International Journal of Advances in Electrical Engineering

E-ISSN: 2708-4582
P-ISSN: 2708-4574
IJAEE 2023; 4(2): 30-33
© 2023 IJAEE
www.electricaltechjournal.com
Received: 18-04-2023
Accepted: 20-05-2023

Sujeet Raosaheb Suryawanshi
Shri Jagdishprasad Jhabarmal Tibrewala University, Churu, Churela, Rajasthan, India

Dr. Prashant B Kumbharkar
JSPM's Rajarshi Shahu College of Engineering, Ashok Nagar, Tathawade, Pimpri, Chinchwad, Maharashtra, India

Dr. Shailesh Kumar
Shri Jagdishprasad Jhabarmal Tibrewala University, Churu, Churela, Rajasthan, India

Correspondence
Sujeet Raosaheb Suryawanshi
Shri Jagdishprasad Jhabarmal Tibrewala University, Churu, Churela, Rajasthan, India

Challenges and research opportunities in self sovereign identity

Sujeet Raosaheb Suryawanshi, Dr. Prashant B Kumbharkar and Dr. Shailesh Kumar

DOI: https://doi.org/10.22271/27084574.2023.v4.i2a.43

Abstract
Self-sovereign identity (SSI) has emerged as a promising concept in the field of digital identity management, offering individuals greater control and owner- ship over their personal data. This journal explores the challenges and research opportunities that accompany the implementation and adoption of self-sovereign identity systems. Through an examination of technical, regulatory, and societal aspects, this paper aims to shed light on the complexities of SSI and provide insights for future research directions in this evolving domain. Self-sovereign identity (SSI) systems are designed to grant individuals control over their personal data and identity information. At the core of SSI lies the principles of decentralization and interoperability, which aim to shift away from traditional centralized identity systems and enable seamless interaction between various SSI platforms. This section delves deeper into the challenges and research opportunities surrounding the concepts of decentralization and interoperability in the context of self-sovereign identity. Extensive initiatives have been undertaken to standardize self-sovereign identity (SSI) and its associated technologies. These endeavors are geared toward establishing a unified framework and a standardized set of proto- cols. The overarching goal is to facilitate interoperability and promote the broad adoption of SSI systems. Standardization efforts are pivotal in ensuring that SSI solutions can seamlessly integrate with various platforms and services, ultimately enhancing their accessibility and utility for users across diverse ecosystems.

Keywords: Self sovereign identity, identity management, OAuth

Introduction
The concept of self-sovereign identity (SSI) has gained traction as a potential solution to the pervasive challenges of digital identity management. SSI empowers individuals with the ability to control and share their personal information securely and selectively, thus reducing the risks associated with centralized identity systems. While the benefits of SSI are evident, there exist several challenges and unexplored research opportunities that must be addressed to realize its full potential.

Technical Challenges
Decentralization and Interoperability
Designing SSI systems that are both decentralized and interoperable presents' technical hurdles. Research is needed to establish standardized protocols and frameworks that allow SSI platforms to seamlessly interact while maintaining data integrity and user privacy [1].

Scalability
As SSI systems grow in adoption, ensuring their scalability becomes critical. Investigating novel approaches to handle a large number of users and transactions without compromising system performance and security is imperative [2].

Security and Privacy
While SSI systems offer enhanced privacy features, vulnerabilities such as identity spoofing and data breaches remain concerns. Exploring cryptographic techniques, zero- knowledge proofs, and robust authentication mechanisms can contribute to mitigating these risks [3].

Regulatory and Legal Challenges
Digital Identity Legislation
Digital Identity Legislation
The legal landscape surrounding digital identity and SSI is often complex and lacks uniformity. Researchers can delve into the development of harmonized legal frameworks that support SSI implementation across jurisdictions, while safeguarding individuals' rights and ensuring compliance with data protection regulations [4].

Liability and Accountability
Determining liability and accountability in SSI systems poses challenges, particularly in cases of identity-related fraud or errors. Investigating liability models and dispute resolution mechanisms within decentralized identity ecosystems is an area of potential research [5].

Societal and Adoption Challenges
User Education and Acceptance
Achieving widespread adoption of SSI requires users to understand its benefits and functionalities. Research can focus on designing effective educational campaigns and user-friendly interfaces that encourage user acceptance and trust in SSI systems [6].

Inclusivity
Ensuring that SSI systems are accessible to all individuals, including marginalized com- munities, is crucial. Exploring ways to bridge the digital divide and address potential biases within SSI implementations is an avenue for further investigation [7].

Research Opportunities
Usability and User Experience
Investigating ways to enhance the usability and user experience of SSI systems can drive greater adoption. This includes research on intuitive user interfaces, seamless integration with existing services, and minimizing user friction [8].

Decentralized Identity Ecosystems
Exploring the evolution of decentralized identity ecosystems beyond SSI presents intriguing research opportunities. This could involve the integration of block chain technology, distributed ledger systems, and decentralized identifiers (DIDs) for broader applications [9].

Interdisciplinary Collaborations
Collaborative research efforts between computer scientists, legal experts, policymakers, and sociologists can yield comprehensive insights into the multifaceted challenges of SSI and guide its development in a holistic manner [10].
Self-sovereign identity holds great promise as a transformative solution in the realm of digital identity management. However, the journey toward its widespread adoption is riddled with challenges that demand careful consideration and innovative research solutions. By addressing the technical, regulatory, and societal aspects outlined in this journal, the research community can pave the way for a future where individuals have greater control and agency over their digital identities.
Self-sovereign identity (SSI) systems are designed to grant individuals control over their personal data and identity information. At the core of SSI lies the principles of decentralization and interoperability, which aim to shift away from traditional centralized identity systems and enable seamless interaction between various SSI platforms. This section delves deeper into the challenges and research opportunities surrounding the concepts of decentralization and interoperability in the context of self-sovereign identity.

Decentralization
Decentralization in SSI refers to the distribution of identity-related functions and control away from a single central authority. Instead of relying on a central entity to manage and validate identity information, SSI systems utilize decentralized technology, often based on block chain or distributed ledger technology, to create a network of trust and consensus. This shift offers several benefits, including enhanced security, reduced risk of data breaches, and increased user privacy.

Challenges
Scalability
Maintaining decentralization while accommodating a growing number of users and transactions presents scalability challenges. Block chain-based SSI systems may face limitations in processing a high volume of identity-related transactions without compromising system performance or increasing transaction costs.

Consensus Mechanisms
Different consensus mechanisms used in decentralized systems, such as proof-of-work and proof-of-stake, have implications for SSI platforms. Selecting the appropriate consensus mechanism while ensuring efficient and secure identity validation is a complex task.

Data Management
Storing identity data on a distributed ledger introduces challenges related to data storage, retrieval, and management. Ensuring data integrity, availability, and efficient access become key considerations.

Research Opportunities
Scalability Solutions
Researchers can explore novel consensus algorithms, sharing techniques, and off-chain solutions to address scalability concerns while preserving the decentralized nature of SSI systems.

Hybrid Architectures
Investigating hybrid approaches that combine the benefits of decentralization with traditional identity systems could provide a balance between scalability and decentralization, especially during the transition phase.

Network Governance
Designing effective governance models for decentralized identity networks is crucial. Research can focus on mechanisms for decision-making, dispute resolution, and network upgrades.

Privacy-Preserving Decentralization
Exploring advanced cryptographic techniques, such as zero-knowledge proofs and homomorphic encryption, can enhance privacy while maintaining decentralization in identity transactions.

Interoperability: Interoperability in SSI pertains to the seamless exchange of identity information and transactions between different SSI systems and platforms. Achieving interoperability is essential to prevent the fragmentation of identity ecosystems and enable users to present their SSI credentials across diverse services and applications.

Challenges

Standardization

The absence of standardized protocols and formats for identity data exchange hinders interoperability. Different SSI platforms may use varying data structures, which can lead to compatibility issues.

Cross-Domain Transactions

Enabling secure and verifiable identity interactions across different domains and industries requires overcoming technical and trust challenges.

Revocation and Expiry

Developing interoperable mechanisms for revoking and expiring SSI credentials across platforms while ensuring data consistency is complex.

Research Opportunities

Standardization Efforts

Researchers can contribute to the development of open standards for SSI data formats, protocols, and interoperability frameworks, fostering a more connected and compatible identity landscape.

Semantic Interoperability

Exploring semantic web technologies and ontologies can facilitate the meaningful exchange of identity data across diverse SSI systems, enhancing data understanding and utilization.

Cross-Platform Identity Mapping

Investigating methods for securely mapping and linking decentralized identifiers (DIDs) from different platforms can enable cross-domain identity interactions while maintaining user privacy.

Trust Frameworks

Developing trust frameworks and reputation systems that span multiple SSI platforms can enhance the confidence in identity transactions between unknown parties.

Decentralization and interoperability are foundational principles of self-sovereign identity, offering enhanced security, privacy, and user control. While they present challenges, these challenges also open avenues for innovative research and collaborative efforts. Addressing these challenges and embracing research opportunities will be instrumental in realizing the full potential of self-sovereign identity systems and revolutionizing the way we manage and exchange identity information in the digital age. Significant efforts have been made to standardize self-sovereign identity (SSI) and related technologies. These efforts aim to create a common framework and set of protocols that enable interoperability and widespread adoption of SSI systems.

Here are some of the key standardization initiatives and organizations involved in SSI

Decentralized Identity Foundation (DIF)

DIF is a consortium of organizations working on the development of open standards for decentralized identity technologies, including SSI. They focus on creating interoperable specifications, protocols, and reference implementations to enable secure and privacy- preserving identity solutions.

World Wide Web Consortium (W3C)

The W3C has been actively working on standards for decentralized identity, particularly through the Verifiable Credentials and Decentralized Identifiers (DIDs) Working Groups. These groups are developing specifications that define how digital credentials can be issued, verified, and exchanged in a decentralized and interoperable manner.

Hyper ledger Indy and Aries

These are open-source projects under the Hyper ledger umbrella that focus on SSI and interoperable identity solutions. Hyper ledger Indy provides the underlying distributed ledger technology, while Hyper ledger Aries offers a toolkit for building interoperable identity agents.

Trust over IP Foundation (To IP)

To IP is a global project that aims to define a new standard for trustworthy and interoperable digital identities. It brings together various stakeholders, including governments, corporations, and non-profit organizations, to collaborate on the development of open standards and protocols for decentralized identity.

Open ID Foundation

While traditionally focused on identity solutions, the Open ID Foundation has also been exploring the development of standards for decentralized identity and SSI. They are working on extensions to the Open ID Connect protocol to support verifiable credentials and decentralized identifiers.

ISO/IEC Standards

The International Organization for Standardization (ISO) and the International Electro-technical Commission (IEC) have also been involved in standardization efforts related to digital identity. ISO/IEC JTC 1/SC 27 has been working on various standards related to IT security techniques, including those that pertain to identity management.

Government Initiatives

Some governments and regulatory bodies have shown interest in standardizing SSI for various use cases, such as digital driver's licenses or government-issued credentials. These initiatives may involve collaboration with international standards organizations and industry stakeholders.

Defining APIs (Application Programming Interfaces) for the standardization of Self-Sovereign Identity (SSI) is a complex and evolving process that involves various components and functionalities. While the exact APIs to be defined may vary based on specific use cases and implementations, here are some key APIs that are typically considered for SSI standardization:

Decentralized Identifier (DID) API

- **Create DID:** An API for generating and registering decentralized identifiers.

- **Resolve DID:** An API to retrieve the associated DID document for a given DID.
- **Update DID Document:** Allows updating the DID document with new information,
- Such as public keys or service endpoints.

Verifiable Credential API
- **Issue Credential:** An API for issuing verifiable credentials to a subject (user) by an issuer.
- **Present Proof:** Enables a holder to present a verifiable credential to a verifier for verification.
- **Verify Credential:** Validates the authenticity and integrity of a received verifiable credential.

Verifiable Presentation API
- **Create Presentation:** An API to create a verifiable presentation containing one or more verifiable credentials.
- **Verify Presentation:** Validates the integrity and authenticity of a verifiable presentation.

Key Management API
- **Generate Key Pair:** Generates a new public-private key pair for use in cryptographic operations.
- **Sign Data:** Signs data using a private key associated with a DID.
- **Verify Signature:** Validates the signature of a piece of data using the associated public key.

Credential Schema and Definition API
- Define Credential Schema: Allows issuers to define the structure of verifiable credentials.
- Define Credential Definition: Creates a credential definition for a given schema,
- Specifying attributes and rules.

Revocation API
- Revoke Credential: An API for revoking a previously issued verifiable credential.
- Check Revocation Status: Verifies whether a credential has been revoked.

It's important to note that the SSI ecosystem is still evolving, and the specific APIs required for standardization may expand or evolve over time. Collaborative efforts within organizations like the Decentralized Identity Foundation (DIF), World Wide Web Consortium (W3C), and other standardization bodies are actively working on defining these APIs to ensure interoperability and seamless integration across different SSI implementations and platforms.

Self-Sovereign Identity has been supported by various different emerging standards that include W3C VC, W3C DID, and others. But implementation and inter-operability have been left open ended, hence it's important to study existing standards and conclude whether with given standards and format a solution/implementation is available that can be used or there is need to enhance existing work that has happened. Most of the implementation rely on blockchain implementation but because of disadvantages of blockchain - inability to scale its practical implementation remains questionable hence need to study whether there is any alternative to blockchain or There is any solution to the problems of inability to scale.

References

1. Datta J. Self-sovereign identity on blockchain: A review of current research. In: 2020 10th International Conference on Cloud Computing, Data Science Engineering (Confluence); c2021. p. 152-157.
2. Kishore G. Self-sovereign identity: A review. In: Self-sovereign Iden- tity: A Review. In Proceedings of 2019 IEEE 9th International Conference on Advanced Computing (IACC) IEEE; c2019. p. 36-41.
3. Hardjono S. A decentralised architecture for user-centric digital identity. In: International Journal of Information Security; c2016. p. 99-112.
4. Devuyst D. A distributed and blockchain-based architecture for digital identity management. In: Computers in Human Behavior; c2018. p. 213-219.
5. Riedl P. In availability, reliability, and security in information systems. In: Legal Compliance in Decentralized User-centric Identity Management, Springer; c2017. p. 234-245.
6. Derakhshanmanesh K. A comprehensive review on blockchain-based self-sovereign identity systems. In: A Comprehensive Review on Blockchain-Based Self-Sovereign Identity Systems, IEEE Access; c2018. p. 24501-24516.
7. Thomas CRG. In proceedings of the 2018 International Conference on Data Science and Engineering (ICDSE). In: An Investigation of Privacy, Security and Identity Management in Self-Sovereign Identity Systems; c2018. p. 68-72.
8. Iruthayarajan L. A review on blockchain technology and blockchain-based applications. In: Journal of Computer and Communication Engineering; c2018;6(1):55-58.
9. Hardjono SMT. Architecture and use cases for decentralized identity. In: In Proceedings of the 2nd ACM International Workshop on Blockchain for IoT and Cyber-Physical Systems; c2017. p. 25-30.
10. Saberi K. Blockchain technology and its relationships to sustainable supply chain management. In: International Journal of Production Research; c2019. p. 2117-2135.