).
9. Mühle, A.; Grüner, A.; Gayvoronskaya, T.; Meinel, C. A survey on essential components of a self-sovereign identity. Comput. Sci. Rev. 2018, 30, 80–86.
10. Evernym. 2022. Available online: https://www.evernym.com/ (accessed on 18 September 2022).
11. Sovrin. Sovrin Glossary v2. 2020. Available online: https://sovrin.org/library/glossary/ (accessed on 23 July 2022).
12. Serto: Trust with Control. 2022. Available online: https://www.serto.id/ (accessed on 13 October 2022).
13. ION: Decentralized Layer 2 Open Permissionless Identity Network. 2022. Available online: https://identity.foundation/ion/ (accessed on 13 October 2022).

14. Trinsic: A Full-Stack Self-Sovereign Identity (SSI) Platform. 2022. Available online: https://trinsic.id/ (accessed on 23 July 2022).
15. SpruceID: Your Keys, Your Data. 2022. Available online: https://www.spruceid.com/ (accessed on 13 October 2022).
16. Stokkink, Q.; Pouwelse, J. Deployment of a blockchain-based self-sovereign identity. In Proceedings of the 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), Halifax, NS, Canada, 30 July–3 August 2018; pp. 1336–1342.
17. Ferdous, M.S.; Chowdhury, F.; Alassafi, M.O. In search of self-sovereign identity leveraging blockchain technology. IEEE Access 2019, 7, 103059–103079.
18. Shuaib, M.; Alam, S.; Alam, M.S.; Nasir, M.S. Self-sovereign identity for healthcare using blockchain. Mater. Today Proc. 2021.
19. Kondova, G.; Erbguth, J. Self-sovereign identity on public blockchains and the GDPR. In Proceedings of the 35th Annual ACM Symposium on Applied Computing, Brno, Czech Republic, 30 March–3 April 2020; pp. 342–345.
20. Dong, C.; Wang, Z.; Chen, S.; Xiang, Y. BBM: A blockchain-based model for open banking via self-sovereign identity. Int. Conf. Blockchain 2020, 12404, 61–75.
21. Schlatt, V.; Sedlmeir, J.; Feulner, S.; Urbach, N. Designing a Framework for Digital KYC Processes Built on Blockchain-Based Self-Sovereign Identity. Inf. Manag. 2021, 59, 103553.