International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Study Of Self-Sovereign Identity Management System Incorporating Blockchain

Dixa Koradia*[1], Dr. Vikram Agrawal[2]

Submitted: 06/05/2024 **Revised**: 19/06/2024 **Accepted**: 26/06/2024

Abstract: Self-sovereignty can be defined as having control over the specifics of your own identity. 'Self-sovereign identity (SSI)' solutions aim to give users the ability to manage their identity without the need for central authorities or intermediaries. One of the key technologies commonly used to implement SSI is decentralized ledger technology, such as blockchain. It is immutable and distributed ledger capabilities provide a robust foundation for identity verification, authentication, and data sharing. Through the use of cryptographic mechanisms and digital signatures, users can maintain ownership of their identity attributes and selectively disclose information as needed. The term 'identity management system (IDMS)' describes the procedure for identifying and authorizing users or persons to access corporate systems and services. Single points of failure cannot be reduced by conventional identity management and authentication systems because they rely so largely on a reliable central authority. In recent years, the field of IDMS has paid a lot of attention to Blockchain (BC) technology, which functions as a decentralized and distributed public ledger in a peer-to-peer (P2P) network. Overall, the survey provides valuable insights into the implementation of a blockchain-based SSI system. It contributes to the growing body of knowledge in the field of identity management and showcases the promising potential of blockchain technology in redefining the way we manage digital identities.

Keywords: *Identity Management, User Centric Identity, Blockchain Technology, Decentralized Ledger, Interoperable, Security Challenges, Verifiable Credentials*

1. Introduction

At the beginning, to define the term "identity". Identity is a central aspect of our everyday life, in the real world as well as in the online world. Due to its versatile applicability, identity exists in various forms which makes identity management very complex. The term "identity management system" (IDMS) refers to the process of identifying and authorizing users or individuals to access corporate systems and services. Traditional identity management and authentication systems often rely heavily on a central authority, leading to potential single points of failure. In recent times, the field of IDMS has shown considerable interest inBlockchain (BC) technology, known for its decentralized anddistributed nature in a peer-to-peer (P2P) network.

Self-sovereignty is the concept of individuals having full control over the specifics of their own identity. This includes the ability to share specific identity attributes and acquired credentials selectively based on the intended recipient of the information. This includes the user's ability to be able to share specific identity attributes and acquired credentials depending on the intended recipient of the information. The user will present a profile to the recipient, where the profile includes only those identity details required by the recipient for a particular operation. Self-sovereign identity (SSI) is a digital identity model that allows individuals to have full control and ownership over their personal information and digital credentials. Self-Sovereign Identity (SSI) empowers consumers to exercise complete control over their online identity. By effectively implementing a BC-based IDMS, the level of privacy and security for a user's SSI can be significantly enhanced.[1].

In this passage, a summary is given of the key contributions madein the paper. The paper delves into ecosystems for IDMS (IdentityManagement Systems) based on blockchain technology. We start by providing clear and concise explanations of blockchain technology and outline the progression towards decentralized approaches using Distributed Ledger systems.

2. Literature Review

This section includes key concepts regarding self sovereign identity and blockchain followed by theoretical framework and related work in digital IDMS framework.

2.1. Key Concepts

To get a better understanding of this concept some

[1]*Gujarat Technological University, Chandkheda, Ahmedabad 380001, Gujarat India*
ORCID ID: 0000-0003-4855-1998
[2]*CE Department, BBIT College, V. V. Nagar 388120, Gujarat, India ORCID ID: 0000-0001-9408-4919*
** Correcponding Author Email: dixadholakiya@gmail.com*

definitions and abbreviations are explained in more detail. Identity system: Electric information associated with an individual in a particular identity system is called a digital identity. Identity systems can beused for authentication and authorization of these identities [2]. Federated instance: or a federated identity in information technology is the process of linking a person's electronic identity and attributes, stored across multiple distinct identity management systems.

Personally identifiable information (PII): Any information that could potentially identify a person. Examples include full name, social security number and email address.

Distributed Ledger Technology (DLT): A distributed ledger is a consensus of replicated, shared, and synchronized digital datageographically spread across multiple sites, countries, or institutions.

Decentralized Identifier (DID): Independent self-controlled identifier used to resolve to a DID document containing all the

information required to interact with the identity.

2.2. Self-Sovereign Identity Framework

Self-sovereign identity (SSI) solutions aim to give users the ability to manage their identity without the need for central authorities or intermediaries. However, there remains a lack of organization in research regarding the integration of BC-based IDMS to provide users with SSI. Further exploration and study are needed to establish a systematic approach for offering self-sovereign identity through the integration of blockchain technology in identity management systems.[3]

One of the key technologies commonly used to implement SSI is decentralized ledger technology, such as blockchain. The SSI architecture is composed of seven key technologies defined by the W3C. The seven technologies are:[4] Decentralized Identifiers, Verifiable Credentials, Decentralized Public Key Infrastructure, Blockchain and Distributed Ledger Technology, Verifiable Data Registry, Agents, Digital Wallets the SSI framework has huge possibilities of implementations across manydomains where there is a drive toward individual privacy.[4] SSI brings greater privacy, security, and ownership to user data than previous identity models.[1]. Both offline and online, identityplays a significant role in our daily lives.

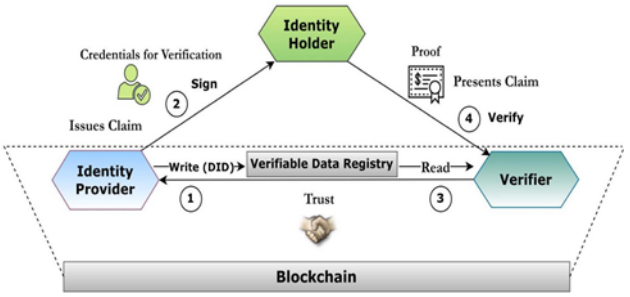

Fig. 1. Illustration of the roles in SSI with a credential flow[3]

However, it's essential to keep in mind that while SSI has great potential, its widespread adoption and standardization are stillevolving, and various projects and standards are actively being developed to realize its full potential.

The SSI framework can be described as a Peer-to- Peer model where entities with their independent identity act as a peer and make connections with others. Connections are used so people or organizations can attest information of others by issuing claims or credentials. Roles in SSI are the identity owner, credential issuers, verifiers or relying parties. Every entity can have each role in the system. The roles in SSI are illustrated in Fig 1.[3]

In step 1 ,Issuers give out credentials to make statements to othersor even themselves. Since credentials are used for verification in a Self-Sovereign Identity (SSI) system, the identity owner stores their self-attested information and credentials in a digital wallet instep 2. The wallet acts as an agent in the SSI ecosystem and allows the identity owner to have full control over their data. Issuers provide credentials, and if necessary, qualifications are not met, they can revoke these credentials.

In step 3 and 4 ,Identity owners can present their credentials or parts of them, along with self-attested claims, to verifiers. They have the freedom to disclose or withhold specific information as they see fit, giving them complete control over data sharing. Verifiers request the necessary information from identity owners, who must give consent before sharing it. Public information, like issuer DIDs and public keys, can be verified in public registries toprevent forgery.

Presentations of credentials can be created and verified without contacting the issuer, similar to presenting a physical ID in the real world. The underlying technology, often a blockchain or distributed ledger, serves as the root of trust, storing essential information for the SSI ecosystem, such as public DIDs or DID documents.[3][4]

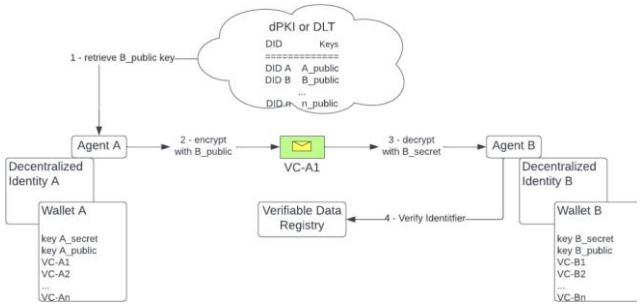

Fig. 2.SSI with a authentication flow with DID protocol[3]

Additionally, there might be an optional off-ledger backend-storage component. Some DID methods use this for storing information off the main ledger, such as DID documents, using permissioned or publicly available storage systems like IPFS. This off-ledger storage can also be used to back up wallet data for easy recovery in case of loss.

2.3. Blockchain for Self sovereign identity management

Everybody regularly uses their identity documents across many platforms, and these documents are shared with third parties without their express permission. Wrong authorisation is a significant risk in the identity management systems that are now in use, making them rarely secure. Users must identify themselves using one of several government-issued IDs, such as a national ID, a passport, a birth certificate, or a vaccination card. Sharing several IDs increases the risk of identity theft, and using numerous login and password combinations for various services on an online platform increases the risk of a data breach. For access privileges to various tiers of infrastructure, an IDMS must enable users to authenticate themselves first.[5] Here's how SSI can be implemented using blockchain:

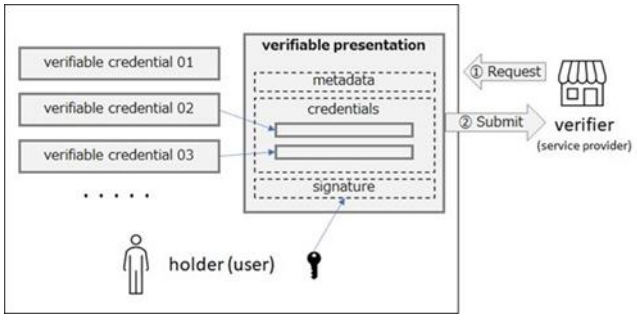

Fig. 3. SSI components:[6]

Decentralized Identity Management SSI solutions use a decentralized network to manage identity information. Instead of storing identity data in a central database, each individual has a unique digital identifier (usually a cryptographic key pair) associated with their identity.

Distributed Ledger The identity information is stored on a distributed ledger that is shared among multiple participants in the network. The ledger contains a chain of immutable blocks,and all participants can access and validate the data without relying on a single central authority.

Verifiable Credentials SSI relies on the concept of verifiable credentials. These are digital documents containing identity attributes or claims (e.g., name, date of birth, address) issued by trusted entities known as issuers. Verifiable credentials are cryptographically signed and can be verified by anyone using the issuer's public key.

Decentralized Identifiers (DIDs) DIDs are unique identifiers assigned to individuals in the SSI ecosystem. They are generated using cryptographic techniques and serve as the root of trust for an individual's identity. DIDs are designed to be self-owned and globally resolvable.

Selective Disclosure and Zero-Knowledge Proof With SSI, individuals have the capability to selectively disclose specific attributes or credentials to different parties without revealing unnecessary personal information. Zero-knowledge proofs play a vital role in allowing verifiers to verify the authenticity of credentials without accessing the underlying data,illustrated inFig 3.

Consent and Control Users have full control over their identity data and can decide whom to share it with and for what purpose. This enables better privacy and reduces the risk of data breaches and identity theft.

By combining blockchain's decentralized, immutable, and secure nature with cryptographic techniques for identity verification and selective disclosure, SSI on blockchain offers a user-centric, privacy preserving, and trustworthy approach to managing digital identities. It addresses many of the challenges faced by traditional centralized identity management systems and empowers individuals with greater control and ownership over their identity data.

2.4. Related Work

In 2016, Christopher Allen proposed ten guiding principles for SSI, and although it is a blog post, it is treated as a whitepaper in the area [8]. The ten principles are as follows. (SSI PRINCIPLES) The SSI paradigm focuses primarily on the user including the objective of bringing the control of the digital identity and its data back to the user. Allen coined the SSI paradigm by ten principles. The principles are categorized inTable 1.

Table 1. Allen's SSI principles are categorized by the sovrin foundation [9].

Security	Controllability	Portability
Protection	Existence	Interoperability
Persistence	Control	Transparency
Minimization	Consent	Access

Existence: The identity reflects a human user. The user is able to access digital services with support of the identity.

Control: The user exerts definite control about its digital identity and attributes. This characteristic differ- entities SSI from traditional models where the ultimate control resides with the IdP (cf. Section I).

Access: The user is always able to access the associated data of the identity. Especially, the user is fully aware of associated verifiable claims.

Transparency: Applications that support the user to manage its identity must be transparent in composition and management.

Persistence: The identity of a user should be enduring, and lasts as long as the user wishes it.

Portability: The user should be able to transfer its identity from one provider to another. There should be no lock-in to a single TTP.

Interoperability: The identity of a user should be as practicable as possible. This implies widespread usage at many SPs.

Consent: Usage of the identity and unveiling of attributes must only be allowed with the consent of the user.

Minimization: During the usage of the identity, especially when disclosing attributes, only a minimum amount of data must be disclosed to third parties. The principle of data economy should be adhered to.

Protection: The axiom of protection implies the precedence of user rights. In case of a conflict between the identity holder and the network, the decision should be in Favor of the identity holder. The usage of SSI solutions at the side of the SP should not compromise these principles. Thus, the SSI paradigm is not undermined.

2.4.1. Blockchain based SSI solutions

Sovrin: Sovrin is a public blockchain that's accessible to anyone without the need for prior authorization [9]. It's built on the permissioned Hyperledger Indy blockchain framework, meaning only verified nodes can participate in the consensus process. Sovrin uses a voting ledger system to grant permissions to nodes, which are categorized as validators and observers. Validators can add new transaction blocks to the blockchain, while observers canonly read data. To join the network, nodes, especially validators, must have unique privileges granted by a quorum of trustees. These trustees can elect new members and appoint stewards, who are trusted organizations responsible for consensus and validator node management. Sovrin enhances privacy by employingZero-Knowledge Proofs (ZKPs) for all valid identity claims, reducing data exposure [10].

Sora: Sora's identity solution uses blockchain technology based on JSON-LD standardized key-value pairs, enabling selective disclosure of information. Users can create multiple identities and store the private key using a master password [11]. Users have full control and access to their data, ensuring consent and protection against unauthorized access. The platform supports the issuance of verifiable claims by users.

uPort: uPort is a decentralized identity framework that aims to provide individuals with a decentralized identity . Its approach involves utilizing an open-source, public permission less Ethereum blockchain along with various smart contracts to uphold SSI. The framework incorporates a mobile application, several Ethereum smart contracts, and a public registry for uPort identities [12]. Through this system, users have the ability tosecurely reveal their identity by sharing credentials for various services, conducting transaction signings, as well as managing keys and data in a secure manner.

LifeID: LifeID is a SSI platform that allows users to create their independent online identities . Users have control over their identity data and can approve third-party requests for information, ensuring consent is always obtained. LifeID uses zero-knowledgeproofs to minimize data disclosure while providing secure verification[13]. Identity backup and recovery options protect against theft and provide users with the ability to deactivate and reactivate their identity.

EverID: EverID is a blockchain platform that prioritizes identity verification and value exchange, with a user-centric approach. Its main objective is to allow individuals to validate their identity, documents, and biometrics through third-party sources [13]. Additionally, it facilitates decentralized fund transfers among members of the network. In contrast to other SSI solutions available in the market, EverID does not rely on physical devices. Instead, it offers a secure

cloud-based storage solution for digital identities including biometrics and government-issued IDs.

SelfKey: SelfKey is a SSI network where users' data is stored on their devices, ensuring total control over their identity. Users can choose to reveal specific data to third parties through zero-knowledge proofs, meeting the consent and minimization requirements[14]. Identity authentication utilizes force-resilient, decentralized algorithms, and identity claims can be verified only by trusted entities.

Overall, these blockchain-based SSI platforms offer enhanced control, privacy, and security to users, making them promising solutions for identity management in a decentralized and trustless manner.

2.4.2. Non Blockchain based SSI solutions

PDS: Personal Data Storages (PDS) are environments that give users full control over the access of other parties. It offers both local and distributed online storage options. The data stored locally allows users to process queries on the PDS itself, ensuring control and minimal exposure of information. Online storage involves nodes communicating to protect against unauthorized access by distributing undecipherable data chunks across multiple storage nodes[14]. PDS lacks standardized formats for storing information, providing users with more control but limiting probability of identity.

IRMA: IRMA implements the Idemix attribute based credential scheme, allowing users to selectively disclose attributes received from trusted issuers. IRMA puts users in control over their digital identity, using zero-knowledge proofs to meet minimization requirements. However, losing a phone means losing identity attributes, affecting persistence[14].

Significant challenges perceived in the use of SSI are the vulnerabilities that can be found in the system components[15]. As some of these SSI components like digital wallets store all consolidated PII, an implementation software bug or exploitable system vulnerability, would result in significant personal and financial concern to the user.

Table 2. Comparison of this work with existing surveys and reviews. (Y: addressed, No: not addressed, NA: not applicable)

SSI Principles[1]	UPORT[12]	Sovrin[3]	Life ID[7]	Sora[18]	EverID[7]	SelfKey[5]
Blockchain	Ethereum	Hyperledger Indy	Ethereum	Hyperledger Iroha	Ethereum	Ethereum
Type of network	Public/private	Public/Private	Public	Private	Private	Public/Private
Existence	Y	Y	Y	Y	Y	Y
User Control	Y	Y	Y	Y	Y	Y
Access	Y	Y	Y	Y	Y	Y
Transparency	Y	Y	Y	Y	No	Y
Persistence	Y	Y	Y	No	Y	Y
Portability	No	No	Y	Y	Y	Y
Interoperability	Y	Y	Y	Y	Y	Y
Consent	Y	Y	Y	Y	Y	Y
Cost	Paid	-	Paid	Free for school	Paid	Paid
Minimization	No	No	Y	Y	No	Y
Open source Code Base	Y	Y	Y	Y	Y	Y

Table 3. Comparison of this work based on claimed properties of the analyzed blockchain implementations.applicable).

Blockchain Components	ID Management	Authentication	Trust	Security Attacks
uPort[12]	Attribute based,Group of Trustees	Wallet based Authentication and ZKP	Consensus mechanism-Proof of stack	smart contract vulnerabilities
Sovrin[3]	Manages by social recovery(no self management)	ZKP and Digital Signature	Plenum-Practical Byzantine Fault Tolerance	Vulnerabilities not Specified
Life ID[7]	Attribute based,Group of Trustees	ZKP with biometric master key	Consensus mechanism (Not Specified)	51% Attack,Sybil Attacks
Sora[18]	Set of Attributes only	Key pairs with hash,Master key	Sora Byzantine Fault Tolerance	Dictionary attack
EverID[7]	Set of attribute,PIN,biometric	Cryptographic algorithm	Consensus mechanism (Not Specified)	51% Attack,Sybil Attacks
SelfKey[5]	Not Provided	ZKP can be implemented	Consensus mechanism-Proof of stack	smart contract vulnerabilities
IRMA[14]	Key share server by IBM Zurich	ZKP and Key based digital signature	Non repudiation-attribute	DDos,Identity theft

3. Methodology

Given that decentralized identity, specifically Self-Sovereign Identity, is still in its early stages of development, the research field lacks a defined structure. In this study, we adhered to the following inclusion criteria.

When assessing SSI solutions, it is important to take into account the available schemes and frameworks. For our evaluation, we specifically examined SSI implementations on the Ethereum and Hyperledger Indy blockchains. However, when considering non-blockchain based platforms, we only looked at free options. In order to assess these solutions effectively, we utilized Allen's concepts as a benchmark for both blockchain-based and non-blockchain-based research studies. Our examination concentrated on several key factors including authentication, privacy, trustworthiness, security, and simplicity within blockchain technology.

At the conclusion of the study, it is crucial to accomplish several primary research goals:

(i) Discover a captivating research topic centered arounddecentralized and Self-Sovereign Identity.

(ii) Determine the quantity of decentralized identity solutions that incorporate the principles of Self-Sovereign Identity.

(iii) Identify various types of research conducted and the research methodology employed in pertinent academic papers.

(iv) Recognize domains and areas within IT that are explored in

relevant scholarly works.

4. Analysis and Discussion

The analysis findings, which are provided in Table 2, illustrate the similarities and differences in naming between different sets ofprinciples[9]. Each row in the table represents a specific characteristic, while each entry indicates how an SSI solutionfulfills it. Notably, uPort and Sovrin are two widely recognizedcommercial solutions for Self-Sovereign Identity (SSI). Inaddition to principles, the types of blockchain and network of the solution are specified. It has been observed that a majority of SSIsolutions have been implemented using ethereum and hyperledgerindy. Trust is a crucial aspect in the Self-Sovereign Identity (SSI)ecosystem due to its decentralized infrastructure where there is no central institution to establish trust. Table 3 presents comparisonsbased on blockchain components within the SSI ecosystem. Building trust within this ecosystem requires achieving accountability and ensuring reliable information that cannot betampered with - but this also poses one of the major challenges[8].Table 4 presents the implementation parameters ofthe SSI solution that should be taken into account for the survey. Trust cannot be solely established in decentralized systems byrelying on a single identity system. This is especially true when users can self-attest their identity attributes without any centralregistry to verify trustworthiness.[10] To address this issue, standardized, open-source, and transparent processes are implemented using technologies like blockchain or distributed ledger technology. These technologies enable the accurate management of Decentralized Identifiers (DIDs) andcryptographic signatures, effectively shifting the responsibility ofidentity management from centralized institutions to individualusers themselves.

Table 4. Comparison of experimental parameters of DID protocols for analyzed blockchain

Experimental Parameter	UPORT[12]	Sovrin[3]	Life ID[7][13]	EverID[7]
Decentralized identifier(DID)	W3C	W3C	W3C DID Spec	FIDO2
Verifiable Credentials	W3C	W3C Verifiable Credentials Data Mode	Smart Contracts	FIDO2
Authentication protocol	uPort Connect(uPort Network)	DIDComm	OpenID Connect	CTAP, WebAuthn
Decentralized wallet	Mobile Wallet	Sovrin Wallet	SmartPhone App	Web 3 Wallet
System	PKI	PKI	PKI	Extended PKI
SSI Standards	DIF	W3C,DIF	W3C	Web 3 based FIDO
Zero knowledge proof	Yes	As per W3C criteria	Yes	NA
DLT	Public Blockchain	Public Permissioned Blockchain	Public Blockchain/Permissioned	Public blockchain/permissioned access
SDK	uPort SDK	NA	OpenID SDK	Everkey SDK

5. Future Scope

5.1. Research challenges: Web of Trust

The concept of a Web of Trust is explored, where trust isestablished based on peer-to-peer relationships and interactions emphasizing the importance of community consensus and cooperation in establishing trust within the ecosystem. By adopting standardized and transparent processes, the SSI ecosystem aims to achieve a level of trust that enables secure and privacy-preserving interactions among users and verifiers, ensuring the protection of data from fraud, profiling, and attacks.

5.2. SSI security challenges

While Self-Sovereign Identity (SSI) holds great promise for improving identity management, like any technology, it also comes with certain vulnerabilities and challenges. Here are some key vulnerabilities associated with SSI:

Privacy Risks: While SSI is designed to enhance user privacy by allowing selective disclosure of information, improper handling of personal data or poor implementation can still lead to privacy breaches. Users must be cautious about sharing sensitive information and ensure that their digital wallets are adequately secured.

Key Management: The cryptographic keys used in SSI are criticalfor identity verification and authentication. If a user loses their private key, it could result in a complete loss of access to their digital identity and credentials. Proper key management and backup procedures are essential to avoid this risk.

Revocation Challenges: While SSI allows issuers to revoke credentials, ensuring that revoked credentials are promptly and accurately updated in all relevant systems can be challenging. Users and verifiers must have mechanisms to detect and handle revoked credentials.

Regulatory Compliance: Compliance with legal and regulatory frameworks can be complex in SSI ecosystems, especially when dealing with cross border interactions and adherence to various data protection laws.

Scalability: As SSI adoption grows, the system's scalability becomes a concern. Handling a large number of identity interactions on a blockchain or distributed ledger can lead toperformance issues.

Blockchain Security Risks: SSI systems built on blockchain technology may be vulnerable to attacks targeting the underlying blockchain network. This includes 51% attacks, smart contract vulnerabilities, and other blockchain-specific risks.

Interoperability Challenges: Different SSI platforms and implementations may use varying standards and protocols, leading to interoperability issues between different systems.

User Experience: The usability and user experience of SSI solutions can be a barrier to adoption. If the technology is difficult to use or requires a steep learning curve, users may be reluctant to embrace it fully.

Centralization of Identity Issuers: In some SSI ecosystems, the concentration of dominant issuers can create a power imbalance, limiting the true decentralization of the identity management system.

To address these vulnerabilities and challenges, ongoing research and development are needed to improve the security, usability, and scalability of SSI solutions. [24]Users, organizations, and developers should collaborate to implement best practices and security measures to protect against potential risks and ensure the successful and responsible adoption of Self-Sovereign Identitysystems.

6. Conclusions

Self-sovereign identity is an emerging trend that puts control of identity management into the hands of the individual. It allows users to create their own unique digital identities and services thatare tailored to their individual needs. As such, the SSI concept provides individuals with the power to build trust and secure transactions using a wide variety of tools including digital IDs, decentralized authentication, and biometrics.

Blockchain-based systems have been proposed as the best way to implement SSI systems, due to their decentralized, immutable, and tamper-resistant nature. The use of this technology in SSI systems offers numerous benefits including enhanced security, transparency, and integrity as well as faster and cheaper verifications and verifiable credentials.

While there are a number of challenges that need to be addressed, the potential benefits of self-sovereign identity systems offer great promise. As they continue to evolve, the SSI ecosystem willgain momentum. With the right tools, resources, and strategic investments, the SSI ecosystem can help further the vision of a self-sovereign Internet and improve online security and freedom.

Acknowledgements

This research was supported by the Gujarat Technological University (GTU). We thank Dr. Vikram Agrawal, Ph.D. Supervisor, for assistance with security , and comments thatgreatly improved the manuscript.

Author contributions

Author 2 took the lead in conceptualizing and overseeing the project's development, offering guidance and direction throughout the process. Meanwhile, Author 1 meticulously crafted the article, receiving valuable assistance and input from Author 2 during the implementation phase**.**

Conflicts of interest

The authors declare no conflicts of interest.

References

[1] Mauricio de Vasconcelos Barros, Frederico Schardong, and Ricardo Felipe Custódio. “Leveraging Self-Sovereign Identity, Blockchain, and Zero-Knowledge Proof to Build Privacy-Preserving Vaccination Pass”. In:arXiv (2202.09207) (Feb. 2022).

[2] Van Bokkem, Dirk, et al. "Self-sovereign identity solutions: The necessity of blockchain technology." arXiv preprint arXiv(1904.12816) (2019).

[3] Yang Liu et al. “Blockchain-based identity management systems: A review”. In: Journal of Network and Computer Applications 166 (2020)(1084-8045). p. 102731.

[4] Reece, Morgan, and Sudip Mittal. "Self-Sovereign Identity in a World of Authentication: Architecture and Domain Usecases."arXiv preprint arXiv: (2022)(2209.11647).

[5] Md. Rayhan Ahmed et al. “Blockchain- Based Identity Management System and Self- Sovereign Identity Ecosystem: A Comprehensive Survey”. In: IEEE Access 10 (2022), pp. 113436–113481.

[6] Vincent Schlatt et al. “Designing a Framework for Digital KYC Processes Built on Blockchain-Based Self-Sovereign Identity”. In: Information Management 59.7 (2022)(0378- 7206)p. 103553.

[7] Andreas Gruner, Alexander Muhle, and Christoph Meinel. “ATIB: Design and Evaluation of an Architecture for BrokeredSelf- Sovereign Identity Integration and Trust- Enhancing Attribute Aggregation for Service Provider”. In: IEEE Access 9 (2021), pp. 138553– 138570.

[8] Nitin Naik and Paul Jenkins. “Self-Sovereign Identity Specifications: Govern Your Identity Through Your Digital Wallet using Blockchain Technology”. In: 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud). (2020), pp. 90– 95.

[9] A. Tobin and D. Reed, ‘‘The inevitable rise of self-sovereign identity,’’ Sovrin Found., vol. 29, (2016), p. 18, Damiano Di Francesco Maesa et al. “Self sovereign and blockchain based access control: Supporting attributes privacy with zero knowledge”. In: Journal of Network and Computer Applications 212 (2023)(1084-8045) p. 103577.

[10] Makoto Takemiya and Bohdan Vanieiev. “Sora Identity: Secure, Digital Identity on the Blockchain”. In: 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC). Vol. 02.(2018)(10299.) pp. 582–587.

[11] Lundkvist, Christian, et al. "Uport: A platform for self-sovereign identity." URL: https://whitepaper. uport. me/uPort_ whitepaper_DRAFT20170221. pdf 128 (2017)pp. 214

[12] B. Reid and B. Witteman. (2018). EverID Whitepaper Decentralized Identity Platform.

[13] T. T. Tram Ngo et al. “A Systematic Literature Mapping on Using Blockchain Technology in Identity Management”. In: IEEE Access 11 (2023), pp. 26004–26032. doi: 10.1109/ACCESS. 2023.3256519.

[14] Samir, Efat, et al. "DT-SSIM: A decentralized trustworthy self-sovereign identity management framework." IEEE Internet of Things Journal 9.11 (2021)pp. 7972-7988.

[15] Čučko, Špela, et al. "Towards the classification of self-sovereign identity properties." Ieee Access 10 (2022)(3199414) pp. 88306–88329.

[16] Sampath, S., et al. "Decentralized Digital Identity Wallet using Principles of Self-Sovereign Identity Applied to Blockchain." 2022 IEEE 7th International Conference on Recent Advances and Innovations in Engineering (ICRAIE). Vol. 7.(2022)(2022.10054286_pp. 337–341.

[17] Mohameden Dieye et al. “A Self-Sovereign Identity Based on Zero-Knowledge Proof and Blockchain”. In: IEEE Access 11 (2023)(3268768) pp. 49445–49455.

[18] Hai Zhang and Feng Zhao. “Cross-domain identity authentication scheme based on blockchain and PKI system”. In: High-Confidence Computing 3.1 (2667-2952) (2023). 100096.

[19] Belchior, Rafael, et al. "A survey on blockchain interoperability: Past, present, and future trends." ACM Computing Surveys (CSUR) 54.8 (2021)(. 10.1145/3471140.)pp. 1-41.

[20] Sroor, Maha, et al. "How modeling helps in developing self-sovereign identity governance

framework: An experience report." Procedia Computer Science 204 (2022)(1877-0509) pp: 267-277.

[21] Saha, Rahul, et al. "A blockchain framework in post-quantum decentralization." IEEE Transactions on Services Computing 16.1 (2021)(.doi: 10.1109/TSC.2021.3116896) pp. 1-12.

[22] Ghirmai, Siem, Daniel Mebrahtom, Moayad Aloqaily, Mohsen Guizani, and Merouane Debbah. "Self-sovereign identity for trust and interoperability in the metaverse." In 2022 IEEE Smartworld, Ubiquitous Intelligence & Computing, Scalable Computing & Communications, Digital Twin, Privacy Computing, Metaverse, Autonomous & Trusted Vehicles (SmartWorld/UIC/ScalCom/DigitalTwin/PriComp/Meta),(202 2) (2303.00422)pp. 2468-2475.