RESEARCH ARTICLE OPEN ACCESS

DECENTRALIZED IDENTITY MANAGEMENT USING BLOCKCHAIN AND IPFS

Vishwas Bhagwat*, Leena Patil**

*(Computer Science and Engineering, Priyadarshini College of Engineering, Nagpur
Email: vishwasamr@gmail.com)

** (Associate Professor, Computer Science and Engineering, Priydarshini College of Engineering, Nagpur
Email: leena.patil@pcenagpur.edu.in)

----------**********----------

Abstract:

The rise of decentralized technologies, particularly blockchain and peer-to-peer storage systems such as the InterPlanetary File System (IPFS), has transformed traditional approaches to identity management and access control. Centralized identity and storage systems are increasingly vulnerable to cyberattacks, insider threats, and operational failures, exposing the limitations of single points of trust. Blockchain technology offers an immutable, distributed ledger for enforcing access policies and recording identity actions without central intermediaries. Concurrently, IPFS enables tamper-proof, verifiable storage of data across decentralized networks. This paper presents a comprehensive literature review on blockchain-based identity and access management (IAM) systems and IPFS-enabled decentralized storage, highlighting their principles, applications, advantages, and challenges. Particular attention is given to hybrid architectures integrating both technologies for enhanced security, auditability, and resilience. Furthermore, this review identifies existing research gaps in usability, scalability, role-based access differentiation, and the integration of encryption techniques within decentralized systems. The findings underscore the potential of blockchain-IPFS systems to revolutionize digital identity frameworks while emphasizing the need for practical, user-centric, and scalable solutions for real-world deployment.

Keywords — **Blockchain, Identity Management, Access Control, Smart Contracts, IPFS, Decentralized Storage, Flask.**

----------**********----------

I. INTRODUCTION

The exponential growth of digital ecosystems has necessitated advancements in how identities are managed and access to digital resources is controlled. Traditional centralized architectures for identity management and access control (IAM) are increasingly becoming insufficient to counter modern cybersecurity threats. Centralized IAM systems inherently possess a single point of failure; if compromised, they expose the entirety of user credentials and sensitive resource access information, leading to potentially catastrophic breaches.

Emerging decentralized technologies, particularly blockchain, offer a paradigm shift by removing reliance on centralized authorities. Blockchain networks maintain distributed, tamper-proof ledgers where trust is not placed in any single party but collectively secured by cryptographic consensus. Smart contracts—self-executing code deployed on blockchains—have enabled the encoding of access policies and identity verifications without intermediaries. This reimagining of IAM mechanisms aligns with the requirements of

modern secure systems, where transparency, auditability, and decentralization are paramount.

Parallel to blockchain's evolution, decentralized storage systems such as the InterPlanetary File System (IPFS) have risen to prominence. Unlike traditional location-based storage paradigms, IPFS utilizes content-addressable mechanisms, generating cryptographic hashes of files to ensure their integrity and facilitating efficient decentralized file distribution. This method not only provides tamper-evidence but also promotes censorship resistance and resilience to node failures.

The integration of blockchain and IPFS technologies paves the way for building secure, scalable, and resilient IAM systems. While blockchain ensures trustworthy authentication, authorization, and activity logging, IPFS secures the actual content being accessed or managed in a decentralized, verifiable manner. Together, they form a powerful combination that addresses the limitations inherent in traditional centralized security models.

Despite significant theoretical and prototype advances, several challenges hinder mainstream adoption of blockchain-IPFS based IAM systems. These include usability barriers for non-technical users, lack of standardized role-based access models, performance bottlenecks on public blockchains, and issues related to data confidentiality and persistence in decentralized storage networks.

This paper systematically reviews the current literature addressing blockchain and IPFS-based identity and access management systems, identifies prevailing trends and research gaps, and outlines future research directions necessary for achieving scalable, user-friendly, and production-grade decentralized IAM solutions.

II. LITERATURE REVIEW

A. Blockchain-Based Identity and Access Control Systems

Blockchain technology, renowned for enabling trustless financial transactions, has demonstrated significant potential for revolutionizing identity and access management (IAM). Traditional IAM models such as Role-Based Access Control (RBAC) rely heavily on centralized authorities for user authentication, authorization, and audit logging. The centralization of such processes introduces vulnerabilities, including insider threats, downtime, and single points of failure.

Blockchain-based IAM leverages smart contracts to decentralize and automate access control mechanisms. These contracts embed predefined access policies into tamper-proof code that is immutably recorded on the blockchain. When a user attempts to access a resource, the smart contract autonomously validates the user's credentials and permissions, eliminating the need for a centralized gatekeeper [1].

Recent studies such as Al-Bassam (2021) have proposed Smart Contract-based Public Key Infrastructures (SCPKIs), where blockchain replaces traditional certificate authorities by immutably recording identity credentials [1]. Such approaches offer higher resilience against forgery, unauthorized privilege escalation, and certificate tampering.

Mathur et al. (2023) explored deploying decentralized IAM systems over private Ethereum blockchains simulated using Ganache, demonstrating the feasibility of creating cost-effective, locally hosted identity verification systems that retain blockchain's security guarantees without incurring public network transaction costs [5].

Despite these advantages, usability challenges persist. Most decentralized IAM systems require end-users to manage private keys, interact with blockchain wallets, and understand transaction costs ("gas fees"), imposing a steep learning curve. Furthermore, transaction confirmation latencies on public blockchains can impede real-time access control operations.

In response, hybrid off-chain solutions are gaining popularity, where access decisions are calculated off-chain and only critical events are logged on-chain to balance trust guarantees with system performance. Nevertheless, achieving intuitive, user-friendly decentralized IAM remains an active research frontier.

B. *Decentralized Storage and IPFS-Based Systems*

As blockchain alone is ill-suited for large data storage, decentralized storage systems such as IPFS

have emerged as complementary technologies. IPFS shifts from location-based addressing to content-addressed storage, where each file is identified by a cryptographic hash (Content Identifier or CID). Any alteration to file content produces a different CID, ensuring tamper detection [2].

The inherent design of IPFS offers numerous advantages for secure data storage. Files distributed across IPFS nodes are resilient to localized failures, and the decentralized architecture promotes fault tolerance and data availability. Content-addressed retrieval further ensures that clients receive the exact file they requested, or the retrieval fails—thereby detecting tampering or inconsistencies.

Rejeb et al. (2021) highlighted IPFS's applicability in enhancing transparency across supply chains by providing verifiable data trails [3]. Similarly, Zhang et al. (2022) demonstrated IPFS's role in decentralized medical record management, ensuring data integrity while decoupling data ownership from centralized providers [4].

However, challenges persist. IPFS does not inherently enforce data confidentiality. Files stored on IPFS are accessible to any party possessing the corresponding CID, necessitating encryption for sensitive data. Additionally, IPFS nodes are under no obligation to retain data indefinitely unless content is "pinned," raising concerns regarding long-term data availability.

Emerging solutions involve integrating encryption techniques alongside IPFS storage, ensuring only authorized users can decrypt retrieved content. Furthermore, private IPFS networks and incentivized storage markets (e.g., Filecoin) offer avenues for improving data persistence and privacy in decentralized storage environments.

C. Hybrid Blockchain-IPFS Architectures

The synergy between blockchain and IPFS offers a compelling architecture for decentralized IAM systems. In hybrid models, blockchains record access policies, identity credentials, and file metadata, while IPFS stores the actual files. Blockchain entries store only CIDs, ensuring tamper-evidence without burdening the blockchain with large file data [2][4].

Ahmed et al. (2023) implemented a secure criminal record management system integrating Hyperledger Fabric with IPFS. Their architecture ensured that any manipulation of records, whether in the blockchain or IPFS, would be detectable due to the interlinking of CIDs and transaction logs [6]. Similarly, Abhilash et al. (2023) proposed a secure decentralized cloud storage solution that combined user authentication via blockchain and file storage over IPFS, emphasizing user autonomy and censorship resistance [7].

1. These hybrid architectures exhibit significant strengths:
2. They achieve tamper-evident and verifiable storage.
3. They enhance scalability by offloading large data to IPFS.
4. They maintain auditability through immutable blockchain records.

However, they also inherit challenges from both domains. Managing data confidentiality over IPFS remains complex, requiring robust encryption strategies. Moreover, ensuring availability of data over time demands proactive pinning or replication strategies, since IPFS alone offers no guarantee of permanent storage.

Furthermore, usability remains an issue. End-users often still face the need to manage blockchain wallets, transaction confirmations, and CID retrievals—tasks that necessitate considerable technical proficiency.

There is an increasing emphasis on developing middleware solutions that abstract these complexities, offering intuitive interfaces while preserving the decentralized and verifiable nature of the underlying system.

D. Research Gaps Identified

Despite significant advancements, several critical research gaps continue to impede the practical deployment of blockchain-IPFS based IAM systems:

Usability Barriers: Systems often require end-users to interact with low-level blockchain and IPFS components, limiting accessibility for non-expert users. Seamless abstractions and intuitive user experiences remain underdeveloped [5][6] [22][20].

Role-Based Access Control (RBAC): Although blockchain supports decentralized authentication, few solutions effectively implement dynamic, hierarchical RBAC systems suitable for real-world enterprises or governmental contexts [6] [12][11].

Confidentiality and Privacy: Current models often overlook built-in support for encrypting IPFS-stored data. Advanced solutions must integrate end-to-end encryption, decentralized key management, and selective disclosure mechanisms [4][7] [25][14].

Persistence and Availability: Ensuring that IPFS-stored content remains perpetually available requires proactive strategies such as pinning, incentives, or hybrid private-public node architectures [7] [26][9].

Performance and Scalability: Public blockchains introduce confirmation delays and transaction costs that inhibit real-time access control applications. Emerging solutions such as Layer-2 protocols or hybrid on/off-chain architectures merit further exploration [5] [24][16].

Addressing these gaps is essential for transitioning decentralized IAM systems from academic prototypes to production-grade solutions across industries.

III. DISCUSSION

The integration of blockchain and decentralized storage systems such as IPFS represents a transformative step towards building resilient, secure, and transparent identity management frameworks. Smart contracts facilitate autonomous enforcement of access policies, ensuring that users' privileges are dictated by predefined, immutable logic rather than mutable centralized databases.

IPFS complements blockchain's strengths by offering verifiable, distributed storage of sensitive resources. Together, they embody the principles of decentralization, tamper-evidence, and resilience.

However, practical deployment necessitates overcoming significant hurdles. The trade-off between decentralization and user-friendliness remains a critical bottleneck. Without intuitive interfaces that hide blockchain and IPFS complexities, adoption beyond technologically literate communities will be limited.

Security and privacy enhancements, particularly encrypted storage and decentralized key management, are also essential to ensure that sensitive data does not remain vulnerable even within decentralized architectures.

Performance optimization through off-chain computation, sidechains, and event-driven blockchain models is vital for scaling decentralized IAM systems to production use.

In sum, while the theoretical foundations for blockchain-IPFS based IAM are robust, real-world deployment demands concerted research efforts focused on usability, scalability, and comprehensive security assurance.

IV. CONCLUSION

This review has examined the convergence of blockchain technology and decentralized storage systems like IPFS in addressing the critical need for secure and resilient identity and access management. The inherent properties of these technologies—immutability, transparency, content verifiability, and decentralization—position them as promising enablers of next-generation IAM systems.

While research prototypes demonstrate technical feasibility, the challenges of usability, role differentiation, confidentiality, availability, and performance scalability require focused attention. Practical decentralized IAM systems must balance cryptographic rigor with intuitive design, secure storage with accessibility, and resilience with performance.

Future research must prioritize building comprehensive frameworks that integrate decentralized identity, encrypted decentralized storage, role-based access control, and scalable architectures, validated through real-world pilot deployments.

Through such advancements, blockchain-IPFS based IAM systems could redefine digital trust infrastructures across sectors such as healthcare, education, finance, and governance.

REFERENCES

[1] [1] M. Al-Bassam, "SCPKI: A Smart-Contract-Based Public-Key Infrastructure," arXiv preprint arXiv:2104.04242, 2021.
[2] [2] J. Benet, IPFS White Paper (updated ed.), Protocol Labs, 2021.
[3] [3] A. Rejeb, K. Rejeb, S. J. Simske, and H. Treiblmaier, "Blockchain Technology in Supply-Chain Transparency: A Literature Review," Technol. Forecast. & Social Change , vol. 173, Art. 121080, 2021.

[4] [4] M. Zhang, J. Ma, and W. Chen, “Blockchain- and IPFS-Based System for Secure Medical-Record Management,” IEEE Trans. Emerg. Topics Comput. , early access, 2022.

[5] [5] S. Mathur, M. Verma, and P. Sharma, “GANACHE: A Robust Framework for Efficient and Secure Storage of Data on Private Ethereum Blockchains,” Int. J. Adv. Comput. Sci. & Appl. , vol. 14, no. 1, pp. 120-128, 2023.

[6] [6] E. Ahmed, I. Yaqoob, I. A. T. Hashem, I. Khan, A. I. A. Ahmed, M. Imran, and A. V. Vasilakos, “Blockchain and IPFS Integration for Secure Criminal Record Management,” IEEE Access , vol. 11, pp. 31725-31738, 2023.

[7] [7] B. Abhilash, S. Kumari, and V. Patel, “Secure File-Sharing over Blockchain and IPFS,” World J. Adv. Res. & Rev. , vol. 19, no. 2, pp. 18-27, 2025.

[8] [8] S. Sayeed and H. Marco-Gisbert, “Assessing the Security of Blockchain Smart Contracts,” Int. J. Inf. Secur. , vol. 19, no. 3, pp. 243-264, 2020.

[9] [9] T. Nododile and C. Nyirenda, “A Hybrid Blockchain-IPFS Solution for Secure and Scalable Data Collection and Storage for Smart Water Meters,” arXiv preprint arXiv:2502.03427, 2025.

[10] [10] A. Hossain, M. Rahman, Z. Ali, and S. Kaiser, “Blockchain-Based Identity-Management System,” Int. J. Adv. Comput. Sci. , vol. 14, no. 2, pp. 87-96, 2025.

[11] [11] S. Roy and P. N. Gupta, “Decentralized Identity Management: A Blockchain-Based Approach for Secure Digital-Identity Verification,” in Proc. Int. Conf. Cyberspace Security , 2025, pp. 112-118.

[12] [12] C. Nyirenda and P. Mutasa, “ACS-IoT: Smart-Contract-Assisted Framework for Access-Control Systems in Enterprise IoT,” Sensors , vol. 24, no. 3, Art. 1046, 2024.

[13] [13] K. Patel, A. Sharma, M. Das, and S. Mishra, “A Systematic Review of Blockchain-Based Identity-Management Systems,” in Proc. Int. Conf. Recent Advances in Science , 2023, pp. 55-63.

[14] [14] L. Huang, Y. Chen, and J. Song, “Self-Sovereign Identity on the Blockchain: Contextual Analysis and Frameworks,” Frontiers in Blockchain , vol. 7, Art. 1443362, 2024.

[15] [15] Dock Labs, “Self-Sovereign Identity: The Ultimate Guide,” White Paper, Apr. 2025.

[16] [16] F. Iqbal and V. Rao, “Towards an SDN-Based Smart-Contract Solution for IoT Access Control,” Computer Networks , vol. 242, Art. 109584, 2024.

[17] [17] A. Habib, T. Refat, and M. T. Ahad, “Blockchain-Based Secured Refugee-Identity Management Using Smart Contracts,” Int. J. Comput. Appl. , vol. 183, no. 31, pp. 11-17, 2023.

[18] [18] R. Selvanambi, B. Taneja, and P. Agrawal, “Blockchain-Based Identity-Management Systems,” in Blockchain Applications , Singapore: Springer, 2022, pp. 233-256.

[19] [19] Y. Li, D. Wang, H. Zhao, and P. Zhou, “Blockchain-Based Decentralized Identity System: Design and Implementation,” IACR ePrint , no. 2024/597, 2024.

[20] [20] Rapid Innovation, “AI & Blockchain Fusion: Advancing Digital Identity in 2024,” Tech Brief, 2024.

[21] [21] P. C. Rodriguez and J. R. Nieto, “Blockchain-Assisted Self-Sovereign Identities in Education: A Survey,” Electronics , vol. 3, no. 1, Art. 3, 2024.

[22] [22] A. M. Schmidt, R. Baumann, and L. Klee, “Are We There Yet? A Study of Decentralized-Identity Applications,” arXiv preprint arXiv:2503.15964, 2025.

[23] [23] T. K. Nair and S. Sharma, “Review on Blockchain-Based Decentralized Identity Management,” J. Emerg. Technol. Innov. Res. , vol. 11, no. 4, pp. 417-426, 2024.

[24] [24] R. Gao, J. Xiao, and Q. Liu, “Blockchain-Driven Decentralized Identity Management: A Task-Structure Perspective,” Computer Networks , vol. 242, Art. 109861, 2024.

[25] [25] T. S. Nguyen, P. B. Vo, and D. Fischer, “Analyzing the Threats to Blockchain-Based Self-Sovereign Identities,” Applied Sciences , vol. 14, no. 1, Art. 139, 2024.

[26] [26] S. Hamza and J. Lee, “A Hybrid Architecture for Decentralized Data Storage with Centralized CID Indexing,” Data Intelligence , vol. 5, no. 4, pp. 685-702, 2023.

[27] [27] T. N. Inayat and Z. Pervez, “Blockchain-Based Decentralized Identity: A Survey of Privacy Applications,” arXiv preprint arXiv:2411.16404, 2024.