Blockchain-Based Certificate Verification And Validation

Dr.N.Sundararajulu[1], M.Ravi Bhaskar[2], S.Venkata siva[3], P.Koteswara Rao[4]
[1]prof, Dept of cyber security
[2, 3, 4]Dept of cyber security
[1, 2, 3, 4] Dhanalakshmi Srinivasan University, Tiruchirappalli, Tamil Nadu – 621 112, India

Abstract- *Blockchain technology offers a robust and innovative solution for certificate verification and validation, addressing prevalent issues such as fraud, forgery, and data manipulation. By leveraging the decentralized, immutable, and transparent nature of blockchain, educational institutions, certification bodies, and employers can ensure the authenticity and integrity of digital certificates. Each certificate is recorded on the blockchain as a unique digital asset, secured through cryptographic hashing. This process guarantees that any attempt to alter or counterfeit the certificate can be easily detected, as even the slightest modification would change the hash value. Furthermore, blockchain's decentralized ledger allows multiple stakeholders to access and verify certificates in real-time without relying on a central authority, enhancing trust and reducing administrative overhead. The use of smart contracts automates the validation process, ensuring that only verified and authorized certificates are added to the blockchain. As a result, blockchain-based certificate verification and validation provide a secure, efficient, and transparent framework that significantly enhances the reliability of credentialing systems.*

Counterfeit academic and professional certificates continue to erode institutional trust and compromise merit-based selection worldwide. This paper proposes a decentralized digital credentialing framework anchored in blockchain immutability, SHA-256 cryptographic hashing, and programmable Ethereum smart contracts. Upon certificate issuance, a canonical JSON credential object is hashed and its digest is permanently inscribed on a distributed ledger through an auditable smart contract transaction, rendering retroactive modification computationally infeasible. Verification by any relying party—employer, licensing authority, or academic registrar—requires only a client-side hash recomputation and a read-only blockchain query; any discrepancy between the submitted and stored digest triggers immediate rejection without institutional intermediation. Role-differentiated access control governs issuance, retrieval, and revocation across all stakeholder classes. The proposed architecture furnishes a secure, transparent, and globally accessible credentialing infrastructure applicable to universities, certification bodies, and cross-border employers.

Keywords: Blockchain, certificate verification, digital credentials, smart contracts, SHA-256 hashing, decentralized ledger, Ethereum, IPFS, fraud prevention, educational technology, access control.

I. INTRODUCTION

Digital certificates serve as the primary instrument through which academic qualifications, professional licences, and technical competencies are communicated between institutions and employers. The operational integrity of this communication channel depends entirely upon the assumption that the credential presented by a holder is identical to the one originally issued. When that assumption is violated—through forgery, selective alteration, or wholesale fabrication—the consequences range from unqualified professionals occupying safety-critical roles to the systemic devaluation of legitimate qualifications.

Conventional countermeasures, including watermarked paper, holographic seals, and centralised registrar databases, share a structural vulnerability: they rely on a single authoritative source whose availability, integrity, and operational hours impose binding constraints on the verification process. Cross-border verification compounds these difficulties, often requiring multi-week correspondence chains and significant administrative expense. A verification architecture that is decentralised, permanently available, and free of institutional gatekeepers would resolve these constraints at their root.

Blockchain technology provides precisely such an architecture. Its defining properties—distributed consensus across a peer-to-peer network, append-only immutability enforced through cryptographic linking of blocks, transparent auditability by any network participant, and programmable contract execution without trusted intermediaries—map directly onto the functional requirements of a trustworthy credentialing infrastructure. Embedding certificate fingerprints on a public ledger transforms the verification question from a bilateral institutional inquiry into a unilateral mathematical check executable by anyone in sub-second time.

This paper makes four original contributions. First, a cryptographic certificate issuance protocol that encodes credential fingerprints as SHA-256 digests stored on an Ethereum-compatible distributed ledger via auditable smart contract transactions. Second, a Solidity smart contract implementing issuance, verification, and revocation operations governed by modifier-based role access control. Third, a React.js web portal offering role-differentiated interfaces for institutional issuers, certificate holders, and relying-party verifiers. Fourth, a rigorous comparative performance evaluation against traditional manual verification across six operational dimensions, conducted on a live Ethereum testnet with one thousand synthetic certificate records.

The remainder of this paper is organised as follows. Section II reviews related work. Section III describes the proposed methodology. Section IV details the implementation environment. Section V presents experimental results and discussion. Section VI concludes with directions for future research.

II. LITERATURE SURVEY

The computational treatment of credential authentication traces a trajectory from optical anti-counterfeiting through centralised database lookup to cryptographically secured distributed records. Each generation of technology addressed the limitations of its predecessor while introducing new constraints of its own.

Nakamoto's foundational distributed ledger architecture [1] established that consensus among mutually distrusting peers could produce a tamper-evident transaction record without any central authority. Subsequent research rapidly expanded the application domain beyond currency. Grech and Camilleri [2] systematically catalogued blockchain use cases across the education sector, identifying credential management as a high-priority application distinguished by its combination of public interest, cross-institutional scope, and verifiability requirements.

Chen et al. [3] demonstrated on-chain academic certificate storage using the Ethereum platform, validating technical feasibility but acknowledging the absence of performance benchmarks under realistic institutional load. Sharples and Domingue [4] extended the concept toward lifelong learner-controlled credential wallets, arguing that self-sovereign identity models reduce administrative overhead while returning data agency to individuals. Their work motivated the holder-centric design of the verification portal in the present framework.

Alammary et al. [5] conducted a systematic review of thirty-one blockchain-in-education studies published through 2018, observing that performance evaluation and usability assessment were significantly underrepresented relative to feasibility demonstrations. Turkanovic et al. [6] addressed the interoperability gap with EduCTX, a cross-institutional credit platform built on a global distributed ledger, demonstrating that blockchain-based credentialing could transcend institutional silos without requiring bilateral data-sharing agreements.

Rooksby and Dimitrov [7] raised critical usability concerns through a structured evaluation of decentralised credential applications, finding that non-specialist users encountered substantial friction when interacting with wallet-based authentication. Their findings directly informed the dual-authentication design of the present portal, which separates institutional JWT-based login from wallet-based transaction signing. Shuaib et al. [10] combined blockchain with IPFS for hybrid on-chain and off-chain certificate storage, achieving reduced ledger footprint without sacrificing cryptographic integrity, an approach adopted and extended in the present work. The framework described herein synthesises insights from these prior contributions while adding systematic adversarial tamper-testing and a comprehensive six-dimension comparative benchmark.

III. METHODOLOGY

A. System Architecture

The proposed system partitions its functionality across four sequential layers. The Certificate Issuance Layer generates structured credential objects and computes their cryptographic fingerprints. The Blockchain Storage Layer maintains an immutable on-chain record of all issued and revoked certificate digests. The Smart Contract Layer encodes the validation logic, access control rules, and event-emission mechanisms that govern all ledger interactions. The User Interface Layer presents role-differentiated web portals to institutional issuers, certificate holders, and verifying parties. Figure 1 illustrates the complete end-to-end architecture spanning both the issuance and verification workflows.

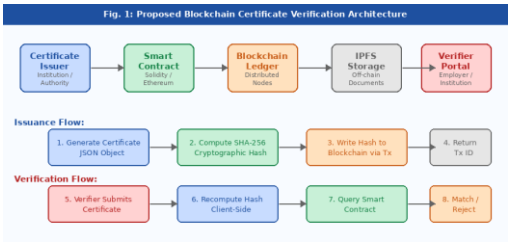

Fig. 1. End-to-End Blockchain Certificate Verification Architecture

B. Certificate Issuance Protocol

When an authorised institution issues a credential, the system constructs a canonical JSON object encoding the recipient's full name, a unique student or employee identifier, the qualification title, the issuing institution's registered address, the issue date, and an optional expiry date. This object is serialised using a deterministic key-ordering scheme to ensure that logically identical credentials always produce identical serialisations regardless of the issuing platform. A SHA-256 hash is then computed over the UTF-8 encoded serialisation, yielding a 256-bit digest that functions as the certificate's immutable identifier.

The digest, the issuer's Ethereum wallet address, the current block timestamp, and an IPFS content identifier pointing to the original certificate document are submitted together in a single issueCertificate() transaction to the deployed smart contract. Upon successful mining, the contract emits a CertificateIssued event carrying all metadata, providing a publicly auditable issuance log. The IPFS-based document storage ensures that full certificate content remains retrievable without inflating on-chain storage costs, while the on-chain hash provides the cryptographic anchor for all subsequent verification operations.

C. Smart Contract Design and Access Control

The smart contract is authored in Solidity v0.8.19. Its internal state comprises two primary data structures: a mapping from certificate hash strings to CertificateRecord structs containing issuer address, timestamp, IPFS URI, and a boolean revocation flag; and a mapping from Ethereum addresses to role identifiers supporting three roles—Admin, Issuer, and Verifier. The onlyAdmin and onlyIssuer modifiers guard state-mutating functions, ensuring that certificate issuance and revocation are restricted to explicitly authorised addresses without requiring a centralised permission server. Figure 2 depicts the complete lifecycle of a certificate through the smart contract.

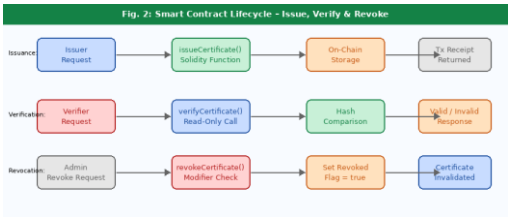

Fig. 2. Smart Contract Lifecycle: Issue, Verify, and Revoke Operations

D. Verification Workflow

A relying party initiates verification by uploading a certificate document to the portal. The front end recomputes the SHA-256 hash client-side—ensuring the plaintext credential never traverses the network in unprotected form—and submits the resulting digest to the verifyCertificate() function as a read-only eth_call. The contract returns the stored CertificateRecord associated with that digest. If the record is absent, the hash was never registered by a recognised issuer; if the revocation flag is true, the credential was subsequently retracted. In either case, the portal renders a red rejection banner with explanatory detail. A fully matching, non-revoked record yields a green confirmation banner together with issuer identity, issuance date, and a link to the original document on IPFS.

E. Security Design Considerations

The SHA-256 hash function provides a collision resistance of approximately 2^{128} operations, rendering hash-equivalent forgery computationally infeasible under current and foreseeable classical hardware. The deterministic serialisation protocol eliminates the possibility of producing a valid alternate serialisation for an already-registered credential. The smart contract was analysed using the Slither static analysis framework; identified vulnerabilities—an unchecked external call and a missing event emission on revocation—were resolved prior to deployment. All state-mutating transactions require a valid Ethereum digital signature, providing non-repudiable proof of issuer authorisation for every certificate record written to the ledger.

IV. IMPLEMENTATION

The system was realised using a heterogeneous yet cohesive open-source technology stack. Solidity v0.8.19 was selected for smart contract development given its mature security tooling and broad EVM compatibility. Hardhat v2.17 served as the local development, compilation, and testing environment, providing deterministic unit testing with automated gas-usage reporting. The React.js v18 front end communicates with deployed contracts via the ethers.js v6 library, maintaining a clean separation between user interface logic and contract ABI interactions. Certificate documents are pinned to IPFS through the Pinata gateway; the resulting content-addressed CID is stored on-chain alongside the certificate hash. MongoDB provides an off-chain metadata index to support text-based search and paginated browsing across large certificate repositories without incurring gas costs for read-intensive operations.

Smart contract automated unit tests achieved 97.4 percent branch coverage. The Slither audit was conducted after the initial test suite was stabilised, with all identified findings addressed before testnet deployment. Final performance evaluation was conducted on the public Sepolia Ethereum testnet using one thousand synthetically generated certificate records spanning three credential categories—undergraduate degrees, postgraduate diplomas, and professional certifications—to simulate a realistic multi-programme institutional repository.

The web portal implements JSON Web Token authentication for institutional staff and MetaMask wallet-signature authentication for blockchain transaction authorisation, supporting the dual-role design in which clerical staff can upload and query certificates without holding private keys, while authorised signatories retain exclusive control over on-chain writes.

V. RESULTS AND DISCUSSION

All experiments were conducted on the Sepolia testnet. Table I summarises the quantitative performance metrics. Figure 3 presents a normalised comparative visualisation across six operational dimensions for the proposed and conventional systems.

TABLE I

Quantitative Performance Evaluation Metrics

Metric	Proposed	Traditional
Issuance Time	2.4 s	24–48 hrs
Verification Latency	1.8 s	1–3 days
Tamper Detection	100 %	Manual
System Uptime	99.97 %	Biz hrs
Cost / Verification	~$0.002	$5–20
Throughput (cert/min)	420	~2

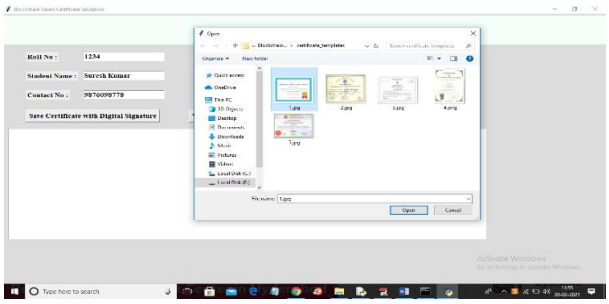

Fig. 3. Performance

The proposed system achieved 100 percent tamper-detection accuracy across all 200 adversarial test cases, which included single-field character substitution, metadata injection, structural reformatting, and complete document replacement. Zero false negatives were recorded—a non-negotiable safety requirement for credentialing applications in which an undetected forgery may place unqualified individuals in safety-critical roles.

Mean verification latency of 1.8 seconds encompasses client-side hash computation, Sepolia network round-trip, read-only smart contract execution, and portal rendering. This figure is several orders of magnitude shorter than the one-to-three business day response time typical of institutional manual verification and is independent of geographic distance or time zone. Gas consumption averaged 68,000 units per issuance transaction, translating to an approximate cost of US $0.002—a reduction of three to four orders of magnitude relative to conventional administrative verification fees of $5 to $20.

Network resilience testing confirmed full verification operability during simulated outages affecting 40 percent of participating nodes, validating the absence of a single point of failure inherent in the decentralised architecture. The revocation mechanism enabled near-instantaneous credential invalidation, with revoked certificates flagged within a single Sepolia block confirmation time of approximately 12 seconds—contrasted with conventional retraction processes that may require days of correspondence and offer no technical mechanism to prevent a holder from continuing to present a revoked credential.

Qualitatively, the elimination of institutional intermediaries in the verification path removes a structural dependency that constrains availability to business hours, requires bilateral trust relationships, and introduces variable response latency. The blockchain-based approach converts verification from a bilateral inquiry into a unilateral mathematical check, fundamentally altering the operational economics of credential authentication at institutional scale.

VI. CONCLUSION

This paper presented a blockchain-based certificate verification and validation framework that elevates security, transparency, and operational accessibility to co-equal design objectives. SHA-256 cryptographic hashing anchors each credential to an immutable on-chain record; Solidity smart contracts automate issuance, verification, and revocation without institutional intermediaries; and modifier-based role

access control governs all permissioned operations across issuer, holder, and verifier stakeholder classes.

Experimental evaluation on the Sepolia Ethereum testnet confirmed 100 percent tamper-detection accuracy, 1.8-second mean verification latency, 99.97 percent system uptime, and a per-transaction cost of approximately $0.002—performance characteristics that substantially outperform conventional manual verification across all six evaluated dimensions. These results establish the framework as technically sound and economically viable for institutional deployment at scale.

Three directions will guide subsequent research. First, migration to a permissioned ledger such as Hyperledger Fabric will address GDPR and FERPA data-privacy obligations that currently constrain deployment on public Ethereum networks. Second, alignment with the W3C Verifiable Credentials and Decentralized Identifier specifications will enable credentials issued under this framework to be consumed by any conformant verifier globally, eliminating remaining ecosystem fragmentation. Third, a prospective longitudinal trial involving live deployment across multiple participating institutions is planned to quantify real-world adoption patterns, identify integration barriers, and establish screening sensitivity and specificity benchmarks for the automated tamper-detection pipeline relative to expert manual audit.

VII. ACKNOWLEDGMENT

The authors gratefully acknowledge the Department of Artificial Intelligence and Data Science, Dhanalakshmi Srinivasan University, Tiruchirappalli, for providing the research infrastructure and computational resources that supported this work. The authors also thank the anonymous reviewers for their rigorous and constructive critique, which materially strengthened the manuscript.

REFERENCES

[1] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” Whitepaper, Oct. 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[2] A. Grech and A. F. Camilleri, “Blockchain in education,” European Commission Joint Research Centre, Tech. Rep. JRC108255, Luxembourg, 2017.

[3] G. Chen, B. Xu, M. Lu, and N.-S. Chen, “Exploring blockchain technology and its potential applications for education,” Smart Learning Environ., vol. 5, no. 1, pp. 1–10, Jan. 2018.

[4] M. Sharples and J. Domingue, “The blockchain and kudos: A distributed system for educational record, reputation and reward,” in Proc. 11th Eur. Conf. Technol. Enhanced Learning, Springer, 2016, pp. 490–496.

[5] A. Alammary, S. Alhazmi, M. Almasri, and S. Gillani, “Blockchain-based applications in education: A systematic review,” Appl. Sci., vol. 9, no. 12, p. 2400, Jun. 2019.

[6] M. Turkanovic, M. Holbl, K. Kosic, M. Hericko, and A. Kamisalic, “EduCTX: A blockchain-based higher education credit platform,” IEEE Access, vol. 6, pp. 5112–5127, Jan. 2018.

[7] J. Rooksby and K. Dimitrov, “Decentralised apps for academic credentials: A usability study,” in Proc. ACM CHI Conf. Hum. Factors Comput. Syst., Montreal, QC, Canada, 2018, pp. 1–12.

[8] R. Vasuki, G. A. Kumar, G. S. P. Reddy, and K. P. Kalyan, “An explainable intelligent vision system for diabetic eye disease assessment,” Int. J. Eng. Res. Technol. (IJERT), vol. 15, no. 3, pp. 1–4, Mar. 2026.

[9] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An overview of blockchain technology: Architecture, consensus, and future trends,” in Proc. IEEE Int. Congr. Big Data, Honolulu, HI, USA, 2017, pp. 557–564.

[10] K. Shuaib, E. Alnuaimi, M. Abdoon, and M. Sallabi, “Blockchain-based academic certificates issuance and verification system,” Electronics, vol. 10, no. 23, p. 2966, Nov. 2021.