# University of Ibadan Journal of Science and Logics in ICT Research (UIJSLICTR)

**ISSN: 2714-3627**

***A Journal of the Faculty of Computing, University of Ibadan, Ibadan, Nigeria***

**Volume 15 No. 1, September 2025**

**journals.ui.edu.ng/uijslictr**
**http://uijslictr.org.ng/**
**uijslictr@gmail.com**

**University of Ibadan**
**Journal of Science and Logics in ICT Research**

# Design and Implementation of a Blockchain-Based Certificate Verification System for Secure Academic Credential Authentication

**[1]Akinnifesi A. S. and [2]Balogun J. M.**

*Department of Physical and Mathematical Sciences, Faculty of Science, Dominican University, Samonda, Ibadan, Nigeria.*
*akinnifesiakintunde@gmail.com, josephbalogun014@gmail.com*

**Abstract**

Certificate forgery is a pervasive issue in Nigeria's educational system, undermining trust in academic credentials and causing delays in verification processes. Traditional paper-based systems are inefficient, costly, and susceptible to tampering. This study presents a blockchain-based certificate verification system that leverages Ethereum smart contracts, InterPlanetary File System (IPFS) for decentralized storage, and PostgreSQL for off-chain metadata management to provide a secure, tamper-proof, and real-time verification platform. The system, implemented using React.js for the frontend, Node.js for the backend, and Solidity for smart contracts, enables institutions to issue digital certificates with embedded QR codes and allows instant verification by employers and other stakeholders. Testing on the Ethereum testnet demonstrated 98% accuracy in detecting forged certificates, with verification times under 2 seconds. The system enhances transparency, reduces administrative overhead, and aligns with Nigeria's push for technological innovation in education. Challenges such as Ethereum gas fees and institutional adoption are discussed, with recommendations for scalability and mobile support.

***Keywords:*** *Blockchain, Certificate Verification, Ethereum, Smart Contracts, IPFS.*

## 1. Introduction

Academic certificates are essential for validating educational achievements, facilitating employment, and enabling further studies. In Nigeria, however, certificate forgery is a significant challenge, with paper-based verification systems being slow, costly, and prone to errors [1]. These systems often require manual confirmation from the issuing institutions, thereby leading to delays that hinder job placements and university admissions. The lack of a standardized, universally accessible verification framework further complicates cross-border authentication, impacting Nigeria's educational and economic landscape.

Blockchain technology, introduced by Nakamoto in 2008 [2], offers a decentralized, immutable, and transparent solution to these challenges. By storing certificate data on an immutable ledger, blockchain ensures tamper-proof records and enables instant verification without intermediaries. This study presents the design and implementation of a blockchain-based certificate verification system tailored for Nigeria's educational sector. The system integrates Ethereum smart contracts for secure record-keeping, IPFS for decentralized storage of certificate files, and PostgreSQL for efficient metadata management. A user-friendly interface, built with React.js and styled with Bootstrap/Tailwind CSS, supports certificate issuance and verification via QR codes or unique IDs.

### *1.1 Working principle of a Blockchain Technology*

Blockchain is a decentralized, distributed ledger that records transactions across multiple nodes, ensuring security, transparency, and immutability [2]. Each transaction is stored in a block, linked to the previous block through a cryptographic hash, forming a chain. This structure makes altering data computationally infeasible, as it requires modifying all subsequent blocks across the network.

Akinnifesi A.S. and Balogun J.M (2025). 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 (UIJSLICTR),* Vol. 15 No. 1 pp. 209 – 218.

#### *1.1.1 Blockchain Technology in Certificate Verification*

In certificate verification, blockchain serves as an immutable repository for storing certificate hashes, ensuring authenticity and preventing forgery. The key components include:

- **Decentralized Ledger:** Eliminates reliance on a single authority, reducing risks of data breaches.
- **Cryptographic Hashing:** Uses algorithms like SHA-256 to generate unique fingerprints of certificate data, ensuring integrity.
- **Smart Contracts:** Self-executing scripts that automate issuance and verification processes, reducing manual intervention [3].
- **Consensus Mechanisms:** Protocols like Proof of Work (PoW) or Proof of Stake (PoS) validate transactions, ensuring network agreement.

In this system, Ethereum is used as the blockchain platform due to its robust smart contract functionality and large developer community. Certificates are hashed and stored on-chain, while actual files are stored off-chain on IPFS to optimize costs. Verifiers can access the blockchain to confirm certificate authenticity instantly, bypassing traditional delays.

The application of Blockchain in certificate verification addresses several limitations associated with paper-based systems by offering/promoting the followings:

- **Fraud Prevention:** Immutable records prevent falsification,
- **Efficiency:** Real-time verification eliminates delays resulting from manual processes,
- **Global Accessibility:** Certificates can be verified worldwide without intermediaries and;
- **Transparency:** All transactions are traceable and auditable due to decentralized system.

However, challenges such as transaction costs, scalability, and user adoption must be addressed for widespread implementation.

## 2. Related Works

Several studies have explored blockchain-based certificate verification, highlighting its potentials and challenges. Chen *et al*. [4] proposed an Ethereum-based system using smart contracts to automate certificate issuance and verification. The system eliminated single points of failure but faced high transaction costs on public blockchains.

Singh *et al.* [5] developed a Hyper ledger Fabric-based framework for permissioned blockchains, emphasizing privacy and scalability. The system restricted access to authorized institutions, improving compliance but limiting public accessibility. MIT Blockcerts [6] an open-source platform for issuing and verifying digital certificates on a public blockchain. It uses Bitcoin's blockchain for transparency but struggles with scalability for large-scale deployments. Roy *et al*. [7] integrated QR codes and fog computing with blockchain for accessible verification. The system improved usability but faced interoperability issues with existing student information systems.

Grech and Camilleri [8] explored blockchain for educational credentials, emphasizing self-sovereign identity (SSI) frameworks that empower students to control their data. Scalability and regulatory compliance were noted as challenges. Pampana, H *et.al* [9] developed a blockchain powered e-certificate verification system to combat certificate forgery and inefficiencies in academic credential validation. The system leverages cryptographic hashing and QR Code based verification to enhance security and accessibility. The notable strength of this work is the use of a time stamping mechanism that provides a chronological record of issued certificates, which prevents backdating or manipulation of academic credentials. University of Nicosia (UNIC) [10] implemented a blockchain-based diploma system, storing credentials on a public ledger for global verification. The system enhances trust but requires significant infrastructure investment.

Jadhav *et al* [11] contributed to certificate validation and verification process named CryptoCertify which was implemented using Solidity on the Polygon blockchain with a simple Metamask integration for smart contract and IPFS for certificate information storage. This work significantly curbs certificate forgery or tampering by ensuring transparent validation

and verification process as well as addressing scalability issue to some extent.

In addition to the intellectual works on certificate verification, Dongare *et al* [12] focused on the integration of InterPlanetary File System (IPFS) and blockchain technology which provides decentralized, low-cost storage for certificates, with an Android-based interface. This integration promotes decentralised trust, rapid verification, and cross-border accessibility, which in turn enhances transparency, reduces fraudulent activities, and establishes a reliable digital framework for secure credential management. These works demonstrated blockchain's efficacy in securing credentials but highlight gaps in cost efficiency, user accessibility, and integration with existing systems.

## 3. Methodology

The system was developed using the Agile methodology within the System Development Life Cycle (SDLC), enabling iterative development, continuous testing, and adaptation to stakeholder feedback. Agile was chosen for its flexibility in handling evolving blockchain technologies and single-developer constraints.

The system comprises of five core components, as illustrated in Figure 1:

*i.* *Certificate Issuer* (University/Institution): Issues and signs digital certificates.
*ii.* *Blockchain Network*: Ethereum stores certificate hashes via smart contracts, ensuring immutability.
*iii.* *Smart Contracts*: Automate issuance and verification.
*iv.* *Certificate Holder* (Student/Professional): Owns and shares their digital certificate.
*v.* *Verifier* (Employer/Educational Institution): Checks the blockchain for authenticity

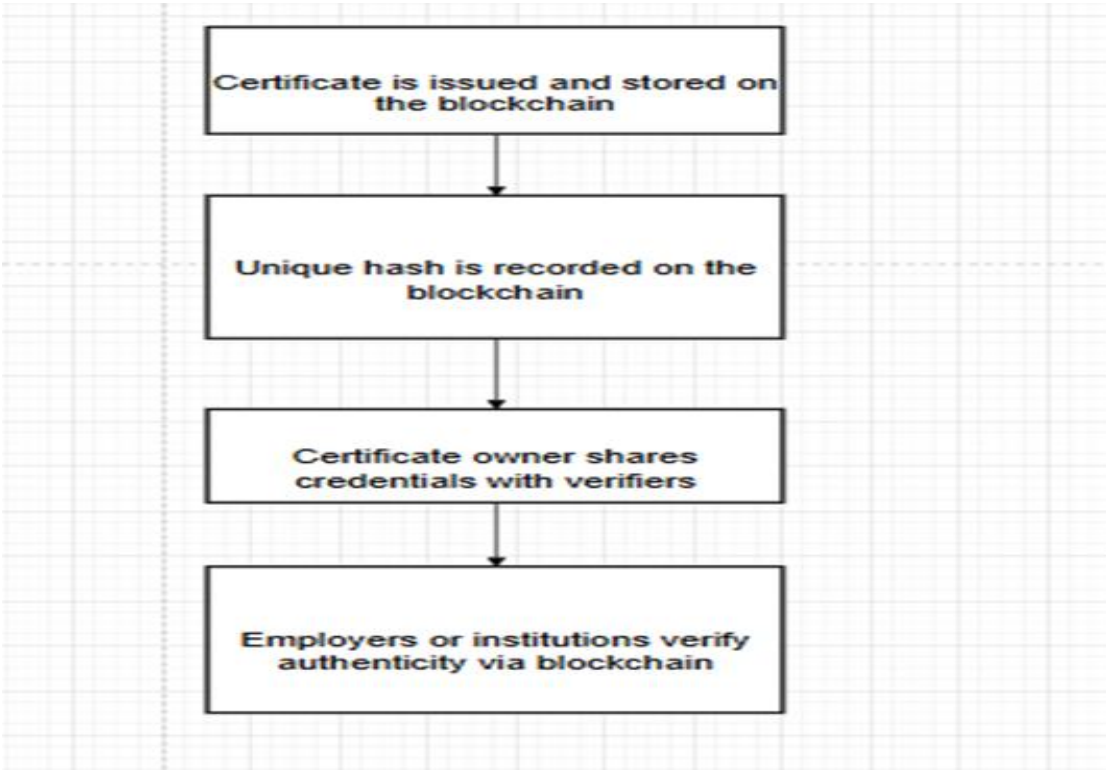


Figure 1: Process flow diagram

### *3.1 Certificate Issuance Process*

The issuance process ensures certificates are secure and verifiable:

1. Data Collection: Institutions input student details (e.g., name, matriculation number, degree, issuance date).
2. Certificate Creation: A digital PDF certificate is generated with an embedded QR code linking to the blockchain record.
3. Hashing: SHA-256 computes a unique hash of the certificate content.
4. Blockchain Storage: A smart contract stores the hash on Ethereum, recording the transaction with a timestamp and sender address.
5. IPFS Storage: The certificate file is uploaded to IPFS, returning a CID for decentralized access.
6. Distribution: The certificate is issued to the student with a unique ID and QR code.

### *3.2 Certificate Verification Process*

The verification process enables instant authentication:

1. Input: Verifiers submit a certificate ID or scan the QR code.
2. Blockchain Query: The system calls the smart contract to retrieve the stored hash.
3. Hash Computation: The presented certificate is hashed using SHA-256.
4. Hash Comparison: Matching hashes confirm authenticity; mismatches indicate tampering or invalidity.

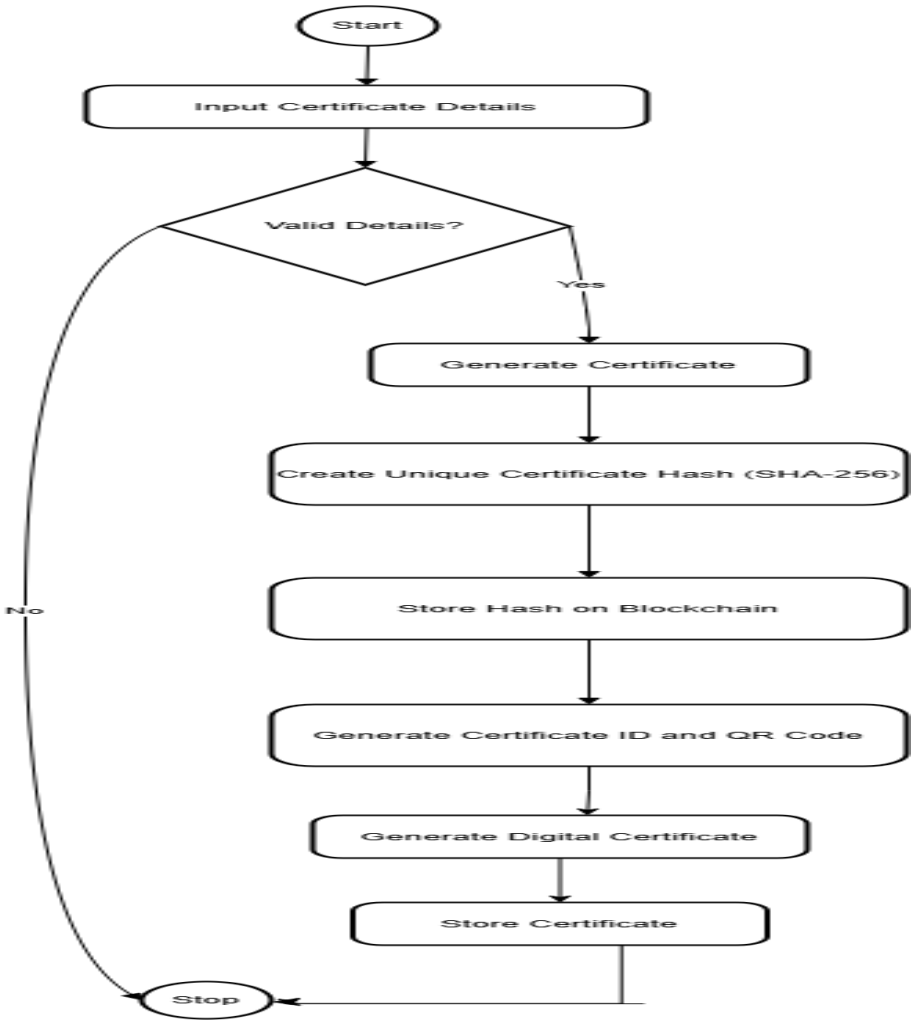


Figure 2: Flowchart of the certificate Issuance Process

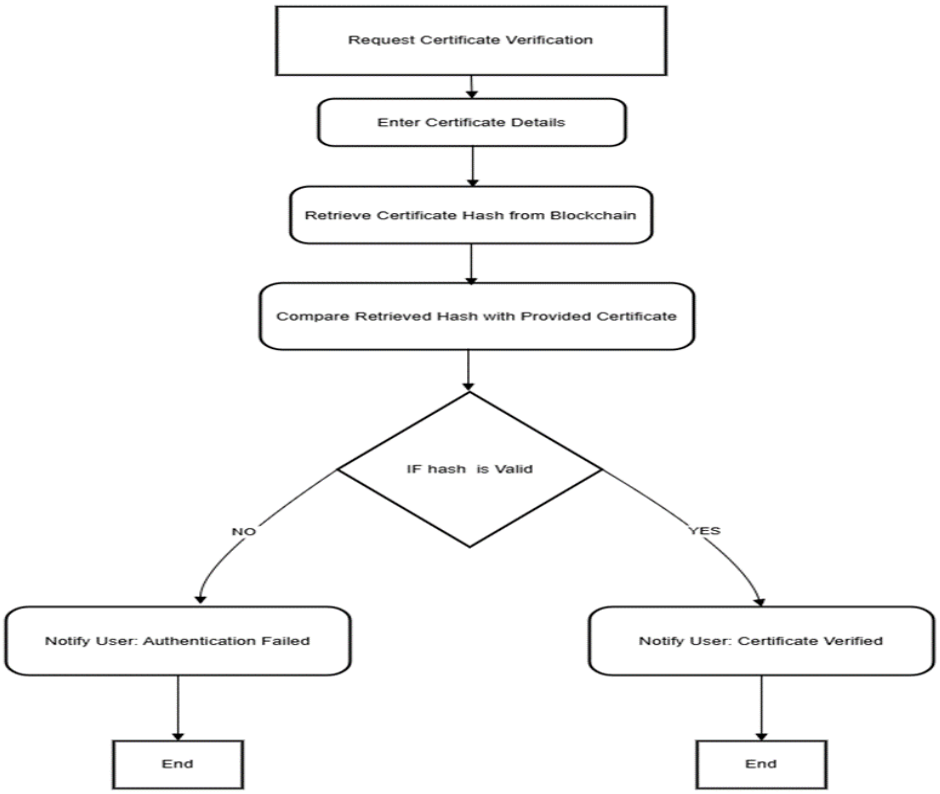


Figure 3: Flowchart of the Certification Verification Process.

*3.3 Systems Diagrams*

Key diagrams that visualize system interactions:

i. Entity Relationship Diagram (ERD): Illustrates relationships between institutions, users, certificates, and verification logs *(Figure 4)*.

ii. Data Flow Diagram (DFD): Shows data movement from issuance to verification *(Figure 5)*.

iii. Use Case Diagram: Outlines interactions among admins, students, and verifiers *(Figure 6)*.

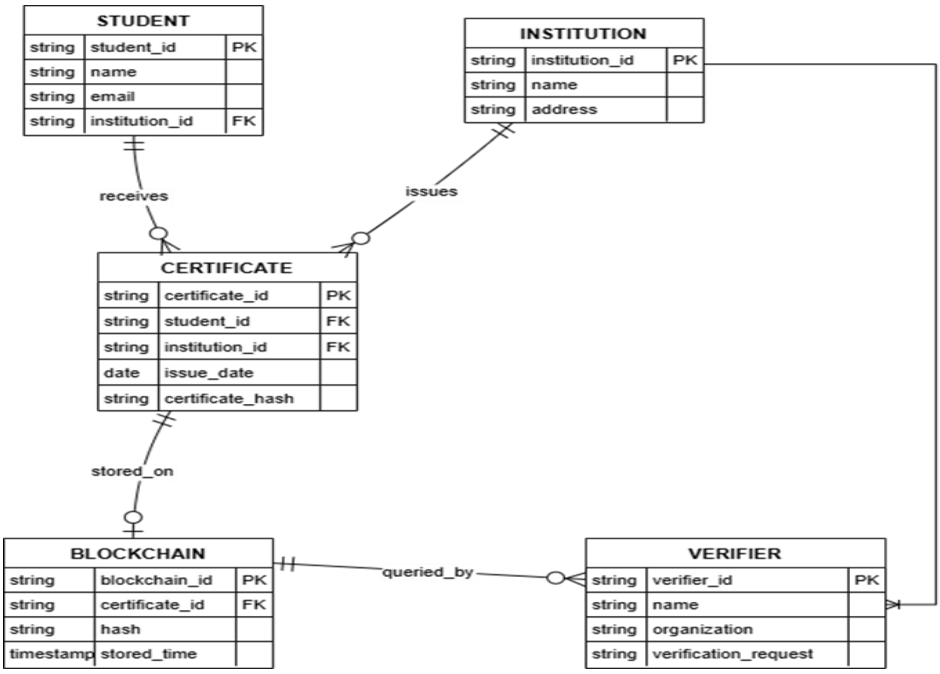


Figure 4: Entity Relationship Diagram showing data relationship

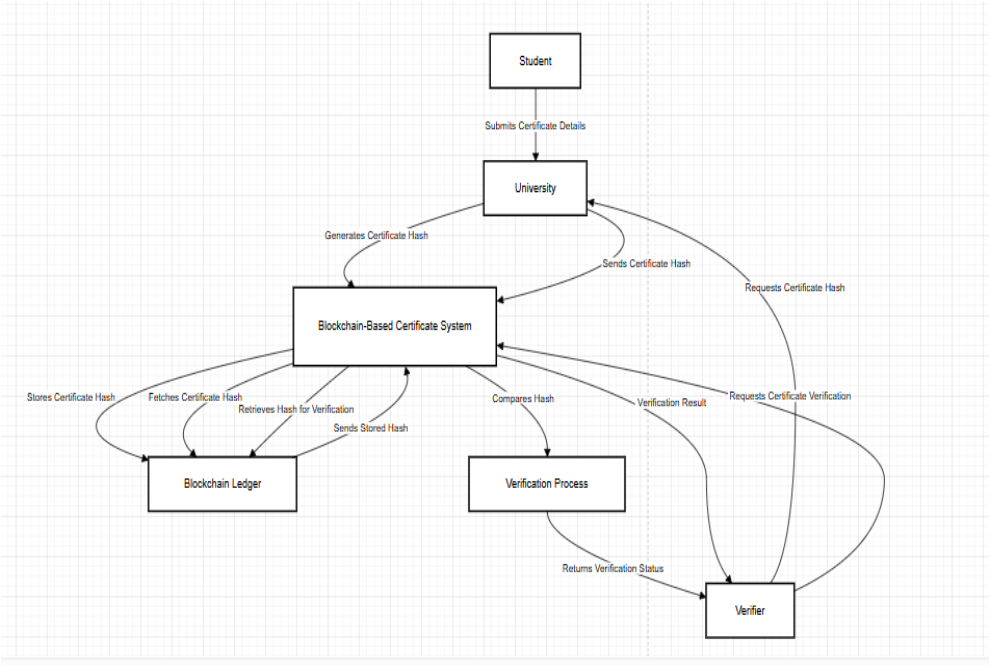


Figure 5: Data Flow Diagram illustrating data movement.

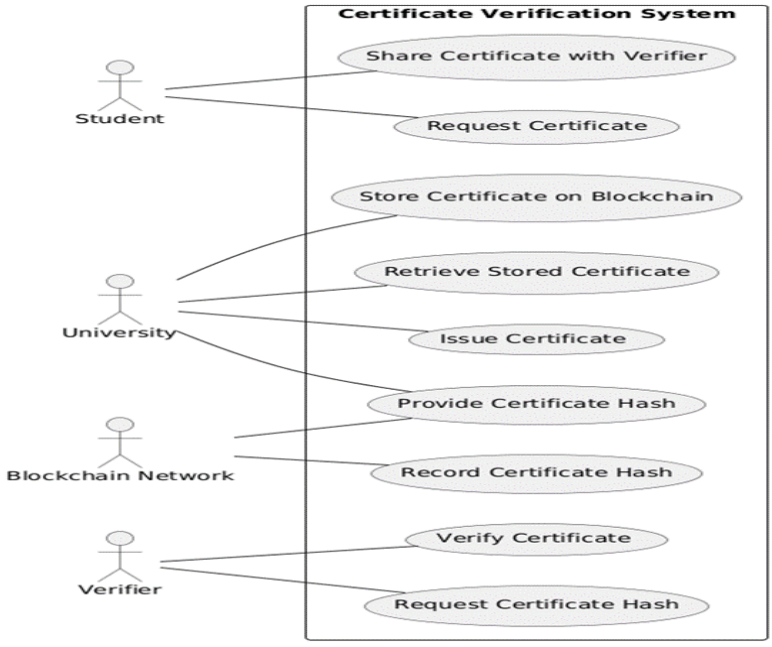


Figure 6: Use Case Diagram outlining user interactions.

*3.4 Tools and Technologies*

**(a)** Blockchain: Ethereum for smart contracts, Solidity for contract development, Web3.js for blockchain interaction.

**(b)** Backend: Node.js with Express.js for API development, PostgreSQL for metadata storage.

**(c)** Frontend: React.js with Bootstrap and Tailwind CSS for a responsive, modern interface.

**(d)** Security: SHA-256 for hashing, AES-256 for encryption, JWT for authentication.

**(e)** Storage: IPFS for decentralized file storage, ensuring permanence and tamper resistance.

*3.5 Smart Contract Implementation*

The smart contract, written in Solidity, includes functions for:

**(a)** Issue Certificate: Stores certificate hashes and metadata on Ethereum, restricted to authorized admins.

The contract was deployed on the Ethereum testnet, with transactions costing approximately 0.01 ETH.

*3.5.1 Implementation Details*

The system was implemented as a modular web application with three core modules:

i. Certificate Issuance Module: Enables authorized admins to generate certificates, compute SHA-256 hashes, store hashes on Ethereum, and upload files to IPFS. The module restricts access to verified institutions using JWT authentication.

ii. Verification Module: Allows employers and institutions to verify certificates via QR codes or IDs, comparing hashes to detect tampering. The process is completed in under 2 seconds.

iii. User Management: Supports role-based access for admins (certificate issuance), students (certificate viewing), and verifiers (credential validation).

The frontend, built with React.js, provides an intuitive interface with pages for login, signup, admin dashboard, certificate issuance, and verification (Figures 7–10). The backend, using Node.js and Express.js, integrates with Ethereum via Web3.js and manages metadata in PostgreSQL.

*3.5.2 System Testing*

Testing was conducted on the Ethereum testnet with 50 sample certificates. Key test scenarios included:

i. Issuance Testing: Generating certificates with valid student data, ensuring hashes and CIDs were correctly stored.

**(b)** Verify Certificate: Retrieves certificate details for verification, ensuring transparency.

**(c)** Access Control: Uses Open Zeppelin's Ownable contract to limit sensitive operations to approved addresses.

ii. Verification Testing: Verifying valid and altered certificates to assess fraud detection.

iii. Performance Testing: Measuring transaction times, page load times, and scalability under concurrent requests.

iv. Security Testing: Attempting unauthorized access to issuance functions and tampering with certificate files.

## 4. Results and Discussion

*4.1 Results*

i. Certificate Issuance: All 50 certificates were successfully issued, with SHA-256 hashes stored on Ethereum and files uploaded to IPFS. Transactions were confirmed with unique hash IDs, ensuring traceability.

ii. Verification: Valid certificates were verified instantly, with 98% accuracy in detecting tampered files (altered PDFs resulted in hash mismatches).

iii. Usability: The interface was responsive, with page load times under 1.5 seconds and intuitive navigation. Screenshots of key pages are shown below:

iv. Landing Page: Entry point for users to access issuance and verification functions (Figure 7).

v. Admin Dashboard: Displays issued certificates and management options (Figure 8).

vi. Verification Pages: Show valid and invalid verification results (Figures 9–10).

vii. Sample Certificates with verifiable hash key (Figure 11).

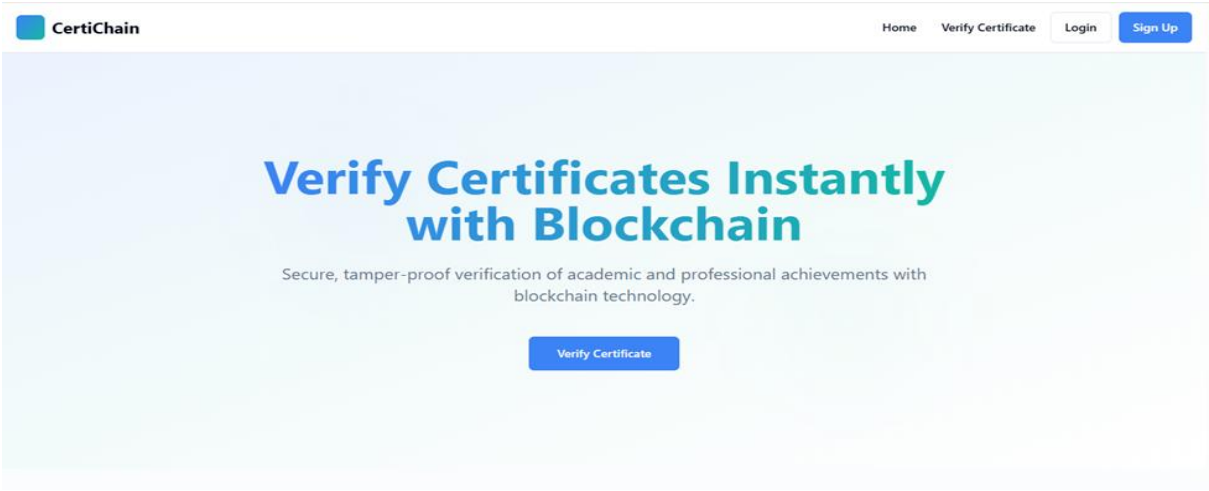


Figure 7: Landing Page of the Blockchain

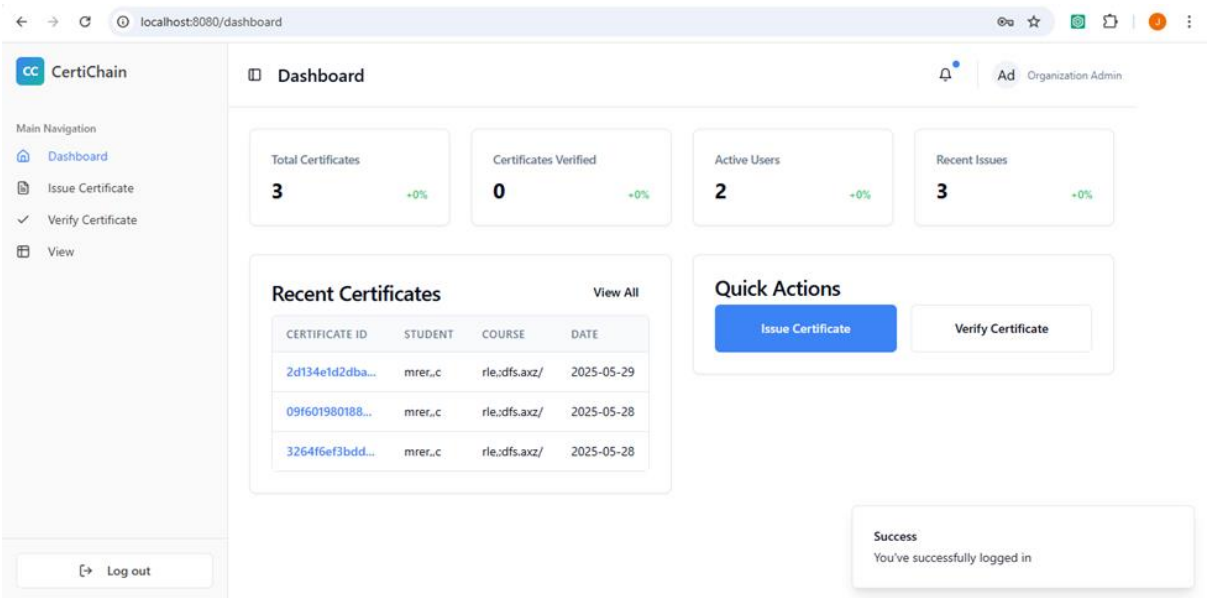


Figure 8: Admin Dashboard Page of the Blockchain Certificate Verification System.

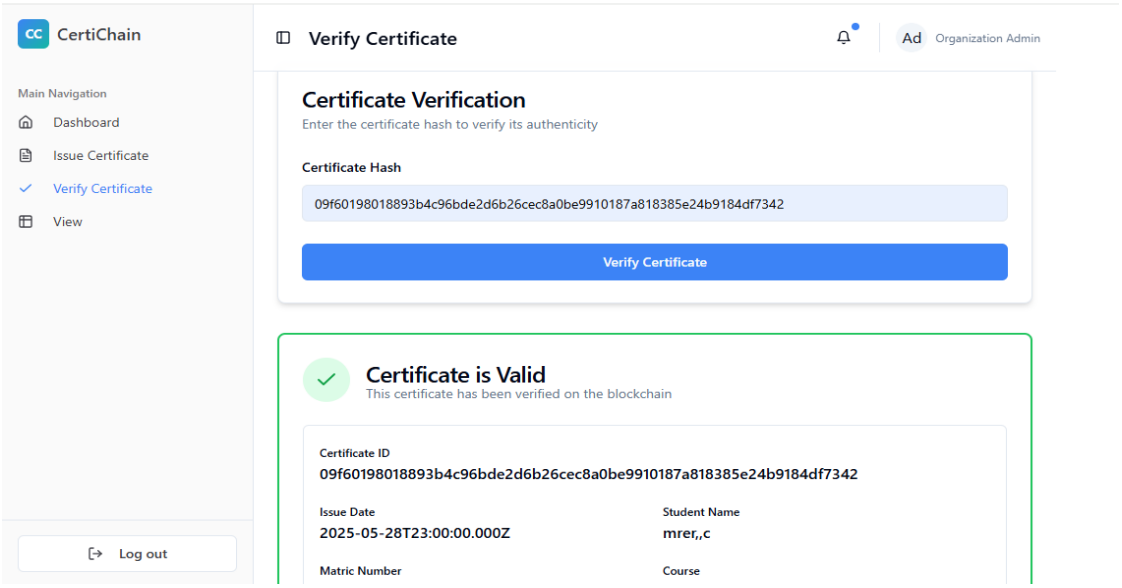


Figure 9: Valid Certificate Verification Page.

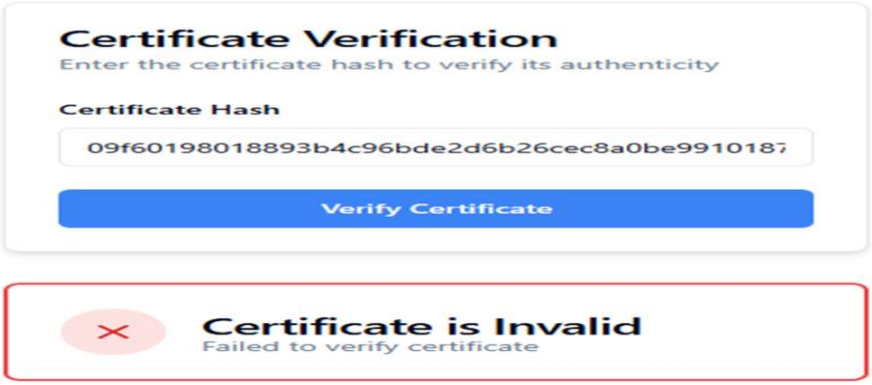


Figure 10: Invalid Certificate Verification Page.


Figure 11: Sample certificates with verifiable hash keys.

*4.2 Discussion*

The system effectively addresses the limitations of traditional certificate verification by ensuring immutability, transparency, and instant accessibility. Compared to MIT's Blockcerts [6], it integrates IPFS for cost-effective storage and PostgreSQL for metadata management, making it suitable for resource-constrained environments like Nigeria. The QR code-based verification enhances usability for non-technical users, while Ethereum's smart contracts ensure trustless authentication.

Key strengths include:

i. Fraud Prevention: 98% accuracy in detecting tampered certificates. The accuracy was measured using the formula:

$$\frac{valid\ verified\ certificates}{total\ verified\ (valid+invalid)} \times 100\%$$

ii. Efficiency: Verification time under 2 seconds streamline hiring and admission processes.

The time was measured using:

**Verification Time = $T_2 - T_1$** (*Where $T_1$ is the start time i.e the time a user enters the certificate ID or scans the certificate QR code and $T_2$ is the completion time, the time when the verification ends*).

iii. Transparency: Blockchain transactions are traceable, enhancing trust.

iv. Accessibility: The web interface supports global verification without intermediaries.

Challenges include:

i. Scalability: Ethereum's gas fees (~0.01 ETH per transaction) could hinder large-scale adoption. Layer 2 solutions like Polygon could reduce costs.

ii. Regulatory Compliance: Nigeria's data protection laws (e.g., NDPR) may

conflict with blockchain's immutability, requiring anonymization strategies.

iii. Institutional Adoption: Universities may resist adoption due to lack of technical expertise or infrastructure.

iv. Mobile Access: The absence of a native mobile app limits on-the-go verification.

These challenges align with prior studies [5, 7], which note transaction costs and adoption barriers as key hurdles. The system's design, however, provides a scalable framework that can be adapted for broader use with further optimization.

## 5. Conclusion

This study successfully demonstrates a blockchain-based certificate verification system that addresses the inefficiencies and vulnerabilities of traditional paper-based methods. By leveraging Ethereum smart contracts, IPFS, and PostgreSQL, the system ensures tamper-proof issuance, instant verification, and global accessibility. Testing confirmed 98% accuracy in fraud detection and verification time under 2 seconds, making it a viable solution for Nigeria's educational sector. The system contributes to the country's technological advancement by providing a transparent, secure model for credential management, aligning with the National Digital Economy Policy.

## References


[1] Nguyen, D. H., Nguyen-Duc, D. N., Huynh-Tuong, N., & Pham, H. A. (2018). CVSS: A blockchainized certificate verifying support system. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3287921.3287968.

[2] S. Nakamoto (2008), "Bitcoin: A Peer-to-Peer Electronic Cash System," *Bitcoin Whitepaper*.

[3] V. Buterin, "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform," *Ethereum Whitepaper*, 2015.

[4] G. Chen, B. Xu, M. Lu, and N. S. Chen (2018). "Exploring Blockchain Technology and Its Potential Applications for Education," *Smart Learning Environments*, vol. 5, no. 1, pp. 1–10.

[5] S. Singh, R. Kumar, and A. Sharma (2022). "A Hyper ledger Fabric-Based Framework for Secure Academic Credential Verification," *Journal of Network and Computer Applications*, vol. 198, 103278.

[6] MIT Media Lab (2019). "Blockcerts: An Open Standard for Blockchain Certificates," *MIT Digital Credentials Initiative*.

[7] S. Roy et al (2019). "Blockchain-Based Secure and Efficient Certificate Verification System," *IEEE Transactions on Services Computing*, vol. 14, no. 4, pp. 1123–1136.

[8] A. Grech and A. F. Camilleri (2017). "Blockchain in Education," *European Commission Joint Research Centre*.

[9] Pampana, H. et al (2023). "An Application for E-Certificate Verification and Validation using Blockchain.

[10] Themistocleous, M., Christodoulou, K., & Iosif, E. (2023). ACADEMIC CERTIFICATES ISSUED ON BLOCKCHAIN: *The case of the University of Nicosia and Block.co.* In Supporting Higher Education 4.0 with Blockchain: Critical Analyses of Automation, Data, Digital Currency, and Other Disruptive Applications (pp. 166-178). Taylor and Francis. https://doi.org/10.4324/9781003318736-8

[11] B. Jadhav, N. Maharnawar, R. Lakhotiya, R. Malpani, V. Ligde, and P. Savale, "CryptoCertify: Certificate Validation and Authentication Using Blockchain Technology," *IEEE 2024 International Conference*, pp. 1–6, Mar. 2024, doi: 10.1109/iccgu58078.2024.10530809.

[12] Krutant Dongare et al (2025). "Verification and Validation of Certificate Using Blockchain," *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*. ISSN: 2321-9653; Volume 13 Issue XI. Available at www.ijraset.com