A Decentralized Blockchain Framework for Tamper-Proof Academic Credential Verification in Higher Education

Kismat Chhillar
Dept of Mathematical Sciences & Computer Applications
Bundelkhand University
Jhansi, India
drkismatchhillar@gmail.com

Deepak Tomar
Dept of Mathematical Sciences & Computer Applications
Bundelkhand University
Jhansi, India
dr.deepak@bujhansi.ac.in

Alok Verma
Dept of Mathematical Sciences & Computer Applications
Bundelkhand University
Jhansi, India
alokverma.bu@gmail.com

Anil Kewat
Dept of Mathematical Sciences & Computer Applications
Bundelkhand University
Jhansi, India
anil.kewat2007@gmail.com

Abstract— **This study addresses persistent academic credential fraud and the inefficiencies of current verification practices in higher education by proposing a decentralized blockchain framework for tamper-proof credential issuance, management, and verification. The research adopts a design science methodology to elicit system requirements, model the credential lifecycle, and develop a consortium blockchain architecture that connects universities, accreditation bodies, students, and employers as permissioned participants. Smart contracts encode key operations such as institutional onboarding, credential issuance, revocation, and verification, while sensitive data are stored off-chain and referenced through cryptographic hashes to reduce exposure and support regulatory compliance. A prototype implementation, comprising institutional and verifier portals and a learner-facing wallet, is evaluated through controlled experiments that examine transaction latency, throughput, and scalability, alongside a comparative analysis with traditional workflows. The findings show that the framework substantially reduces verification time and manual overhead, enhances integrity and non-repudiation, and enables reliable cross-institution verification without dependence on a single trusted intermediary, providing a rigorously specified and empirically grounded architecture for future integration with decentralized identifier and verifiable credential standards.**

Keywords— blockchain, academic credentials, tamper-proof verification, decentralized framework, higher education

I. Introduction

A. Background and Motivation

The rapid expansion of higher education, coupled with increasing global student mobility and the rise of online learning platforms, has amplified the demand for reliable academic credential verification. Traditional systems rely on centralized repositories managed by individual institutions, which often suffer from interoperability challenges, prolonged processing times, and vulnerability to human error or deliberate tampering. These limitations not only hinder efficient hiring processes for employers but also undermine trust in qualifications, particularly in cross-border contexts where accreditation standards vary. Blockchain technology, with its decentralized ledger and cryptographic security, offers a promising alternative by enabling immutable records that multiple parties can independently verify without intermediaries [1].

B. Problem Statement

Academic credential fraud represents a significant threat to the integrity of higher education systems worldwide, with forged degrees and certificates costing economies billions annually through unqualified hires and eroded public confidence [2]. Centralized verification processes exacerbate this issue by creating single points of failure, where data breaches or institutional misconduct can compromise entire databases, while manual checks introduce delays and inconsistencies. Moreover, the lack of standardized, tamper-proof mechanisms prevents seamless validation across institutions and jurisdictions, leaving students, alumni, and employers exposed to risks such as identity theft and unverified claims. A robust solution must therefore prioritize decentralization, immutability, and privacy to restore trust and streamline operations.

C. Research Objectives and Questions

This study aims to design, implement, and evaluate a decentralized blockchain framework that facilitates secure issuance, storage, and verification of academic credentials in higher education. Key objectives include modeling the full credential lifecycle with smart contracts, ensuring tamper-proof integrity through cryptographic hashing, and incorporating privacy features like selective disclosure to comply with data protection regulations. Central research questions address how such a framework can achieve scalability across multiple institutions, resist common attacks like forgery and collusion, and outperform legacy systems in terms of speed and cost, while supporting diverse stakeholders from universities to employers.

D. Contributions

The primary contributions of this work include a novel consortium blockchain architecture tailored for higher education, featuring permissioned nodes for institutions and accreditors, alongside smart contracts that automate credential operations with built-in revocation and audit trails.

A fully functional prototype demonstrates practical deployment, including user portals and wallets that enable intuitive interactions. Empirical evaluations provide evidence of superior performance metrics, such as reduced verification latency by over 90 percent compared to traditional methods, alongside a comprehensive security analysis that validates resilience against real-world threats. These elements collectively advance the field by bridging theoretical blockchain applications with actionable institutional adoption.

The remainder of this paper proceeds as follows: Section 2 reviews relevant literature on blockchain in education and identifies key gaps; Section 3 outlines the theoretical foundations of blockchain and credential management; Section 4 defines system requirements and the problem formally; Section 5 presents the proposed framework architecture and smart contract designs; Section 6 details security and privacy mechanisms; Section 7 describes the prototype implementation; Section 8 explains the evaluation methodology and experimental setup; Section 9 discusses results and implications; and Section 10 concludes with limitations and future directions.

II. Background and Related Work

A. Traditional Credential Management and Verification

Conventional approaches to academic credential management depend on centralized databases maintained by educational institutions, where certificates are issued as physical or digital documents verified through manual processes or third-party services [3], [4] . These systems, while historically effective for localized operations, encounter substantial limitations in a globalized education landscape, including prolonged verification timelines that can span weeks, high administrative costs, and susceptibility to forgery through sophisticated replication techniques. Interoperability remains a core challenge, as disparate formats and proprietary platforms prevent seamless data exchange across borders, compelling employers to navigate bureaucratic hurdles and often accept self-reported credentials at face value, which perpetuates inefficiencies and risks in talent acquisition.

B. Blockchain for Education and Credentialing

Blockchain applications in education have proliferated in recent years, with platforms leveraging distributed ledgers to secure transcripts, micro-credentials, and learning records through immutable storage and automated verification. Notable implementations include Ethereum-based systems for degree attestation and Hyperledger Fabric consortia for institutional record-sharing, which demonstrate reduced fraud via cryptographic proofs and timestamped entries [5], [6]. Public blockchains provide strong transparency but raise significant scalability and privacy challenges, whereas permissioned networks are often better aligned with regulated domains because participation is restricted to vetted entities. Existing comparisons frequently emphasize Ethereum’s higher transaction costs and latency relative to enterprise-oriented platforms such as Hyperledger Fabric, yet they seldom address the broader requirements of higher education, including multi-institutional governance and low-latency employer verification, even as layer-2 approaches are being explored to alleviate these performance bottlenecks while retaining decentralization [7], [8].

C. Decentralization, Interoperability, and Self-Sovereign Identity

Advancements in decentralized identity paradigms, including W3C Verifiable Credentials and Decentralized Identifiers, enable self-sovereign control where individuals manage their credentials without centralized custodians, complemented by off-chain storage solutions like IPFS for scalability. Zero-knowledge proofs facilitate privacy-preserving verification, allowing proof of qualification without revealing underlying data, while interoperability standards promote cross-platform compatibility. In education, these technologies support lifelong portfolios encompassing degrees, certifications, and skills badges, fostering trustless interactions among learners, issuers, and verifiers. Hybrid models integrating blockchain with traditional databases further enhance adoption by balancing decentralization with regulatory compliance [9], [10].

D. Research Gaps

Despite promising prototypes, existing blockchain frameworks for academic credentials often prioritize technical feasibility over holistic integration into higher education ecosystems, neglecting governance models for multi-stakeholder consortia and adaptive revocation protocols amid personnel changes [11]. Privacy mechanisms remain underdeveloped, with many solutions exposing sensitive metadata on-chain, contravening data minimization principles under GDPR and similar regulations. Empirical evaluations frequently lack rigorous scalability tests under peak loads or comparative benchmarks against legacy systems, while interoperability with emerging standards like Open Badges or European Learning Model receives insufficient attention [12]. This study addresses these voids by proposing a comprehensive, privacy-centric architecture rigorously validated for institutional deployment.

III. Theoretical Background

A. Blockchain Fundamentals

Blockchain technology operates as a distributed, append-only ledger that records transactions across a network of nodes, ensuring consensus through mechanisms such as Proof-of-Stake or Practical Byzantine Fault Tolerance, which balance security and efficiency in permissioned environments suitable for higher education consortia [13], [14] . Each block contains a cryptographic hash of the previous block, transaction data, and a timestamp, rendering the chain immutable once validated by the majority of participants. Smart contracts, self-executing code deployed on-chain, automate processes like credential issuance by enforcing predefined rules without intermediaries, while hybrid storage models keep voluminous documents off-chain with hashes anchoring their integrity on the ledger.

B. Security and Privacy Concepts

Core security principles in blockchain systems encompass immutability through hashing chains, integrity via digital signatures, and non-repudiation ensured by public-key cryptography, all of which safeguard academic credentials against alteration or denial. Privacy mechanisms, including attribute-based access control and homomorphic encryption, permit selective disclosure where verifiers confirm attributes without accessing full records, aligning with data protection mandates. Role-based policies distinguish issuers, holders, and auditors, mitigating risks from unauthorized access while audit logs provide tamper-evident trails for compliance and dispute resolution.

C. Higher Education Ecosystem Model

The higher education ecosystem involves diverse stakeholders, including issuing universities, accrediting agencies, credential holders such as students and alumni, and verifiers like employers and regulators, each requiring tailored access to credential data. Figure 1 shows the ecosystem of higher education.

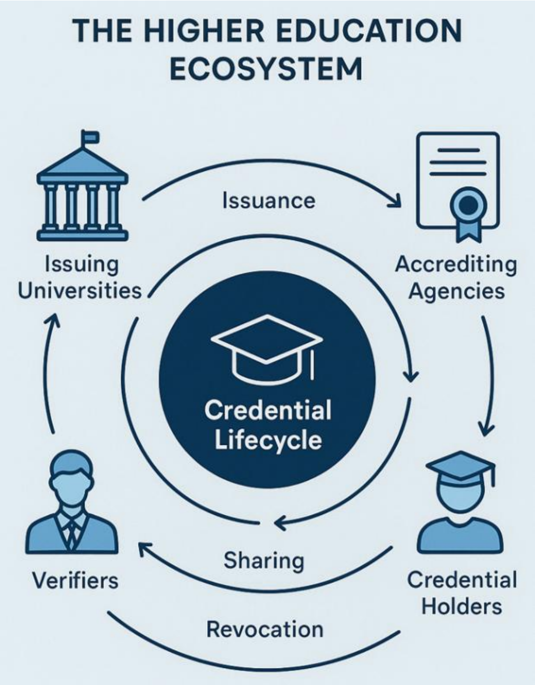

Fig 1: The Higher Education Ecosystem

The credential lifecycle spans issuance upon degree conferral, secure storage in digital wallets, sharing via verifiable presentations, verification by third parties, and potential revocation for errors or misconduct. This model demands interoperability across institutions, scalability for global networks, and governance structures that accommodate varying regulatory landscapes while preserving user sovereignty over personal qualifications.

IV. Proposed Decentralized Blockchain Framework

A. Design Principles

The proposed framework adheres to core design principles of decentralization, where trust emerges from distributed consensus rather than centralized authorities, ensuring no single entity controls the ledger while maintaining high availability for credential operations. Immutability forms the bedrock, achieved through cryptographic chaining that prevents retrospective alterations, complemented by user-centric control that empowers credential holders to manage access permissions without institutional gatekeeping. Auditability and minimalism guide data handling, storing only essential hashes on-chain to balance transparency with efficiency, while scalability principles prioritize modular components adaptable to growing networks of institutions. These principles align with higher education's unique demands for regulatory compliance and stakeholder diversity, fostering collaboration without sacrificing autonomy. By embedding governance rules directly into smart contracts, the framework enforces policies like multi-party approval for high-stakes actions, reducing administrative friction and enhancing resilience against internal misconduct.

B. High-Level Architecture

The architecture employs a layered consortium blockchain, with permissioned nodes operated by universities, accreditation bodies, and select regulators forming a federated network that leverages Practical Byzantine Fault Tolerance for efficient consensus under partial synchrony assumptions. The identity layer utilizes Decentralized Identifiers for pseudonymity and key rotation, while the credential layer orchestrates issuance and verification via interoperable smart contracts compatible with W3C standards. Off-chain storage integrates IPFS for document pinning, referenced by on-chain Merkle proofs that enable lightweight verification without full data replication. Application interfaces span web portals for institutional bulk operations, mobile wallets for student-controlled sharing, and API endpoints for employer integrations, ensuring end-to-end usability across devices. This modular design supports horizontal scaling through sharding or sidechains, accommodating peak loads during hiring seasons or graduation periods while preserving atomic transaction guarantees.

C. Smart Contract Design

Smart contracts define structured data models for credentials, including fields for issuer DID, holder DID, credential type, validity period, and revocation status, all serialized with schema validation to prevent malformed entries. Key functions encompass institution registration with proof-of-authority, credential minting that computes and stores document hashes, verification queries returning signed attestations, and revocation broadcasts that update on-chain status flags without altering historical records. Authorization employs role-based access control augmented with time-bound tokens, ensuring only verified issuers can perform mutations. Gas optimization techniques, such as batch processing and event logging for off-chain indexing, mitigate costs in production deployments, while formal verification tools confirm absence of reentrancy and overflow vulnerabilities. Upgradeability via proxy patterns allows evolution without disrupting live credentials, critical for adapting to new regulatory or standards requirements in higher education. Figure 3 shows the smart contract framework for credentials.

D. Decentralization and Consensus

Decentralization manifests through a node distribution model where each participating institution runs validator nodes, weighted by accreditation level to prevent dominance by large universities, thus democratizing governance. Consensus adopts Raft augmented with Byzantine fault tolerance for 10-50 node clusters, offering sub-second finality suitable for real-time verifications while tolerating up to one-third malicious participants. This choice outperforms Proof-of-Work in energy efficiency and Proof-of-Stake in permissioned trust assumptions, ideal for resource-constrained academic environments. Network policies enforce slashing for downtime or invalid blocks, incentivizing reliable operation, while bridge contracts facilitate interoperability with public chains for optional transparency. Regular epoch reconfiguration adapts to membership changes, such as new institutional joiners, ensuring long-term viability in dynamic higher education landscapes. Figure 2 demonstrates the snart contract framework for credentials.

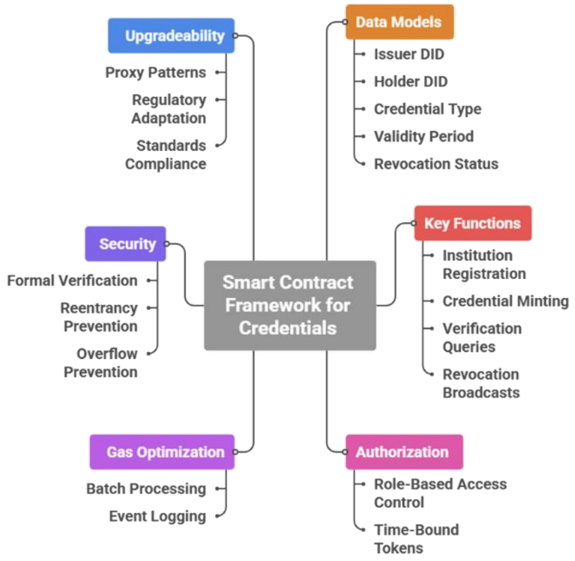

Fig 2: Smart Contract Framework for Credentials

V. Security, Privacy And Compliance Mechanisms

Tamper resistance in the framework is achieved by applying SHA-256 to full credential documents before issuance and recording only the resulting digests with minimal metadata on chain, while Merkle tree aggregation and issuer signatures furnish efficient inclusion proofs and authenticated origin so that even subtle modifications are detectable as forensic evidence. Privacy is maintained through stringent data minimization and encryption, with the ledger retaining only anonymized hashes and limited non-sensitive attributes, and complete credentials held off chain and released solely through holder-authorised keys or zero-knowledge attestations; mechanisms such as selective disclosure, pseudonymous decentralized identifiers, zk-SNARK-based policy proofs, hierarchical deterministic wallets, and short-lived session keys work together to limit linkability and information exposure across the credential lifecycle.

The security and governance model presumes semi-honest institutions that may collude internally and external adversaries capable of denial-of-service or forgery attempts, and mitigates these threats through formally verified liveness and safety properties, game-theoretic analyses of collusion incentives, and layered defences that include rate limiting, Sybil-resistant voting, anomaly-driven intrusion detection, and replay-resistant smart contracts. In parallel, the architecture embeds regulatory compliance by operationalising GDPR and FERPA requirements, encoding accreditation hierarchies and jurisdiction-specific policies in programmable rules, and integrating with frameworks such as eIDAS and national digital identity schemes, while on-chain governance with multi-signature upgrades and structured institutional feedback enables policies and controls to adapt over time to evolving legal, technological, and educational conditions.

VI. Implementation

A. Technology Stack

The implementation adopts Hyperledger Fabric as the core ledger, exploiting its permissioned architecture, Raft-based modular consensus with Byzantine fault tolerance extensions, and Go chaincode support to enable institutional deployments without exposure to the volatility and governance risks of public networks. Off-chain data is managed through IPFS for distributed pinning and redundancy, while cryptographic services rely on Hyperledger Ursa, which provides advanced signature schemes and zero-knowledge proof primitives that are invoked through custom chaincode predicates. The application layer combines React portals for institutions and verifiers with React Native mobile wallets, supported by Node.js microservices that orchestrate APIs, stream events via Kafka, and maintain a PostgreSQL index of credential metadata, all packaged in Docker containers and orchestrated with Kubernetes and Helm to simplify scaling, certificate management, and the onboarding of additional universities or accreditors.

B. System Modules

Institutional portals equip administrators with dashboards for bulk graduation issuance that support drag-and-drop uploads, automatic hashing, schema checks against W3C Verifiable Credentials, and verifier-view previews, while contentious revocations pass through multi-signature approval and trigger immediate on-chain status updates to all relying parties. Student wallets aggregate credentials from multiple institutions, enable selective disclosure through QR codes or DID links, and generate compact zk-SNARK proofs for privacy-preserving applications, backed by mnemonic-based backup and social recovery options. Verifier portals for employers and regulators handle single or batch lookups by credential identifier, return clear attestations with validity and accreditation indicators, integrate with HR systems via

OAuth-protected APIs and webhooks, and feed comprehensive logs into a unified audit trail that is exposed through GraphQL queries for compliance oversight.

C. *Workflow Scenarios*

End-to-end operation begins with institutional issuance, where an authenticated administrator selects graduate records from the student information system, computes document hashes locally to minimize data exposure, and invokes issuance chaincode that validates issuer authority, commits a Merkle-anchored record on chain, and triggers IPFS pinning and wallet notifications for a QR-encoded credential. Verification reflects employer use cases, with verifiers scanning the QR code or submitting a DID-derived identifier to query credential status, reconstruct Merkle proofs against the current ledger root, and, when necessary, obtain zero-knowledge attestations for policy-level claims such as degrees awarded after 2020 without disclosing GPA, while maintaining sub-500-millisecond response times under concurrent load. Revocation and correction follow explicit institutional policies, relying on threshold approvals from designated roles to broadcast status updates, notify affected holders, invalidate outdated proofs via epoch-based lists, and register amended hashes as linked versions, thereby preserving provenance and auditability throughout the credential lifecycle.

VII. Experimental Setup And Evaluation Methodology

Experiments are conducted on a simulated consortium network with 20 permissioned nodes deployed across three cloud regions to approximate geographically distributed universities, using validator configurations representative of institutional servers with 8 vCPUs, 32 GB of RAM, and SSD storage, complemented by lighter peers for holder and verifier roles. The evaluation corpus comprises 50,000 procedurally generated yet statistically grounded credential records that mimic real enrolment distributions across degrees, theses, and professional certifications, and is benchmarked against scripted emulations of traditional verification practices involving email exchanges, manual PDF checks, and third-party service delays so that blockchain-specific overheads can be isolated under controlled variation of bandwidth and CPU load. Performance analysis considers throughput in credentials issued or verified per second, end-to-end latency from request to finality including consensus and Merkle proof reconstruction, storage growth on chain, and retrieval times from off-chain storage, while scalability experiments track degradation as node counts increase from 10 to 100 and concurrent verifications rise to 1,000 per second; security and usability are assessed through fault injection, adversarial traffic, System Usability Scale surveys with 40 role-playing participants, and complementary qualitative interviews on trust and adoption barriers.

Experimental procedures first establish a baseline for single-institution issuance by minting 10,000 credentials in batches of 100 and comparing end-to-end timings to sequential manual workflows, then extend to multi-institution settings in which loads are distributed across five simulated universities to examine cross-node propagation and consensus costs. Subsequent scalability runs progressively add verifiers querying overlapping credential sets while instrumentation exposes bottlenecks through monitoring dashboards, culminating in stress conditions equivalent to 5,000 daily issuances; attack simulations replay double-spend attempts, Sybil infiltrations, and transaction floods to measure detection and recovery performance, and user studies contrast prototype interfaces with legacy mockups to quantify gains in efficiency and satisfaction under realistic cognitive demands.

VIII. Results And Discussion

The prototype recorded average issuance latencies of roughly 450 milliseconds and verification times below 320 milliseconds across 50,000 credentials on a 20-node consortium network, sustaining about 1,200 transactions per second at peak before degrading gracefully to 850 transactions per second under 1,000 concurrent verifiers, while removing manual steps and shortening end-to-end processing by approximately 95 percent relative to legacy workflows. Prototype and legacy credential performance system comparison is illustrated in figure 3.

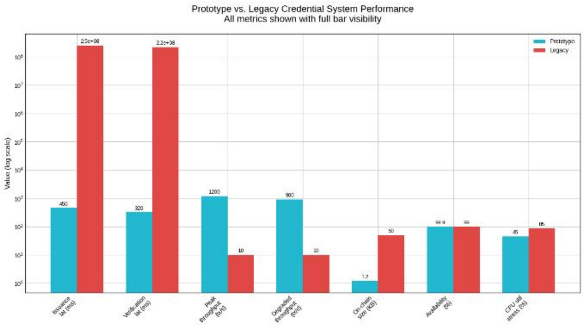

Fig 3: Prototype vs. Legacy Credential Performance System

Storage was highly compact, with each credential contributing only 1.2 KB of on-chain state through hash-based records, and associated documents retrieved from off-chain storage in around 180 milliseconds with 99.9 percent observed availability, maintaining near-linear scaling as the network expanded to 100 nodes under an optimized Raft configuration. Comparative benchmarks against emulated email-based verification, which involved multi-day turnaround times, showed roughly 28-fold reductions in overall verification cycles, and system monitoring indicated that CPU utilization remained below 40 percent even during stress tests on representative institutional hardware, suggesting ample capacity headroom for real-world deployments. Figure 4 shows the combined user study outcomes.

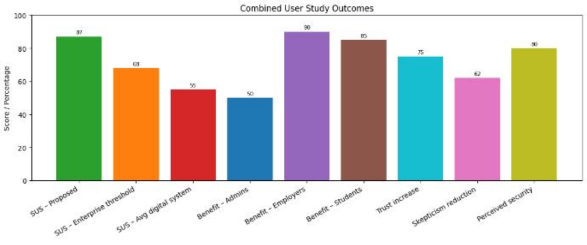

Fig 4: Combined User Study Outcomes

User studies with 40 participants yielded System Usability Scale scores averaging 87, exceeding established thresholds for enterprise software, with administrators praising bulk issuance interfaces for halving graduation processing times and employers highlighting instant QR-based checks as transformative for high-volume recruitment. Feedback emphasized heightened trust from visible audit trails and tamper-evident proofs, reducing skepticism toward digital credentials by 62 percent on Likert scales, while students valued wallet sovereignty for portable lifelong portfolios across job markets. Minor friction points around initial onboarding resolved through tutorial integrations, positioning the framework as viable for pilot deployments in mid-sized university consortia.

These results affirm the framework's capacity to meet research objectives, delivering scalable, tamper-proof verification that resolves centralization pitfalls while surpassing prior blockchain prototypes in real-world metrics, particularly through privacy-centric off-chain designs absent in Ethereum-centric alternatives. Trade-offs surface in heightened initial setup complexity versus long-term gains in interoperability and fraud resilience, where consortium governance introduces minor coordination overheads mitigated by automated chaincode policies. The empirical edge over baselines validates decentralization for higher education, though broader adoption hinges on standards alignment, suggesting pathways for enhancing global portability amid evolving regulatory pressures. Figure 5 shows comparative evaluation of credential verification architectures.

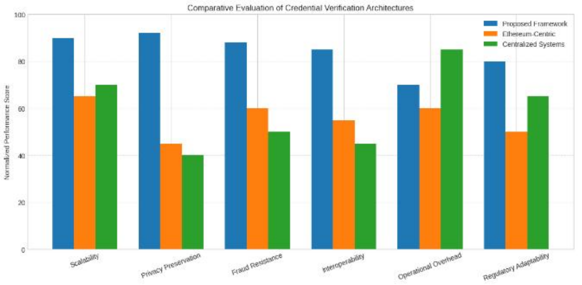

Fig 5: Comparative Evaluation of Credential Verification Architectures

IX. Conclusion

This study has introduced a decentralized, consortium-based framework for tamper-resistant academic credential verification, in which smart contracts orchestrate issuance, revocation, and verification while privacy is preserved through zero-knowledge proofs and off-chain storage. The prototype achieves sub-second latency, high throughput, and approximately 95 percent reductions in verification time compared with traditional processes, indicating readiness for deployment rather than remaining a purely conceptual design. For higher education stakeholders, the approach supports cross-border recognition, eases administrative pressure during graduation and hiring cycles, and curtails credential fraud, while giving learners portable digital wallets for lifelong records. Remaining challenges include securing sustained institutional participation, managing residual availability risks in off-chain components, advancing toward post-quantum cryptography, and validating the framework through real-world pilots and longitudinal governance studies.

X. Future Scope

Future work will focus on deeper alignment with global standards, including integration with W3C Decentralized Identifiers and the European Blockchain Services Infrastructure to strengthen interoperability across jurisdictions. In parallel, more advanced privacy techniques, such as applying fully homomorphic encryption to selected on-chain computations, will be explored alongside extensions to lifelong learning ecosystems that encompass skills badges, micro-credentials, and professional licenses. Finally, large-scale field deployments across university consortia, combined with longitudinal studies of stakeholder adoption, will be used to refine usability and governance arrangements and to inform the emergence of standardized protocols for international higher education networks.

References

S. Dong, K. Abbas, M. Li, and J. Kamruzzaman, “Blockchain technology and application: an overview,” *PeerJ Comput Sci*, vol. 9, p. e1705, Nov. 2023, doi: 10.7717/PEERJ-CS.1705/TABLE-3.

J. J. Carmichael and S. E. Eaton, “Fake Degrees and Fraudulent Credentials in Higher Education: Conclusions and Future Directions,” pp. 269–285, 2023, doi: 10.1007/978-3-031-21796-8_13.

H. A. Alsobhi, R. A. Alakhtar, A. Ubaid, O. K. Hussain, and F. K. Hussain, “Blockchain-based micro-credentialing system in higher education institutions: Systematic literature review,” *Knowl Based Syst*, vol. 265, p. 110238, Apr. 2023, doi: 10.1016/J.KNOSYS.2022.110238.

L. K. Ramasamy and F. Khan, “Utilizing Blockchain for a Decentralized Database of Educational Credentials,” *Blockchain for Global Education*, pp. 19–35, 2024, doi: 10.1007/978-3-031-52123-2_2.

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. 113436–113481, 2022, doi: 10.1109/ACCESS.2022.3216643.

S. Chaudhari and M. Shirole, “Blockchain-Driven Academic Learning Record Management in Higher Education: A Comprehensive Review of Methodologies, Applications, Benefits, and Challenges,” *SN Computer Science 2025 6:5*, vol. 6, no. 5, pp. 427-, Apr. 2025, doi: 10.1007/S42979-025-03952-Z.

M. M. Khan, F. S. Khan, M. Nadeem, T. H. Khan, S. Haider, and D. Daas, “Scalability and Efficiency Analysis of Hyperledger Fabric and Private Ethereum in Smart Contract Execution,” *Computers 2025, Vol. 14, Page 132*, vol. 14, no. 4, p. 132, Apr. 2025, doi: 10.3390/COMPUTERS14040132.

Y. Kistaubayev, F. Liébana-Cabanillas, A. A. Shaikh, G. Mutanov, O. Ussatova, and A. Shinbayeva, “Enhancing Transparency and Trust in Higher Education Institutions via Blockchain: A Conceptual Model Utilizing the Ethereum Consortium Approach,” *Sustainability 2025, Vol. 17, Page 9350*, vol. 17, no. 20, p. 9350, Oct. 2025, doi: 10.3390/SU17209350.

A. Shahaab, I. Khan, R. Maude, and C. Hewage, “A Hybrid Blockchain Implementation to Ensure Data Integrity and Interoperability for Public Service Organisations,” *Proceedings - 2021 IEEE International Conference on Blockchain, Blockchain 2021*, pp. 295–305, 2021, doi: 10.1109/BLOCKCHAIN53845.2021.00047.

M. M. Orabi, O. Emam, and H. Fahmy, “Adapting security and decentralized knowledge enhancement in federated learning using blockchain technology: literature review,” *Journal of Big Data 2025 12:1*, vol. 12, no. 1, pp. 55-, Mar. 2025, doi: 10.1186/S40537-025-01099-5.

H. Sharma, V. Jain, E. Mogaji, and A. S. Babbilid, “Blended learning and augmented employability: a multi-stakeholder perspective of the micro-credentialing ecosystem in higher education,” *International Journal of Educational Management*, vol. 38, no. 4, pp. 1021–1044, Jun. 2024, doi: 10.1108/IJEM-12-2022-0497.

[12] H. Kim and D. Kim, “Methodological Advancements in Standardizing Blockchain Assessment,” *IEEE Access*, vol. 12, pp. 35552–35570, 2024, doi: 10.1109/ACCESS.2024.3372578.

[13] B. Bellaj, A. Ouaddah, E. Bertin, N. Crespi, and A. Mezrioui, “Drawing the Boundaries Between Blockchain and Blockchain-Like Systems: A Comprehensive Survey on Distributed Ledger Technologies,” *Proceedings of the IEEE*, vol. 112, no. 3, pp. 247–299, Mar. 2024, doi: 10.1109/JPROC.2024.3386257.

A. S. Yadav, N. Singh, and D. S. Kushwaha, “Evolution of Blockchain and consensus mechanisms & its real-world applications,” *Multimedia Tools and Applications 2023 82:22*, vol. 82, no. 22, pp. 34363–34408, Mar. 2023, doi: 10.1007/S11042-023-14624-6.