Radius: Journal of Science and Technology
Vol. 2, Issue 1, (2025) 251009 (9pp)

Block Chain Based Identify Management for Secure & Decentralised Web Application

Kartik Sisodia[1,*] | Garima Sharma[2]

[1]Research Scholar, [2]Assistant Professor
Department of Computer Science, School of Engineering & Technology, Shri Venkateshwara University, Gajraula, Uttar Pradesh

*Corresponding author: kartiksisodia2019@gmail.com

Abstract: The research presents a blockchain-based identity management system for protecting decentralized web applications by operating through decentralized processes. Through its permissioned Ethereum network The-system enables automatic operations for identity lifecycle management to register authenticate authorize and revoke users while maintaining privacy of user data (anonymization and encryption of user data). Users receive hashed credentials which the blockchain ledger retains forever as secure storage alongside complete PII data privacy. Smart contracts determine access through comparison between incoming requests and permanent role statements stored on the blockchain network. Large attribute storage operates by connecting to Inter Planetary File System (IPFS) gateway servers that store blockchain reference data through content hash keys. Users accomplish authentication via a zero-knowledge proof module which enables attribute disclosure under zk-SNARK's parameters to reduce identity exposure. The consensus model deployed in the system supports execution of more than 5000 TPS transactions by completing them within sub-second periods. Performance evaluation confirms scalability, reliability, and real-time access control, demonstrating its viability for modern web applications requiring high throughput and low-latency operations. Security testing establishes that the network withstands Sybil attacks together with replay and man-in-the-middle attacks and privacy evaluation demonstrates unauthorized entities have no ability to derive user profiles. The evaluated benchmark results demonstrate that the framework's performance potential by testing 50 nodes in a test network locally. Research indicates that blockchain identity management develops an resistant system which has enormous potential capacity alongside privacy protection capabilities superior to conventional centralized identity management systems.

Keywords: Blockchain Identity Management, Decentralized Web Applications, zk-SNARKs Authentication, Smart Contracts, Permissioned Ethereum Network

1. Introduction

The new decentralized web system Web 3.0 received its name from web specialists who observed quick technological progress of the internet. Users exercise digital resource control through this system which includes personal identification features [1-3]. The user identity management system functions as the basis for Web 3.0 which demands users to perform registration along with identity validation to establish ownership.

Centralized identity systems encounter three major problems including solitary failure points and invasive privacy violations and insufficient user capabilities to handle their personal data.

https://doi.org/10.5281/zenodo.15366215
Received: 25 April 2025 | **Revised:** 05 May 2025
Accepted: 06 May 2025 | **Published Online:** 08 May 2025

Research into DID systems built with blockchain technology emerged due to centralized identity problems since these systems provide immutable data combined with transparent functionality and decentralized consensus methods that replace intermediary trust systems [4–6]. The authors introduce an identity management solution based on blockchain that uses permissioned Ethereum networks for controlled access within a high-throughput environment. The identity life cycle management operates autonomously through smart contracts while hashed credentials get stored on-chain while large data is handled off-chain by using Inter Planetary File System (IPFS). Users can authenticate their identity using zero-knowledge proof (zk-SNARK) which verifies identities without exposing private information to others. Computational evaluations show that the system defeats Sybil attack attempts together with replay and man-in-the-middle attack scenarios. The 50-node experimental testbed reached confirmation of framework robustness by performing more than 5000 transactions per second [7–9].

Permissioned Ethereum offers greater control over participant access and transaction throughput, making it more suitable for enterprise-level identity management, ensuring privacy and efficiency. However, it sacrifices decentralization and trustless operations found in public blockchains. While more secure and scalable, it may lack the openness and censorship resistance of public chains. The research exhibits that blockchain identity management systems provide identity solutions superior to conventional centralized systems because they offer security alongside reliability features when operated independently or with decentralized applications.

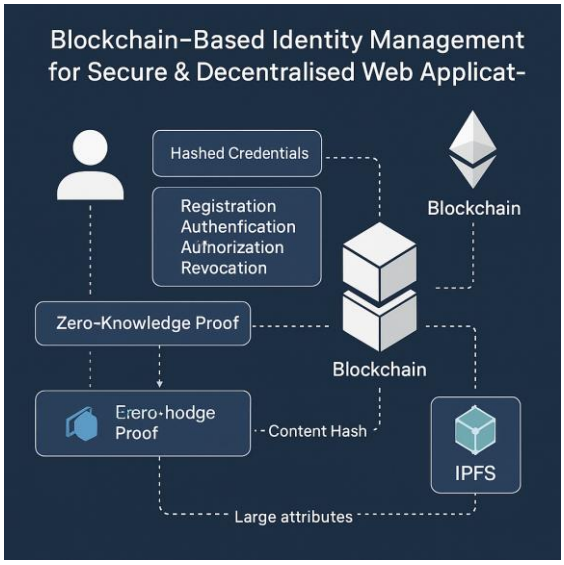

Figure 1: Blockchain-based Identity Management

2. System Architecture

The identity management framework establishes decentralized security systems which work together with security capabilities and privacy operational features. Three fundamental components within the framework unite blockchain technology through Ethereum with smart contracts and IPFS data storage and zero-knowledge cryptography for privacy security systems. Transparent auditing along with high performance levels can be achieved through the decentralized operation model which protects user privacy [10-12].

Network Framework

The infrastructure base uses a trusted Ethereum blockchain network that includes nodes operated by institutions and stakeholders. Permissioned networks enable specific network access controls that simultaneously boost security and expand operational size. The consensus mechanism achieves maximum efficiency through its capability to process 5000 transactions per second with finality reaching less than one second. The network topology with clearly defined access controls reduces system attacks by Sybil nodes while ensuring complete transparency of node activities. To enhance trust and accountability, the infrastructure incorporates public audit logs and transparent access policies within the permissioned Ethereum blockchain network. All node interactions and consensus-related activities are recorded immutably, enabling external and stakeholder audits. Access policies are enforced through smart contracts, defining permissions for data access, transaction validation, and node participation. This ensures that only authenticated entities can perform critical operations while maintaining visibility into network behavior. Combined with PBFT's deterministic consensus, these controls support secure, verifiable, and governance-compliant operations across the blockchain-based infrastructure.

Identity authentication services become immediately accessible because the Practical Byzantine Fault Tolerance (PBFT) algorithm offers dependable and rapid verification procedures as a deterministic consensus method. Practical Byzantine Fault Tolerance (PBFT) is a consensus algorithm designed for distributed systems to reach agreement despite malicious nodes. It tolerates up to ff faulty nodes in a network of 3f+13f+1 total nodes. Thus, it ensures reliability as long as fewer than one-third of nodes are compromised. [13-15].

Identity Lifecycle Management

The system fully automates the identity lifecycle through smart contracts deployed on the blockchain. Smart contracts enforce role-based access control (RBAC) by mapping user identities to predefined roles and associated permissions within the contract logic. Each role is assigned specific access rights, and only users with verified credentials matching role requirements can execute authorized actions. Dynamic policy updates enable real-time permission revocation and reassignment. These smart contracts handle four key operations:

- **Registration:** The first step during user onboarding includes the hash process of personal identifiable information (PII) through cryptographic algorithms. The blockchain infrastructure gives permanent storage to credential hash values after their generation during hashing procedures. The blockchain database contains PII data hash values exclusively for protecting user privacy throughout the system.
- **Authentication:** Users must provide their identity credentials to the system which validates them against role statements found in smart contracts before authorization. Users can achieve verified identity authentication without revealing personal details through this system process.
- **Authorization:** Users obtain authorized access to their contracted resources through identity verification on smart contracts. The implementation of access control logic exists within smart contracts because this component represents fundamental programming code for roles.

- **Revocation:** Through smart contracts the system performs automatic termination of user permissions when security policies update thereby reducing security vulnerabilities caused by breached accounts.

The system employs SHA-256 for hashing personally identifiable information (PII) before storing it on-chain, ensuring data integrity and collision resistance. For smart contract operations on the Ethereum-based network, Keccak-256 (Ethereum's variant of SHA-3) is used, aligning with Ethereum's native cryptographic standards for secure and consistent identity verification.

Storage via IPFS

Large identity attributes undergo storage on IPFS (Inter Planetary File System) networks for efficient data distribution and scalability purposes. Data accessibility is improved through the peer-to-peer network which allows content availability when one node keeps the data. The system ensures data integrity because of content-addressing which provides each file with a cryptographic hash. The cryptographic hash system allows for tamper-proof access while removing trust in off-chain identity data since any unauthorized modifications to the data change its hash signature which acts as a protection mechanism. The system employs Inter Planetary File System (IPFS) technology to handle blockchain storage limitations which specifically affect massive identity features such as biometric information and documents. Users can access Inter Planetary File System (IPFS) as a distributed file system which allows them to find files by cryptographic hash keys instead of using conventional spatial coordinates. The system saves extensive data files in IPFS when users perform registration or identity updates yet it stores just hash contents on the blockchain. Users can securely access stored data on IPFS but blockchain requirements stay minimal due to this system protecting data integrity [16].

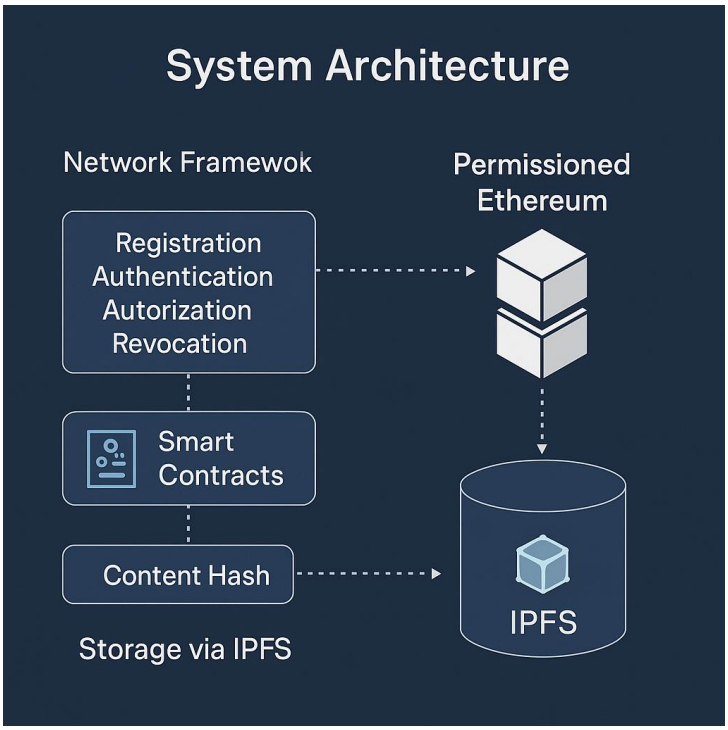

Figure 2: System Architecture

3. Privacy-Preserving Mechanisms

zk-SNARKs Authentication

zk-SNARK enables parties to demonstrate their knowledge of specific data through proofs that preserve their confidentiality to other parties. zk-SNARK uses a proof system which offers fast and secure operations because its proof size is compact and verification occurs without needing multiple exchanges between parties during the evaluation process. This functionality makes blockchain systems operate efficiently while maintaining data privacy. The system brings zero-knowledge proofs through zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) as its main innovation. Users can demonstrate credential validity through zk-SNARKs yet maintain absolute privacy because the system does not expose their personal information. Users create zero-knowledge proofs of their valid credentials when authenticating their identity. Smart contracts operating as verifiers possess enough capability to validate proofs but cannot access user attributes which protects privacy during authentication. In the system, ZoKrates is used for generating zk-SNARK proofs, providing a high-level framework for creating and verifying zero-knowledge proofs on Ethereum. Additionally, SnarkJS is utilized for efficient proof verification and interacting with zk-SNARK circuits on-chain [17].

Data Minimization

System design relies on minimal data methods because the system needs to execute privacy rules. The system maintains a small attack surface and meets GDPR standards alongside global privacy requirements since it uses on-chain storage of hashed identifiers combined with access control policies. Users maintain complete protection of personal identification information during authentication tasks because the identity framework upholds their right to data privacy. Metadata leakage is prevented through the use of zero-knowledge proofs (zk-SNARKs) and off-chain storage. Only hashed credentials are stored on-chain, while sensitive data like personal details and attributes are securely stored off-chain, minimizing exposure and ensuring privacy.

4. Performance and Security Evaluation

The laboratory evaluation tested both functionality and dependability features of the blockchain-based identity management system. The tests evaluated system performance through transactions per second processing ability together with latency performance and scalability assessment for resistance against typical security threats [18].

Benchmarking and System Performance

An experimental system implementation took place on a simulated network design with 50 nodes. The network employed permissioned Ethereum clients who operated with a PBFT consensus mechanism. The environment provided testing space for smart contracts and IPFS. A virtual machine (VM) runs the environment with 4 vCPUs along with 16GB RAM and 200GB storage for handling high speeds and concurrent operations. A permissioned Ethereum network executing on Geth (Go Ethereum) forms the base of the software stack which collaborates with Solidity for smart contract development as well as IPFS for off-chain data storage. Both SHA-256 and Keccak-256 serve as the cryptographic operations in the application. The network infrastructure provides scalable performance with private operations while maintaining knowledgeable access controls and authorization functionalities.

Table 1: Performance Metrics of Identity Management System

Metric	Value	Description
Transactions per second (TPS)	5,270 TPS	Sustained throughput measured across 50-node testbed
Transaction finality time	< 0.8 seconds	Time for a transaction to be considered final
Smart contract execution time	~120 milliseconds	Average time to execute registration/authentication
IPFS file retrieval latency	~500 milliseconds (avg)	Delay in fetching attribute files via IPFS gateway
zk-SNARK proof generation	~1.5 seconds (user side)	Time taken by user to generate zero-knowledge proof
zk-SNARK proof verification	~30 milliseconds	Time taken by smart contract to verify proof

The obtained results demonstrate that the system delivers high performance which makes it appropriate for real-time authentication operations in decentralized platforms. Proof generation speed for zk-SNARK exhibits a minimal additional load because of its cryptographic complexity which does not obstruct practical application usage.

Security Analysis

Identity management systems require security as their main priority element. The proposed framework underwent complete testing through multiple identified cyber attacks such as Sybil attacks, replay attacks as well as man-in-the-middle (MitM) attacks. While permissioned blockchain networks provide controlled access and enhanced security, they are still vulnerable to Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. These attacks can overwhelm network resources, disrupt operations, or degrade performance. Though the number of nodes is limited, making it harder for malicious actors to gain control, the risk of DoS/DDoS remains. Implementing rate limiting, network monitoring, and redundancy can help mitigate these threats, ensuring the resilience of the blockchain network against such attacks.

Table 2: Security Threat Resistance Evaluation

Attack Type	Mitigation Mechanism	Outcome
Sybil Attack	Permissioned network and node identity verification	Prevented
Replay Attack	Use of nonces and timestamps in transactions	Neutralized
Man-in-the-Middle	zk-SNARKs with encrypted channels and hash validation	Prevented
Unauthorized Access	Role-based smart contract enforcement and hashing	Denied with no data leakage
Data Breach	Off-chain storage, zero-knowledge proofs, and hashing	No sensitive data exposed

The pre-verified node process included in permissioned architecture helps prevent Sybil attacks from occurring. Each transaction runs only once avoiding replay attacks because of the

implementation of exclusive transaction identifiers known as nonces. End-to-end encryption in combination with zk-SNARKs shields meaningful authentication data from attackers during the process of authentication.

Privacy Evaluation

The researchers tested the privacy elements by allowing adversarial actors to try guessing user profiles or identity attributes from the on-chain information. User profiles cannot be reconstructed by attackers because both the blockchain system does not store PII as well as zk-SNARKs prevent adversaries from learning underlying information.

Table 3: Privacy Protection Analysis

Privacy Metric	Result
PII stored on-chain	No
PII leaked during authentication	No
Ability to infer user profile	Not possible
Identity traceability	Zero traceability ensured by zk-SNARKs

These results validate the system's ability to preserve user anonymity and data confidentiality, even in hostile environments.

5. Discussion

The unified use of blockchain technology with decentralized identity management brings new applications which secure high-security needs for privacy-oriented and trust-based features. Through identity lifecycle tracking and privacy defense capabilities users gain six benefits (i.e. enhanced privacy through zk-SNARK authentication, secure and automated identity lifecycle management via smart contracts, immutable data storage, transparent access control, real-time role-based access updates, and robust defense against unauthorized access or data breaches, ensuring users' identity protection and privacy throughout their interactions) from smart contracts and zk-SNARK-based authentication tools while utilizing the system. Ethereum maintains operational quality through IPFS storage even though its limited platform enables high performance scaling.

Benchmark tests confirm that the system can execute multiple transactions per second thus demonstrating successful performance in real decentralized web applications testing. Security tests prove the system stops multiple attack methods to maintain complete protection of user information together with privacy of personal data.

The restricted blockchain endorsement among users and regulatory barriers along with zk-SNARK technology expenses create significant challenges to its mass adoption. The deployment of decentralized systems requires standardized universal identity technology that needs both the advancement of cryptographic speed and global identity standards. Compared to existing Decentralized Identity (DID) frameworks like Sovrin, uPort, and Microsoft ION, the proposed system offers enhanced privacy and scalability through the use of zk-SNARKs for confidential authentication and a permissioned Ethereum network for controlled access and high throughput. Sovrin and uPort focus on decentralized identity management but may lack automated lifecycle tracking or strong privacy safeguards. Microsoft ION provides a scalable

DID solution but doesn't emphasize granular access control and privacy as effectively as the proposed blockchain-based framework.

zk-SNARKs are computationally intensive, especially in the proving phase. This challenge is addressed by using more efficient cryptographic techniques, such as precomputing trusted setup parameters and leveraging hardware acceleration, which reduces the computational burden on users and validators.

6. Conclusion and Future Work

The implementation of a new blockchain identity management system brings resilient protection towards decentralized web applications with protected security methods. Protected user identity lifecycle operations along with private user interaction and high scalability emerge from the $\mathbb{F}$ blockchain system through zk-SNARKs combined with IPFS smart contracts executed on a permissioned Ethereum network. Security examination of the system proves it shields against Sybil attacks and malicious replays and demonstrates swift operation speed with temporary performance delays in testing.

Blockchain-based identity management in decentralized web applications enhances security through self-sovereign IDs, cryptographic proofs, and tamper-proof authentication. Unlike alternatives like Filecoin or Arweave, which focus primarily on decentralized storage, identity chains emphasize user control and verifiable credentials. While Filecoin offers content-addressable storage with economic incentives and Arweave ensures permanent data storage, they lack native identity verification frameworks. Blockchain ID systems, in contrast, enable fine-grained access control and secure interactions, making them more suitable for authentication-driven web services.

The solution introduces an innovative identity protection system because users receive authentication abilities while other individuals remain unaware of their confidential details. Investigation of the existing system merits requires research on how to integrate new systems with legacy platforms coupled with the execution speed challenges from zero-knowledge proof computations.

The upcoming research focuses on zk-SNARK efficiency optimization to integrate DID for cross-platform identification and on user interface improvements to increase public acceptance. A global implementation framework can establish conditions which enable decentralized identity to compete against existing worldwide identity management systems.

References

1. Lu, Y. (2018). Blockchain and the related issues: A review of current research topics. *Journal of Management Analytics*, *5*, 231-255. https://doi.org/10.1080/23270012.2018.1516523
2. Weerapanpisit, P., Trilles, S., Huerta, J., & Painho, M. (2022). A decentralized location-based reputation management system in the IoT using blockchain. *IEEE Internet of Things Journal*, *9*, 15100-15115. https://doi.org/10.1109/JIOT.2022.3147478
3. Ahmed, M. R., Islam, A. M., Shatabda, S., & Islam, S. (2022). Blockchain-based identity management system and self-sovereign identity ecosystem: A comprehensive survey. *Ieee Access*, *10*, 113436-113481. https://doi.org/10.1109/ACCESS.2022.3216643
4. Guthoff, C., Anell, S., Hainzinger, J., Dabrowski, A., & Krombholz, K. (2023, May). Perceptions of distributed ledger technology key management-an interview study with finance professionals.

In 2023 IEEE Symposium on Security and Privacy (SP), 588-605. https://doi.org/10.1109/SP46215.2023.10335652

5. Beloor, V., Vijaykumar, M., Swamy, D. R., & Navneeth, S. (2024). Block chain enabled Indian Agricultural supply chain using ISM DEMATEL approach. *OPSEARCH*, 1-28. https://doi.org/10.1007/s12597-024-00861-2
6. Zhang, C., Yang, Q., Zhang, J., Gou, L., & Fan, H. (2023). Topic mining and future trend exploration in digital economy research. *Information*, *14*, 432. https://doi.org/10.3390/info14080432
7. Pustišek, M., Chen, M., Kos, A., & Kos, A. (2022). Decentralized Machine Autonomy for Manufacturing Servitization. *Sensors (Basel, Switzerland)*, *22*, 338. https://doi.org/10.3390/s22010338
8. Beyene, M., Toussaint, P. A., Thiebes, S., Schlesner, M., Brors, B., & Sunyaev, A. (2022). A scoping review of distributed ledger technology in genomics: thematic analysis and directions for future research. *Journal of the American Medical Informatics Association : JAMIA*, *29*, 1433–1444. https://doi.org/10.1093/jamia/ocac077
9. Harrell, D. T., Usman, M., Hanson, L., Abdul-Moheeth, M., Desai, I., Shriram, J., de Oliveira, E., Bautista, J. R., Meyer, E. T., & Khurshid, A. (2022). Technical Design and Development of A Self-Sovereign Identity Management Platform for Patient-Centric Health Care Using Blockchain Technology. *Blockchain in healthcare today*, *5*. https://doi.org/10.30953/bhty.v5.196
10. Alamri, B., Crowley, K., & Richardson, I. (2022). Cybersecurity Risk Management Framework for Blockchain Identity Management Systems in Health IoT. *Sensors (Basel, Switzerland)*, *23*, 218. https://doi.org/10.3390/s23010218
11. Javed, I. T., Alharbi, F., Bellaj, B., Margaria, T., Crespi, N., & Qureshi, K. N. (2021). Health-ID: A Blockchain-Based Decentralized Identity Management for Remote Healthcare. *Healthcare (Basel, Switzerland)*, *9*, 712. https://doi.org/10.3390/healthcare9060712
12. Khurshid, A., Holan, C., Cowley, C., Alexander, J., Harrell, D. T., Usman, M., Desai, I., Bautista, J. R., & Meyer, E. (2021). Designing and testing a blockchain application for patient identity management in healthcare. *JAMIA open*, *4*, ooaa073. https://doi.org/10.1093/jamiaopen/ooaa073
13. Sabrina, F., Li, N., & Sohail, S. (2022). A Blockchain Based Secure IoT System Using Device Identity Management. *Sensors*, *22*, 7535. https://doi.org/10.3390/s22197535
14. Abdul-Moheeth, M., Usman, M., Harrell, D. T., & Khurshid, A. (2022). Improving Transitions of Care: Designing a Blockchain Application for Patient Identity Management. *Blockchain in healthcare today*, *5*. https://doi.org/10.30953/bhty.v5.200
15. Ishmaev G. (2021). Sovereignty, privacy, and ethics in blockchain-based identity management systems. *Ethics and information technology*, *23*, 239–252. https://doi.org/10.1007/s10676-020-09563-x
16. Zhu, X., & Badr, Y. (2018). Identity Management Systems for the Internet of Things: A Survey Towards Blockchain Solutions. *Sensors (Basel, Switzerland)*, *18*, 4215. https://doi.org/10.3390/s18124215
17. Gamage, H. T. M., Weerasinghe, H. D., & Dias, N. G. J. (2020). A survey on blockchain technology concepts, applications, and issues. *SN Computer Science*, *1*, 114. https://doi.org/10.1007/s42979-020-00123-0
18. Liang, X., Alam, N., Sultana, T., Bandara, E., & Shetty, S. (2024). Designing A Blockchain-Empowered Telehealth Artifact for Decentralized Identity Management and Trustworthy Communication: Interdisciplinary Approach. *Journal of medical Internet research*, *26*, e46556. https://doi.org/10.2196/46556