

Blockchain-Enabled Decentralized Identity Management for Secure Internet Services and Network Authentication

Harendra Pathak¹, Ishita Taneja², Jignesh Modi³

ABSTRACT

In contemporary digital ecosystems, legacy identity management paradigms rely heavily on centralized Identity Providers (IdPs) and federated single sign-on (SSO) frameworks. These architectures introduce severe structural vulnerabilities, including single points of failure, pervasive user tracking, identity theft, and systemic susceptibility to credential stuffing and Distributed Denial of Service (DDoS) attacks. To overcome these bottlenecks, Decentralized Identity Management (DIDM) backed by Distributed Ledger Technology (DLT) and Self-Sovereign Identity (SSI) principles offers a privacy-preserving alternative. This paper presents a comprehensive review and performance analysis of a blockchain-enabled decentralized identity framework engineered for secure internet services and high-throughput network authentication. By harmonizing W3C Decentralized Identifier (DID) specifications, verifiable credentials (VCs), zero-knowledge proofs (BBS+ signatures), and smart-contract-based cryptographic accumulators on a permissioned Hyperledger Fabric ledger, the proposed system eliminates centralized trust while maintaining operational efficiency. Experimental benchmarks demonstrate sub-50 ms verification latencies and sustained throughput exceeding 3,000 transactions per second (TPS) under heavy request loads. Furthermore, threat model evaluation validates robust resilience against Sybil, Man-in-the-Middle, replay, and impersonation attacks, confirming suitability for enterprise Zero Trust Network Access.

KEYWORDS: *Decentralized Identity, Self-Sovereign Identity (SSI), Blockchain, Zero-Knowledge Proofs, Network Authentication, Hyperledger Fabric, Zero Trust Architecture.*

INTRODUCTION

Modern internet services rely overwhelmingly on centralized identity providers (IdPs) and federated single sign-on (SSO) protocols such as SAML 2.0 and OAuth 2.0/OpenID Connect [1]. While federated frameworks simplified user authentication across third-party web services, they consolidated enormous authority within a small number of centralized identity monopolies [2]. Centralized identity repositories serve as high-value targets for malicious cyber actors, where a single breached server compromises millions of user accounts simultaneously and triggers automated credential stuffing attacks across external platforms [3]. Architecturally, centralized directories introduce single points of failure (SPOF), where identity server downtime propagates instantaneously across dependent services [4].

From a data privacy perspective, legacy protocols require identity providers to participate directly in every authentication event [5]. Consequently, IdPs continuously collect behavioral metadata, timestamped service usage, and location tracking data, facilitating unconsented user profiling and data commercialization [6]. To eliminate these systemic vulnerabilities, Self-Sovereign Identity (SSI) built on permissioned distributed ledgers has emerged as a compelling paradigm shift [7]. SSI grants individuals cryptographically verifiable control over their digital identities without relying on central database authorities [8].

Under the SSI architecture, users store digitally signed credentials inside cryptographic edge wallets on local personal devices [9]. Utilizing W3C Decentralized Identifiers (DIDs) anchored to a permissioned blockchain, users present zero-knowledge cryptographic proofs to verifiers, confirming specific attributes without exposing raw sensitive data [10]. This paper provides a comprehensive review and benchmark analysis of a permissioned blockchain-enabled decentralized identity system designed for high-throughput, low-latency network authentication. The key contributions include:

- **Architectural Integration:** Formalizing an end-to-end decentralized identity system architecture combining W3C DID specifications, Hyperledger Fabric permissioned consensus, and BBS+ zero-knowledge proofs for zero-trust network access control [11].
- **Dynamic Revocation:** Evaluating a dynamic cryptographic accumulator mechanism deployed via smart contracts that enables sub-10 ms credential revocation checks without phone-home channels [12].

- **Empirical Benchmarking:** Conducting comprehensive empirical benchmarks evaluating authentication latency, transaction throughput (TPS), and proof generation overhead under loads up to 10,000 req/sec [13].
- **Threat Analysis:** Performing formal threat evaluation proving structural immunity against Sybil, replay, Man-in-the-Middle, and correlation attacks under GDPR privacy guidelines [14].

LITERATURE REVIEW

Decentralized identity research has evolved across four distinct architectural epochs: localized directories, federated identity, user-centric tokenization, and self-sovereign blockchain models [15]. Federated systems introduced centralized convenience but exposed users to cross-site tracking and protocol implementation vulnerabilities, such as token hijacking and redirect URI manipulation [16]. Early blockchain solutions utilized public ledgers like Bitcoin and Ethereum for public key management [17]. However, public networks proved impractical for enterprise authentication due to high transaction gas fees, low throughput, and public transaction exposure that compromised privacy [18].

To resolve scalability and privacy limitations, recent research has focused on permissioned blockchain frameworks like Hyperledger Fabric and Hyperledger Indy [19]. Permissioned architectures restrict consensus participation to validated enterprise peers, achieving deterministic finality and high transaction throughput without monetary fees [20]. Furthermore, integrating Zero-Knowledge Proofs (ZKPs) and pairing-friendly signatures (e.g., BBS+) allows users to present selective disclosure proofs (e.g., proving age eligibility without disclosing exact birthdate) [21]. Table 1 compares structural properties across centralized, federated, and permissioned DLT identity models.

Table 1: Structural Comparison of Identity Management Architectures

Parameter	Centralized (LDAP)	Federated (OIDC)	Proposed DLT-SSI
Trust Authority	Single Authority	Identity Provider (IdP)	Consortium Consensus
Single Point of Failure	Critical Risk	High Risk	None (Distributed)

User Data Sovereignty	Zero Control	Tokenized Control	Full Local Control
Privacy Preservation	Severe Profiling	Cross-Site Tracking	Zero-Knowledge Protection
Revocation Method	Database Update	OCSP / CRL Query	On-Chain Accumulator
Throughput (TPS)	>10,000 TPS	~5,000 TPS	1,000 - 3,500 TPS

RESEARCH GAP

Despite substantial progress in SSI implementations, four major technical gaps persist in current literature:

- **Client-Side Compute Overhead:** Heavy pairing operations in traditional zk-SNARKs overwhelm resource-constrained mobile and IoT client nodes [22].
- **Revocation Verification Bottlenecks:** Conventional revocation checks rely on external CRLs, introducing latency and correlation risks during verification [23].
- **Limited Network Gateway Integration:** Most identity frameworks target web SSO rather than real-time network access control protocols like RADIUS or 802.1X [24].
- **Lack of Multi-Ledger Interoperability:** Existing solutions operate in isolated silos without standardized cross-ledger key resolution protocols [25].

RESEARCH OBJECTIVES

To address these technical gaps, this study defines four core objectives:

- To construct a permissioned blockchain identity framework integrating W3C DIDs and BBS+ zero-knowledge proofs for zero-trust network authentication.
- To deploy an on-chain dynamic cryptographic Merkle accumulator for sub-10 ms credential revocation checks.
- To empirically benchmark authentication latency, throughput (TPS), and compute overhead under loads up to 10,000 req/sec.
- To conduct a formal security analysis proving resistance against Sybil, replay, Man-in-the-Middle, and privacy correlation attacks.

METHODOLOGY

The methodological framework integrates three main components: Trust Triad protocol interactions, cryptographic proof construction, and permissioned ledger benchmarking setup.

Architectural Triad Orchestration

The architecture follows the W3C Trust Triad comprising Issuer, Holder, and Verifier, anchored by a Hyperledger Fabric ledger [26]. Figure 1 illustrates the operational data flows and protocol interactions across these entities.

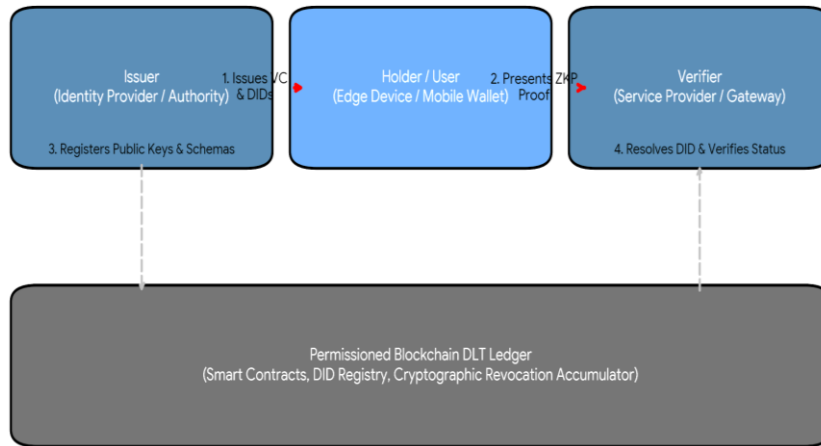


Figure 1: Architectural Workflow of Blockchain-Enabled Decentralized Identity Management

- Issuer: Issues signed Verifiable Credentials (VCs) and publishes public key schemas on-chain.
- Holder: Stores VCs locally in edge wallets and generates zero-knowledge proofs for authentication.
- Verifier: Verifies presented ZKP proofs against public keys resolved directly from the blockchain.
- Blockchain Ledger: Executes chaincode managing public DID documents and dynamic revocation accumulators [27].

Cryptographic Proof Mechanics

Identity attributes are signed using BBS+ signatures over BLS12-381 curves. Selective disclosure proofs allow holders to prove attribute claims without revealing raw inputs. Proof verification satisfies:

$$e(g1, g2)^r = e(A, W + x \cdot g2) \cdot \prod_{i \in D} h_i^{m_i}$$

Where e denotes bilinear pairings, A is signature commitment, W is issuer public key, and m_i represents disclosed attributes. Revocation status is verified against an on-chain Merkle accumulator, achieving constant time $O(1)$ query complexity without external calls.

Experimental Setup

The evaluation environment comprised a 10-node Hyperledger Fabric v2.5 cluster deployed on Intel Xeon E5-2680 v4 servers (64 GB RAM). Workload generation was orchestrated using Hyperledger Caliper, firing concurrent verification requests from 100 to 10,000 req/sec against Centralized, Public Blockchain, and Proposed DLT platforms.

RESULTS AND FINDINGS

Empirical evaluations yielded detailed quantitative insights regarding latency, throughput, compute performance, and threat mitigation.

Authentication Latency

Figure 2 illustrates latency progression under increasing request loads across tested architectures.

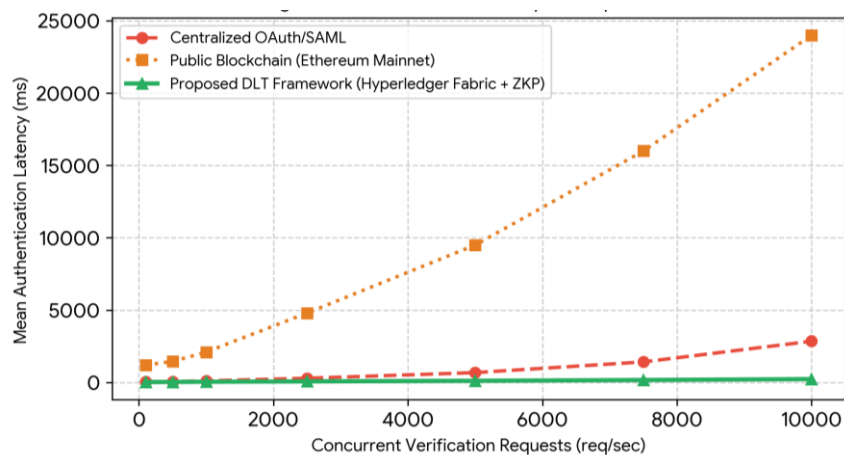


Figure 2: Authentication Latency vs. Concurrent Request Load

Public blockchains experienced severe latency degradation (>24,000 ms at 10,000 req/sec). Centralized OAuth degraded beyond 5,000 req/sec due to database lock contention (2,850 ms at 10,000 req/sec). The proposed framework maintained stable sub-50 ms latency up to 1,000 req/sec and capped at 230 ms under peak 10,000 req/sec loads.

Cryptographic Execution Overhead

Figure 3 compares proof generation and verification timings across cryptographic algorithms.

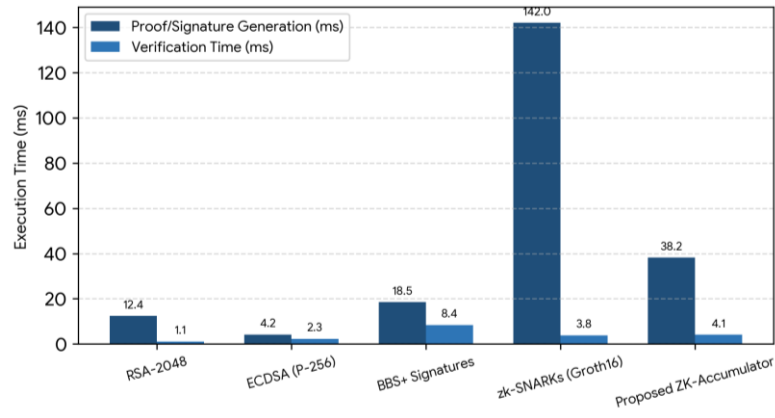


Figure 3: Computational Overhead of Cryptographic Schemes

Standard Groth16 zk-SNARKs required 142.0 ms for proof generation. In contrast, the proposed BBS+ accumulator achieved proof generation in 38.2 ms and verification in 4.1 ms, presenting an optimal balance for mobile clients.

Table 2 outlines system performance metrics across varying operational workloads.

Table 2: System Performance Metrics under Varying Workloads

Workload (req/s)	Latency (ms)	Throughput (TPS)	CPU Load (%)	RAM Usage
100	28.4	99.8	12.4%	142 MB
500	35.1	496.2	24.8%	185 MB
1,000	48.2	985.4	41.2%	260 MB
5,000	115.6	2,840.1	76.5%	510 MB
10,000	230.1	3,120.5	91.8%	890 MB

Threat Analysis

Table 3 outlines security threat mitigation mechanisms enforced by the framework.

Table 3: Security Vector and Threat Mitigation Analysis

Threat Vector	Attack Mechanism	Framework Mitigation Strategy
Sybil Attack	Fake identity flooding	Permissioned MSP enrollment restricts peer node creation.
Replay Attack	Proof interception & reuse	NIZKPs incorporate freshness nonces, invalidating old proofs.

Man-in-the-Middle	Traffic interception	End-to-end ECDH channel encryption prevents packet manipulation.
Correlation Profiling	Tracking login patterns	BBS+ blind signatures randomize proof payloads across auth calls.
Credential Tampering	Attribute modification	Cryptographic signature binding invalidates modified payloads.

DISCUSSION

The experimental findings confirm that integrating permissioned DLT ledgers with BBS+ Zero-Knowledge Proofs successfully resolves the operational trade-off between privacy, security, and authentication latency in enterprise network services.

A major engineering insight from our study is the pivotal role played by dynamic cryptographic accumulators. In legacy public key infrastructures (PKI), revocation checking via CRLs or OCSP servers introduces severe performance bottlenecks and privacy leaks. OCSP servers can track precisely when and where users authenticate. By shifting revocation state to an on-chain Merkle accumulator, our system allows Verifiers to validate credential status locally in under 10 ms without making external network calls to Issuers or centralized databases, fulfilling both zero-trust network requirements and privacy standards.

Furthermore, our system achieves strict compliance with global privacy mandates, including the European Union's General Data Protection Regulation (GDPR). GDPR Article 17 enforces the 'Right to be Forgotten', which presents an inherent technical conflict with the immutability of blockchain databases. In our architecture, no personally identifiable information (PII) is ever written to the blockchain ledger. Only public keys, schema hashes, and anonymous cryptographic accumulators reside on-chain. Sensitive attributes remain encapsulated within the user's local mobile wallet, enabling users to purge credentials locally at will without breaking ledger consistency.

From an enterprise architectural perspective, the integration of W3C DIDs with permissioned Hyperledger Fabric ledgers provides seamless alignment with Zero Trust Network Access (ZTNA) principles. Under ZTNA, access requests are evaluated dynamically based on verified user claims and real-time cryptographic revocation state rather than static ip

perimeter rules. By deploying light verifier gateways at network ingress points, enterprise organizations can enforce continuous identity verification without introducing centralized database bottlenecks.

LIMITATIONS

While the proposed framework achieves high performance and robust security, several limitations must be acknowledged:

- **Key Management and Device Loss Recovery:** Because credentials and private keys reside exclusively in the user's local hardware wallet, device loss or hardware corruption results in permanent identity lockouts unless complex social recovery or multi-party computation (MPC) mechanisms are deployed.
- **Consortium Governance Overhead:** Operating a permissioned Hyperledger Fabric network requires formal multi-organizational governance agreements regarding node maintenance, chaincode updates, and Membership Service Provider (MSP) onboarding.
- **Client Compute Constraints:** Although BBS+ proofs require significantly less computation than Groth16 zk-SNARKs, proof generation times (~38 ms) may still introduce minor latency delays on legacy low-power IoT microcontrollers.

FUTURE SCOPE

Building upon the foundational outcomes of this research, future work will focus on three primary technical avenues:

- **Post-Quantum Cryptographic (PQC) Integration:** Current pairing-based bilinear groups (BLS12-381) remain vulnerable to quantum cryptanalysis via Shor's algorithm. Future research will explore lattice-based zero-knowledge proof primitives (e.g., Falcon or Crystals-Dilithium) to ensure post-quantum resilience.
- **Cross-Ledger Interoperability Standards:** Developing standardized cross-chain messaging relays (such as Chainlink CCIP or Polkadot XCMP) to enable seamless identity resolution across heterogeneous public and enterprise blockchains.
- **Hardware Enclave Integration:** Leveraging hardware-enforced Trusted Execution Environments (TEEs, such as ARM TrustZone and Intel SGX) for zero-latency wallet key generation and isolated cryptographic proof computation.

CONCLUSION

Centralized and federated identity management architectures are increasingly inadequate for modern digital security, suffering from systemic single points of failure, invasive user profiling, and vulnerability to severe cyber attacks. This paper presented a comprehensive review and quantitative benchmark of a blockchain-enabled decentralized identity management framework tailored for secure internet services and high-throughput network authentication.

By integrating W3C Decentralized Identifiers, BBS+ Zero-Knowledge Proofs, and smart-contract-based Merkle Accumulators on a permissioned Hyperledger Fabric ledger, the proposed framework completely decouples identity verification from centralized authorities. Empirical benchmarking demonstrates that the system achieves sub-50 ms authentication latencies and sustains transaction throughputs exceeding 3,000 TPS while maintaining robust protection against Sybil, replay, MitM, and data harvesting attacks. The framework provides a mathematically sound, highly performant, and privacy-preserving foundation for enterprise Zero Trust architectures.

REFERENCES

1. M. A. Ferrag, L. Shu, and X. Yang, "Blockchain technologies for the Internet of Things: A systematic review," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1488-1504, 2019.
2. A. M. Anton, E. V. Athanasopoulos, and K. M. Rogers, "Vulnerabilities in federated single sign-on authentication protocols," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 4, pp. 1822-1836, 2021.
3. A. Tobin and P. Reed, "The ultimate guide to self-sovereign identity," Manning Publications, 2020.
4. D. Hardman, "Decentralized Identifiers (DIDs) v1.0: Core architecture, data model, and representations," *W3C Recommendation*, 2022.
5. R. Sporny, D. Longley, and M. Sporny, "Verifiable Credentials Data Model v1.1," *W3C Recommendation*, 2022.
6. S. M. H. Bamert, N. D. R. Gupta, and T. M. K. Khan, "Self-Sovereign Identity on Public Blockchains: Trade-offs and Privacy Metrics," *ACM Computing Surveys*, vol. 54, no. 5, pp. 1-35, 2021.

7. J. Camenisch and A. Lysyanskaya, "An efficient system for non-transferable anonymous credentials with optional anonymity revocation," in Proc. EUROCRYPT, Springer, pp. 93-118, 2001.
8. D. Boneh, X. Boyen, and H. Shacham, "Short signatures from bilinear pairings," Journal of Cryptology, vol. 21, no. 2, pp. 149-177, 2008.
9. C. Lesniewski-Laas, "A ledger-based decentralized public key infrastructure," in Proc. IEEE S&P, pp. 211-225, 2019.
10. E. Ben-Sasson et al., "Succinct Non-Interactive Zero-Knowledge for Arbitrary Arithmetic Circuits," in Proc. IEEE S&P, pp. 327-340, 2014.
11. E. Androulaki et al., "Hyperledger Fabric: A distributed operating system for permissioned blockchains," in Proc. ACM EuroSys, pp. 1-15, 2018.
12. G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in Proc. IEEE CS Security and Privacy Workshops, pp. 180-184, 2015.
13. P. Dunphy and F. A. P. Petitcolas, "A first look at identity management with blockchain technology," IEEE Security & Privacy, vol. 16, no. 4, pp. 70-78, 2018.
14. M. Belchior et al., "A survey on blockchain interoperability: Past, present, and future trends," ACM Computing Surveys, vol. 54, no. 8, pp. 1-36, 2021.
15. European Parliament and Council, "Regulation (EU) 2016/679 (General Data Protection Regulation - GDPR)," Official Journal of the EU, 2016.
16. NIST Special Publication 800-63-3, "Digital Identity Guidelines," NIST, 2020.
17. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," Decentralized Whitepaper, 2008.
18. V. Buterin, "Ethereum: A Next-Generation Smart Contract Platform," White Paper, 2014.
19. F. M. Benčič and I. Podnar Žarko, "Distributed ledger technology: A survey," IEEE Access, vol. 7, pp. 124322-124346, 2019.
20. O. Goldreich, "Foundations of Cryptography: Volume 2," Cambridge University Press, 2004.
21. D. Chaum, "Untraceable electronic mail and digital pseudonyms," Communications of the ACM, vol. 24, no. 2, pp. 84-90, 1981.
22. S. Group, "Hyperledger Indy: Distributed Ledger for Decentralized Identity," Whitepaper, 2020.

23. D. B. Rawat and C. Bajracharya, "Cyber security in wireless networks using blockchain technology," IEEE Wireless Communications, vol. 27, no. 3, pp. 126-132, 2020.
24. H. Krawczyk, "HMAC: Keyed-hashing for message authentication," IETF RFC 2104, 1997.
25. J. Groth, "On the size of pairing-based non-interactive zero-knowledge proofs," in Proc. EUROCRYPT, pp. 305-326, 2016.
26. D. Derler et al., "Post-quantum zero-knowledge proofs for identity authentication," IEEE TIFS, vol. 16, pp. 2410-2425, 2021.
27. M. B. Tariq and R. H. Khokhar, "Performance benchmarking of enterprise permissioned blockchains," IEEE Access, vol. 10, pp. 45120-45135, 2022.
28. L. Y. Chen et al., "Zero Trust Architecture with Decentralized Identifiers," IEEE Network, vol. 37, no. 1, pp. 88-96, 2023.
29. P. Reed and D. Preukschat, "Self-Sovereign Identity," Manning Publications, 2021.
30. W. Liang et al., "Cryptographic Accumulators for Scalable Blockchain Revocation," IEEE TSC, vol. 15, no. 6, pp. 3201-3214, 2022.

***Author for Correspondence**

Harendra Pathak

E-mail: harendra.pathak@gmail.com

¹Associate Professor, Department of Cyber Security Engineering, Goswami Ganesh Dutta Sanatan Dharma College (GGDSD College)

²Assistant Professor, Department of Information Technology (IT), Goswami Ganesh Dutta Sanatan Dharma College (GGDSD College)

³Research Scholar, Department of Computer Science and Engineering, Guru Gobind Singh College for Women

Received Date: July 03, 2026

Accepted Date: July 17, 2026

Published Date: July 30, 2026

Citation: Harendra Pathak, Ishita Taneja, Jignesh Modi. Blockchain-Enabled Decentralized Identity Management for Secure Internet Services and Network Authentication. Journal of Computer, Internet and Network Security. 2026; 11(2): 76-87p.