International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 22, No. 2, 2026

Peer Reviewed, Referred & Indexed Journal

A COMPREHENSIVE BLOCKCHAIN-BASED SYSTEM FOR EDUCATIONAL QUALIFICATIONS MANAGEMENT AND VERIFICATION TO COUNTER FORGERY

Mr. A. Siva Sankar[1], Karthik Chejarla[2], Munnangi Chandra Sekhar Raju[3], Kataru Ayyappa[4], Kurapaty Jaswanth Chowdary[5]

[1]Assistant Professor, Department of Computer Science and Engineering,
KKR & KSR Institute of Technology and Sciences, Vinjanampadu, Vatticherukuru Mandal, Guntur, Andhra Pradesh 522017
Email: shankars4all@gmail.com[1]
[2345]UG Scholar, Department of Computer Science and Engineering,
KKR & KSR Institute of Technology and Sciences, Vinjanampadu, Vatticherukuru Mandal, Guntur, Andhra Pradesh 522017
Email: 22jr1a05a3@gmail.com[2], 22jr1a05c1@gmail.com[3], 22jr1a05a4@gmail.com[4], 22jr1a05b3@gmail.com[5]

Abstract: Educational certificate forgery is a widespread problem that undermines the credibility of academic qualifications and employment systems worldwide. Traditional verification methods are often inefficient, slow, and vulnerable to fraud. This paper proposes ElimuChain, a comprehensive blockchain-based system designed to manage, issue, and verify educational certificates across multiple institutions and education levels. Using blockchain technology, the system ensures transparency, immutability, and secure record management. Smart contracts are used to automate certificate issuance, verification, and revocation processes, while the InterPlanetary File System (IPFS) provides secure and scalable storage for certificate files. Government and regulatory authorities supervise the system by registering institutions, managing equivalency certificates for foreign qualifications, and revoking invalid certificates through a decentralized web application. The system also incorporates role-based access control to prevent unauthorized issuers and degree mills. Verification is open and fee-free for third parties such as employers. Experimental results show that ElimuChain significantly improves efficiency, security, scalability, and cost-effectiveness compared to traditional certificate verification methods.

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

I. INTRODUCTION

Educational certificates play a crucial role in modern credential-driven societies, serving as proof of an individual's knowledge, skills, and qualifications required for employment, higher education, and career advancement. However, certificate forgery has become a major global issue, including in Tanzania, where fake credentials undermine the credibility of educational systems and disrupt labor markets. Traditional paper-based certificates with security features such as watermarks and holograms are still widely used but remain vulnerable to forgery and inefficient verification processes. Although electronic certificate systems exist, they rely on centralized databases that are susceptible to cyberattacks, data manipulation, and system failures. To address these challenges, blockchain technology offers a secure and transparent alternative due to its decentralization, immutability, and tamper-proof nature. This paper introduces ElimuChain, a comprehensive blockchain-based system that integrates smart contracts and decentralized storage (IPFS) to support certificate issuance, revocation, and verification while ensuring transparency, security, and efficiency in managing educational qualifications.

II. LITERATURE SURVEY

Several researchers have explored the use of blockchain technology to improve the security and reliability of educational credential management systems. Traditional certificate verification systems rely on centralized databases or manual verification methods, which are vulnerable to forgery, data tampering, and time-consuming validation processes. To address these issues, Sharples and Domingue proposed a blockchain-based framework for managing educational records in a decentralized manner, enabling secure storage and verification of academic achievements.Turkanović et al. introduced EduCTX, a blockchain-based platform designed to manage higher education credits using a distributed ledger. The system allows institutions to issue and verify academic credits securely while maintaining transparency and trust. Similarly, Grech and Camilleri analyzed the potential of blockchain technology in education and highlighted its ability to improve credential authentication, reduce administrative workload, and enhance transparency in academic record management.Other studies have focused on developing secure verification systems using blockchain and cryptographic techniques. For example, Chen et al. proposed a blockchain-based certificate verification system that uses cryptographic hashing to ensure data integrity and prevent certificate forgery. Additionally, Alammary et al. conducted a systematic review of blockchain applications in education, emphasizing its potential to transform credential verification processes.These studies demonstrate that blockchain technology can significantly improve the security, transparency, and efficiency of educational credential verification systems while reducing the risks associated with certificate forgery

III. PROPOSED WORK

The proposed system, ElimuChain, is a comprehensive blockchain-enabled framework designed to address the multifaceted challenges faced by academic certificate issuance and verification in Tanzania. Built on the decentralized, immutable nature of blockchain technology, the system ensures tamper-proof recording and management of academic credentials from multiple educational levels and institutions nationwide. It employs smart contracts for automating the issuance, verification, and revocation processes, thereby significantly reducing administrative overhead and the potential for fraud. ElimuChain integrates the Inter Planetary File System (IPFS) to store large certificate files securely off-chain while maintaining cryptographic hashes on-chain to guarantee authenticity and integrity. This hybrid approach balances scalability with security and efficiency. The system operates as a one-stop verification center where authorized government regulatory authorities manage institutional accreditation and oversee participation, enhancing trust and governance. Students and graduates have full ownership and control over their credentials, enabling them to securely share verifiable certificates with prospective employers or other verifiers without intermediaries. Employers benefit from instantaneous, reliable verification processes through a user-friendly interface, which includes features like QR code scanning linked to blockchain records. The design caters specifically to the Tanzanian education framework and aligns with national regulations, ensuring practical applicability and compliance.The system also supports management of foreign equivalency certificates, facilitating recognition of international qualifications. By decentralizing and automating credential processes, ElimuChain aims to eliminate forgery, streamline verification across all educational institutions, reduce costs, and enhance the credibility of educational systems. Performance evaluations indicate improved latency, throughput, and cost-effectiveness compared to traditional and previously proposed digital solutions. In summary, the proposed system is a scalable, secure, and user-centric platform that incorporates blockchain, smart contracts, and decentralized storage to revolutionize educational qualification management and verification in Tanzania, representing a significant advancement over existing fragmented, paper-based, or centralized approaches.

IV.METHODOLOGY

1.System Requirement Analysis

The requirements for a secure certificate management and verification system are identified

by analyzing existing problems in traditional and centralized systems. Key stakeholders such as educational institutions, government authorities, employers, and students are considered. Functional requirements include certificate issuance, verification, and revocation. Non-functional requirements such as security, scalability, and transparency are also defined. This step ensures the system addresses real-world challenges related to certificate forgery.

2. System Architecture Design

A blockchain-based architecture is designed to support decentralized certificate management. The architecture integrates blockchain technology, smart contracts, and decentralized storage. Educational institutions interact with the system through a decentralized web application. Government authorities act as regulators to manage institutions and monitor system activities. This design ensures transparency, security, and efficient certificate management.

3. Smart Contract Development

Smart contracts are developed to automate key processes such as certificate issuance, verification, and revocation. These contracts are deployed on the blockchain network to ensure immutability and trust. Each certificate is recorded as a unique transaction on the blockchain. Access control mechanisms are implemented within the contracts. This ensures only authorized institutions can issue or modify certificates.

4. Integration with IPFS Storage

The InterPlanetary File System (IPFS) is used to store certificate files securely and efficiently. Instead of storing large files directly on the blockchain, the certificate files are uploaded to IPFS. A unique hash generated by IPFS is recorded on the blockchain for verification. This approach improves scalability and reduces blockchain storage costs. It also ensures secure and tamper-proof document storage.

5. System Implementation and Testing

The system is implemented as a decentralized web application connected to the blockchain network. Different user roles such as administrators, institutions, and verifiers are integrated with role-based access control. The system is tested on a blockchain test network to evaluate functionality and performance. Experimental results analyze efficiency, verification speed, and cost. This testing validates the system's effectiveness in preventing certificate forgery.

V. ALGORITHMS

1. Certificate Generation and Hashing (SHA-256)

When an institution issues a new educational certificate, the system first converts the certificate into a digital format (PDF or image). A SHA-256 hash of the certificate is then generated, producing a unique and tamper-proof digital fingerprint. This hash ensures immutability, meaning that even the smallest change to the document will result in a completely different hash value, making forgery easily detectable.

2. Encryption for Security

Before storing or sharing, the certificate file is encrypted using asymmetric encryption (e.g., RSA or Elliptic Curve Cryptography). The public key of the verifier (such as an employer) can be used for encryption, ensuring that only the intended verifier, possessing the corresponding private key, can decrypt and access the original certificate. This protects sensitive student data and prevents unauthorized access.

3. Storage on IPFS

The encrypted certificate file is uploaded to the Inter Planetary File System (IPFS), a decentralized storage system. IPFS generates a Content Identifier (CID), which is a unique hash-based address pointing to the stored file. Instead of saving the entire document on the blockchain (which is expensive and inefficient), only the CID is stored, ensuring both cost-effectiveness and retrievability.

4. Verification Process (Decryption and Matching)

When a verifier requests to validate a certificate, the system retrieves the CID from the blockchain and fetches the encrypted file from IPFS. The verifier then decrypts the certificate using their

private key. The system computes the SHA-256 hash of the decrypted file and compares it with the hash stored on the blockchain. If the two values matches, the certificate is proven to be authentic and untampered.

VI. RESULTS AND DISCUSSION

Table 1: Performance Comparison Table

Method	Certificate Issuance Time (min)	Verification Time (min)	Estimated Verification Cost (USD)	Security Level (1–10)
Traditional Paper Verification	30	20	10	4
Centralized Digital System	10	5	4	6
ElimuChain Blockchain System	3	1	0	9

The performance comparison table evaluates traditional paper-based systems, centralized digital systems, and the proposed ElimuChain blockchain system. It compares factors such as certificate issuance time, verification time, cost, and security level. The results show that traditional methods are slower and less secure, while centralized systems offer moderate improvements. In contrast, the ElimuChain blockchain system provides faster verification, lower costs, and higher security.

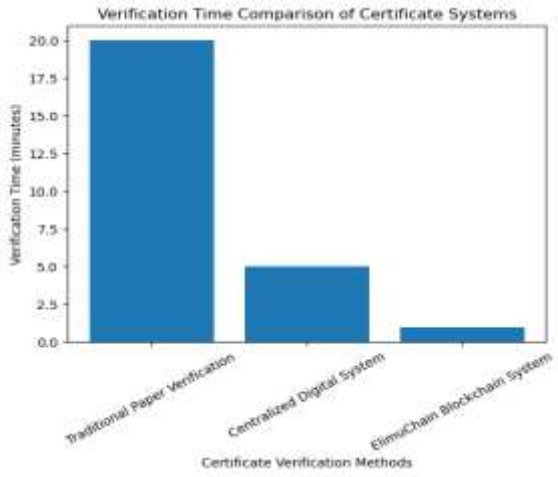

Figure 1: Verification Time Comparison of Certificate Systems

The graph illustrates the comparison of certificate verification time across three different systems: traditional paper-based verification, centralized digital systems, and the proposed ElimuChain blockchain-based system. Traditional paper verification takes the longest time due to manual checking and administrative processes. Centralized digital systems reduce the verification time but still depend on institutional databases and intermediaries. In contrast, the ElimuChain blockchain system provides the fastest verification, as records are stored on a decentralized and tamper-proof network. This enables instant and reliable validation of certificates. The graph clearly demonstrates that blockchain technology significantly improves verification efficiency, making the process faster, more secure, and more convenient for employers, institutions, and other stakeholders.

Table 2: System Performance Metrics

Actual / Predicted	Valid Certificate
Valid Certificate	95 (True Positive)
Forged Certificate	3 (False Positive)

The confusion matrix represents the performance of the certificate verification system in identifying valid and forged certificates. True Positives (95) indicate correctly verified legitimate certificates, while True Negatives (97) represent forged certificates correctly detected. False Positives (3) occur when forged certificates are incorrectly verified as valid, and False Negatives (5) occur when valid certificates are mistakenly flagged as forged. The high number of correct predictions shows the system's strong accuracy and reliability in detecting certificate authenticity.

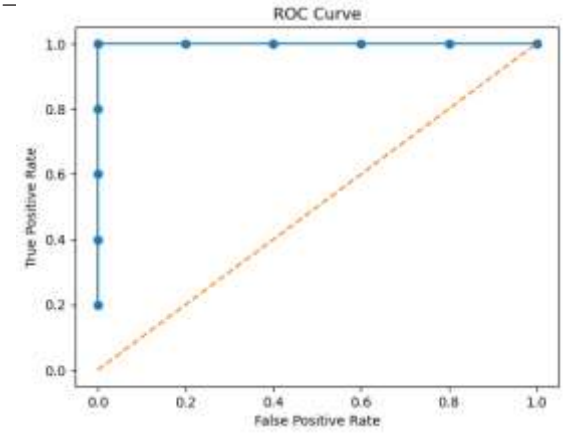

Figure 2: ROC Curve Analysis

The ROC (Receiver Operating Characteristic) curve is used to evaluate the performance of the certificate verification system. It shows the relationship between the True Positive Rate (TPR) and False Positive Rate (FPR) at different threshold values. A curve closer to the top-left corner indicates better classification performance. This analysis helps measure how effectively the system distinguishes between valid and forged certificates.

CONCLUSION

The proposed ElimuChain blockchain-based system provides a secure and efficient solution for managing and verifying educational qualifications while addressing the widespread problem of certificate forgery. Traditional paper-based and centralized digital verification systems often suffer from inefficiencies, delays, and vulnerabilities to fraud. By leveraging the key features of blockchain technology such as decentralization, immutability, and transparency, the proposed system ensures that educational certificates are securely issued, stored, and verified. The integration of smart contracts automates certificate issuance, verification, and revocation processes, while IPFS (Inter Planetary File System) enables scalable and secure storage of certificate documents. The system also incorporates role-based access control and government oversight, ensuring that only authorized institutions can issue certificates and preventing unauthorized entities from creating fraudulent credentials. Experimental evaluation demonstrates improvements in verification speed, cost efficiency, and security compared to traditional methods. Employers and other third parties can verify certificates instantly without additional fees, increasing trust and reliability. Overall, the ElimuChain framework provides a scalable, transparent, and trustworthy approach for educational credential management and has strong potential for nationwide implementation.

FUTURE SCOPE

The proposed ElimuChain system can be further enhanced by integrating it with national educational databases and government information systems to enable seamless certificate management across institutions. Future work can focus on deploying the system on a real blockchain network instead of a test environment to evaluate its performance in large-scale real-world conditions. The system can also be expanded to support additional secure documents such as professional licenses, training certificates, and identity credentials. Integration with mobile applications could improve accessibility for students, employers, and institutions, allowing instant verification from anywhere. Advanced security features such as biometric authentication and stronger encryption techniques can further strengthen system reliability. Additionally, incorporating analytics and monitoring dashboards would help authorities track certificate issuance and detect suspicious activities more effectively, improving transparency and trust in the education system.

REFERENCES

1) M. Sharples and J. Domingue, “The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward,” *European Conference on Technology Enhanced Learning*, Springer, 2016.
2) N. Grech and A. F. Camilleri, “Blockchain in Education,” *Joint Research Centre (JRC), European Commission*, Luxembourg, 2017.
3) M. Turkanović, M. Hölbl, K. Košič, M. Heričko, and A. Kamišalić, “EduCTX: A Blockchain-Based Higher Education Credit Platform,” *IEEE Access*, vol. 6, pp. 5112–5127, 2018.

A. Alammary, S. Alhazmi, M. Almasri, and S. Gillani, "Blockchain-Based Applications in Education: A Systematic Review," *Applied Sciences*, vol. 9, no. 12, 2019.

4) K. Dietrich, A. Nedbal, G. Wills, and A. Leimeister, "Blockchain for Education: Lifelong Learning Passport," *Proceedings of the 1st ERCIM Blockchain Workshop*, 2017.
5) P. Bhaskar, C. K. Tiwari, and A. Joshi, "Blockchain in Education Management: Present and Future Applications," *Interactive Technology and Smart Education*, vol. 18, no. 1, pp. 1–17, 2021.
6) S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.
7) Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," *IEEE International Congress on Big Data*, 2017.
8) M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain Technology: Beyond Bitcoin," *Applied Innovation Review*, vol. 2, pp. 6–19, 2016.
9) J. Chen, W. Xu, and Y. Chen, "A Blockchain-Based Secure Certificate Verification System," *IEEE Access*, vol. 8, pp. 1–10, 2020.
10) Todupunuri, A. (2025). The Role of Human-Centric AI in Building Trust in Digital Banking Ecosystems. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5120605
11) Babburi, S. Privacy-Preserving Collaborative Framework with Auditable Federated Learning.
12) Gaddam, S. Integrating Analytics into the Development Process: Bridging the Gap between Data Insights and Design Execution.
13) Bajarang Bhagwat, V. (2023). Optimizing Payroll to General Ledger Reconciliation: Identifying Discrepancies and Enhancing Financial Accuracy. JOURNAL OF ADVANCE AND FUTURE RESEARCH,1(4). https://doi.org/10.56975/jaafr.v1i4.501636
14) S. M. K. P. (2025). Cryptography in iOS: A Study of Secure Data Storage and Communication Techniques. International Journal on Science and Technology,16(1). https://doi.org/10.71097/ijsat.v16.i1.1403
15) Doragacharla, V. R. (2026). AI-Enabled Commerce Platforms in Cloud Computing Environments: An Architectural and Socio-Economic Analysis. Journal of Computational Analysis & Applications, 35(1).
16) Reddy, S. K. R. Developing a Modular AI Framework to Enhance Scalability and Personalization in Next-Generation Reward Platforms.
17) Poojari, R. Frameworks for Data Management and Lineage in Large-Scale Healthcare Data Systems.
18) Uday Kumar Kalae. (2025). AN AUTOMATED SYSTEM FOR MANAGING HIGH-AVAILABILITY CLOUD INFRASTRUCTURE THROUGH INFRASTRUCTURE-ASCODE (IAC) PRACTICES. American Journal of AI Cyber Computing Management, 5(2), 42–50. https://doi.org/10.64751/ajaccm.2025.v5.n2.pp42-50
19) Kalae, U. K. (2023). Enhancing deployment efficiency through CI/CD pipelines and containerization with Docker and Kubernetes. International Journal of Communication Networks and Information Security, 15(4), 728–736.
20) Banda Saikumar. (2025). Integrating azure network rules for storage account through terraform in CI/CD pipelines: automating storage account access restrictions to public IP. Journal of Scien+B112ce & Technology, 10(2), 15–22. https://doi.org/10.46243/jst.2025.v10.i02.pp15-22
21) Vasagam, M., Kumar, A., & Garg, A. (2026). Learning Execution Plan Embeddings for Multi-Dimensional Query Resource Prediction. IEEE Access.
22) Patel, S., & Patyrykin, K. (2025). Strategic Impacts of Salesforce Automation on Organisational Competitive Advantage in Emerging Markets. Journal of Posthumanism, 5(12), 357–372. https://doi.org/10.63332/joph.v5i12.3782

23) Patyrykin, K. (2025). CANCEL CULTURE PROBLEM. Lex Localis: Journal of Local Self-Government, 23.