IJARETY

International Journal of Advanced Research in Education and TechnologY (IJARETY)

Volume 12, Issue 4, July-August 2025

Impact Factor: 8.152

www.ijarety.in editor.ijarety@gmail.com

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 4, July - August 2025 ||

DOI:10.15680/IJARETY.2025.1204078

Blockchain Based Identity Verification System

Shrushti, Sinchana Hegde, Soumya S

Department of Computer Application, CMR Institute of Technology, Bengaluru, India

ABSTRACT: In today's digital world, securing and verifying identity has become a critical challenge. Traditional centralized systems are prone to breaches, fraud, and exclusion. Blockchain-based identity frameworks address these issues by leveraging decentralization, transparency, and tamper resistance. They empower individuals with greater control over their data and enhance trust among stakeholders. This paper explores the design of blockchain-based identity systems, focusing on self-sovereign identity (SSI) and their applications in finance, healthcare, and government services. We also highlight real-world use cases, technological limitations, and regulatory considerations, demonstrating how blockchain can transform digital identity verification by shifting control from institutions to individuals.

KEYWORDS: Blockchain, Digital Identity, Self-Sovereign Identity (SSI), Decentralized Identity, Data Security, Privacy, Trust.

I. INTRODUCTION

Identity verification is an essential component of internet interactions, but mainstream systems are founded on centralized authorities that are vulnerable to hacking, information leakage, and inefficiency [1], [3]. With online services increasing at a rapid pace, attacks such as identity theft and privacy violations have become major concerns [2]. Blockchain technology provides a decentralized and tamper-evident scheme with the use of cryptographic security, transparency, and immutability [4], [6].

Self-sovereign identity (SSI) and decentralized identifiers (DIDs) allow humans to control their digital identity without intermediaries [9]. Unlike current passports, licenses, and diplomas to be safely stored in digital wallets [8]. Once verified, they may be reused on multiple platforms to facilitate faster sign-up, seamless authentication, and enhanced efficiency both for consumers and service providers [10].

As illustrated in Fig. 1, blockchain-based identity solutions combine ease of use with strong security through features such as QR scanning, one-click authentication, and real-time notifications [5]. This ensures that even non-technical users can benefit from greater privacy, security, and convenience in managing their digital identity.

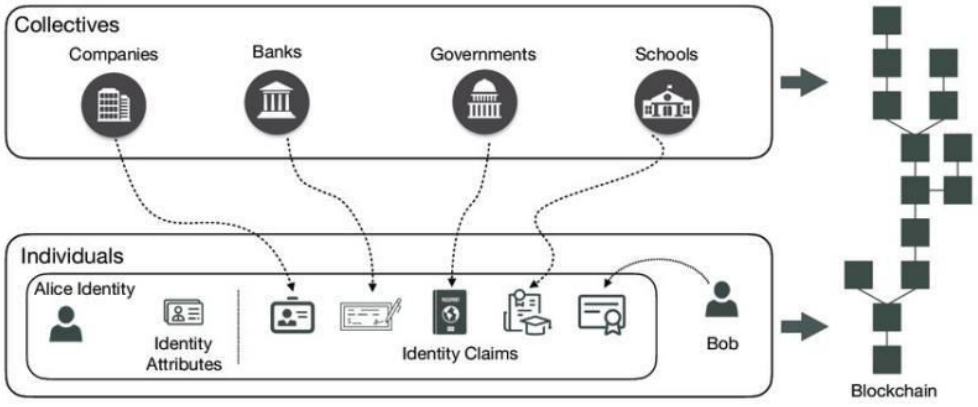

Fig. 1 Overview of blockchain based identity management solutions

Once verified, digital identities can be seamlessly reused across multiple services, enabling faster registration and secure authentication within seconds. This methodology excises redundancy, preserves user time, and enhances efficiency for service providers. In addition to this, blockchain-based identity solutions normally incorporate user-

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 4, July - August 2025 ||

DOI:10.15680/IJARETY.2025.1204078

friendly interfaces in the form of well-recognized mobile applications, with features like QR code scanning, one-click authentication, and real-time notifications.

II. PREFACE OF BLOCKCHAIN

Blockchain has evolved over the past decade from being a niche technology behind cryptocurrencies to a robust framework with many applications [1]. Essentially, blockchain is a decentralized, tamper-evident digital ledger that writes data securely and transparently. Blockchain distributes information across multiple participants, as opposed to centralized databases controlled by one authority, which makes unauthorized modifications very hard to achieve without group consensus [4], [6].

Many industries such as finance, supply chain, healthcare, and more recently identity management have shown interest in this decentralized architecture [8], [10]. Blockchain provides a new model of digital identity where individuals can safely share verified information, own and control their data, and verify themselves without relying on many third-party intermediaries [9].

This paper examines how blockchain can transform identity verification by enabling enhanced security, fraud prevention, and user control. The subsequent sections discuss the core concepts of blockchain, the design of decentralized identity systems, and the challenges and opportunities surrounding real-world implementations.

III. WORKING OF BLOCKCHAIN

Blockchain may be described as a digital ledger that is distributed over a network of computers, referred to as nodes. In contrast to traditional centralized systems in which information is stored within one point of contact, blockchain stores data across multiple nodes, rendering it open, secure, and very tamper-resistant.

A transaction is entered into a "block," and each block has three key elements:
•\tInformation (e.g., identity credentials or transactional data),
•\tHash (a digital fingerprint that uniquely identifies the contents of the block),
•\tPrevious block hash (which connects the block to the previous one).

Blockchain is used to describe the chain of blocks with referencing each other that are produced by this procedure. It is split and the network is alerted if an attempt is made to change a block since its hash changes.

Consensus algorithms such as Proof of Work (PoW) or Proof of Stake (PoS) are employed to verify the block prior to adding it to the chain whenever new data is being added. All nodes that are involved synchronize the new ledger upon its verification.

These systems ensure transparency, immutability, and resistance to fraud through this decentralized verification process. By making it impossible to tamper with or duplicate a credential after it has been verified and stored, digital identity systems facilitate trust among users and service providers.

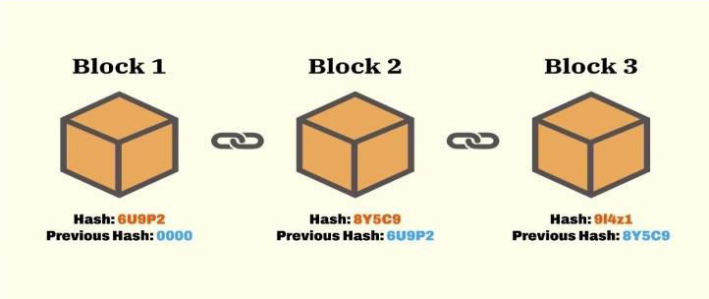

Fig. 2 Blocks in Blockchain

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 4, July - August 2025 ||

DOI:10.15680/IJARETY.2025.1204078

IV. INTRODUCTION OF SMART CONTRACT

Under certain circumstances, smart contracts—software programs executed on a blockchain independently—are able to complete agreements in an automated fashion [2]. Smart contracts operate without intermediaries, reducing costs, speeding up processes, and increasing security levels in comparison to conventional contracts that utilize third parties to enforce their conditions [4].

Smart contracts enable trust in machine identity proofing. As an example, the contract can verify a user's input verified credential (e.g., state-issued ID) automatically and grant access to the subject service without human interaction [8], [9]. It reduces fraud risk, maximizes compliance, and reduces delays.

Smart contract's function based on an "if-this-then-that" approach. A customer, for example, can be granted access to an application or service as soon as they are authenticated by a trusted third-party [10]. Their conditions cannot be changed once they have been deployed, making them transparent and tamper-proof [6].

Smart contracts enable automatic identity authentication by putting rules and logic into the blockchain, making the process more effective, secure, and reliable [5].

V. WORKING OF SMART CONTRACT

Smart contracts are computer programs that execute automatically when triggered, which have been loaded onto the blockchain with pre-established logic [1]. Following is a description of how they function:

Coding the Contract: Developers employ Solidity (for Ethereum) as a programming language to code contract logic. Needs are established in regulations, i.e., granting access if identity is verified [2].

Deployment: The contract can neither be altered nor tampered with when it is deployed onto the blockchain [3].

Triggering Events: The contract ensures compliance with specified rules every time a user interacts with the system (e.g., by presenting an original digital ID) [4].

Execution: The contract executes the action automatically, e.g., granting access, issuing tokens, or modifying records, when the conditions are satisfied [5].

Record-keeping: In the name of transparency and auditability, every transaction which is carried out is retained on the blockchain indefinitely [6].

Smart contracts enable the automation of authorization, revocation, and validation processes in identity verification systems [7]. It enhances scalability and trust in digital identity management, reduces latency, and reduces third-party middlemen dependency [8].

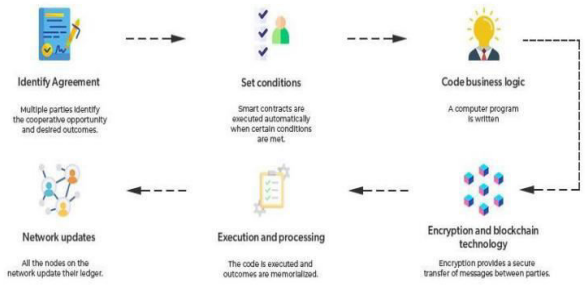

Fig. 3 How does a Smart Contract Work

a. Choose the Identity Framework Choose an identity framework, for example, Self-Sovereign Identity (SSI). Specify the credential type (national ID, school credentials). Choose the trusted issuers, e.g., banks, government authorities, schools [1].

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 4, July - August 2025 ||

DOI:10.15680/IJARETY.2025.1204078

b. Choose an Appropriate Blockchain ArchitectureConsider transaction fees, developer support, and adaptability while selecting a blockchain network. Ethereum, Polygon, and Hyperledger Indy are commonly employed networks. Identity standards and smart contract standards must be maintained through the selected platform [2].

c. Create Decentralized Identifiers (DIDs) Assign each user a unique blockchain-based identifier. To add extra privacy, associate DIDs with off-chain metadata and use W3C interoperability standards [3].

d. Issue and Manage Verifiable Credentials (VCs) Credentials are stored in digital wallets after being cryptographically signed by trusted issuers. On-chain DID references are used by verifiers to prove these credentials [4].

e. Utilize Smart Contracts for AutomationRevocation, access control, and identity verification are guaranteed through smart contracts. They are able to automate functions like login authentication and Know Your Customer (KYC) verification [5].

f. Develop Identity Wallet AppsImplement user-friendly mobile or web wallets with features of consent management, recovery procedures, and selective sharing to handle credentials [6].

g. Promote Legal Compliance and Interoperability Obey the CCPA, HIPAA, and GDPR regulations. For interoperability, adopt global standards such as W3C and Decentralized Identity Foundation (DIF) [7].

h. Test and Continuous Monitoring Perform usability testing, stress testing, and security audits; use users' feedback for optimizing the system performance [8].

i. Deployment and Continuous Monitoring Deploy the solution on the master blockchain network after pilot deployment. For enabling incremental improvement, track user uptake, credential usage, and invocation of smart contracts [9].

VI. ANALYSES OF BEHAVIOUR

The behavior of blockchain-based identity verification systems reflects how users, issuers, and verifiers adapt to a decentralized trust model. Users At first, users are cautious, frequently because they don't fully understand blockchain technology. Once they are accustomed to it, though, they are more likely to appreciate the privacy and control that identity wallets offer, particularly the capacity to share data selectively [1]. Governments and banks are among the issuers that exhibit cautious adoption, giving compliance, data security, and integration with legacy systems top priority [2]. When systems conform to international standards such as Verifiable Credentials and W3C DIDs, their involvement increases [3]. Platforms or service providers acting as verifiers favor trustless, real-time verification techniques that lessen reliance on outside parties [4]. Overall, the system behaves in a deterministic and rule-bound manner, propelled by consensus protocols and smart contracts [5]. How well these systems work for end users while meeting institutional and regulatory requirements will determine their adoption and effectiveness [6].

VII. USES OF BLOCK CHAIN- GROUNDED IDENTITY VERIFICATION SYSTEMS

a. Financial Services
hired for secure and reusable KYC verification to lower fraud and onboarding time.

b. Healthcare
enables secure management and exchange of confirmed medical records by patients.

c. Government Services
ensures cross-border identification validation, electronic voting cards, and public assistance.

d. Education
enables accredited institutions to award degrees and certificates.

DOI:10.15680/IJARETY.2025.1204078

e. Employment
enables quick validation of credentials and job history by employers.

f. E-commerce
validates users' identities to combat fraud and enable secure transactions.

g. Travel and Hospitality
facilitates immigration, check-in, and booking identity verification.

h. Telecommunications
supports secure number portability and SIM registration by virtue of digital identity support.

VIII. CONCLUSION

Blockchain-based identity verification systems offer a transformative shift from centralized, vulnerable models to decentralized, secure, and user-controlled frameworks. By leveraging cryptographic trust, smart contracts, and verifiable credentials, these systems enhance privacy, reduce fraud, and streamline verification across industries. While challenges remain in regulation, adoption, and interoperability, the growing interest in self-sovereign identity signals a future where individuals regain control over their digital identities. As blockchain technology matures, its integration into identity systems holds the potential to redefine how trust is built in the digital world.

REFERENCES

[1] B. Cao, S. Xiao, L. Shi, T. Wang, and J. Chen, "Web 3.0: A Survey on the Architectures, Enabling Technologies, Applications, and Challenges," IEEE Communications Surveys & Tutorials, 2025. [Online]. Available: https://ieeexplore.ieee.org/document/11082313
[2] A. Almomani, A. Alâāśqerem, M. Alauthman, "Ethical Foundations of AI-Driven Avatars in the Metaverse for Innovation and User Privacy," IEEE Access, 2025. [Online]. Available: https://ieeexplore.ieee.org/document/11082154
[3] W. Sarah, "Application of DES, AES, and RSA in Blockchain and IoT Security Frameworks," ResearchGate, 2025. [Online]. Available: https://www.researchgate.net/publication/393975356
[4] H. V. A. Le, Q. D. N. Nguyen, N. Tadashi, and T. H. Tran, "Blockchain-Based Decentralized Identity Management System with AI and Merkle Trees," Computers, vol. 14, no. 7, 2025. [Online]. Available: https://www.mdpi.com/2073-431X/14/7/289
[5] S. Murasaki, K. Omote, and K. Emura, "On the Consideration of Vanity Address Generation via Identity-Based Signatures," arXiv preprint arXiv:2507.12670, 2025. [Online]. Available: https://arxiv.org/abs/2507.12670
[6] D. Liu, G. Wang, Y. Liu, L. Wang, and Z. Liu, "A Security-Enhanced Pairing-Free Certificateless Aggregate Signcryption Scheme for Decentralized Vehicular Sensor Networks," IEEE Internet of Things Journal, 2025. [Online]. Available: https://ieeexplore.ieee.org/document/11083554
[7] X. Peng, C. Zheng, J. Shi, and X. Cui, "A Decentralized Defense Model for Covert Zero-Dynamic Attacks in Industrial Control Systems," Reliability Engineering & System Safety, Elsevier, 2025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0951832025006830
[8] K. N. Singh, A. K. Upadhyay, and A. Mewada, "Blockchain Innovation in IoT-Based Healthcare: Issues and Future Opportunities," in Applications of Blockchain Technology in Healthcare, CRC Press, 2025. [Online]. Available: https://www.taylorfrancis.com/chapters/edit/10.1201/9781003545620-12
[9] S. N. Lohar, S. D. Babar, and P. N. Mahalle, "A Self-Sovereign Identity Framework for Context-Aware De-Centralized Identifier Creation and Credential Verification," Engineered Science, 2025. [Online]. Available: https://www.espublisher.com/journals/articledetails/1629
[10] V. Punitha, U. Sundhar, D. Kanthasamy, and P. C. Devi, "Dynamic Secure Access of e-Health Care System Using Cloud Computing and Blockchain," International Journal of Engineering Research & Technology, 2025. [Online]. Available: https://www.enggjournal.in/images/paper%209

International Journal of Advanced Research in Education and Technology

ISSN: 2394-2975 Impact Factor: 8.152

www.ijarety.in editor.ijarety@gmail.com