International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

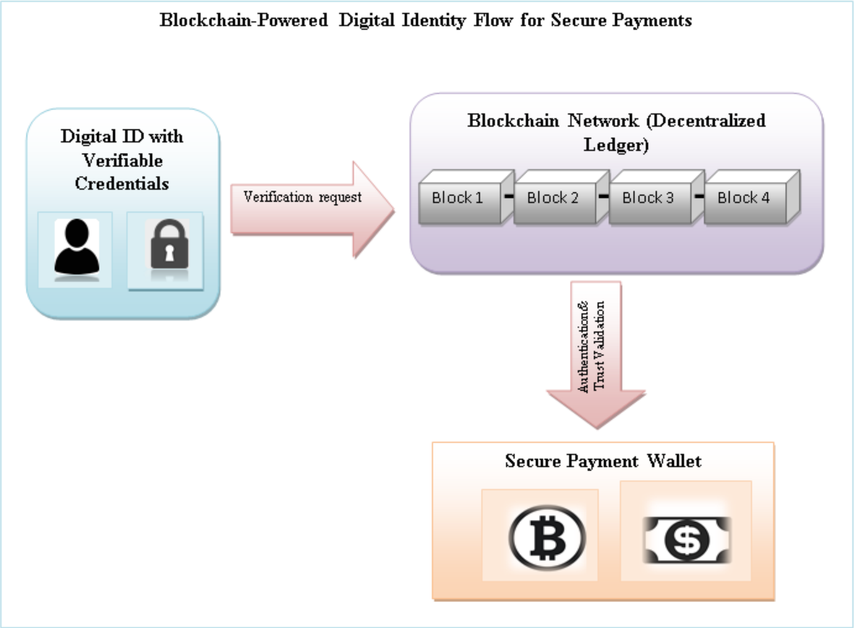
Blockchain-Powered Digital Identity Management for Secure Digital Payments

Vijay Kumar Soni

Submitted: 02/11/2024 **Revised:** 18/12/2024 **Accepted:** 25/12/2024

Abstract: As digital payment ecosystems continue to expand, the need for secure, efficient, and privacy-preserving identity verification becomes increasingly vital. Traditional identity management systems, based on centralized or federated models, often suffer from vulnerabilities such as data breaches, limited user control, poor interoperability, and regulatory compliance challenges. This paper proposes a blockchain-based digital identity framework that addresses these limitations by leveraging Decentralized Identifiers (DIDs), Verifiable Credentials (VCs), and Self-Sovereign Identity (SSI) principles. In this framework, users securely store their credentials such as mobile driving licenses (mDLs) according to ISO 18013-5 in identity wallets, allowing selective disclosure of personal characteristics while retaining complete control over their information. The solution addresses these needs by improving trust, security, user control, and cross-platform interoperability, while complying with major international data protection laws like GDPR, CCPA, and Dodd-Frank Act CFPB Rule 1033. These laws highlight the consumer's right to consent data sharing and increased transparency. Additionally, the study investigates the activities of global standardization organizations such as EMVCo, the OpenID Foundation (OID4VC and OID4VCI protocols), and the Decentralized Identity Foundation (DIF) in promoting large-scale adoption, interoperability, and security of decentralized identity systems. Comparative analysis proves that blockchain-based identity frameworks are superior to conventional centralized and federated systems on several parameters such as security, trust, usability, interoperability, and cost-effectiveness. The results show the revolutionary capability of decentralized identity in digital payment systems, enabling a more secure, user-controlled, and transparent digital economy. This research unveils new research avenues for the future growth of scalable and compliant decentralized identity solutions.

Keywords: *Blockchain Technology, Digital Identity, Self-Sovereign Identity (SSI), Decentralized Identifiers (DIDs), Verifiable Credentials (VCs), Digital Payments, Cybersecurity, Identity Management, Privacy, Interoperability.*


Blockchain-Powered Digital Identity Flow for Secure Payments
Digital ID with Verifiable Credentials
Verification request
Blockchain Network (Decentralized Ledger)
Block 1
Block 2
Block 3
Block 4
Authentication& Trust Validation
Secure Payment Wallet

Discover Financial Services, USA, Expert Enterprise Architect

I. Introduction

1.1 Background on Digital Identity in the Digital Payments Landscape

The digital economy requires digital identity as a method to achieve easy access to digital financial and payment services. Digital identity technologies are expanding their use in payment verification processes because e-commerce websites and mobile banking applications and contactless transactions continue to rapidly grow [1]. A digital identity consists of personal attributes ranging from name and date of birth to biometric information which exists within electronic storage for identity authentication purposes. The implemented identifiers act as payment system safeguards for sensitive transactions because they authorize proper users and foster trust while lowering fraud risks and improving customer experiences [2]. Current digital identity management systems operate through centralized database control which banks or authorities and private service providers handle. These independent systems operate as separate units without connection to others while remaining susceptible to attacks through which hackers gain access to personal information. Identity compromise results in broad-reaching consequences affecting both users whose economic value along with reputation suffers from identity theft as well as institutions which face regulatory penalties combined with diminished customer trust [14]. Electronic payment modernization needs a revolutionary system design that strengthens personal security involvement while achieving smooth system communication across all platforms. Blockchain technology emerges as a solution innovation to manage digital identity in secure payment systems within this established framework of information [3] [15]. Current developments like the Mobile Driving License (mDL), which has been standardized by ISO/IEC 18013-5, show how verifiable credential (VC) and decentralized identity (DID) technologies are increasingly being used in mass scale mobile wallet environments. With cryptographically secure decentralized frameworks, mDL-based mobile wallets allow users to safely store, manage, and distribute their government-issued credentials. This innovation is a move away from centralized storage of identities to self-sovereign designs, in line with the larger trend of giving users more privacy, selective disclosure, and direct control over their identity data across digital payment systems [16].

1.2: Current Issues in Digital Identity Management

New developments in fintech and cybersecurity have not eliminated the persistent difficulties in digital identity management which negatively affect digital payment system security and integrity. The most dangerous issue involving identity theft occurs when cyber criminals use stolen account information to pretend as users for unauthorized entry into payment systems. The breach of centrally stored database information from social networks and financial institutions has become regular practice leading to fraud exposure of millions of users. Users have little control over how their data is shared, stored, and used across websites when they have no control over it [7].

Current systems work separately within their own service provider's network making experiences for both users and service providers less effective. Users must present authentication identity proof to various institutions through a repetitive process resulting in confusing and time-consuming procedures. Existing regulatory requirements pertaining to data protection and compliance bring sophisticated barriers to implementation [11]. The General Data Protection Regulation (GDPR) requires user access rights to their personal information as well as rights to modify and delete it whereas applying these obligations to fragmented identity management systems proves difficult to execute. A total transformation of digital identity creation and authentication and regulatory control is essential because of systematic flaws which become more prominent in digital borderless financial transactions [12][13].

1.3 Significance of the Study and Research Objectives

This paper investigates blockchain technology as a secure distributed system which solves digital identity problems during secure digital payment transactions. The combination of immutability with transparency and decentralization functions as the main reasons blockchain represents a superior alternative to traditional non-decentralized and opaque identity systems. Dual identity management puts users in charge of their credentials while blockchain technology helps them manage these credentials without needing middlemen to enhance privacy protection from identity theft. The main research objective aims to develop a conceptual blockchain-based digital identity management framework which satisfies digital payment platform specifications. This research will evaluate if such technology improves both operational security and network compatibility across platforms as well as providing universal privacy standards.

2. Research Context

In this section, we discuss the history of digital identity management, the security loopholes in conventional systems, and how blockchain technology creates a new way forward for enhanced digital identity management. We also discuss a review of existing blockchain-based identity solutions, focusing on significant platforms such as uPort, Sovrin, Civic, and Microsoft ION. Lastly, we discuss both scholarly work and industry initiatives in this area, looking at how they inform the future of decentralized identity management.

2.1 Evolution of Digital Identity Management:

Digital identity management has developed considerably over the years, advancing through three main stages: centralized, federated, and decentralized. Centralized identity management involves a single authority (e.g., a corporation or government) holding an individual's identity information and completely controlling it. Governments' typical model of traditional banking and identification systems is particularly vulnerable. Centralized databases are the ideal targets for cyberattacks, which result in data breaches and identity theft. In addition, the interoperability issue in centralized systems imposes a barrier on users who want to authenticate on different platforms [9]. The need for an alternative arose, which is addressed through federated identity management, which presents a system where several organizations work together to manage identities. The identity authentication in federated systems depends on trusted third-party service providers who both verify and maintain user information for simultaneous authentication of different services. The improved convenience from single-sign on systems reduces password fatigue but maintains its status as a centralized system with one potential failure point [10]. Decentralized digital identity (DID) represents the modern innovation in identity management which utilizes blockchain technology. A decentralized identity system enables users to both retain ownership of their personal data and use cryptographic methods to maintain trust while minimizing dependence on third-party providers. Users achieve better privacy together with security and control when the system changes [4].

2.2 Security Gaps in Traditional Systems

Blockchain technology solves security weaknesses discovered within classic identity management systems whether they use centralized or federated operation models. Data breaches represent the leading operational hazard in identity monitoring systems. Because centrally stored identity data is contained within a single, large database, cybercriminals find it to be a lucrative target for attacks. Attackers who penetrate the central database storage can both steal and distort sensitive data that leads to identity theft alongside fraud and financial loss [6]. The central predicament in federated systems is their dependence on authority control especially when systems face reduced risk for single point failures. The identity provider (IDP) can be compromised or hacked, revealing user credentials across several platforms. Also, how user data is exchanged between various organizations might not be transparent, and hence privacy issues arise. These legacy systems also have interoperability issues, as multiple organizations might employ different standards for identity management, so users cannot switch easily between platforms [9]. Blockchain fills these security loopholes by providing a decentralized, immutable record that maintains identity data in cryptographically secure form. Using decentralized identifiers (DIDs) and verifiable credentials (VCs), identities can be verified without centralized databases or identity providers. This lowers the threat of data breaches because identity data is not kept at a single point, and user information is in complete control [8].

2.3 Blockchain Fundamentals Applied to Identity (DID, VC, SSI)

Blockchain provides the foundational technology behind decentralized identity through such fundamental concepts as Decentralized Identifiers (DIDs), Verifiable Credentials (VCs), and Self-Sovereign Identity (SSI). DIDs are blockchain-registered digital identifiers where the identity owner has complete control over the identity without an intermediary. Unlike email addresses or usernames, for example, the DIDs lie entirely within a user's control and are themselves cryptographically protected and thus may not be practically forged or altered [5]. Verifiable Credentials (VCs) are digitally present statements claimed by issuers (e.g., government of a country, university) of an individual. These credentials are digitally signed and stored on the blockchain so that anyone can verify their authenticity without contacting the issuer personally. VCs enable users to disclose only the necessary information (e.g., age verification or employment status) without disclosing their complete identity [6]. Self-Sovereign Identity (SSI) is a system where individuals maintain complete ownership and control over their identity. With SSI, users can create, control, and share their identities with decentralized technologies without needing a third-party service provider. SSI systems restore control, security, and privacy of one's data to the user and thus represent a significant leap forward from legacy identity management systems [10].

2.4 Blockchain-Based Digital Identity Solutions and Industry Trends

Blockchain-enabled solutions like uPort, Sovrin, Civic, and Microsoft ION revolutionize digital identity management. UPort employs Ethereum for verifiable, secure credentials [8], whereas Sovrin employs Hyperledger Indy for decentralized identity control [4]. Civic enables password-less identity authentication through blockchain [5], and Microsoft ION, built on Bitcoin's blockchain, provides self-sovereign identity management [8]. Scholarly and industrial endeavors showcase blockchain's ability to improve security, privacy, and user control while scalability and regulatory adherence challenges persist. Industry giants like Microsoft and Civic are already deploying blockchain-based solutions, reflecting a significant change towards decentralized identity management [6, 10].

Table 1: Comparison of Traditional vs Blockchain Identity Models

Feature	Traditional Identity Models	Blockchain Identity Models
Control	Centralized, the user has limited control	Decentralized, the user has complete control
Security	Vulnerable to data breaches and central points of failure	Cryptographically secure, decentralized, reduced attack surface
Interoperability	Often lacks interoperability between different systems	Native interoperability with different platforms using universal standards (e.g., DID, VC)
Privacy	Data shared with multiple entities, privacy concerns	Users share only necessary data, maintaining privacy
Cost	High operational cost for managing identity databases	Lower cost due to no need for central database management
Scalability	Limited scalability with centralized infrastructure	Scalable with distributed ledger technology
Regulatory Compliance	Partial compliance (e.g., GDPR/CCPA); siloed systems complicate adherence.	Full alignment with GDPR, CCPA, CFPB Rule 1033; consent-driven sharing via VCs.

2.4.1 Role of Standardization Bodies in Blockchain-Based Digital Identity Solutions

Various organizations worldwide take a leading role in developing standardized approaches for decentralized identity systems which enhance digital payment security and identity authentication processes. EMVCo serves as a global technical body dedicated to managing payment technologies through its responsibility for assuring that decentralized identity-based transactions maintaining compatibility while upholding security and reliability standards across payment systems through mobile VCs. The OpenID Foundation formed two specifications known as OpenID for Verifiable Credentials (OID4VC) and OpenID for Verifiable Credential Issuance (OID4VCI). These protocols create secure standardized techniques to issue and present and verify verifiable credentials through established authentication frameworks that use OAuth 2.0 and OpenID Connect. OID4VC and OID4VCI provide improved communication between credential issuers and holders (users) and verifiers along with various decentralized networks thus minimizing the risk of fragmentation [18]. The Decentralized Identity Foundation (DIF) supports the production of essential infrastructure elements for decentralized identity ecosystems with features that include universal DIDs resolvers as well as credential transfer protocols and safe credential storage solutions. DIF implements open standards and reference implementations that boost blockchain-powered verifiable credential system adoption on a global scale because they establish a shared developing framework for developers and organizations and governments. Standardization efforts and open collaboration demonstrate the essential nature of decentralized identity technology scaling by creating industry compatibility with enhanced user trust in blockchain-powered digital identity management solutions [17].

3. Research Methodology

This study adopts a conceptual and exploratory research design, aiming to propose a robust blockchain-based digital identity framework tailored for secure digital payments. The methodology is grounded in a detailed synthesis of academic literature, current industrial practices, and blockchain architecture principles. This section outlines the architecture and operational logic of the proposed decentralized digital identity system by analyzing existing identity models and blockchain innovations.

3.1 Architecture of Blockchain-Based Identity Management

The proposed framework integrates key blockchain-based identity technologies that collectively support a secure and user-centric digital identity ecosystem fundamentally, the architecture consists of four main elements: Decentralized Identifiers (DIDs), Verifiable Credentials (VCs), a Blockchain Ledger, and Identity Wallets.

3.1.1 Decentralized Identifiers (DIDs): These are globally unique identifiers created and controlled by the user and maintained on a blockchain. DIDs are not attached to a central authority, and people can manage identities independently.

3.1.2 Verifiable Credentials (VCs): These are digitally signed certificates released by trusted parties (banks, governments, payment platforms) that verify some properties of the user, like name, age, KYC status, etc., which can be cryptographically verified.

3.1.3 Blockchain Ledger: Acts as the immutable and decentralized storage layer for publishing revocation registries, public keys, and DIDs. Guarantees trust and transparency in the interactions of identity.

3.1.3 Identity Wallets: Apps (typically mobile apps) that securely store the user's VCs and DIDs. They allow for user-controlled sharing of credentials with institutions or services, enabling consent-driven data exchange.

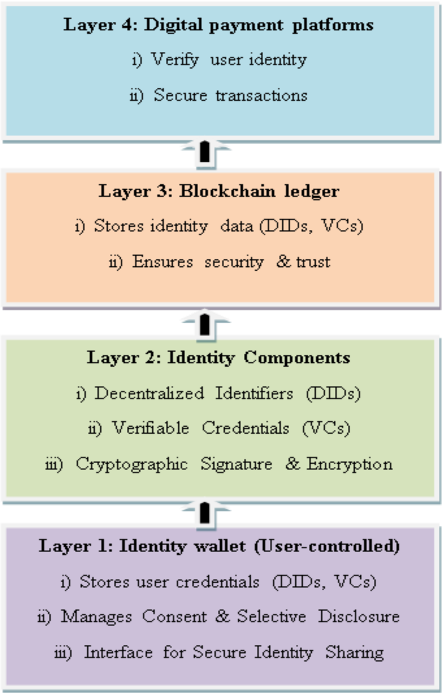

Layer 4: Digital payment platforms
i) Verify user identity
ii) Secure transactions
Layer 3: Blockchain ledger
i) Stores identity data (DIDs, VCs)
ii) Ensures security & trust
Layer 2: Identity Components
i) Decentralized Identifiers (DIDs)
ii) Verifiable Credentials (VCs)
iii) Cryptographic Signature & Encryption
Layer 1: Identity wallet (User-controlled)
i) Stores user credentials (DIDs, VCs)
ii) Manages Consent & Selective Disclosure
iii) Interface for Secure Identity Sharing

Figure 1: Layered Architecture of Blockchain-Based Digital Identity Management

3.2 Identity Lifecycle in Digital Payments

The blockchain-powered digital identity life cycle for the purpose of digital payments aims at giving users control over identity data while offering safe, verifiable, and privacy-enhancing interactions. This life cycle can be decomposed into five key stages: Creation, Issuance, Storage, Verification, and Revocation/Update. These stages are all crucial to preserving integrity and usability of digital identities across payment systems.

3.2.1 Creation: A user begins the lifecycle by setting up a Decentralized Identifier (DID). A secure digital identity wallet contains the cryptographically verifiable globally unique DID after its creation. A DID Document which includes public keys, service endpoints and metadata is constructed during the same time blockchain technology publishes it to the ledger. DIDs exist without needing a central authority so users keep complete control of their personal identifiers.

3.2.2 Issuance: Once DID are established, reliable parties such as banks, governmental institutions, or payment service providers issue Verifiable Credentials (VCs). These credentials, asserting various user properties (e.g., legal name, date of birth, KYC confirmation), are digitally signed and delivered to the user identity wallet. The issuer's digital signature ensures data validity and integrity.

3.2.3 Storage: The Verifiable Credentials are securely stored in the user's identity wallet, which is encrypted. The wallet can be a mobile app or a cloud-based system that employs cryptographic protections. The storage means are intended to support selective disclosure, with the capacity to disclose only the information needed rather than showing complete credentials, which ensures the minimization of data and privacy.

3.2.4 Verification: In a transaction or identity-proofing activity like logging in to an online payment system or making a financial transaction, the user may selectively present some of their VCs. The verifier (for instance, the payment gateway or merchant) verifies the credentials' validity by confirming the issuer's digital signature and cross-checking the DID Document on the blockchain. This is done in real-time without needing direct communication with the credential issuer.

3.2.5 Revocation/Update: If a credential becomes invalid, for example, due to expiration, fraud detection, or user account changes, the issuing authority can revoke it on the blockchain. The DID Document revocation registry enables verifiers to obtain an updated status of credentials thus maintaining system integrity. Digital users gain the capability to modify their login details at any time in order to maintain updated and accurate identity information.

The lifecycle establishes an identity system that enables users to exclusively manage their identity data through self-sovereign identity (SSI). Malfunctioning centralized parties become unnecessary under this system which simultaneously eliminates identity theft risks and breaches and improper access and creates a smooth multi-platform payment experience.

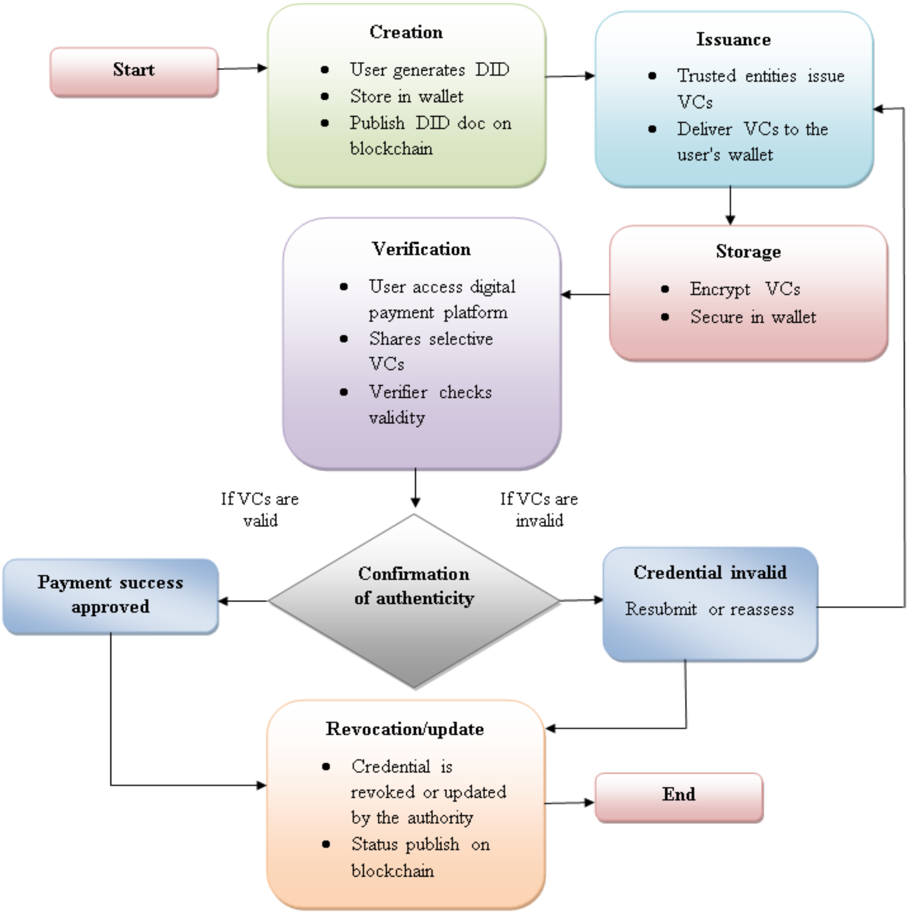


Figure 2: Flow Diagram of Identity Lifecycle in Digital Payments

The payment system operation process with digital identities managed by blockchain appears as illustrated in Figure 2. Blockchain operations start with user creation of decentralized IDs (DID) which users store securely within a protected wallet. Banks constitute dependable parties that distribute verifiable credentials (VCs) for encryption before storage. Users select their desired VCs before passing them to receive payment while the blockchain conducts authentication checks. The payment process leads to success when users demonstrate valid credentials. Users must resubmit their information or renew their credentials in case their credentials do not verify. The identity management system features a mechanism for revoking credentials and blockchain version updates while maintaining privacy protections as well as user control at every stage of identity lifecycle existence.

4. Integration with Digital Payments

The online financial ecosystem relies heavily on extremely secure systems to validate user identities for smooth transactions and strong data protection on the internet. Centralized identity management systems are usually the basis of traditional payment infrastructures, leaving users vulnerable to threats like data breaches, identity theft, and tampering. Combining blockchain technology with digital identity solutions reverses this paradigm by allowing decentralized, tamper-proof, and user-agnostic identification systems. Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) are the building blocks of this digital identity infrastructure. These are stored securely in identity wallets and can be selectively disclosed to digital payment systems when required. This enables payment service providers either banks, digital wallets, or e-commerce sites to authenticate user identities in real time using cryptographic proofs on the blockchain, without accessing or storing sensitive personal information.

In the field of e-commerce, this integration is particularly important for payment online, authentication of the buyer and seller, and preventing fraud. In case of e-KYC of digital wallets or bank accounts, VCs may be issued by authenticated bodies and digitally signed by financial institutions without physical exchange of documents. Likewise, when customers log in to online shopping sites or proceed to checkout, they may introduce custom credentials (e.g., name, age, or account status), which have been authenticated on-chain for guaranteeing privacy and regulatory compliance. All these mechanisms also enable biometric login, multi-factor authentication, and revocation of credentials, thus making fraud based on identity much more difficult. Once a credential is revoked on the blockchain, reuse is technically impossible because blockchain is immutable. Blockchain identity verification is not just useful for e-commerce but also useful for general application in fintech and decentralized finance (DeFi). It enables real-time identity verification for large-value transactions and provides for regulatory compliance alongside protecting user anonymity. Ultimately, a blockchain-enabled identity infrastructure secures digital payment systems through security enhancement, guarantees interoperability, meets GDPR requirements, and minimizes reliance on centralized data monopolies.

4.1 Decentralized Identity and Verifiable Credentials in Mobile Driving License (mDL) Issuance

Mobile Driving Licenses (mDLs) use Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) as defined by ISO/IEC 18013-5:2021 to operate within mobile wallets. ISO/IEC 18013-5:2021 defines security standards to implement smartphone-based driving license management from issuance through storage until presentation. Through DIDs and VCs users can authorize which specific verified elements such as name and age and license status to share in identity verification scenarios without sharing additional personal details. The decentralized identity functionality inside mobile wallets protects credentials using powerful encryption methods and enables users to approve all online and offline verification procedures. Digital payment processes benefit from mDL technology because users gain instant access to verify age or legal identity checks through trusted secure credentials which simultaneously improve security and user experience. Digital wallet standards using blockchain technology serve as a foundational element for implementing decentralized identity across financial services with e-commerce and government digital environments [16].

5. Security and Privacy Considerations

In the American digital economy, where identity theft and data breaches continue to be challenged, blockchain-based identity systems for the digital age present a radical solution for protecting identity information used in digital transactions. Blockchain's immutability and cryptographic authentication permit the establishment of decentralized consensus, which provides a robust environment wherein identity data can be tamper-evident and cryptographically secured. These very features eliminate the reliance upon a central authority and reduce the single points of failure present in traditional identity constructs.

Online payment systems in the U.S. require privacy for identity authentication where compliance depends on it. The privacy technology of selective disclosure enables users to present minimal necessary identity details in KYC situations while keeping their full identity information confidential. Solutions based on Zero-Knowledge Proofs (ZKPs) gain increasing importance in protected high-confidence systems such as login authentication and Know Your Customer (KYC) procedures for non-revelation authentication of identity attributes. The technologies improve user confidence at high levels while respecting U.S. data protection regulations. Across the country, the United States maintains its privacy laws structure sector-based, with every sector developing individual rules for its field of operation. The California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA) are such laws that provide consumers with the right to control availability and sharing of their data via deletion and restriction rights. In the financial industry, the Consumer Financial Protection Bureau (CFPB) Rule 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act requires consumer-consented data sharing, with the guarantee that the people have explicit rights of access, control, and safe sharing of their finance data. Decentralized identity systems based on blockchain comply with such regulatory ideals through facilitating individuals' ability to possess and share selectively their verifiable credentials independently, without dependence on central agencies, thereby strengthening consumer sovereignty, privacy, and security. In finance, the Gramm-Leach-Bliley Act (GLBA) safeguards personal financial information management. Patients have protection under the Health Insurance Portability and Accountability Act (HIPAA) regarding health-related details during transactions. Digital identity systems need to build their frameworks on consent-based sharing together with data minimization and robust privacy safeguards according to these requirements.

Digital identity systems must implement enhanced consent mechanisms and reduced data visibility while requiring immediate verification through credentials to prevent misuse under these framework standards. All such systems operate under NIST Digital Identity Guidelines (Special Publication 800-63) because they either have current government implementation or have plans to implement government functions. The identity proofing and authentication best practices along with federation guidelines from these standards can achieve further enhancements by employing blockchain-powered DIDs and VCs. Technical restrictions plus potential hazards remain present. For example, because blockchain maintains data integrity, the visibility of public ledgers may violate the metadata. To prevent fraud or lockouts, the various revocation mechanisms and key recovery models must be standardized. By utilizing privacy-focused blockchain networks and deploying sensitive attributes to be stored in an off-chain environment, these problems could be fixed.

6. Result and Comparative Analysis

This section examines three major security identity systems used in payment safety which include Centralized solutions and Federated systems alongside Blockchain-Based (Self-Sovereign Identity/SSI). Security along with Trust and Usability together with Interoperability and Cost Efficiency serve as the five fundamental assessment criteria.

6.1 Comparative Performance Evaluation of Identity Models

Performance measurements issue scores to the three identity management models including Centralized, Federated and Blockchain-Based through five key evaluation factors. The Blockchain-Based (SSI) model has the best aggregate score (22/25), performing best in security, trust, and interoperability. Centralized systems perform well in usability but lack security and user control. Federated models have an average balance but still have central authority dependency. This grid emphasizes blockchain's promise as a strong, user-focused solution for secure digital identity management. Figure 3 indicates that the Blockchain-based model excels in Security, Trust, and Interoperability, albeit marginally lower in usability because it demands technical literacy.

Model	Security	Trust	Usability	Interoperability	Cost Efficiency	Total Score (out of 25)
Centralized	2	1	5	2	3	13
Federated	3	3	4	3	3	16
Blockchain-Based (SSI)	5	5	3	5	4	22

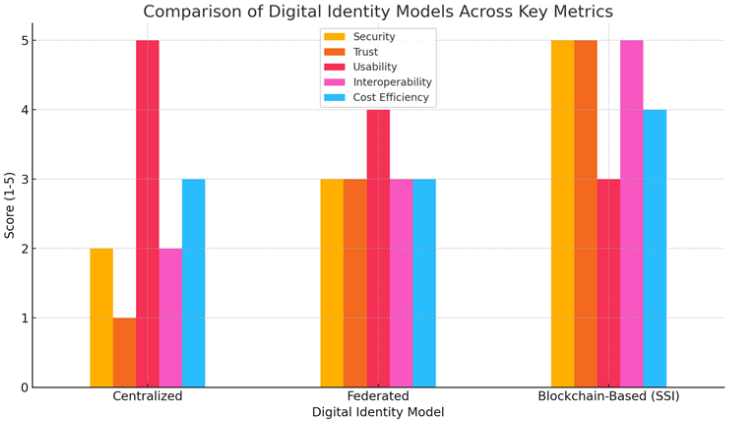


Figure 3: Key Metric Comparison across Identity Models

6.2 Security Analysis

Security is a building block of managing digital identities within the financial infrastructure. Out of the three models under study, the blockchain-based model shows the greatest degree of protection based on its cryptographic foundation, decentralized consensus, and tamper-proof nature. With a breach resistance score of 5 out of 5, it far outperforms federated models that have a moderate score of 3 and centralized systems that only have a score of 1 because they are susceptible to single points of failure. The blockchain model is very secure and offers data integrity and identity theft resistance, so it's the most secure framework for digital payment ecosystems. Figure 4 emphasizes how Blockchain-based identities radically surpass conventional methods of protecting against data breaches and fraud.

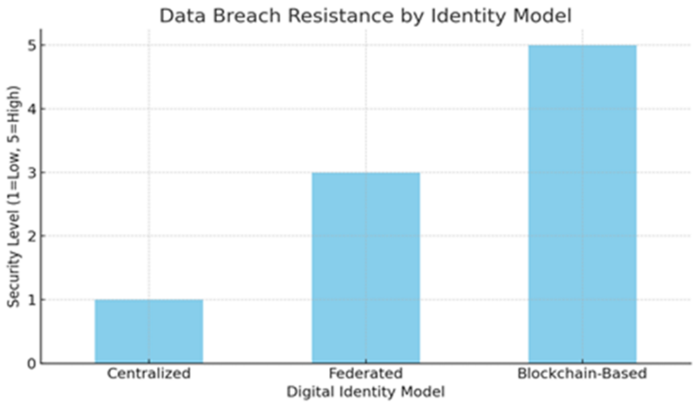


Figure 4: Data Breach Resistance graph

6.3 Cost Distribution

The cost evaluation considers both initial infrastructure setup and long-term maintenance. Centralized systems factor in the highest total cost, around 40%, mainly because of continuous upkeep, security updates, and compliance overhead. Federated systems and blockchain-based models constitute about 30% of lifecycle costs; however, their cost structures differ. Federated systems impose average costs on setup and maintenance, whereas blockchain models involve higher setup deployment expenditure but enjoy much lower maintenance owing to automation, decentralization, and less dependence on third-party monitoring. In the long run, blockchain offers a more sustainable and cost-effective identity management solution. The long-term cost profile of blockchain-based systems is more balanced, as shown in Figure 5, which makes them viable for scalable digital payment environments.

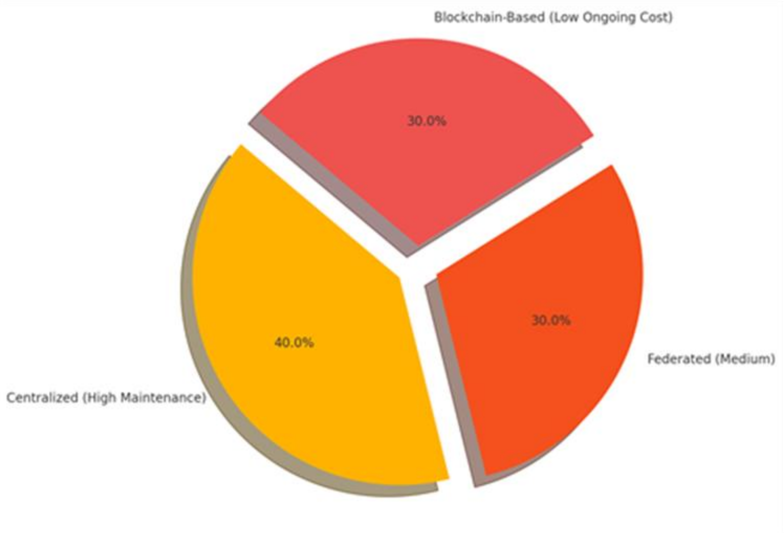


Figure 5: Lifecycle Cost Distribution graph

7. Conclusion and future work

This research indicates that decentralized identity systems, which are based on DIDs, VCs, and SSI principles, provide robust identity theft protection, enhance user privacy, and enable enhanced interoperability for financial platforms. Blockchain technology facilitates real-time, tamper-evident identity verification, mitigating the threats of breaches and making digital payments more transparent and user-centric. Increasing traction from companies such as EMVCo, the OpenID Foundation (its OID4VC and OID4VCI specifications), and the Decentralized Identity Foundation (DIF) is essential in making these technologies reach scale across sectors. It supports making sure decentralized identity systems are secure, workable together, and prepare to be deployed in large volume.

Although the suggested framework holds great potential, scaling should be enhanced in future work, ease of use for identity wallet apps should be increased, and simple integration with legacy payment infrastructures should be ensured. Further efforts are also required to enhance privacy protection, e.g., employing Zero-Knowledge Proofs (ZKPs), and compliance with regulations such as GDPR, CCPA, Dodd-Frank Rule 1033, and NIST standards. Long-term research is advised to quantify the cost-effectiveness and security advantage of blockchain-based identity management systems within real-world financial environments.

References

[1] Ayebo, I. S., & Ojo, O. Digital Identity and Blockchain: Regulatory Challenges and Opportunities.

[2] Mole, C., Chalstrey, E., Foster, P., & Hobson, T. (2023). Digital identity architectures: comparing goals and vulnerabilities. arXiv preprint arXiv:2302.09988.

[3] Rota, L. (2024). Decentralized Identity Management: Building and Integrating a Self-

Sovereign Identity Framework (Doctoral dissertation, Politecnico di Torino).

[4] Ibor, A., Hooper, M., Maple, C., Crowcroft, J., & Epiphaniou, G. (2024). Considerations for trustworthy cross-border interoperability of digital identity systems in developing countries. AI & SOCIETY, 1-22.

[5] Mole, C., Chalstrey, E., Foster, P., & Hobson, T. (2023). Digital identity architectures: comparing goals and vulnerabilities. arXiv preprint arXiv:2302.09988.

[6] Ghosh, A., & Agarwal, R. (2023). Digital identity and blockchain: Regulatory challenges and opportunities. ResearchGate.

[7] Gangwani, P., Joshi, S., Upadhyay, H., & Lagos, L. (2023). IoT device identity management and blockchain for security and data integrity. Int. J. Comput. Appl, 184(42), 49-55.

[8] Campbell, M. (2023). The road to decentralized identity: The techniques, promises, and challenges of tomorrow's digital identity. Computer, 56(6), 96-100.

[9] Lee, J., & Park, S. (2023). Challenges in Centralized Identity Systems and Interoperability Gaps. Journal of Digital Identity Research, 15(2), 101–114.

[10] Kumar, V., & Sharma, S. (2023). Challenges with Securing Digital Identity. Academia.edu.

[11] Putrevu, J., & Mertzanis, C. (2024). The adoption of digital payments in emerging economies: challenges and policy responses. Digital Policy, Regulation and Governance, 26(5), 476-500.

[12] Comb, M., & Martin, A. (2024). Mining digital identity insights: patent analysis using NLP. EURASIP Journal on Information Security, 2024(1), 21.

[13] Degen, K., & Teubner, T. (2024). Wallet wars or digital public infrastructure? Orchestrating a digital identity data ecosystem from a government perspective. Electronic Markets, 34(1), 50.

[14] Mora-Cantallops, M., & Sánchez-Alonso, S. Blockchain-Powered Identity-as-a-Service (IDaaS): Revolutionizing Digital Identity Management.

[15] Buttar, A. M., Shahid, M. A., Arshad, M. N., & Akbar, M. A. (2024). Decentralized Identity Management Using Blockchain Technology: Challenges and Solutions. In Blockchain Transformations: Navigating the Decentralized Protocols Era (pp. 131-166). Cham: Springer Nature Switzerland.

[16] Dock.io. (2023). ISO 18013-5: The New Mobile Driver's License Standard. Retrieved from https://www.dock.io/post/iso-18013-5

[17] EMVCo. (2024). About EMVCo. Retrieved from https://www.emvco.com/about-emvco/

[18] OpenID Foundation. (2024). OpenID for Verifiable Credentials (OID4VC) and OpenID for Verifiable Credential Issuance (OID4VCI). Retrieved from https://openid.net/sg/openid4vc/