International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 06 | June - 2023 SJIF Rating: 8.176 ISSN: 2582-3930

Comparative Study of Blockchain-Based Identity Management Systems and Self-Sovereign Identity

Akash Phadte[1], Ganesh Manerkar[2]

[1]Student, Information Technology, Goa College of Engineering, Goa, India
[2]Assistant Professor, Information Technology, Goa College of Engineering, Goa, India

---***---

Abstract - The emergence of blockchain technology has significantly impacted multiple industries, including identity management systems. This comparative study aims to assess and analyze various Blockchain-Based Identity Management Systems (BIMS) and Self-Sovereign Identity (SSI) ecosystems. The study delves into the essential characteristics, advantages, and challenges related to each approach, while also exploring their potential applications and the implications for privacy and security. Through this comparative analysis, the study seeks to offer valuable insights into the strengths and weaknesses of BIMS and SSI, empowering organizations and individuals to make well-informed decisions when selecting an identity management solution.

Key Words: Blockchain-based identity management systems, Self-sovereign identity, Privacy, Comparative analysis, Decentralization

1.INTRODUCTION

.

The Identity Management System (IDMS) encompasses policies and technologies that ensure authorized users within an organization can access technology resources like applications, systems, services, data, and cloud platforms. It safeguards against unauthorized access to these resources and generates alerts for any suspicious attempts. However, traditional IDMS faces challenges such as theft, fraud, lack of control, and data loss. To overcome these issues, organizations are exploring new solutions.

Blockchain technology [2] and distributed ledger (DL) have gained attention across various industries, particularly the financial sector. Blockchain enables decentralized, self-governing identities where each participating node maintains independence while adhering to common standards. This decentralization necessitates a secure identity authentication system.

Blockchain possesses properties like transparency, immutability, credibility, tamper resistance, traceability, and decentralization, making it suitable for identity management applications. Digital identity verification is crucial for establishing trust, and blockchain-based authentication schemes record personal information on the blockchain, securing it with a hash.

Self-Sovereign Identity (SSI) is an identity management approach that empowers individuals with control over their digital identities. It enables individuals to verify their identities using trusted third parties and public credentials like passports or national identity cards. The use of a distributed ledger, such as blockchain, ensures that everyone in the network has access to the same truth regarding the legitimacy of credentials without exposing sensitive information.

Numerous IDMS solutions are available in the market, offering various implementation options and features such as multifactor authentication, one-time passwords (OTPs), and biometric logins. Mobile devices like smartphones have popularized features like fingerprint, facial, and retinal scans for enhanced security.

The objective of this comparative study is to analyze and evaluate different BIMS and SSI ecosystems, providing a comprehensive understanding of their key features, benefits, and challenges. By exploring their potential applications and implications for privacy and security, this study aims to offer insights into the strengths and weaknesses of these approaches. Ultimately, the research aims to empower organizations and individuals in making informed decisions when selecting an identity management solution.

2. Background

2.1. Blockchain-Based Identity Management Systems (BIMS)

Blockchain-Based Identity Management Systems (BIMS) leverage blockchain technology to revolutionize traditional identity management practices. BIMS utilize the inherent characteristics of blockchain, such as decentralization, immutability, and transparency, to create a secure and trusted environment for managing digital identities. By employing cryptographic techniques, BIMS ensure secure identity verification, data storage, and transaction management. Smart contracts play a vital role in executing identity-related operations and enforcing predefined rules and conditions.

BIMS are built on various types of blockchain networks, including public, private, or consortium networks. These networks define the structure and participants involved in the identity management process. Identity data is securely stored on the blockchain, either through encryption or hashing mechanisms, ensuring privacy and integrity. Consensus mechanisms, such as proof-of-work or proof-of-stake, are employed to maintain the immutability and trustworthiness of identity-related transactions. Integration with existing identity systems, such as Active Directory or LDAP, allows for seamless interoperability.

BIMS find applications in diverse industries. In the financial sector, BIMS streamline Know Your Customer (KYC) processes, allowing for efficient and secure customer identity verification. Healthcare systems benefit from BIMS by ensuring secure and interoperable management of patient records across multiple healthcare providers. Government agencies utilize BIMS for digital identity solutions, enabling e-governance services, secure voting systems, and efficient public service delivery. Supply chain management can leverage BIMS to verify the authenticity and origin of products. In the education sector, BIMS facilitate the verification of credentials and certificates.

BIMS offer numerous benefits over traditional identity management systems. Firstly, they provide enhanced security by leveraging decentralized data storage and cryptographic techniques, minimizing the risk of data breaches and unauthorized access. Secondly, BIMS empower individuals by allowing them to have control over their personal information and determine the extent of data sharing. This promotes privacy and data sovereignty. Additionally, BIMS reduce identity fraud and provide a tamper-proof audit trail of identity-related transactions. The automation enabled by smart contracts also leads to increased efficiency and cost savings.

While BIMS offer significant advantages, they face several challenges and limitations. Scalability is a prominent concern due to the distributed nature of blockchain networks, as transaction throughput and latency can become obstacles. Regulatory and legal considerations regarding data protection and privacy may vary across jurisdictions, posing challenges for the adoption and implementation of BIMS. Moreover, user experience and usability can be affected, as blockchain technology may require technical expertise and may not be easily accessible to all individuals. Integrating BIMS with existing identity systems may also present interoperability challenges that need to be addressed.

2.2. Self-Sovereign Identity (SSI) Ecosystem

Self-Sovereign Identity (SSI) represents a paradigm shift in identity management, where individuals have full control and ownership of their digital identities. SSI eliminates the need for centralized authorities and intermediaries, putting individuals at the center of the identity ecosystem. With SSI, individuals can independently manage and share their identity attributes while maintaining privacy and security.

SSI is based on key principles and concepts. Decentralized Identifiers (DIDs) are unique identifiers assigned to individuals, allowing them to establish their digital presence. Verifiable Credentials (VCs) are digitally signed claims about an individual's identity attributes, issued by trusted entities. Peer-to-peer networks and trust frameworks ensure secure interactions and establish trust between parties. Selective disclosure and zero-knowledge proofs enable individuals to share specific attributes without revealing their complete identity information.

SSI ecosystems rely on established technical components and standards. [1] The World Wide Web Consortium (W3C) has developed standards for DIDs and VCs, providing a common framework for their implementation. Decentralized Public Key Infrastructure (DPKI) ensures secure key management and authentication within the SSI ecosystem. Protocols such as DIDComm facilitate secure communication and data exchange between entities participating in the SSI ecosystem.

SSI ecosystems find applications in various domains. Digital wallets serve as repositories for managing and storing individuals' verifiable credentials. SSI enables authentication and access control in online services, where individuals can provide verifiable proof of their identity without revealing unnecessary personal information. Cross-border identity verification and mobility are facilitated by SSI, allowing individuals to securely share their identity attributes across different jurisdictions.

SSI offers several advantages over traditional identity management systems. The key advantage is that individuals have full control and ownership of their identity data, allowing them to determine who can access their information and under what circumstances. SSI promotes privacy by enabling selective disclosure, minimizing the amount of personal data shared in identity transactions. Interoperability is also enhanced in SSI ecosystems, as standardized protocols and formats ensure compatibility between different systems and organizations. SSI has the potential to reduce identity-related fraud and theft by increasing the trustworthiness of identity information.

The adoption and integration of SSI ecosystems face challenges due to the nascent stage of the technology and the need for widespread acceptance. Managing decentralized identity ecosystems can be complex, requiring appropriate governance models and coordination among various stakeholders. Legal and regulatory implications, such as liability and compliance with data protection laws, need to be carefully addressed. Additionally, technical challenges related to scalability, performance, and user experience may require further research and development efforts to overcome.

3. Comparative Analysis

In this section, a comparative analysis of Blockchain-Based Identity Management Systems (BIMS) and Self-Sovereign Identity (SSI) ecosystems will be conducted. The analysis will focus on various key factors to provide a comprehensive understanding of the strengths and weaknesses of each approach.

SSI Platforms:

1.**Sovrin[3]**: Sovrin is an open-source SSI platform that focuses on decentralized identity management. It utilizes a public permissioned blockchain to anchor identity data and provides individuals with control over their digital identities.
Features: Sovrin offers features like decentralized identifiers (DIDs), verifiable credentials, and selective disclosure. It enables users to manage their personal information, selectively share data, and maintain privacy in digital interactions.
Use Cases: Sovrin is suitable for scenarios where individuals require full control over their identities and want to interact securely with organizations, governments, and other entities while maintaining privacy.

2.**uPort[5]**: uPort is an SSI platform built on the Ethereum blockchain. It enables users to create and manage their digital

identities, control personal data, and selectively disclose information.
Features: uPort provides secure key management, selective disclosure of data, and user-controlled consent. It integrates with Ethereum smart contracts, allowing for decentralized identity verification and interactions.
Use Cases: uPort is well-suited for applications requiring user-centric identity management, such as decentralized finance, digital wallets, and decentralized applications (DApps).

3.**Evernym[4]**: Evernym's Verity platform focuses on decentralized identity solutions based on DIDs and verifiable credentials. It aims to provide secure and privacy-enhanced digital identity management.
Features: Verity enables the creation, management, and exchange of verifiable credentials. It supports interoperability and scalability in identity systems by utilizing decentralized technology.
Use Cases: Evernym's platform is useful in scenarios where multiple entities need to interact, exchange credentials, and verify identities while maintaining trust and privacy.

BIMS Tools:

1.**Microsoft Azure Active Directory (Azure AD)[7]:** Azure AD is a BIMS solution that integrates blockchain technology into Microsoft's identity and access management system. It adds enhanced security and privacy features to identity management.
Features: Azure AD leverages blockchain networks for decentralized identity capabilities within the Microsoft ecosystem. It provides options for identity verification, authentication, and access control.
Use Cases: Azure AD is suitable for organizations already using Microsoft technologies and seeking to enhance their identity management with blockchain-based security and privacy features.

2.**IBM Blockchain Identity[6]**: IBM Blockchain Identity is a BIMS tool that focuses on secure and trusted identity verification, authentication, and authorization services using blockchain technology.

Features: IBM's solution utilizes blockchain for data integrity and trust. It offers identity management features such as verification of identity attributes and access control.
Use Cases: IBM Blockchain Identity can be applied in industries where strong identity verification and secure access control are crucial, such as financial services and supply chain management.

3.**Civic[8]**: Civic is a BIMS tool that uses blockchain for identity verification and protection. It aims to enable individuals to securely store and manage their digital identities while reducing reliance on centralized identity providers.
Features: Civic provides identity verification services without disclosing sensitive personal information. It allows users to control their identity data and selectively share it when required.
Use Cases: Civic is applicable in various industries where secure identity verification is essential, including fintech, online marketplaces, and Know Your Customer (KYC) processes.

4. Discussion

Comparing Sovrin and Evernym, both platforms offer self-sovereign identity solutions with their own unique features and capabilities. Sovrin is known for its open-source approach and utilization of a public permissioned blockchain network. It focuses on decentralized identity management, giving individuals control over their digital identities. Sovrin's emphasis on DIDs and verifiable credentials provides a robust foundation for secure and privacy-enhanced interactions.

On the other hand, Evernym's Verity platform also focuses on decentralized identity solutions, leveraging DIDs and verifiable credentials. It aims to provide secure and trusted identity verification while ensuring interoperability and scalability. Evernym's platform offers features for creating, managing, and exchanging verifiable credentials, enabling multiple entities to interact and verify identities while maintaining trust and privacy.

If privacy and user control over personal data are paramount, Civic's emphasis on secure identity verification and selective data sharing may be appealing. Civic's platform is designed to empower individuals with control over their digital identities, enhancing privacy and security in interactions.

On the other hand, IBM Blockchain Identity offers a comprehensive suite of identity verification, authentication, and authorization services. It emphasizes data integrity and security, providing a robust infrastructure for managing identities across diverse applications and systems. IBM's solution may be particularly suitable for organizations seeking a scalable and enterprise-grade identity management solution.

5. Conclusion

The study has highlighted the key features, benefits, and challenges associated with each approach, along with their potential applications and implications for privacy, security, ethics, and integration.
compare this tools.

The analysis has revealed that BIMS leverage the inherent characteristics of blockchain technology to create secure and trusted identity management systems. They offer enhanced security, control over personal data, and tamper-proof audit trails. However, BIMS face challenges related to scalability, regulatory considerations, user experience, and interoperability.

On the other hand, SSI ecosystems empower individuals by providing them with full control and ownership of their digital identities. They enable selective disclosure and promote privacy while enhancing interoperability and reducing reliance on centralized authorities. However, SSI ecosystems face challenges related to governance, regulatory compliance, scalability, and technical complexities.

REFERENCES

1. W3C. Decentralized Identifiers (DIDs) v1.0.[Online] Available: https://www.w3.org/TR/did-core/.
2. Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. Decentralized business review, page 21260, 2008
3. Sovrin. "Sovrin - Self-Sovereign Identity Network." Sovrin, https://sovrin.org/.
4. Evernym. "Evernym - Self-Sovereign Identity Solutions." Evernym, https://www.evernym.com/.
5. uPort.[Online] Available: https://www.uport.me/.
6. IBM "IBM Blockchain Identity." IBM. URL:https://www.ibm.com/blockchain/solutions/identity.
7. Microsoft. "Azure Active Directory." Microsoft, https://azure.microsoft.com/en-us/services/active-directory/.
8. Civic. "Civic: Secure Identity Verification and Protection." Civic https://www.civic.com/.