Self-Sovereign Identity (SSI)

Subjects: Computer Science, Interdisciplinary Applications

Contributor: Parul Agarwal , Mohammed Shuaib , Noor Hafizah Hassan , Sahnius Usman , Shadab Alam , Surbhi Bhatia

Self-sovereign identity (SSI), a new concept, is becoming more popular as a secure and reliable identity solution for users based on identity principles. SSI provides users with a way to control their personal information and consent for it to be used in various ways. In addition, the user's identity details are stored in a decentralized manner, which helps to overcome the problems with digital identity solutions.

land registry SSI compliance identity principle

1. Introduction

A recent survey highlighted that 37% of employees in US firms reset their passwords more than 50 times each year and have been losing around 426 USD annually due to password glitches, in addition to the fact that this is affecting their efficacy at work [1]. Additionally, a world bank survey revealed that around 14% of the global population lacks proof of identity in any form [2][3]. Providing individuals with an identity and maintaining secure and reliable identity storage are major challenges. Compared with providing individuals with an identity, managing a secured and reliable identity is a far more significant challenge. In a recent incident, Cambridge Analytica leaked 87 million Facebook users' PII details due to a security breach in the system of a third-party service provider [3]. There are many examples of data breaches due to the centralized nature of data recordings and the use of third-party service providers. Digital identities and their security are becoming more critical with the advancement and adaptation of online services.

The land registry system provides a way to transfer land ownership while protecting the rights of the people, which increases the trust among people. There are numerous loopholes in the current land registry system which pose risks for crimes such as land stealing or force land-grabs, resulting in most civil court cases. Most of these cases take months, years, or even decades to resolve since they go from local courts to the Supreme Court. Plus, majority of people in the country do not have the time and money they would need to spend on these cases [4][5].

The main problem with the current system is inadequately coordinated information across different government departments that are not coordinated adequately, making it easy for unscrupulous officials to modify official land records. Many fraud cases related to land titling are only detected locally, which means that a centralized system is insufficient in this case [6]. As a result, land records may be tampered with, and forged.

Verifying the identity of all participants in a transaction is essential to avoid fraud [7]. Current land registry systems have several shortcomings which can be avoided by utilizing blockchain technology [8]. A limitation in blockchain-based land registry systems is the lack of suitable identity solutions [9][10][11]. The use of a digital identity in blockchain-based land registry systems saves time, decreases the fraud risk, and reduces data loss [12]. The SSI concept fills this gap by providing a decentralized identity and giving individuals complete control over their identities and personal data [13].

Self-sovereign identity (SSI) is a next-generation identity management model that secures and manages reliable identity records [14]. The identity records are stored in a decentralized manner and provide users with control over their identity details [15]. In this way, SSI can handle the shortcomings of traditional identity solutions. Users of SSI solutions have full control over their personal identity information (PII), and give their consent for using the PII. Therefore, the issues with the centralized storage and identity theft can be resolved [16][17]. SSI is a new paradigm, and several researchers are working in this domain to review it and analyze its applications; however, the academic literature is still limited. Some of the related literature can be found in [15][18][19][20]. In [18], the authors explored the concept of self-sovereign identity and presented its challenges and opportunities in a rather informal way. However, in [15][19][20][21], the authors focused on the application of self-sovereign identity to explore how a self-sovereign identity system could be built and developed.

SSI was designed based on Christopher Allen's ten identity principles. SSI solutions must adhere to the following principles: existence, control, access, transparency, persistence, portability, interoperability, consent, minimalization, and protection [22]. At present, several initiatives and government agencies are actively developing SSI solutions on the blockchain platform. Several blockchain-based SSI frameworks, such as Sovrin [1], uPort [23], Civic [24], Blockstack [25], Selfkey [26], and ShoCard [27], are available and are being used in various domains. A successful SSI solution needs to comply with all the SSI principles [19][28]. None of the existing self-sovereign identity frameworks fully comply with the SSI principles. There are several building blocks for the development of an SSI framework. These building blocks are also referred to as SSI components. To identify SSI components for the SSI framework in compliance with SSI principles.

The essential purpose of SSI for land registry is to provide people with IDs so that they may communicate with land management services. There are approximately one billion people who have no access to identifying themselves. SSI allows individuals to build a gradually more secured and trustworthy identity in place of a government-issued identification document by collecting certificates from reputable third parties, such as a land registry and financial institutions [29]. Even with the lack of legal documents, SSI can help the public to establish evidence of property ownership, such as a certified survey plan or a notarized declaration. The SSI's credentials should not be limited to only the digital equivalent of the traditional paper-based certificate, but should also provide a framework for transforming data into credentials that administrative entities can trust. For example, a person can submit proof of ownership claims utilizing their verified location history using a mobile carrier's location verification, transaction details and land registry certificates [30].

In the absence of land registries, SSI may directly connect people to land plots while also providing a means for recording property claims and related data to gain access to additional services such as banking, loans, and government benefits. SSI holders can use a verifiable claim to land ownership. Individuals could submit a digital title to seek financial aid or agricultural subsidies. A verifiable claim is a permanent document established by a government institution that acknowledges the rights of a property owner at a specific point in time. The provable verifiable claim will be kept, even if property certificates are lost or the owners relocate [31][32].

2. Self-Sovereign Identity (SSI)

SSI solutions allow users to gain control over their personal identities. Users will decide precisely what information they need to reveal about themselves, to whom, and in which contexts. Under the SSI model, no one can prohibit a person from exercising basic human rights, such as the right to be expression and privacy. Individuals do not need to retain their identities physically. They can choose any identity operator. The pre-requisite for SSI is that digital identities must be scalable and interoperable across different platforms. Therefore, individuals are free to choose the identity operator and switch from one operator to another [33][34]. While no clear definition of SSI exists so far, a set of requirements have been defined as the key principles needed to function as an SSI [22]. These principles can be regarded as a criterion to check the existing identity solution to comply with these principles.

- Existence: Users have an independent existence and are not dependent on the details found in their digital identifiers.
- Control: Users have full control their identities and be able to transform, update, refer and hide them. Users have full authority to disclose or choose privacy on their identity details.
- Access: Individuals should have access to their data and should have the ability to be able to retrieve it when necessary.
- Transparency: Systems and algorithms used to handle and run digital identities must be accessible and transparent. The public must be able to track the operation and maintenance of the system.
- Persistence: The identity must be long-lived, and the individual's identity must be preserved for as long as the individual wants.
- Portability: Information and resources concerning identity must be transportable, and not owned by a single third party, even though they are trusted.
- Interoperability: Identities are available for common use in all contexts instead of being limited to one siloed environment.
- Consent: Individuals should give consent to use their identities. The data sharing by third parties must occur with the consent of the data subject.

- Minimization: The disclosure of claims should be kept to a minimum and should only be disclosed when necessary to perform a task.

- Protection: The individual‘s right to privacy must be protected at all costs, even though this would go against the identity providers’ interests.

These principles would benefit the users and form the basis of the SSI solution and need compliance to provide an SSI solution to the users [22]. None of the SSI solutions today comply with all these principles [35]. Several competing SSI solutions have emerged during the development process, adopting various ideas and using different blockchains [36][37]. In [38], the authors reviewed the available SSI solutions based on blockchain and discuss their implementations concerning the SSI principles. An analysis of the SSI concept’s potential and evaluation of blockchain-based SSI solutions, namely Sovrin, Multichain, Blockstack and uPort has been carried out [39]. Comparative analyses of uPort and Sovrin were performed by reference [40]. A detailed analysis of the ShoCard Sovrin, Civic and uPort was carried out. These systems use certain decentralization techniques based on the author’s criteria and principles, none of which complied with the SSI requirements [35]. However, it is still rare for SSI systems to be compared with the SSI design principles. Therefore, to fill this gap in the next section, the researchers compared the existing blockchain-based self-sovereign identity (BC-SSI) solution uPort, Sovrin, Civic and ShoCard on the principle of SSI to identify whether the existing BC-SSI solution complies with the SSI principles or not.

3. Comparison of Self-Sovereign Identity Solutions on the SSI Principle

There are several SSI solutions available based on the blockchain platform. Only uPort, Civic, ShoCard, and Sovrin have been shortlisted for comparison because of their innovative SSI identity management approaches. These SSI solutions cover the broader landscape of BC-SSI solutions. The analysis for each selected SSI solution to comply with the SSI principles is shown in **Table 1**. First, the analysis with uPort, which is an identity and communication platform based on the Ethereum blockchain [23], was conducted. Second, the Sovrin Foundation has set out to standardize and implement the SSI architecture using blockchain so that anyone can issue and verify [1]. Third, Civic offers an SSI ecosystem to allow low-cost and reliable access to identity verification and customer know your customer (KYC) processes [24]. Finally, the ShoCard-based identity ecosystem provides authentication, an attestation to the credentials, and proper authentication [27].

4. Steps and Requirements for SSI Adoption

For adopting and standardizing any new technology, there are several guidelines and regulations prescribed by government agencies and autonomous institutions authorized for standardizing such technologies. There is a range of guidelines for developing a digital identity framework. Some of the sources are International Telecommunication Union (ITU) [41], Financial Action Task Force (FATF) [42], European Union [43] and the Open Identity Exchange (OIX) [44]. Although these guidelines were not exclusive to self-sovereign identity, they also refer

to the SSI application. Identity systems may be classified into three groups, depending on the legislation's origins that define liability. There are three types of identity structures [44]. The Digital Identity Level I scheme is the law applicable to all digital identity solutions. Tier II is a public law applicable only to certain jurisdictions. Tier III is a contract law that many businesses are complying with. The type of digital identity scheme, according to the OIX, is shown in **Table 2**.

Table 1. Digital identity scheme and governing laws as per OIX.

Source for Rules Regulating Liability	General Law	Identity-Specific Law	Contract-Based Rules
Level	1	2	3
Type of rule	Public Law	Public Law	Private Law
Usefulness	Everyone within the jurisdiction	Persons in ID system jurisdiction covered by the statute	Entities that adhere to the terms of the contract

Numerous steps are required to create a scalable, operational and autonomous SSI ecosystem. Such measures can differ based on the amount of government involvement. **Table 3** shows the requirements for the governments to adopt the SSI model. Many governments allow users to use digital identities at the national level. In Estonia, the national ID card system offers access to all electronic facilities, such as banking, and is used by 98% of the population [45].

Table 2. Requirement for the adoption of SSI by governments.

S.No	Requirements	Description
1	Creating a trustworthy registry	The government shall establish and manage the public register. If people want to use a blockchain network, they need to define who can join the network and who can not.
2	Build new digital wallets	Certain government organizations have been granted the authority to trusted digital wallets providers.
3	Attractions of individuals	The government would allow its citizens to register their digital IDs for government-based services to promote e-government services.
4	Development of DIDs	The government would require one DID method and allow wallet providers to use it.
5	Identification of standards	Recognition of decentralized identifiers and verifiable credentials must be adopted by world leaders such as ISO, ITU, IEEE or NIST.
6	Issuing of verifiable credentials/certifications	The government will develop relevant systems and protocols for issuing digital ID documents (e.g., a digital passport).
7	Acceptance by service providers	The authentication of SSI-compliant digital identities is more convenient for service providers because they can verify customers more easily, more

S.No	Requirements	Description
		effectively and with higher security levels.

l services chain and trust lists using a self-sovereignty strategy. The government will no longer have the responsibility of verifying to make sure that the certificates are valid. In the SSI system, the government only needs to issue digital certificates and register cryptographic proofs in certificates in a public and decentralized network, removing the government's need to maintain additional infrastructure [46][47]. Individuals will have full control over the sharing of data. The government does not need to validate and authorize digital credentials issued by government agencies explicitly.

References

1. Windley, P.; Reed, D. SovrinTM: A Protocol and Token for Self-Sovereign Identity and Decentralized Trust; Sovrin Foundation: Provo, UT, USA, 2018; Available online: https://sovrin.org/wp-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf (accessed on 1 August 2020).
2. World Bank. ID4D 2018 Global Dataset; World Bank Group: Washington, DC, USA, 2018; Available online: https://id4d.worldbank.org/global-dataset (accessed on 21 December 2020).
3. Idrees, S.; Nowostawski, M. Transformations through Blockchain Technology; Springer: Berlin/Heidelberg, Germany, 2022.
4. Toaha, M.; Khan, S. Automated digital archive for land registration and records. In Proceedings of the 11th International Conference on Computer and Information Technology, Khulna, Bangladesh, 24–27 December 2008; pp. 46–51.
5. Rahman, A.; Hossain, R. The uncomfortable truth about land disputes in Bangladesh: Insights from a household survey. Land Use Policy 2020, 95, 104557.
6. Rabbani, M.; Hossain, F. Digitisation of land administration. The Daily Star, 28 November 2019.
7. Antonio, T.; Lilyana, P. Directive (EU) 2018/843 of the European parliament and of the council. Off. J. Eur. Union 2018, 2018, 32.
8. Aslam, T.; Maqbool, A.; Akhtar, M.; Mirza, A.; Khan, M.A.; Khan, W.Z.; Alam, S. Blockchain based enhanced ERP transaction integrity architecture and PoET consensus. Comput. Mater. Contin. 2022, 70, 1089–1109.
9. Andrew, S.; Andrew, B. The Future of Real Estate Transactions. 2019. Available online: https://www.sbs.ox.ac.uk/sites/default/files/2019-03/FoRET-ReportSummary_0.pdf (accessed on 2 April 2022).
10. Krupa, K.S.; Akhil, M.S. Reshaping the Real Estate Industry Using Blockchain. In Lecture Notes in Electrical Engineering; Springer: Singapore, 2019; Volume 545, pp. 255–263.

11. Graglia, J.M.; Mellon, C. Blockchain and Property in 2018: At the End of the Beginning. Innov. Technol. Gov. Glob. 2018, 12, 90–116.
12. Idrees, S.M.; Nowostawski, M.; Jameel, R.; Mourya, A.K. Security aspects of blockchain technology intended for industrial applications. Electronics 2021, 10, 951.
13. Bouras, M.A.; Lu, Q.; Zhang, F.; Wan, Y.; Zhang, T.; Ning, H. Distributed Ledger Technology for eHealth Identity Privacy: State of The Art and Future Perspective. Sensors 2020, 20, 483.
14. Shuaib, M.; Hassan, N.H.; Usman, S.; Alam, S.; Bhatia, S.; Mashat, A.; Kumar, A.; Kumar, M. Self-Sovereign Identity Solution for Blockchain-Based Land Registry System: A Comparison. Mob. Inf. Syst. 2022, 2022, 8930472.
15. 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.
16. European Commission. Trends in Electronic Identification: An Overview; European Commission: Brussels, Belgium, 2018.
17. ESSIF. European Self-Sovereign Identity Framework; European Commission: Den Haag, The Netherlands, 2021.
18. Der, U.; Jahnichen, S.; Sürmeli, J. Self-sovereign Identity $-$ Opportunities and Challenges for the Digital Revolution. arXiv 2017, arXiv:1712.01767.
19. Baars, D. Towards Self-Sovereign Identity Using Blockchain Technology; University of Twente: Twente, The Netherlands, 2016.
20. Coelho, P.; Zúquete, A.; Gomes, H. Federation of Attribute Providers for User Self-Sovereign Identity. J. Inf. Syst. Eng. Manag. 2018, 3, 32.
21. Muhle, A.; Gruner, A.; Gayvoronskaya, T.; Meinel, C. A survey on essential components of a self-sovereign identity. Comput. Sci. Rev. 2018, 30, 80–86.
22. Allen, C. The path to self-sovereign identity. Coin Desk. 25 April 2016. Available online: http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html (accessed on 18 May 2020).
23. Lundkvist, C.; Heck, R.; Torstensson, J.; Mitton, Z. Uport: A Platform for Self-Sovereign Identity; Blockchainlab: London, UK, 2016.
24. Civic Technologies Inc. Civic Whitepaper. 2017. Available online: https://tokensale.civic.com/CivicTokenSaleWhitePaper.pdf (accessed on 13 January 2021).

25. Ali, M.; Shea, R.; Nelson, J.; Freedman, M.J. Blockstack: A New Internet for Decentralized Applications. Doylestown, United States. 2017. Available online: https://github.com/stacksgov/stacks-co (accessed on 2 August 2020).
26. SelfKey Foundation. Self-Sovereign Identity for more Freedom and Privacy—SelfKey. Selfkey. September 2017. Available online: https://selfkey.org/ (accessed on 13 April 2020).
27. Ebrahimi, A. Identity management verified using the blockchain. ShoCard, Tech. Rep. 2019. Available online: https://shocard.com/wp-content/uploads/2019/02/ShoCard-Whitepaper-2019.pdf (accessed on 22 April 2020).
28. Mehendale, D.K.; Masurekar, R.S.; Patil, H.V. Implications of Block Chain in Real Estate Industry. Int. J. Recent Technol. Eng. 2019, 8, 500–503.
29. Graglia, M.; Mellon, C.; Robustelli, T. The Nail Finds a Hammer Self-Sovereign Identity, Design Principles, and Property Rights in the Developing World. New America Weekly, 17 October 2018; p. 93.
30. Senturk, S. Future of property rights: Self-Sovereign Identity and Property Rights. New America Weekly, 12 June 2019; p. 2.
31. Shang, Q.; Price, A. A Blockchain-based Land Titling Project for the Republic of Georgia. Innovations 2018, 12, 72–78.
32. Piore, A. Can Blockchain Finally Give Us The Digital Privacy We Deserve? Newsweek 2019, 172, 1–16. Available online: http://ezproxy.library.yorku.ca/login?url=https://search.proquest.com/docview/2185863710?accountid=15182 (accessed on 14 November 2021).
33. Alam, S. Identity Model for Blockchain-Based Land Registry System: A Comparison. Wirel. Commun. Mob. Comput. 2022, 2022, 1–17.
34. Wang, F.; de Filippi, P. Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion. Front. Blockchain 2020, 2, 28.
35. Ellingsen, J. Self-Sovereign Identity Systems: Opportunities and Challenges. Master's Thesis, Norwegian University of Science and Technology, Trondheim, Norway, 2019.
36. Shuaib, M.; Alam, S.; Alam, M.S.; Nasir, M.S. Self-sovereign identity for healthcare using blockchain. Mater. Today Proc. 2021, 1–8.
37. Shuaib, M.; Alam, S.; Nasir, M.S.; Alam, M.S. Immunity credentials using self-sovereign identity for combating COVID-19 pandemic. Mater. Today Proc. 2021, 1–6.
38. van Bokkem, D.; Hageman, R.; Koning, G.; Nguyen, L.; Zarin, N. Self-Sovereign Identity Solutions: The Necessity of Blockchain Technology. arXiv 2019, arXiv:1904.12816.

39. Schaffner, M. Analysis and Evaluation of Blockchain-Based Self-Sovereign Identity Systems; Technical University of Munich: Munich, Germany, 2020.
40. Naik, N.; Jenkins, P. Governing Principles of Self-Sovereign Identity Applied to Blockchain Enabled Privacy Preserving Identity Management Systems. In Proceedings of the 2020 IEEE International Symposium on Systems Engineering (ISSE), Vienna, Austria, 12 October–12 November 2020; pp. 1–6.
41. Naik, N.; Jenkins, P. Digital Identity Roadmap Guide; International Telecommunications Union: Geneva, Switzerland, 2019.
42. The National Archives. Guidance on Digital Preservation; 2013. Available online: http://www.nationalarchives.gov.uk/information-management/projects-and-work/guidance.htm (accessed on 13 January 2021).
43. Lyons, T.; Courcelas, L.; Timsit, K. Blockchain for Government and Public Services. In Proceedings of the Eupopean union Blockchain Observatory & Forum, Brooklyn, NY, USA, 7 December 2018.
44. OIX. The Open Identity Exchange. 2019. Available online: https://openidentityexchange.org/members/anon/new.html?destination=%2Findex.html (accessed on 13 January 2021).
45. e-Estonia. e-Identity. 2019. Available online: https://e-estonia.com/solutions/e-identity/id-card/ (accessed on 13 January 2021).
46. López, M.A. Self-Sovereign Identity: The Future of Identity: Self-Sovereignity, Digital Wallets, and Blockchain; Inter-American Development Bank: Washington, DC, USA, 2020.
47. Bamasaq, O.; Alghazzawi, D.; Bhatia, S.; Dadheech, P.; Arslan, F.; Sengan, S.; Hassan, S.H. Distance Matrix and Markov Chain Based Sensor Localization in WSN. Comput. Mater. Contin. 2022, 71, 4051–4068.