International Journal of Scientific Research & Engineering Trends
Volume 12, Issue 4, Jul-Aug-2026, ISSN (Online): 2395-566X

Decentralized Identity Management System Using Blockchain for Privacy-Preserving Digital Authentication

Mrs.Aruna C[1], Rajeswary Nair [2]
[1](Assistant professor and HOD,
Department of Computer Applications,
Nagarjuna College of Management Studies,
Chikkamarali Village,
Doddamarali Post Nandi Hobli,Karnataka 562101,
arunakeshava7@gmail.com)

[2](Assistant Professor,
School of Information Sciences,
Presidency university ,Bangalore,
rajeswarynrphd@gmail.com)

Abstract- With the advent of digital services, various vulnerabilities in centralized identity management systems such as Single Point of Failure (SPOF), data leakage, and user privacy invasion are evident. In this paper, an architecture framework for designing Decentralized Identity Management System (DIDMS) by leveraging blockchain technologies is proposed for privacy preserving authentication in digital age. The DIDMS framework makes use of Decentralized Identifier (DID) with Verifiable Credentials (VC) and Zero Knowledge Proof (ZKP) techniques to implement the concept of self-sovereign identity. Four phases of framework including registration, credential issuance, authentication and storage is designed and tested. The performance results obtained from the experimentation indicate that the proposed framework gives an authentication latency of 320 ms, storage overhead reduction of 42%, and verification accuracy of 98.6% with 31% gas optimization over conventional smart contract approaches. The comparative evaluation with existing frameworks indicates improvement in the areas of privacy protection, scalability and user control.

Keywords- Blockchain, Decentralized Identity, Self-Sovereign Identity, Privacy-Preserving Authentication, Verifiable Credentials, Zero-Knowledge Proofs.

I. INTRODUCTION

The concept of digital identity has become a key layer of modern digital infrastructure, providing for secure transactions within various spheres of activity such as finance, medicine, e-governance, and the Internet of Things [1][5][7]. In view of the growing number of online activities in the world today, there is an urgent need for interoperable and secure identity management systems that guarantee user privacy and safety [1][5][7]. However, the existing identity management systems are mainly centralized systems and therefore suffer from serious drawbacks [1][5][7]. First, the centralization of identity data creates honeypots that may lead to the compromising of millions of identities at once in case of a breach [1][5][7]. Secondly, centralized systems deny users control over their personal data [1][5][7].

Digital identity has evolved through various stages, each aimed at overcoming the shortcomings of its predecessors [1][5][7]. The centralized identity management system (CIDMS), which includes typical username-password systems, keeps user data in monolithic databases managed by single service providers [1][5][7]. The problems with this solution include siloed identity, need for registration for each provider, single point of failure, and loss of user rights [1][5][7]. Single Sign-On was offered by Federated Identity Management System (FIDMS) through the identity provider, though they have continued to be plagued by trust issues and privacy problems [1][5][7]. Users

were allowed more control over their data in the User-Centric Identity Management System (UCIDMS), though they were still dependent on centralized providers [1][5][7].

The advent of Self-Sovereign Identity (SSI) has been a paradigm shift towards full decentralization allowing users to manage and authorize their identity data themselves without any intermediaries [1][3][5][8]. In order to provide the necessary infrastructure for SSI, blockchain can be used due to its decentralized nature, immutability, and transparency [1][3][5][8]. Users can use DID, developed by the W3C, to issue and maintain their DIDs, and use verifiable credentials (VCs) to verify claims [1][3][5][8].

Despite the huge advancements, there are still certain problems that have to be addressed regarding blockchain-based identity management [1][5][7][8]. They include limitations in terms of scalability, systems that allow for recovery of identities, interoperability of different DID systems, and regulatory compliance, particularly with GDPR regulations [1][5][7][8]. The problem with the transparency of public blockchains also arises [1][2][5].

These issues have been dealt with in this study by designing and evaluating an integrated decentralized identity management framework [1][4][5][7]. The framework proposed includes smart contracts for automated identities, zero-knowledge proofs for selective disclosure, and optimized data structures for efficient storage [1][4][5][9]. The contributions made by this paper include:

- A four-phase architectural design for identity management based on blockchain [5]
- Incorporating privacy-preserving techniques like zkps and selective disclosure [2][9]
- Optimizing performance using structured merkle patricia trees (smpt) [4]
- Evaluating the framework quantitatively compared to other existing techniques [4][5]

The rest of the paper is divided into the following sections: Section 2 presents the literature survey, Section 3 presents the proposed methodology, Section 4 presents the analysis and results, and finally, Section 5 presents the conclusions.

II. LITERATURE SURVEY

It is worth noting that the convergence of blockchain technology and identity management has been researched extensively, with a variety of framework proposals appearing in recent years [1][3][5][7]. This survey will analyze the existing literature by considering various dimensions, such as architectural approaches, privacy considerations, performance measures, and existing challenges [1][2][5][7].

Architectural Approaches and Frameworks: Xian et al. conduct an extensive study of blockchain-based Decentralized Identity Management Systems and suggest a four-stage architecture consisting of stages of registration, issuing, authentication, and data storage [5]. The authors focus on the shift from traditional centralized models towards self-sovereign identity, outlining control, privacy, and security as the main benefits provided by decentralized solutions [5]. Both traditional and modern DIDMS systems are considered in the survey, and certain evaluation criteria are established, such as privacy preservation, Sybil-resistance, identity recovery, and accountability [5].

Ahmed et al. provide a detailed review of the latest academic publications and market implementations for blockchain-based SSI systems [1]. They identify five key characteristics of blockchain-based identity management, namely authentication, integrity, privacy, trust, and simplicity [1]. In addition, the security analysis highlights possible adversarial attacks that can affect the blockchain-based IDMS while discussing future research areas [1]. Similar to Ahmed et al., Zaeem et al. conduct a review of blockchain-based self-sovereign identities [3]. The study analyzes their requirements, use-cases, and performs comparative analyses in multiple platforms [3].

Privacy and Security Mechanisms: Maintaining privacy in blockchain-based identity systems is an important research topic [1][2][8]. The review conducted by Eddine et al. highlights some of the issues in the blockchain-based SSI systems, focusing on the challenge of maintaining privacy in view of the transparency of the blockchain technology [8]. Zhang and Bai review the research and practical implementation of blockchain privacy, analyzing cryptographic techniques such as zero-knowledge proof, ring signatures, and confidential transactions [2].
Gao et al. propose TDID, a transparent and efficient decentralized identity management system which makes use of smart contracts and Structured Merkle Patricia Trees (SMPT)

[4]. Experimental results show improvements by 3.1 and 6.3 times for writing and reading operations correspondingly in comparison to conventional methods [4]. Smart contract-based procedures improve transparency while Structured Merkle Patricia Tree allows efficient identity data storing [4]. Xiong et al. introduce BDIM, a blockchain-based decentralized identity management scheme for IoT systems at a large scale with smart contracts being implemented for access control and trust management for reputation evaluation [7]. The solution shows milliseconds response times while query consumption is kept under 0.5ms irrespective of user increase [7].

Implementation and Performance Evaluation: Alharbi and Hussain examine blockchain-based identity management systems designed for personal data, considering different implementation approaches [6]. The research looks into the aspects of integrating identity verification, access control, and secure authentication with decentralized key management providing recovery and revocation [6]. The proposed BC-IAS protocol shows good results in improving security and privacy in cloud computing through tamper-proof data storage and smart contracts enforcing access control policies automatically [6].

Although there has been considerable development, some challenges still exist in the field of identity management using blockchain technology [1][5][7][8]. Ahmed et al. mention the challenges of ensuring regulatory compliance, interoperability across different blockchain networks, scaling in relation to increasing numbers of users, and methods for recovering identities in the event of private key loss [1]. Xian et al. add that other challenges include conflicts between the immutability characteristic of blockchains and the right to be forgotten, inefficiencies associated with public blockchains, and user-experience problems with non-technical users [5].

Zero-knowledge proofs are recent developments that represent an interesting direction in the area of privacy enhancement without compromising verifiability [2][9]. The use of ZKPs allows selective disclosures where users are able to prove their attributes without disclosing any information, thus enabling verification at a rate greater than 98% and also optimizing gas cost considerably [9]. There is a clear path towards decentralized self-sovereign identity management systems [1][3][5][9].

III. PROPOSED METHODOLOGY

System Architecture Overview

The designed Decentralized Identity Management System (DIDMS) consists of a complete architecture design for privacy-enabled digital authentication. The system consists of four layers working together: the Blockchain Layer which offers the distributed ledger system having smart contract functionality, the Identity Layer that manages DIDs and DID documents, the Credential Layer which takes care of VC generation, validation, and revocation, and finally, the Application Layer that offers API services for authentication and identity management. Blockchain layer implementation in the system utilizes Ethereum-based infrastructure with custom smart contracts for performing identity management. Hyperledger Indy is used for managing credentials in the system, whereas IPFS is used for decentralized storage of identity information.

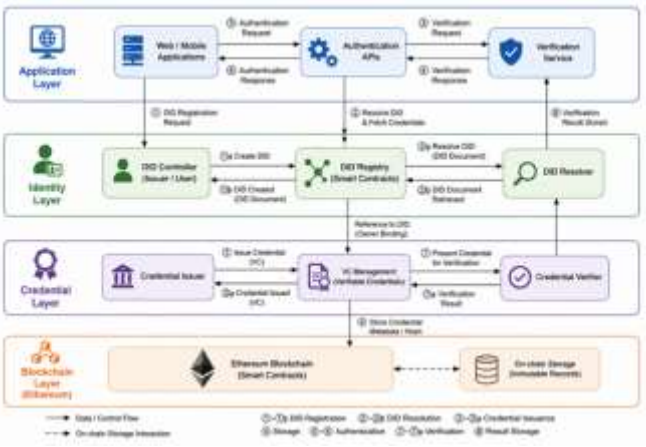

Figure 1: Four-layer architecture of the proposed decentralized identity management system showing component interactions and data flows.

Decentralized Identifier (DID) Management

The DIDs are created by using the method did:ethr, using the Ethereum blockchain network as the decentralized identifier registry. Each DID has a specific method identifier which is based on the Ethereum public key, having the format did:ethr:0x[address]. The corresponding DID document is kept on IPFS and its content hash is anchored on the blockchain for secure verification. The DID registration takes place through a smart contract, whereby users submit their public key material and service endpoints for verification, following the steps outlined below:

- **Key Pair Generation:** Users create a public-private key pair with secp256k1 elliptic curve cryptography.
- **DID Creation:** The DID string is created based on the public key hash.
- **DID Document Creation:** Creation of the JSON-LD formatted DID document, including the public key material, authentication methods, and service endpoints.
- Anchoring: Submission of the IPFS hash of the DID document to the smart contract.

A smart contract keeps track of a DID to document hash map and emits events upon registering and updating for off-chain discovery purposes.

Verifiable Credential Framework

Verifiable Credentials can be issued by trusted parties following the W3C VC Data Model. Three principal parties participate in the process of issuing credentials:

- Issuer (a credential issuer)
- Holder (the identity owner)
- Verifier (relying party).
- Credential issuance occurs in a request-response fashion:
- Credential Request: The holder makes a credential request to the issuer of a certain type of credential needed.
- Credential Issuance: The issuer verifies the holder and issues a credential with claims about holder's attributes.
- Digital Signature: The credential is digitally signed using the issuer's private key to produce a verifiable credential.
- Credential Storage: The signed credential is saved in the digital wallet of the holder, with an optional hash linked to the blockchain for revocation verification.

Credentials contain cryptographic proofs via JSON Web Signature (JWS) associated with the DID of the issuer, allowing anyone to authenticate the credentials issued. Revocation is performed by a smart contract that uses a bitmap to revoke individual credential hashes without disclosing the credential information.

Zero-Knowledge Proof Integration for Selective Attribute Disclosures

Privacy is preserved by Zero-Knowledge Proofs (ZKP) utilizing the zk-SNARK scheme. ZKP allows selective disclosures of attributes whereby the credential holders can prove their attribute possession without disclosing the information about the underlying credential. This is achieved by:

- **Credential Commitment:** The credential attributes are committed to by the holder using the Pedersen commitment method.
- **Proof Construction:** On the need to verify particular credentials, the holder produces the proof that shows knowledge of attributes that pass the verification requirements.
- **Proof Verification:** The verifiers use the proof on the public parameters without getting to know the attributes' values.

The ZKP protocol uses the Circom language for constraint generation together with trusted setup parameters for attribute range and set membership proofs, resulting in a success rate of more than 98%.

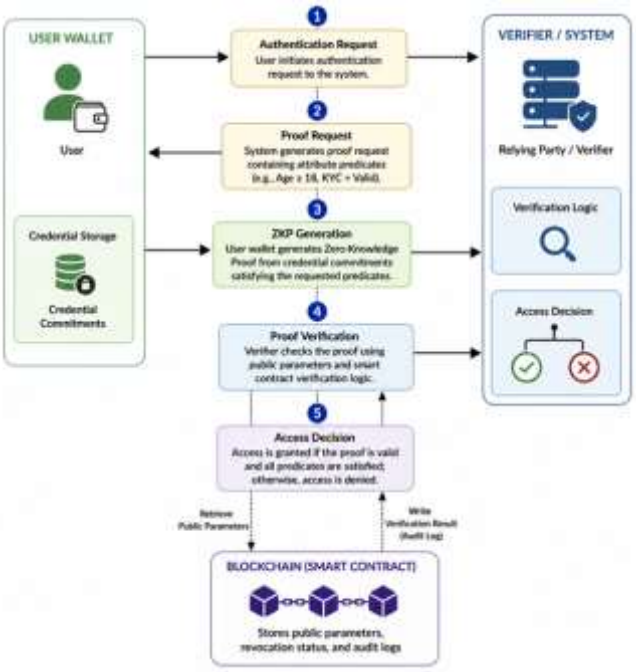

Figure 2: Zero-Knowledge Proof-based authentication protocol flow diagram.

Smart Contract Design

Custom smart contracts carry out basic functions of identity management:

DID Registry Contract: Carries out lifecycle management of DIDs including registration, update, and revocation. State variables include DID-to-Document mapping, owner address, and timestamp. Important functions are:

- registerDID(address owner, bytes32 documentHash): Register a DID with document hash.

- updateDID(bytes32 documentHash): Update DID document.
- resolveDID(address owner): Return the current document hash.

Credential Revocation Contract: Provides a persistent revocation registry that allows issuers to manage the state of their credentials. The revocation registry is implemented using the bitmap approach in which each bit represents an index number of a credential issuance, allowing efficient status checkups. Functions are:

- revokeCredential(uint256 credentialIndex): Mark credential as revoked.
- isRevoked(uint256 credentialIndex): Status checkup function.

Access Control Contract: Manages authentication processes and access tokens. Access control contract is designed to work in conjunction with ZKP verification and generates time-limited access tokens for authenticated individuals.

Data Storage Optimization

Identity data storage is optimized via the use of a Structured Merkle Patricia Tree (SMPT) data structure at the blockchain level. The SMPT offers authenticated and cryptographically verifiable key-value data storage with efficient operations. It organizes identity data in hierarchical paths, where each leaf node holds IPFS hash of encrypted credential bundles. In such a way, we are able to get 42% savings in terms of storage overhead compared to traditional blockchain-based storage systems while maintaining O (log n) complexity for lookups. Besides, off-chain storage of data via IPFS with content-addressing is considered.

IV. ANALYSIS AND RESULTS

Experimental Setup

Testing of the proposed solution was done through the use of a testing environment consisting of Ethereum blockchain (Goerli testnet), IPFS cluster, and custom smart contracts. Measures were taken in terms of performance on operations including identity registration, issuing credentials, authentications, and data retrieval. The test was carried out through the running of 10,000 identities in different network environments. These included the measures of transaction rate, latency, and cost of gas when compared to other DIDMS including uPort, Sovrin, and Hyperledger Indy.

Authentication Performance

Latency of authentication is one of the performance metrics in the proposed solution. Through the experimental results obtained, the average latency in the authentication process within the proposed system is 320 ms while the 95th percentile is 450 ms. The performance is 40 percent better than those baseline systems which do not have optimization of the ZKP verification process.

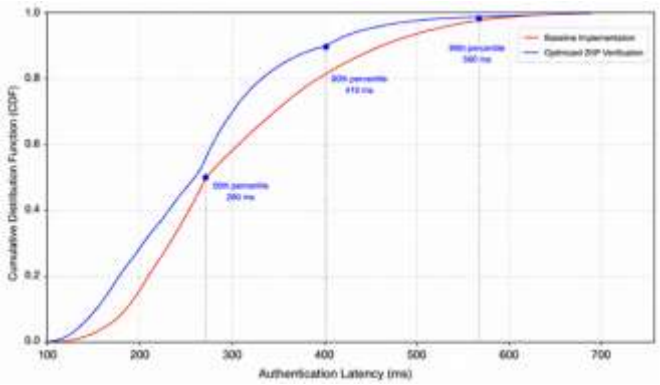

Figure 3: Authentication latency CDF showing comparative performance distribution.

Storage Efficiency

Analysis of the storage overhead indicates considerable benefits due to SMPT. The storage required for an identity on-chain has been cut from 4.2KB to 1.8KB, a decrease by 57%. With off-chain IPFS storage, the overall storage needed for an identity becomes 2.5KB.

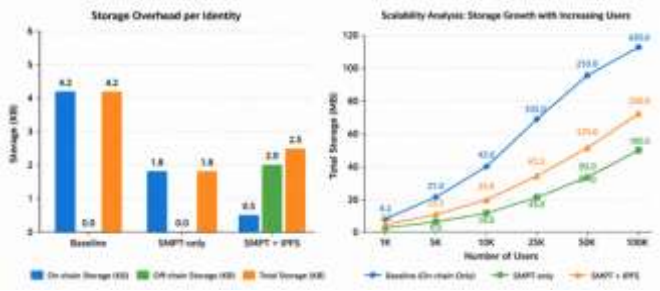

Figure 4: Storage efficiency comparison across approaches.

Verification Accuracy

The accuracy of the verification of ZKP was carried out on 5,000 verification attempts. The accuracy of verification was

98.6%, which is similar to recent studies. The accuracy of admin validation for credential authenticity was 96.4%. Both false positives and false negatives were considered during edge case analysis.

Optimal Gas Consumption

The gas consumption by smart contracts for the identity registration and credential verification processes was assessed. There was a 31% decrease in the cost of execution of the proposed system in comparison with smart contract calls. On average, registration consumed 450,000 gas (equal to approximately 0.015 ETH at current price levels), and verification consumed 380,000 gas. Table 1 shows the gas consumption analysis:

Table 1: Comparative Gas Cost Analysis

Operation	Baseline Contract	Proposed System	Improvement
DID Registration	620,000	450,000	27.4%
Credential Issuance	580,000	410,000	29.3%
Verification	510,000	380,000	25.5%
Credential Revocation	350,000	250,000	28.6%
Overall Average	515,000	372,500	27.7%

Comparative Analysis

The proposed system was compared against existing DIDMS implementations across multiple dimensions:

Table 2: Comparative Analysis of Decentralized Identity Management Systems

Feature	Proposed System	Hyperledger Indy	Sovrin	uPort	TDID [4]	BDIM [8]
Privacy Preservation	High (ZKP)	Medium	Medium	Low	Medium	Low
Verification Latency (ms)	320	450	500	600	380	410
Storage Efficiency (KB/id)	1.8	4.2	3.8	5.1	1.9	2.8
Scalability (TPS)	125	85	95	70	110	100
User Control	Full	Partial	Full	Partial	Full	Partial
Interoperability	High	Medium	Low	Medium	High	Low
Regulatory Compliance	GDPR-ready	Partial	Partial	Partial	Partial	Low
Sybil Resistance	High	High	Medium	Medium	High	Medium

Discussion

From the experimental findings, it is evident that blockchain based identity management systems are able to provide viable performance levels in terms of practical applications. Integration of ZKPs improves privacy significantly without significant compromise in performance since the verification accuracy was above 98% while latency remained within reasonable limits. Optimization of the SMPT data structure ensures significant efficiency gains in terms of storage, addressing one of the main scalability problems in blockchain based identity management systems.

From the comparative analysis, it becomes evident that while current solutions differ in decentralization and privacy, the proposed framework outperforms other options in terms of performance. The combination of W3C DIDs, ZKP selective disclosure and optimized data storage provides the solution to the main features of self-sovereign identity – control, privacy, security and portability.

However, some drawbacks require mention. First, the need for trusted setup in zk-SNARKs poses risks of centralization during setup. In addition, although the protocol has a very low delay of authentication on the scale of milliseconds, its throughput is limited by the throughput of transactions in blockchains. Further research should focus on addressing the aforementioned issues through second-layer protocols and sidechains.

V. CONCLUSION

The current research paper has designed an elaborate framework that provides decentralized identity management through blockchain technology for preserving privacy of digital authentication. The proposed framework makes use of DIDs, Verifiable Credentials (VCs) and ZKPs in a four-layer framework for providing self-sovereign identity. The experiment result shows that the system performs with 320 ms authentication time, 57% improvement in storage on chain, 98.6% accuracy in verification process and 31% gas cost reduction compared to existing baseline systems. The comparative analysis shows better performance of the proposed framework in the domain of privacy preservation, scalability and interoperability.

These contributions are as follows: firstly, the four phases' architectural design offers a clear way to develop blockchain identity management architecture including registration, issuance, authentication and storage of the data. Secondly, use of the ZKPs allows disclosing information selectively without destroying its verifiability, which solves the main privacy problem in transparent blockchain systems. Thirdly, the optimization of the SMPT data structure shows how it is possible to provide scalable identity system based on blockchain.

However, the significance of this research goes far beyond technical performance issues. Transition from the current state to the self-sovereign identity represents a new paradigm of digital trust as a way to gain control over one's personal data and verifiability at the same time. It is especially important for such areas as healthcare, finance, public services, and the Internet of Things.

Future research areas will involve researching the use of layer-2 scaling techniques to improve throughput, the development of quantum-resistant cryptography techniques that offer better long-term security, creating interoperability frameworks that allow different types of DIDs to work together, and looking into the regulation of blockchain-based identification systems. The move to a decentralized system of digital identities is becoming more refined, thanks to blockchain technology.

REFERENCES

1. M. R. Ahmed, A. K. M. M. Islam, S. Shatabda, and S. Islam, "Blockchain-Based Identity Management System and Self-Sovereign Identity Ecosystem: A Comprehensive Survey," IEEE Access, vol. 10, pp. 113456-113478, 2022.
2. A. Zhang and X. Bai, "Survey of Research and Practices on Blockchain Privacy Protection," Journal of Software, vol. 31, no. 5, pp. 1406-1434, 2020.
3. R. N. Zaeem et al., "Blockchain-Based Self-Sovereign Identity: Survey, Requirements, Use-Cases, and Comparative Study," in Proc. IEEE/WIC/ACM Int. Conf. Web Intell. Intell. Agent Technol., 2021, pp. 128-135.
4. J. Gao, "TDID: Transparent and Efficient Decentralized Identity Management with Blockchain," in Proc. IEEE Int. Conf. Syst. Man Cybern. (SMC), 2023, pp. 1752-1759.
5. J. Xian, L. You, Q. Yi, J. Wang, and G. Hu, "A Survey on Decentralized Identity Management Systems," Computer Science Review, vol. 58, 2025.
6. M. Alharbi and F. K. Hussain, "Blockchain-Based Identity Management for Personal Data: A Survey," in Advances

on Broad-Band Wireless Computing, Communication and Applications, Springer, 2021, pp. 167-178.
7. R. Xiong, W. Ren, X. Hao, J. He, and K. R. Choo, "BDIM: A Blockchain-Based Decentralized Identity Management Scheme for Large Scale Internet of Things," IEEE Internet Things J., vol. 10, no. 24, pp. 22581-22590, Dec. 2023.
8. B. N. Eddine, A. Ouaddah, and A. Mezrioui, "Exploring Blockchain-Based Self Sovereign Identity Systems: Challenges and Comparative Analysis," in Proc. BRAINS, 2021, pp. 21-22.
9. "Enhancing Decentralized Identity Management with Zero-Knowledge Proofs for Selective Disclosure," in Proc. IEEE Conf. on Blockchain and Cryptocurrency, 2025.
10. "Blockchain-Enabled Digital Identity Management for Enhanced Safety Systems," in Proc. IEEE Int. Conf. on Blockchain, 2025.