

A Block Chain-Based Framework for Student Certificate Verification Using Ethereum

Abiodun Ibrahim Akintunde^{#1}, Davies Isobo Nelson^{*2}

¹Department of Computer Science, Ignatius Ajuru University of Education (IAUE), Rivers State, Nigeria

²Department of Computer Science, Rivers State University (RSU), Nigeria

²isobo.davies@ust.edu.ng

Abstract

This The increasing incidence of academic certificate fraud and the inefficiencies associated with conventional verification methods, including administrative delays, operational costs, and susceptibility to document manipulation, have created the need for more secure and efficient certificate verification mechanisms. This study presents a blockchain-based framework for student certificate verification using Ethereum. The proposed framework integrates Solidity-based smart contracts for certificate issuance, verification, and revocation; the InterPlanetary File System (IPFS) for off-chain document storage; and a web-based interface developed using React.js and Ethers.js. Cryptographic hashes, certificate metadata, and revocation status are maintained on the Ethereum blockchain to support document integrity and transparent verification, while role-based access control restricts sensitive operations to authorized institutional administrators. The system was deployed and evaluated on the Ethereum Sepolia test network, with Hardhat used for local development and testing. Experimental results showed that the framework achieved 100% functional success across 13 unit tests and five integration tests. Certificate issuance consumed 127,450 gas (approximately 0.00128 ETH), while revocation consumed 29,870 gas (approximately 0.00030 ETH), at a gas price of 10 Gwei. Read-only certificate verification returned results in less than 800 milliseconds under the reported test conditions without requiring a user-paid transaction gas fee. Security tests also confirmed the enforcement of access permissions, detection of document modifications, rejection of duplicate certificate registration, and correct handling of revoked certificates. The findings demonstrate the feasibility of integrating Ethereum smart contracts and IPFS for academic certificate lifecycle management, providing a transparent and independently verifiable approach to certificate authentication. Further evaluation using institutional records and larger transaction volumes is recommended to establish the framework's scalability and suitability for real-world deployment.

Keywords— *Blockchain Technology; Ethereum; Smart Contracts; Student Certificate Verification; InterPlanetary File System (IPFS); Role-Based Access Control; Certificate Revocation*

I. INTRODUCTION

Academic certificates serve as formal evidence of an individual's educational qualifications and are essential for employment, professional licensing, and further studies. Their credibility depends on the ability of employers, regulatory bodies, and other stakeholders to confirm their authenticity and current validity. However, certificate fraud such as document forgery, grade alteration, impersonation of graduates, and fraudulent awards from diploma mills, remains a significant challenge to educational institutions and credential verification authorities [1]. The increasing availability of image-editing software, high-resolution printing technologies, and online platforms for counterfeit documents has further complicated the authentication of academic credentials, particularly across institutional and national boundaries [2].

In recent years, several conventional certificate verification mechanisms face several limitations. Most institutions maintain certificate records in centralized databases, creating potential single points of failure and vulnerabilities to unauthorized modification [3]. Furthermore, verification frequently requires employers or other stakeholders to contact issuing institutions manually, resulting in administrative delays, increased

operational costs, and dependence on institutional availability. Physical certificates remain susceptible to forgery, while digital credentials may be compromised through unauthorized access to institutional systems or signing keys. In addition, incompatible institutional verification systems complicate cross-institutional verification, while the absence of transparent revocation mechanisms allows invalid credentials to remain in circulation [4]. These limitations demonstrate the need for a verification framework that supports independent authentication, data integrity, accessibility, and transparent certificate status management.

Blockchain technology offers a potential solution through its distributed ledger architecture, cryptographic integrity mechanisms, and consensus-based record management [5]. Records committed to a blockchain are replicated across participating nodes, making unauthorized retrospective modification computationally difficult [6]. Ethereum extends these capabilities through smart contracts, which execute predefined rules for managing transactions and access permissions [7]. By implementing certificate issuance, verification, and revocation through smart contracts, the verification process can become transparent and independently auditable. Furthermore, by integrating the InterPlanetary File System (IPFS) for off-chain document storage while

maintaining corresponding cryptographic hashes on Ethereum provides a means of verifying certificate integrity while reducing on-chain storage requirements and limiting the exposure of sensitive academic information [8].

The application of blockchain to academic credential verification has been explored through initiatives such as Blockcerts and the Massachusetts Institute of Technology's digital diploma project, which demonstrated the feasibility of independently verifying credentials using blockchain-based mechanisms [9]. Subsequent studies have proposed different architectures for blockchain-based educational record management. However, existing blockchain-based credential verification approaches still present limitations relating to scalability, storage management, access control, and the completeness of certificate lifecycle management [10, 11]. These limitations reveal the need for an integrated framework that combines certificate issuance, independent verification, and transparent revocation, while enforcing role-based access control and minimizing on-chain storage through IPFS integration.

This study presents a blockchain-based framework for student certificate verification using Ethereum. The aim is to design and implement a decentralized system that enhances certificate authenticity, integrity, and verification transparency. The framework integrates Solidity-based smart contracts with IPFS for off-chain certificate storage, while cryptographic hashes and certificate statuses are maintained on the Ethereum blockchain. Role-based access control regulates certificate issuance and revocation, enabling authorized institutions to manage credentials while allowing independent verification by stakeholders.

Furthermore, the study makes four principal contributions. First, it identifies the limitations of conventional certificate verification mechanisms and establishes the requirements for a blockchain-based alternative. Second, it proposes a layered architecture integrating Ethereum smart contracts with IPFS for secure certificate management and off-chain storage. Third, it implements a publicly auditable revocation mechanism that enables authorized institutions to invalidate certificates issued erroneously or fraudulently while preserving the historical transaction record. Fourth, it incorporates role-based access control to restrict sensitive operations, particularly certificate issuance and revocation, to authorized actors.

II. RELATED WORKS

Academic certificate fraud encompasses fabricated degrees, altered transcripts, misrepresented credentials, and degree mill products [12]. The global scale of the problem is substantial. The Association of Certified Fraud Examiners (ACFE) in its 2020 Report to the Nations estimated that organizations worldwide lose trillions of dollars annually to various forms of fraud [13]. This is considered a significant proportion of which

involves credential misrepresentation in employment contexts.

In Nigeria, [14] conducted an empirical study documenting the widespread prevalence of certificate forgery across public institutions, attributing the problem to weak verification infrastructure, corruption in academic administration, and insufficient regulatory enforcement. Their findings echo those of similar studies across West Africa and suggest that the problem is structurally embedded rather than episodic. Globally, the proliferation of the internet has enabled degree mill operations to scale dramatically, with thousands of unaccredited institutions now offering credentials for sale online.

Recent studies have explored blockchain technology as an alternative to conventional academic certificate verification systems. [15] developed a blockchain-based certificate verification system integrating Ethereum smart contracts, IPFS, and PostgreSQL for academic credential authentication. Their system supports certificate issuance, QR-code-based verification, and decentralized document storage. The implementation achieved a reported 98% accuracy in detecting forged certificates, with verification times below two seconds. Although the study demonstrated the feasibility of integrating blockchain with decentralized storage, its discussion identified Ethereum gas fees and institutional adoption as continuing challenges.

Similarly, [16] proposed a blockchain-powered academic credential verification platform called "ShikkhaChain" which was designed to address certificate fraud and inefficient manual verification in Bangladesh. The framework integrates Ethereum smart contracts with IPFS for off-chain storage and employs a four-tier role-based access model involving government authorities, regulators, educational institutions, and public verifiers. It supports certificate issuance, QR-based validation, and on-chain revocation. Although the framework addresses several aspects of the credential lifecycle, the authors identified Ethereum transaction costs, IPFS availability, and privacy concerns associated with public metadata as areas requiring further attention.

In another study, researchers presented a decentralized certificate issuance and verification system using Ethereum blockchain technology. The proposed architecture provides a mechanism for creating and validating credentials across educational, healthcare, and government domains. The study incorporated experimental evaluation and user feedback to examine performance, usability, scalability, security, and reliability. Its findings support the feasibility of decentralized certificate management, although privacy protection, interoperability, standardization, and institutional adoption remain relevant implementation challenges [17].

[10] developed a blockchain-enabled decentralized framework for academic microcredentials using

Hyperledger Besu, smart contracts, and IPFS. Unlike systems focusing exclusively on conventional academic certificates, their framework addresses the issuance, verification, revocation, and retrieval of credit-bearing microcredentials. The authors evaluated the system using benchmarking scripts and Hyperledger Caliper, reporting throughput between 1.6 and 2.0 transactions per second and average latency ranging from 0.93 to 4.34 seconds. The study demonstrates the feasibility of integrating credential lifecycle management with decentralized storage and performance evaluation. However, its primary focus is microcredential integration into formal academic pathways rather than a student certificate verification framework built specifically on Ethereum.

[18] study on cross-border candidate credential verification proposed a framework combining blockchain, zero-knowledge proofs (ZKPs), and IPFS, with Ethereum and Polygon considered as blockchain platforms. The framework employs digitally signed academic documents, decentralized storage, and blockchain-based cryptographic references to support credential verification while limiting disclosure of sensitive information. The study highlights the importance of combining document authenticity mechanisms with privacy-preserving verification, particularly in international recruitment. However, its principal emphasis is privacy-preserving candidate verification rather than institutional certificate issuance and role-controlled revocation.

[19] proposed a blockchain-based academic credential verification system using the Ethereum Sepolia test network and Solidity smart contracts. Their framework supports credential issuance, verification, and revocation, with SHA-256 hashing employed to protect credential integrity. The study also incorporated batch processing and a web-based interface to facilitate credential management. Its findings demonstrate the feasibility of implementing academic credential lifecycle operations on Ethereum, while the authors identified privacy-enhancing cryptographic mechanisms and decentralized identity standards as directions for further research.

[20] proposed a decentralized document verification framework integrating Ethereum blockchain and IPFS to address the inefficiencies, high costs, and manipulation risks associated with conventional document verification. Their approach combines blockchain-based integrity assurance with decentralized document storage to support secure and transparent verification. The study contributes to the development of decentralized document authentication mechanisms, although the broader application of such frameworks to controlled certificate issuance and transparent revocation requires consideration of institutional authorization and credential lifecycle management. _format”.

III. METHODOLOGY AND DESIGN

A. Research Methodology

This study adopted a design and implementation research approach to develop a blockchain-based framework for student certificate verification using Ethereum. The methodology involved system requirement analysis, architectural design, smart contract development, frontend integration, deployment, and experimental evaluation. The proposed framework integrates Ethereum smart contracts, the InterPlanetary File System (IPFS), and a web-based verification interface to address the limitations of conventional certificate verification mechanisms, particularly centralized record management, unauthorized document manipulation, verification delays, and inadequate revocation transparency.

The system was implemented using Solidity for smart contract development, React.js for the frontend interface, and Ethers.js for communication between the application and the Ethereum blockchain. IPFS was employed for off-chain certificate document storage, while the Ethereum Sepolia test network provided the deployment and transaction environment. Hardhat was used for local development and testing. Furthermore, the evaluation focused on four major dimensions such as functional correctness, transaction cost, verification latency, and security enforcement. Functional correctness was assessed through unit and integration tests, while transaction cost was measured using gas consumption. Verification latency was evaluated through the time required to retrieve and validate certificate records, and security testing examined access control, document integrity, duplicate certificate prevention, and revocation correctness.

B. Dataset and Experimental Environment

The study utilized two categories of experimental dataset known as synthetic test certificates and blockchain transaction records.

The synthetic certificate dataset consisted of fabricated but realistic student records containing student names, certificate identifiers, degree titles, issuing institutions, and graduation dates. Corresponding PDF certificates were generated using a custom script and a LaTeX certificate template. These documents were uploaded to IPFS and used to evaluate certificate issuance, retrieval, integrity verification, and revocation.

The blockchain transaction dataset consisted of transaction records collected during deployment and testing on the Ethereum Sepolia test network and the Hardhat local environment. The records included gas consumption, transaction confirmation information, and smart contract event logs.

C. Proposed System Architecture

Presented in Fig. 1 is the architectural design of the proposed system. The framework adopts a three-layer architecture comprising the presentation layer, smart contract layer, and storage layer. These layers interact to provide certificate issuance, verification, and revocation services.

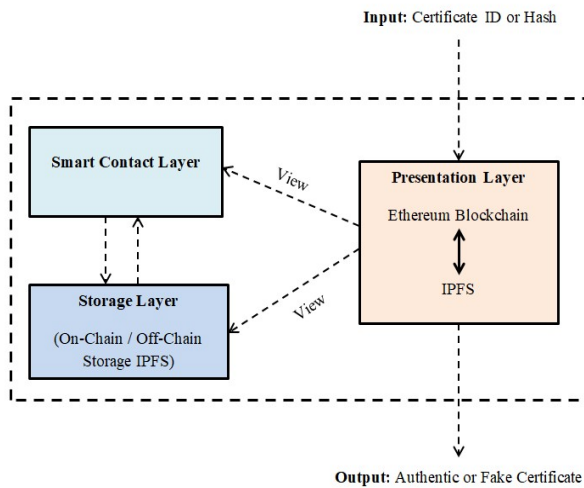


Fig 1: Architecture of the Proposed Blockchain-Based Student Certificate Verification Framework

In this study, the presentation layer consists of a React.js web interface through which institutional administrators issue certificates and users submit certificate identifiers or hashes for verification. Ethers.js provides the communication interface between the frontend and the deployed smart contract, facilitating wallet connection, transaction submission, and event monitoring.

The smart contract layer is implemented in Solidity and deployed on Ethereum. It manages certificate registration, hash storage, verification status, revocation, and role-based authorization. Administrative operations such as issuance and revocation require authorized accounts, whereas certificate verification is performed through read-only contract calls.

The storage layer consists of on-chain and off-chain components. On-chain storage maintains certificate identifiers, cryptographic hashes, IPFS content identifiers (CIDs), issuer information, timestamps, and revocation status. Off-chain storage uses IPFS to store the complete PDF certificate documents. The CID is recorded in the smart contract to enable content retrieval and integrity validation.

The separation of certificate documents from blockchain metadata minimizes on-chain storage requirements while retaining a verifiable relationship between the certificate document and its blockchain record.

D. Mathematical Formulation

The proposed framework employs cryptographic hashing, access control, certificate status validation, and transaction cost computation to achieve secure certificate management.

For this study, each certificate document is represented by a cryptographic hash generated from its digital content.

Let D, H, h_D represent the original certificate document, cryptographic hash function, and generated certificate hash respectively.

The certificate hash is expressed as:

$$h_D = H(D) \quad (1)$$

Here, Ethereum implementation was done using Keccak-256 as follows:

$$h_D = Keccak256(D) \quad (2)$$

The resulting hash serves as a unique content fingerprint for the certificate. Any modification to the document produces a different hash with overwhelming probability.

However, during certificate verification, the hash of the submitted certificate is recomputed and compared with the hash stored on the blockchain.

For example, let h_S represent the hash of the submitted certificate, h_B be the hash recorded on the blockchain, and I be the integrity verification result. The integrity function is defined as:

$$I = \begin{cases} 1, & h_S = h_B \\ 0, & h_S \neq h_B \end{cases} \quad (3)$$

A result of 1 indicates that the submitted document matches the registered certificate content, while 0 indicates a mismatch.

Furthermore, the system employs a role-based access control to restrict sensitive operations. This is represented mathematically as:

$$Auth(u, p) = \begin{cases} 1, & p \in P(A(u)) \\ 0, & p \notin P(A(u)) \end{cases} \quad (4)$$

Where U is the set of system users, R is the set of assigned roles, $A(u)$ is the role assigned to user u , and $P(r)$ is the permission associated with role r .

For this study, the certificate issuance and revocation functions are executed only when the requesting account possesses the required permission.

The study determines the certificate validity by combining record existence, document integrity, and revocation status using the equation below:

$$V = E \times I \times (1 - R) \quad (5)$$

Further, the corresponding decision rule is given as:

$$Status = \begin{cases} Invalid, E = 0 \\ Tampered, E = 1, I = 0 \\ Revoked, E = 1, I = 1, R = 1 \\ Valid, E = 1, I = 1, R = 0 \end{cases} \quad (6)$$

This mathematical formulation ensures that a certificate is classified as valid only when its blockchain record exists, its cryptographic hash matches, and it has not been revoked.

For blockchain transaction cost the proposed study, the computational cost of executing smart contract operations is determined by gas consumption and the prevailing gas price as:

$$C_g = G \times P_g \quad (7)$$

Where C_g the transaction cost in ETH is, G is the gas consumed by the operation, and P_g is the gas price in ETH per gas unit.

Note, for a gas price of 10 Gwei, the proposed system computes the following:

$$P_g = 10 \times 10^{-9} \text{ ETH} \quad (8)$$

The verification latency is represented as the time required to obtain and process a certificate verification response. In the proposed system, this is presented as follows:

$$T_v = t_f - t_i \quad (9)$$

Where T_v is the verification latency, t_i is the time that the verification request was initiated, and t_f is the time the verification response was received.

However, in terms of multiple verification trials, the system computes the average latency as:

$$\bar{T}_v = \frac{1}{n} \sum_{i=1}^n T_i \quad (10)$$

Where n represents the number of verification trials.

E. Certificate Issuance and Validation Algorithm

The three principal operational procedures followed by the proposed system is given below.

Certificate Issuance: An authorized institutional administrator uploads a certificate document through the web interface. The document is stored on IPFS, and its cryptographic hash and CID are submitted to the smart contract. The contract verifies the administrator's permission, checks for duplicate certificate records, and registers the certificate with an active status.

Certificate Verification: A user submits a certificate identifier or hash through the verification portal. The application retrieves the corresponding blockchain record and compares the submitted document hash with the registered hash. The contract's revocation status is also

checked, and the system returns the appropriate verification result.

Certificate Revocation: An authorized administrator initiates a revocation request for a previously issued certificate. The smart contract validates the administrator's permission and updates the certificate status to revoke. The historical transaction remains on the blockchain, while subsequent verification requests return the revoked status.

F. System Evaluation Metrics

The developed system was system was evaluated using functional correctness, gas consumption, verification latency, and security enforcement.

The functional correctness of the system was measured using the below:

$$FC = \frac{N_p}{N_t} \times 100 \quad (11)$$

Where FC is the functional correctness percentage, N_p is the number of passed test cases, and N_t is the total number of test cases.

This metric was used to determine whether the implemented system correctly executed the specified operations under the tested conditions.

IV. RESULTS AND DISCUSSION

The proposed blockchain-based student certificate verification framework was evaluated to determine its functional correctness, computational cost, verification performance, and security enforcement. The experimental evaluation was conducted using the Ethereum Sepolia test network and Hardhat local development environment. The assessment focused on certificate issuance, verification, revocation, role-based access control, document integrity, and transaction efficiency.

The test cases conducted on the developed system is presented in Table 1. While captured in Fig. 2 is the interface visualization of the developed system.

Table 1 Certificate Verification Test Cases

Test ID	Scenario	Expected Output
TC01	Verify an authentic, active certificate	valid
TC02	Verify an unregistered certificate	Not Found
TC03	Verify a modified certificate	Hash Mismatch
TC04	Verify a revoked certificate	Revoked
TC05	Verify an existing certificate using its ID	Valid or Revoked, according to status
TC06	Submit an empty certificate ID	Invalid Input
TC07	Attempt issuance from an unauthorized account	Access Denied
TC08	Attempt duplicate certificate registration	Duplicate Rejected

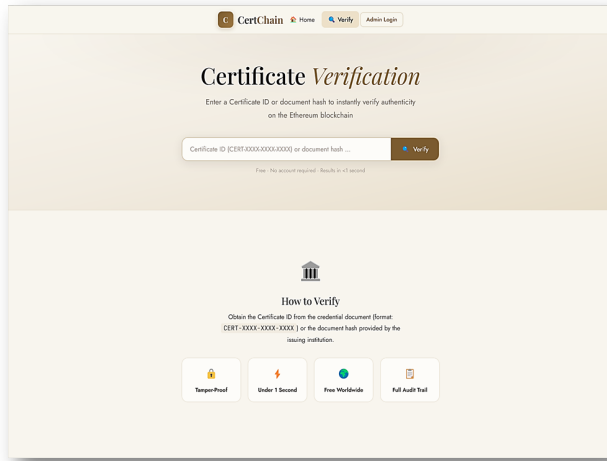


Fig. 2 Screenshot Interface for Certificate Verification

A. Functional Testing Results

The functional evaluation comprised 13 unit tests and five integration tests, covering the major operations of the developed framework. All 18 reported test cases passed, demonstrating that the implemented functions behaved as expected under the tested conditions as shown in Table 2.

Table 2 Functional Testing Results

Test Category	No. of Tests	Passed	Failed	Success Rate
Unit Testing	13	13	0	100%
Integration Testing	5	5	0	100%
Total	18	18	0	100%

B. Gas Consumption and Transaction Cost

The gas consumption of the smart contract operations was evaluated using a gas price of 10 Gwei. The results are presented in Table 3.

Table 3 Gas Consumption of the Smart Contract Operations

Smart Contract Operation	Gas Used	Cost (ETH)	Approximate Cost (₹)
Contract Deployment	1,842,315	0.01842315	69,000
<u>issueCertificate()</u>	127,450	0.00127450	4,800
<u>revokeCertificate()</u>	29,870	0.00029870	1,100
<u>grantAdminRole()</u>	51,230	0.00051230	1,920
<u>verifyCertificate()</u>	0*	0	Free

The results presented in Table 3 show that contract deployment incurred the highest gas consumption, requiring 1,842,315 gas units. This is attributable to the deployment of the smart contract code and initialization of its state.

Certificate issuance consumed 127,450 gas units, reflecting the computational and storage operations associated with registering certificate metadata and its corresponding cryptographic references. Certificate

revocation required 29,870 gas units, while granting an administrative role consumed 51,230 gas units.

The verification function did not require a blockchain state-changing transaction because it was implemented as a read-only operation. Consequently, ordinary verification calls did not incur transaction gas fees.

C. Certificate Verify Performance

The verification performance of the developed framework was evaluated based on response time and the verification procedures required establishing certificate validity. The time comparison of the various certificate verification processes is presented in Table 4.

Table 4 Certificate Verification Time Comparison

Verification Method	Reported Verification Time	Verification Approach
Proposed Ethereum Framework	Less than 800 ms	Blockchain read-only query
Traditional Institutional Verification	2-14 business days	Manual institutional confirmation
Third-party Verification Service	4-48 hours	External verification service
PKI-based Digital Certificate	Less than 30 seconds	Digital signature and revocation checking

The proposed framework returned verification results in less than 800 milliseconds under the reported test conditions. Unlike conventional manual verification, the process retrieves certificate information directly from the smart contract without requiring the verifier to contact the issuing institution.

The results indicate that blockchain-based verification can reduce dependence on manual institutional confirmation. However, the comparison with traditional and third-party methods should be interpreted as indicative because the study did not conduct a controlled head-to-head experiment involving those external services.

D. Security Assessment Results

The security assessment examined the ability of the proposed framework to protect certificate integrity, enforce authorization, prevent duplicate registration, and maintain correct revocation status. Tabulated in Table 5 are the security assessment results of the study.

Table 5 Security Assessment Results

Security Property	Test Procedure	Observed Result	Status
Access control	Attempted sensitive operations	All unauthorized calls reverted	Passed

	using unauthorized accounts		
Certificate integrity	Modified a test PDF and compared its content identifier/hash	Modified document produced a different identifier/hash	Passed
Revocation correctness	Queried certificates after revocation	Revoked status was correctly returned	Passed
Duplicate prevention	Attempted to register an existing certificate hash	Duplicate registration rejected	Passed
On-chain record protection	Attempted direct unauthorized state modification	No successful modification through the tested application and contract interfaces	Passed

The results demonstrate that the implemented authorization rules prevented unauthorized accounts from executing restricted smart contract functions. Furthermore, the content-addressed storage mechanism enabled the detection of document modifications, while the revocation mechanism correctly reflected certificate status during subsequent verification.

Furthermore, the duplicate prevention test also confirmed that an existing certificate hash could not be registered again through the tested issuance function.

E. Discussion of Findings

The experimental findings demonstrate that the proposed framework successfully integrates blockchain-based certificate issuance, verification, and revocation within a single architecture. The 100% functional test success rate indicates that all reported unit and integration test cases were completed successfully.

The gas consumption results further demonstrate that certificate management operations can be executed through Ethereum smart contracts, while read-only verification avoids transaction fees for ordinary queries. The integration of IPFS also separates document storage from blockchain metadata, reducing the need to store complete certificate files directly on-chain.

Furthermore, the access control and revocation tests demonstrate that sensitive certificate management operations can be restricted to authorized institutional accounts, while certificate status remains independently verifiable.

Finally, these findings support the feasibility of the proposed Ethereum-based framework as an alternative to conventional certificate verification mechanisms. Nevertheless, the evaluation was conducted on a test network using synthetic certificates; therefore, further assessment using institutional records, larger transaction volumes, and deployment-scale workloads would be necessary to establish real-world scalability and operational performance.

V. CONCLUSION

This study presented a blockchain-based framework for student certificate verification using Ethereum. The study was motivated by the limitations of conventional certificate verification mechanisms, particularly administrative delays, centralized record management, vulnerability to document manipulation, and inadequate transparency in certificate revocation. To address these challenges, the developed framework integrated Ethereum smart contracts, the InterPlanetary File System (IPFS), and a web-based application to support certificate issuance, verification, and revocation within a unified architecture.

The system was implemented using Solidity, React.js, and Ethers.js, with certificate documents stored off-chain through IPFS while their cryptographic hashes, metadata, and revocation status were maintained on the Ethereum blockchain. Role-based access control was incorporated to restrict certificate issuance and revocation to authorized institutional administrators, while read-only verification enabled independent authentication by external users.

The experimental results demonstrated that the developed framework achieved 100% functional success across the 18 reported unit and integration tests. Certificate issuance consumed 127,450 gas, while certificate revocation required 29,870 gas at a gas price of 10 Gwei. Furthermore, read-only verification returned results in less than 800 milliseconds under the reported test conditions without requiring a user-paid transaction gas fee. The security assessment also confirmed that unauthorized operations were rejected, modified certificate documents could be detected through hash comparison, duplicate certificate registration was prevented, and revoked certificates were correctly identified during subsequent verification.

These findings demonstrate that the integration of blockchain technology and decentralized storage provides a feasible approach to improving the integrity, transparency, and accessibility of academic certificate verification. The proposed framework reduces dependence on manual institutional confirmation and provides a mechanism through which certificate records and their current status can be independently checked.

However, the evaluation was conducted using synthetic certificate records and the Ethereum Sepolia test network. Consequently, the reported results do not

establish performance under large-scale institutional workloads or production deployment conditions. Future research should investigate scalability under increasing certificate volumes, integration with institutional student information systems, enhanced privacy-preserving verification mechanisms, and deployment on a production blockchain environment. Such extensions would provide further evidence of the framework's operational suitability for broader adoption by educational institutions and certificate-verifying organizations.

REFERENCES

- [1] S. E. Eaton and J. J. Carmichael, "Fake degrees and credential fraud, contract cheating, and paper mills: Overview and historical perspectives," *Fake degrees and fraudulent credentials in higher education*, pp. 1-22, 2023.
- [2] G. Das and R. Ramachandra, "From Forgeries to Foundation Models: A Systematic Survey of Identity Document Attack and Detection," *arXiv preprint arXiv:2607.01442*, 2026.
- [3] N. K. Shah and A. B. Parekh, "Enhancing Trust in Education Through Blockchain-Based Credential Authentication," *Journal of Computer Technology & Applications*, vol. 17, pp. 1-7, 2026.
- [4] C. Mazzocca, A. Acar, S. Uluagac, R. Montanari, P. Bellavista, and M. Conti, "A survey on decentralized identifiers and verifiable credentials," *IEEE Communications Surveys & Tutorials*, vol. 27, pp. 3641-3671, 2025.
- [5] B. Lashkari and P. Musilek, "A comprehensive review of blockchain consensus mechanisms," *IEEE access*, vol. 9, pp. 43620-43652, 2021.
- [6] R. Esu, "Blockchain and data protection: developing a functional erasure framework for storage limitation," *Information & Communications Technology Law*, vol. 35, pp. 337-356, 2026.
- [7] I. Achour, H. Idoudi, and S. Ayed, "Access control modeling and validation for ethereum smart contracts," *Concurrency and Computation: Practice and Experience*, vol. 37, p. e70108, 2025.
- [8] M. A. Patel, S. Sobhanayak, and A. Sahoo, "Academic Certificate Verification using Blockchain Technology," in *2025 IEEE International Conference on Contemporary Computing and Communications (InC4)*, 2025, pp. 1-6.
- [9] D. L. Silaghi and D. E. Popescu, "A systematic review of blockchain-based initiatives in comparison to best practices used in higher education institutions," *Computers*, vol. 14, p. 141, 2025.
- [10] A. M. Tanim, M. F. Hossain, H. Saria, and N. Mansoor, "Design and Development of a Blockchain-Enabled Decentralized Framework for Academic Microcredentials," *IET Software*, vol. 2026, p. 7326873, 2026.
- [11] A. Rustemi and F. Dalipi, "From concept to practice: a blockchain-based solution for secure and efficient academic credentials in higher education," *IET Blockchain*, vol. 6, p. e70030, 2026.
- [12] J. J. Carmichael and S. E. Eaton, "Security risks, fake degrees, and other fraud: A topic modelling approach," in *Fake degrees and fraudulent credentials in higher education*, ed: Springer, 2023, pp. 227-250.
- [13] J. Barnes, "Fraud detection: Forensic accounting education and CFE designation impact on auditor's confidence levels," *Journal of Accounting and Finance*, vol. 20, pp. 62-75, 2020.
- [14] L. S. Ezema, C. Ugwu, and F. C. Eze, "Certificate Forgery in Nigeria: Causes, Effects and Way Forward.," *International Journal of Academic Research in Business and Social Sciences*, vol. 9, 2019.
- [15] A. Akinnifesi and J. Balogun, "Design and Implementation of a Blockchain-Based Certificate Verification System for Secure Academic Credential Authentication," *University of Ibadan Journal of Science and Logics in ICT Research*, vol. 15, 2025.
- [16] A. Farabi, I. Khandaker, J. Ahsan, I. K. Shanto, N. Jahan, and M. J. Khan, "Shikkhachain: A blockchain-powered academic credential verification system for bangladesh," *arXiv preprint arXiv:2508.05334*, 2025.
- [17] T. R. Sree, "Decentralized certificate issuance and verification system using Ethereum blockchain technology," *Journal of Network and Computer Applications*, vol. 242, p. 104190, 2025.
- [18] A. Rageshnithin, C. Vanmathi, and R. Mangayarkarasi, "Cross-border candidate credential verification using ZKP and blockchain Ethereum and Polygon perspectives: a scalable solution for authentic global corporate interviews," *Frontiers in Blockchain*, vol. 8, p. 1669666, 2025.
- [19] D. Sheela, "ENHANCING ACADEMIC TRUST AND ACCOUNTABILITY: A SCALABLE BLOCKCHAIN SYSTEM FOR CREDENTIAL VERIFICATION FOR EDUCATION," *International Journal of Applied Mathematics*, vol. 38, pp. 803-819, 2025.
- [20] A. Mishra, S. Mehta, B. Oza, S. Kumar, and H. Kasturiwale, "Blockchain-Based Decentralized Document Verification and Its Applications," *Journal of Information Systems Engineering and Management*, vol. 10, 2025.