COMP-1830-M01-2024-25

Blockchain for FinTech Applications

2024-25 Term 1

Part – 1 Individual Report

Kruthika Mysore Bhaskar

001354599

Msc Data Science

Table of Content

1. Introduction

Blockchain technology has made it possible for the novel idea of Self-Sovereign identifying (SSI), which gives people total control over their personal identifying information without the need for middlemen. SSI provides a decentralized identity management solution in the FinTech industry, where regulatory requirements like Know Your Customer (KYC) and Anti-Money Laundering (AML) checks are crucial. A blockchain-based paradigm replaces conventional centralized data storage methods, guaranteeing improved control, security, and privacy. By using this method, people are given the ability to control their identification data and only give trusted parties the information they need.

To overcome the drawbacks of conventional identity management systems in the FinTech industry, this paper aims to investigate the viability and potential of blockchain-based SSI solutions. Existing blockchain platforms that can support SSI will be investigated, and the compatibility of blockchain principles with the requirement for safe, user-controlled identity management will be examined. We'll also assess the advantages, difficulties, and dangers of putting such solutions into practice. This investigation will evaluate how SSI can revolutionize identity management while providing enhancements in security, privacy, and operational effectiveness for the FinTech sector.

2. Existing Practices

2.1. Current Identity Management Practices

For Know Your Customer (KYC) and Anti-Money Laundering (AML) verification, people must provide financial statements, identification documents, and proof of address to financial institutions or third-party service providers in traditional FinTech identity management systems. Because they are usually kept in centralized systems under the control of financial organizations, these papers are susceptible to security lapses. This strategy raises a number of important concerns:

Data security: According to Zohar (2017), centralized databases are vulnerable to cyberattacks, which can result in identity theft and data breaches. The dangers of central data storage are further highlighted by well-publicized hacking instances.

User Control: Users no longer have control over how their information is used, shared, or preserved after disclosing personal information to third parties (W3C, 2019). Privacy issues are brought up by this lack of control and openness.

Inefficiency: According to Narayanan et al. (2016), customers frequently have to present the same identity documents to multiple institutions, which causes delays, redundancies, and a disjointed experience. This redundancy can slow down procedures and increase operational inefficiencies.

2.2. Constraints of Present Methods

There are also a number of significant disadvantages to traditional identity management systems:

Security Risks: Sensitive personal data is compromised by centralized systems' inherent susceptibility to cyberattacks and data breaches (Zohar, 2017). Centralized databases that include large amounts of personal data are often the focus of malevolent attackers.

Operational Costs: According to Zohar (2017), financial institutions must pay a lot of money to maintain centralized identity databases, guarantee compliance, and check papers. These expenses result from upholding regulatory standards, protecting sensitive data, and maintaining intricate infrastructure.

Fragmented Processes: The customer onboarding process is made redundant and inefficient by financial institutions' frequent use of separate verification systems (Swan, 2015). Customers must submit the same identity documents to multiple entities, which makes the procedure laborious and time-consuming.

A blockchain-based substitute like Self-Sovereign Identity (SSI), which claims to provide improved security, efficiency, and more control over the management of personal data, is desperately needed due to the inefficiencies and security threats of existing conventional methods. SSI offers a decentralized, user-controlled identity management paradigm that tackles the issues of data breaches, redundancy, and inefficiencies.

3. Blockchain-Based Solution

3.1. Fundamentals of SSI and Blockchain

Because blockchain technology decentralizes governance and gives people the ability to manage their own identification data, it has been recognized as a revolutionary solution to the shortcomings of conventional identity management systems. By doing away with the need for centralized authorities, this strategy solves important issues with data security, inefficiency, and user control. The following are some blockchain concepts that are very compatible with the Self-Sovereign Identity (SSI) use case:

Decentralization: People can now freely control their identities, negating the need for central authorities. Decentralization reduces the dangers of centralized data storage, including unwanted access and data breaches (Swan, 2015; Dunphy and Petitcolas, 2018).
Security: To guarantee the integrity, security, and immutability of stored data, blockchain technology makes use of cutting-edge cryptographic algorithms. Distributed consensus techniques preserve data integrity, making unauthorized changes all but impossible (Narayanan et al., 2016; Zohar, 2017).

Transparency and Traceability: The blockchain provides transparency while protecting privacy using cryptographic techniques by recording transactions on an unchangeable ledger. When necessary, methods like zero-knowledge proofs can be used to validate claims while protecting sensitive information (W3C, 2019).

According to the SSI paradigm, users build and manage their digital identities on a blockchain network. Verified credentials, also known as **Verifiable Credentials (VCs)**, are granted by reliable organizations and kept in a safe location. Users can choose to provide their credentials as needed, maintaining complete control over their personal information while guaranteeing adherence to legal obligations including Know Your Customer (KYC) and Anti-Money Laundering (AML) standards (W3C, 2021; Narayanan et al., 2016).

In addition to improving security and efficiency, our decentralized, user-centric strategy also solves the operational expenses related to centralized identity management and the inefficiencies of repeated KYC procedures. SSI offers a scalable answer to the problems with conventional identity systems by utilizing blockchain technology.

4. Blockchain Technology Review

4.1. Blockchain Types

The process of implementing blockchain technology for Self-Sovereign Identity (SSI) include choosing a blockchain type that is suitable for the application's needs. Three primary blockchain kinds that are pertinent to SSI are as follows:

Public Blockchains: Ethereum and other public blockchains are open, decentralized, and available to everybody. They use distributed consensus processes to offer excellent security and transparency. However, their relevance for sensitive identity management activities may be hampered by their limits in terms of privacy and scalability (Buterin, 2014; Narayanan et al., 2016).

Private Blockchains: Hyperledger Fabric and other private blockchains function in a regulated setting with restricted access for approved users. These technologies are perfect for enterprise applications because they put privacy and scalability first. However, their openness is limited by this control, which comes at the cost of complete decentralization (W3C, 2019; Zohar, 2017).

Hybrid Blockchains: These systems combine the advantages of public and private blockchains, as demonstrated by Corda and other similar platforms. Because it strikes a compromise between privacy and transparency, this strategy is especially well-suited for FinTech use cases that need strong security and regulated data access (Zohar, 2017).
A hybrid blockchain approach is frequently chosen by SSI because it strikes a balance between security, privacy, and scalability, which is in line with FinTech requirements and legal requirements.

4.2. Mechanisms of Consensus

Consensus procedures are essential to guarantee blockchain networks' legitimacy and dependability. The following are the most pertinent SSI mechanisms:

Proof of Stake(PoS) : Compared to Proof of Work (PoW), Proof of Stake (PoS) is known for being more scalable and energy efficient. According to Narayanan et al. (2016), it is appropriate for enterprise-level SSI applications where resource optimization and performance are crucial.

Byzantine Fault Tolerance (BFT): Private blockchains use Byzantine Fault Tolerance (BFT) to make sure the network keeps running even in the event that some nodes malfunction or act maliciously. This technique improves the security and dependability of blockchain platforms that are essential to SSI implementations, such as Hyperledger Fabric and Corda (Zohar, 2017).

4.3. Platforms for Blockchain

A number of blockchain systems are especially well-suited for SSI implementation:

Ethereum: Ethereum is a popular public blockchain platform that facilitates decentralized apps and smart contracts. Its scalability for large-scale SSI applications is limited by issues with transaction speed and energy consumption, despite the fact that its flexibility and developer assistance are beneficial (Buterin, 2014).

Hyperledger Fabric: Hyperledger Fabric is a strong solution for identity management in business settings since it is a permissioned blockchain that prioritizes privacy and modularity. Its scalability and sensitive data handling capabilities fit very nicely with SSI's needs in FinTech (W3C, 2019).

Corda: Designed especially for the financial sector, Corda prioritizes safe peer-to-peer transactions, scalability, and anonymity. Because of its design, it is ideal for FinTech digital identity management, meeting security and regulatory requirements (Zohar, 2017).

SSI solutions can overcome the drawbacks of conventional identity systems by fusing the fundamentals of blockchain technology with the distinctive characteristics of each kind and platform. Identity management procedures in the FinTech sector are being revolutionized by the hybrid blockchain model, which is backed by scalable consensus techniques like PoS and BFT and guarantees a balance between efficiency, security, and anonymity.

5. Improvement Analysis

5.1. Qualitative Advantages

Enhanced Security: The immutability and resistance to tampering of identification data held in SSI systems are guaranteed by blockchain technology. Because blockchain's cryptographic algorithms make unauthorized access more difficult, this feature greatly lowers the danger of data being changed or stolen by hackers (Narayanan et al., 2016; Zohar, 2017).

User Autonomy: Self-Sovereign Identity gives people the freedom to autonomously handle their personal information. By guaranteeing users total control over the sharing and use of their data, this autonomy reduces the need for third-party middlemen (W3C, 2019).

Regulatory Compliance: SSI solutions can be set up to comply with laws pertaining to anti-money laundering (AML) and know your customer (KYC). According to Zohar (2018), SSI systems' verifiable credentials can satisfy regulatory requirements while protecting user privacy and streamlining compliance procedures.

5.2. Quantitative Benefits

Cost Reduction: Blockchain-based SSI dramatically lowers operating costs by doing away with the middlemen and central authorities that are typically needed for identity verification. Simplified procedures and lower maintenance costs for centralized identity systems are advantageous to financial organizations (Narayanan et al., 2016; Swan, 2015).

Enhanced Efficiency: By eliminating tedious manual checks, blockchain automation speeds up verification procedures. This improvement boosts the overall effectiveness of identity-related workflows and reduces client onboarding delays (Swan, 2015; W3C, 2019).

6. Critical Evaluation

6.1. Strengths

Decentralized Control: By removing the need for middlemen or centralized agencies, SSI empowers people to independently maintain their identities. Users can fully own their identification data with this method, which improves privacy and control (Buterin, 2014).

Security and privacy: A very safe foundation for handling sensitive data is offered by blockchain's cryptographic security features. Blockchain's decentralization and immutability guarantee that identification data is impenetrable, lowering the possibility of security lapses and unwanted access (Narayanan et al., 2016).

Efficiency: The blockchain-based SSI greatly increases operating efficiency. Automating identity verification makes it a more efficient and economical solution for financial institutions by cutting down on the time and expenses involved in the verification process (Zohar, 2017).

6.2. Obstacles and Viability

Scalability: When managing massive amounts of data, public blockchains like Ethereum experience scalability problems. Large-scale SSI efficacy may be hampered by these issues, which can result in sluggish processing rates and higher transaction costs, particularly during periods of high utilization (Zohar, 2017).

Regulatory Issues: The immutability of blockchain makes it difficult to comply with laws like the GDPR's "right to be forgotten" clause. To achieve wider acceptance, it is still necessary to overcome the persistent difficulty of modifying blockchain protocols to permit data deletion or change in accordance with such standards (W3C, 2019).

User Adoption: Broad user adoption of blockchain technology is essential to SSI's success. But doing so necessitates getting beyond obstacles including a lack of comprehension, technical expertise, and faith in the technology. To guarantee wider adoption of blockchain-based identity solutions, educational programs and intuitive user interfaces are crucial (Swan, 2015).

7. Conclusion

To sum up, blockchain-based Self-Sovereign Identity (SSI) systems offer a viable way to address the issues with conventional identity management in the FinTech industry. SSI improves security, reduces fraud, and boosts operational effectiveness by utilizing blockchain's decentralized structure, especially in the Know Your Customer (KYC) and Anti-Money Laundering (AML) procedures. While the technology's transparency permits increased accountability, its cryptographic security guarantees that identification data remains impenetrable (Buterin, 2014; Narayanan et al., 2016).

But there are still a number of difficulties. Before blockchain-based SSI is widely adopted, scalability, regulatory compliance, and user adoption issues need to be resolved. Scalability issues with public blockchains, like Ethereum, can lead to longer processing times and more expensive transactions, especially when handling massive amounts of identification data (Zohar, 2017). Additionally, the immutability of blockchain makes it difficult to comply with legal frameworks like the General Data Protection Regulation (GDPR), which contains clauses like the "right to be forgotten" (W3C, 2019). Furthermore, users must overcome technological obstacles and develop confidence in decentralized systems in order for SSI to be adopted (Swan, 2015).

Although these difficulties, blockchain-based SSI systems are a desirable option for the FinTech industry's future due to their advantages, which include increased user control, lower operating costs, and enhanced security. Additional research, pilot projects, and cooperation with regulatory agencies will be crucial to overcoming current challenges. Blockchain-based SSI systems can provide a creative, safe, and effective identity management solution for the FinTech sector by tackling these issues.

References

1.Buterin, V. (2014). Ethereum White Paper. Available at: https://ethereum.org/en/whitepaper/ (Accessed: 1 December 2024).

2.Dunphy, P. and Petitcolas, F.A.P. (2018) 'A first look at identity management schemes on the blockchain', IEEE Security & Privacy, 16(4), pp. 20-29. Available at: https://doi.org/10.1109/MSP.2018.3111247 (Accessed: 1 December 2024).

3.Narayanan, A., Bonneau, J., Felten, E., Miller, A., and Goldfeder, S., 2016. Bitcoin and Cryptocurrency Technologies. Draft — Feb 9, 2016. Available at: https://pdfdirectory.com/pdf/0765-bitcoin-and-cryptocurrency-technologies.pdf (Accessed: 1 December 2024).

4.W3C, 2019. Verifiable Credentials Data Model 1.0. Available at: https://www.w3.org/TR/vc-data-model/ (Accessed: 1 December 2024).

5.W3C. (2021) Verifiable Credentials Use Cases. Available at: https://www.w3.org/2018/credentials/ (Accessed: 1 December 2024).

6.Swan, M. (2015) Blockchain: Blueprint for a New Economy. 1st ed. Sebastopol, CA: O'Reilly Media. Available at: https://books.google.co.uk/books?hl=en&lr=&id=RHJmBgAAQBAJ&oi=fnd&pg=PR3&dq=Blockchain:+Blueprint+for+a+New+Economy+by++Melanie+Swan&ots=XStDB0-Rc4&sig=wrtKt1ewwTI4m29BOmGYF3FDd58&redir_esc=y#v=onepage&q=Blockchain%3A%20Blueprint%20for%20a%20New%20Economy%20by%20%20Melanie%20Swan&f=false [Accessed: 1 December 2024].

7.Zohar, A. (2017). 'Securing and Scaling Cryptocurrencies', Proceedings of the International Joint Conference on Artificial Intelligence (IJCAI), pp. 742-748. Available at: https://www.ijcai.org/proceedings/2017/0742.pdf (Accessed: 1 December 2024).