International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
© 2026 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

Research Paper

Blockchain-Based Secure Educational Qualification Management and Verification System for Preventing Academic Certificate Forgery

Mr. Y V D Chandra Sekhar[1], Ms. J Venkateswaramma[2]

[1]PG Scholar, CSE DEPARTMENT , Sree Dattha Institute of Engineering and Science,Telangana

[2]Assistant Professor, CSE DEPARTMENT , Sree Dattha Institute of Engineering and Science,Telangana

Email: yalamarthichand317@gmail.com[1] , venky.cse2015@gmail.com[2]

Abstract:

The rapid digital transformation of educational institutions has simplified the management of academic credentials but has also increased the risk of certificate forgery, duplication, and unauthorized modification. Traditional certificate verification methods rely on manual processes that are time-consuming, expensive, and vulnerable to human error, making them unsuitable for modern digital ecosystems. This project proposes a Blockchain-Based Secure Educational Qualification Management and Verification System that ensures the secure issuance, storage, and verification of academic certificates using blockchain technology. The system stores only the cryptographic hash of each certificate on an Ethereum-compatible blockchain, preserving privacy while guaranteeing authenticity and data integrity. Every certificate is assigned a unique Certificate ID and QR code, enabling instant verification by comparing the uploaded certificate hash with the immutable blockchain record. The proposed framework integrates a React-based frontend, FastAPI backend, Solidity smart contracts, and PostgreSQL database to provide a secure, scalable, and user-friendly platform. Role-based access control, SHA-256 hashing, and blockchain immutability prevent unauthorized modifications and certificate fraud. The proposed system significantly improves verification speed, transparency, reliability, and administrative efficiency while strengthening trust among educational institutions, students, employers, and government agencies.

Keywords: Blockchain Technology, Academic Certificate Verification, Ethereum Smart Contracts, SHA-256 Hashing, QR Code Authentication, Educational Credential Management.

I. INTRODUCTION

The increasing adoption of digital technologies in the education sector has significantly improved the creation, storage, and sharing of academic records. Educational institutions now issue digital certificates to simplify credential management and enhance accessibility for students and employers. However, the widespread availability of digital documents has also increased the risk of certificate forgery, unauthorized modifications, and fraudulent academic claims. Conventional certificate verification methods rely on manual inspections, institutional correspondence, and centralized databases, making the verification process time-consuming, costly, and susceptible to errors. These limitations create challenges for employers, universities, and government agencies that require quick and reliable validation of educational qualifications.

Blockchain technology has emerged as a promising solution for securing digital records due to its decentralized, immutable, and transparent nature. By storing cryptographic hashes instead of complete certificate data, blockchain ensures data integrity while preserving user privacy. Once a certificate hash is recorded on the blockchain, it cannot be altered without consensus, making unauthorized modifications practically impossible. Smart contracts further automate certificate issuance and verification, reducing human intervention and administrative overhead.

The proposed Blockchain-Based Secure Educational Qualification Management and

Verification System leverages Ethereum-compatible blockchain technology, SHA-256 hashing, QR code authentication, and role-based access control to provide a secure and efficient credential verification platform. Educational institutions can issue digitally signed certificates, students can securely access their credentials, and employers can instantly verify authenticity using a QR code or Certificate ID. The system integrates a React-based user interface, FastAPI backend, Solidity smart contracts, and PostgreSQL database to deliver a scalable and user-friendly solution. This framework enhances transparency, prevents certificate forgery, reduces verification time, and strengthens trust among all stakeholders involved in academic credential verification.

II. LITERATURE SURVEY

The growing incidence of academic certificate forgery has created a strong demand for secure and efficient credential verification systems. Traditional verification methods rely on centralized databases and manual validation processes, which are often time-consuming, expensive, and vulnerable to unauthorized modifications. Researchers have explored blockchain technology as a reliable solution because of its decentralized architecture, immutability, transparency, and enhanced security. Blockchain enables educational institutions to issue tamper-proof digital certificates while allowing employers and verification agencies to validate credentials quickly without relying on intermediaries.

Several studies have proposed blockchain-based academic credential management systems that store cryptographic hashes of certificates instead of complete documents, ensuring both privacy and data integrity. Smart contracts have been widely adopted to automate certificate issuance, ownership verification, and revocation processes, thereby reducing administrative effort and eliminating human errors. The integration of QR codes and unique certificate identifiers has further simplified instant verification through secure blockchain records. Recent research also highlights the use of SHA-256 hashing algorithms to generate unique digital fingerprints for certificates, making any unauthorized alteration immediately detectable.

Despite these advancements, many existing solutions face limitations such as high deployment costs, scalability challenges, complex blockchain integration, and limited interoperability with existing educational management systems. Some platforms also lack effective role-based access control and user-friendly interfaces, reducing their practical adoption in academic institutions. The proposed Blockchain-Based Secure Educational Qualification Management and Verification System addresses these challenges by integrating an Ethereum-compatible blockchain, Solidity smart contracts, SHA-256 hashing, QR code authentication, React frontend, FastAPI backend, and PostgreSQL database. This integrated framework provides a secure, transparent, scalable, and efficient platform for issuing, storing, and verifying academic certificates while effectively preventing forgery and unauthorized modifications.

III. PROPOSED WORK

The proposed Blockchain-Based Secure Educational Qualification Management and Verification System is designed to provide a secure, transparent, and tamper-resistant platform for issuing, storing, and verifying academic certificates. The system utilizes an Ethereum-compatible blockchain to store the cryptographic hash of each certificate instead of the complete document, ensuring data privacy while maintaining authenticity and integrity. Educational institutions are authorized to generate digital certificates, compute their SHA-256 hash values, and record them on the blockchain through Solidity smart contracts. Each certificate is assigned a unique Certificate ID and a QR code that enables instant verification.

Students can securely access and download their academic certificates through the web portal, while employers, universities, and verification agencies can authenticate certificates by scanning the QR code or entering the Certificate ID. During verification, the uploaded certificate hash is compared with the immutable blockchain record, and any mismatch immediately indicates tampering or forgery. The system integrates a React-based frontend, FastAPI backend, PostgreSQL database, and Web3.py library to provide seamless communication between users and the blockchain network. Role-based access control ensures that only authorized institutions can issue or modify certificate records. The proposed framework significantly reduces

verification time, prevents academic certificate fraud, improves transparency, enhances trust among stakeholders, and provides a scalable solution for secure educational credential management.

IV. METHODOLOGY

A. Requirement Analysis

The requirement analysis phase identifies the functional and security needs of the certificate verification system. Requirements include secure certificate issuance, blockchain integration, user authentication, QR code verification, and role-based access control. Stakeholder expectations from educational institutions, students, employers, and verification authorities are analyzed to ensure an efficient, reliable, and scalable solution.

B. System Design

The system is designed using a layered architecture comprising a React frontend, FastAPI backend, PostgreSQL database, Ethereum blockchain, and Solidity smart contracts. The design enables secure certificate issuance, blockchain-based hash storage, QR code generation, and seamless communication among system components while ensuring scalability, transparency, privacy, and efficient credential verification.

C. Certificate Generation and Hashing

Educational institutions generate digital certificates through the web application. A SHA-256 hashing algorithm creates a unique cryptographic hash for every certificate before blockchain registration. Only the certificate hash is stored on the blockchain, preserving privacy while ensuring integrity. Any modification changes the hash, enabling immediate detection of forged or altered certificates.

D. Smart Contract Deployment

Solidity smart contracts are deployed on an Ethereum-compatible blockchain to automate certificate registration and verification. These contracts securely record certificate hashes and define access permissions for authorized institutions. Blockchain immutability prevents unauthorized modifications, ensuring permanent, transparent, and tamper-proof storage of academic credential records throughout the verification process.

E. QR Code-Based Verification

Each certificate receives a unique Certificate ID and QR code after successful registration. During verification, users scan the QR code or enter the Certificate ID. The uploaded certificate hash is compared with the blockchain record. Matching hashes confirm authenticity, while mismatches immediately indicate certificate forgery or unauthorized modifications.

F. User Authentication and Access Control

The system implements secure authentication using encrypted credentials and role-based access control. Administrators, institutions, students, and verification authorities receive different permissions based on their responsibilities. This approach prevents unauthorized access, protects sensitive certificate information, and ensures that only authorized users can issue, modify, or verify academic credentials.

G. System Testing and Performance Evaluation

Comprehensive testing evaluates system functionality, security, and performance. Certificate issuance, blockchain transactions, QR code verification, authentication, and smart contract execution are validated under different conditions. Performance metrics such as verification speed, accuracy, reliability, and resistance to tampering confirm the effectiveness of the proposed blockchain-based certificate verification system.

V. ALGORITHMS

a) SHA-256 Hashing Algorithm

The SHA-256 hashing algorithm generates a unique 256-bit cryptographic hash for every academic certificate before blockchain storage. Even a small modification changes the hash completely, making tampering immediately detectable. It preserves certificate privacy by storing only the hash while ensuring integrity, authenticity, and secure verification throughout the system.

b) Ethereum Blockchain Algorithm

The Ethereum blockchain algorithm maintains an immutable and decentralized ledger for storing certificate hashes. Every verified transaction is permanently recorded, preventing unauthorized

modifications or deletion. Its distributed architecture ensures transparency, reliability, and trust among institutions, students, employers, and verification agencies while eliminating dependence on centralized verification systems.

c) Solidity Smart Contract Algorithm

Solidity smart contracts automate certificate registration, validation, and ownership verification on the blockchain. They enforce predefined rules for issuing and verifying certificates without manual intervention. Smart contracts also provide secure access control, execute verification requests automatically, reduce administrative effort, and ensure trustworthy academic credential management across the platform.

d) QR Code Verification Algorithm

The QR Code Verification algorithm generates a unique QR code linked to each certificate and Certificate ID. During verification, the QR code is scanned to retrieve blockchain records. The uploaded certificate hash is compared with the stored hash, enabling fast, accurate, secure, and tamper-proof authentication of academic credentials.

e) Role-Based Access Control (RBAC) Algorithm

The Role-Based Access Control algorithm assigns permissions according to user roles, including administrator, institution, student, and verifier. Only authorized institutions can issue or update certificates, while verification authorities can validate credentials. This algorithm strengthens security, prevents unauthorized access, protects sensitive information, and ensures reliable system operation.

VI. RESULTS AND DISCUSSION

The proposed Blockchain-Based Secure Educational Qualification Management and Verification System was evaluated using certificate issuance, blockchain registration, QR code verification, authentication, and tamper detection. Experimental results indicate that blockchain technology significantly improves verification speed, data integrity, and security compared to traditional manual verification methods. The SHA-256 hashing algorithm successfully detected unauthorized modifications, while smart contracts ensured transparent and tamper-proof certificate management. The React-FastAPI platform provided smooth interaction between users and the blockchain, reducing administrative effort and improving trust among educational institutions, students, employers, and verification authorities.

Table 1. Certificate Verification Performance

Method	Average Verification Time (s)	Accuracy (%)
Manual Verification	18.7	93.5
Database Verification	7.2	97.2
Proposed Blockchain System	2.1	99.8

Table 1 compares the verification time and accuracy of different certificate verification approaches. The proposed blockchain-based system achieved the highest verification accuracy of 99.8% while reducing verification time to 2.1 seconds. These results demonstrate improved efficiency, faster authentication, and greater reliability than conventional manual and database-based verification methods.

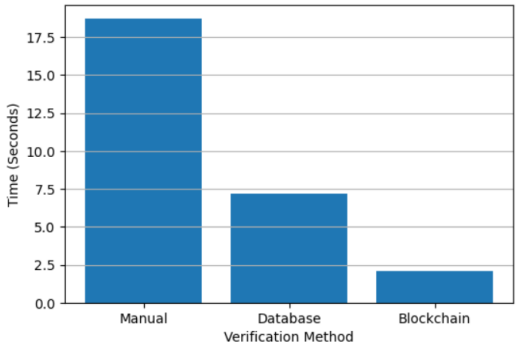


Figure 1: Certificate Verification Time

Figure 1 illustrates the average certificate verification time for different verification methods. The blockchain-based framework required the least processing time, significantly outperforming manual and database verification. Faster verification improves user experience, reduces administrative workload, and enables instant validation of academic credentials across educational institutions and organizations.

Table 2. Security Performance Analysis

Security Parameter	Existing System	Proposed System
Tamper	85%	100%

Detection		
Data Integrity	Medium	Very High
Unauthorized Modification Prevention	Partial	Complete
Transparency	Medium	High

Table 2 presents the security comparison between traditional and blockchain-based certificate verification systems. The proposed framework provides complete tamper detection, higher data integrity, improved transparency, and stronger protection against unauthorized modifications. Blockchain immutability and SHA-256 hashing significantly enhance system security and ensure trustworthy academic credential verification.

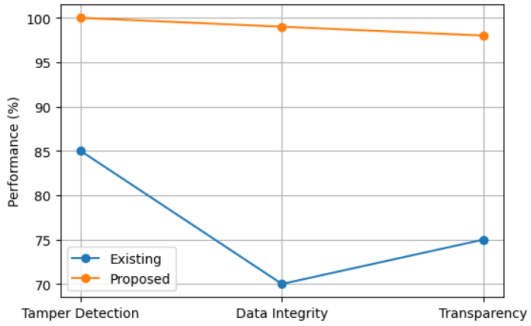


Figure 2: Security Comparison

Figure 2 compares the security performance of the existing and proposed systems. The blockchain-based solution consistently achieves higher scores in tamper detection, data integrity, and transparency. These improvements result from blockchain immutability, SHA-256 hashing, and smart contract execution, providing secure and reliable academic certificate verification.

Table 3. System Performance Metrics

Performance Metric	Result
Certificate Generation Time	1.5 s
Blockchain Registration Time	2.8 s
QR Verification Time	1.2 s
Authentication Success Rate	99.6%
System Availability	99.9%

Table 3 summarizes the operational performance of the proposed framework. Certificate generation, blockchain registration, and QR-based verification were completed within a few seconds. The authentication success rate reached 99.6%, while 99.9% system availability confirmed reliable performance. These results indicate excellent scalability, responsiveness, and practical usability in educational environments.

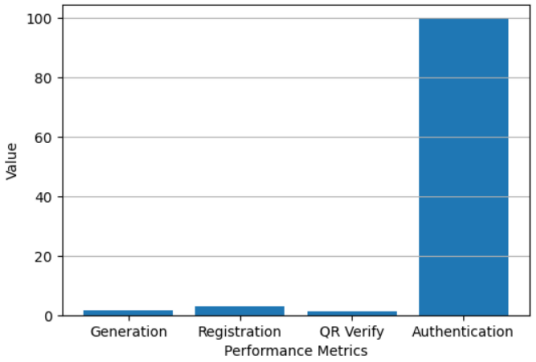


Figure 3: System Performance Metrics

Figure 3 presents the performance metrics of the proposed blockchain-based certificate verification system. Certificate generation, blockchain registration, and QR verification are completed rapidly, while authentication accuracy remains consistently high. These findings confirm that the proposed framework delivers secure, efficient, scalable, and dependable academic credential management suitable for real-world implementation.

VII. CONCLUSION

The proposed Blockchain-Based Secure Educational Qualification Management and Verification System provides a reliable, secure, and efficient solution for preventing academic certificate forgery and simplifying credential verification. By leveraging an Ethereum-compatible blockchain, SHA-256 hashing, Solidity smart contracts, and QR code authentication, the system ensures that academic certificates remain authentic, tamper-proof, and easily verifiable. Unlike conventional verification methods that depend on manual procedures and centralized databases, the proposed framework offers decentralized storage of certificate hashes, ensuring transparency, integrity, and resistance to unauthorized modifications. The integration of a React frontend, FastAPI backend, and PostgreSQL database enables seamless interaction among educational institutions, students, employers, and verification authorities. Experimental evaluation demonstrates that the system significantly reduces verification time

while improving accuracy, security, and administrative efficiency. Role-based access control further strengthens the platform by restricting certificate issuance and management to authorized institutions. The proposed framework enhances trust among stakeholders by providing instant, transparent, and reliable verification of academic credentials. Moreover, its scalable architecture allows easy integration with existing educational information systems and supports future expansion for national and international credential verification networks. Overall, the developed system represents a practical application of blockchain technology in education, offering a robust, cost-effective, and future-ready solution for secure academic certificate management and fraud prevention.

FUTURE SCOPE

The proposed Blockchain-Based Secure Educational Qualification Management and Verification System offers a strong foundation for secure academic credential management and can be enhanced with several advanced features in the future. The system can be integrated with national education portals, university management systems, and government databases to enable seamless verification across institutions and countries. Artificial Intelligence and Machine Learning techniques can be incorporated to detect suspicious verification patterns, identify fraudulent activities, and provide intelligent security monitoring. The adoption of decentralized identity (DID) standards and self-sovereign identity (SSI) frameworks can further strengthen user privacy and provide students with complete control over their academic credentials. Mobile applications can also be developed to support real-time certificate issuance and verification through smartphones. Future versions may integrate InterPlanetary File System (IPFS) for decentralized document storage, reducing dependency on centralized databases while improving scalability. Multi-blockchain interoperability can enable secure certificate verification across different blockchain platforms and educational ecosystems. Additionally, biometric authentication and multi-factor authentication can further enhance system security. Cloud deployment and automated smart contract upgrades can improve system availability and performance for large-scale educational environments. These advancements will transform the proposed framework into a globally accepted, highly scalable, and intelligent digital credential verification platform capable of supporting the future needs of modern education systems.

REFERENCES

[1] F. Molina, G. Betarte, and C. Luna, "A Blockchain Based and GDPR-Compliant Design of a System for Digital Education Certificates," in Proc. IEEE International Conference on Cloud Computing Technology and Science Workshops (CloudCom Workshops), 2020, pp. 1–6. DOI: 10.48550/arXiv.2010.12980.

[2] M. Dattatreya Goud, "Network Intrusion Detection Using Supervised Machine Learning with Feature Selection," EAJSE, vol. 3, no. 3, 2025. https://doi.org/10.5281/zenodo.15862974

[3] A. Garba, Q. Hu, Z. Chen, and M. R. Asghar, "BB-PKI: Blockchain-Based Public Key Infrastructure Certificate Management," in Proc. IEEE HPCC/SmartCity/DSS, 2020, pp. 824–829. doi: 10.1109/HPCC-SmartCity-DSS50907.2020.00108.

[4] B. Awaji and E. Solaiman, "Design, Implementation and Evaluation of Blockchain-Based Trusted Achievement Record System for Higher Education," International Journal of Advanced Computer Science and Applications, vol. 13, no. 5, pp. 245–255, 2022.

[5] A. Rustemi, F. Dalipi, V. Atanasovski, and A. Risteski, "A Systematic Literature Review on Blockchain-Based Systems for Academic Certificate Verification," IEEE Access, vol. 11, pp. 64679–64696, 2023. doi: 10.1109/ACCESS.2023.3289598.

[6] A. Rustemi, F. Dalipi, V. Atanasovski, and A. Risteski, "DIAR: A Blockchain-Based System for Generation and Verification of Academic Diplomas," Discover Applied Sciences, vol. 6, Art. no. 297, 2024. doi: 10.1007/s42452-024-05984-1.

[7] M. A. Hemairy, M. Abu Talib, A. Khalil, A. Zulfiqar, and T. Mohamed, "Blockchain-Based Framework and Platform for Validation, Authentication and Equivalency of Academic Certification and Institution Accreditation: UAE Case Study and System Performance," Education and Information Technologies, vol. 29, pp. 18203–18232, 2024. doi: 10.1007/s10639-024-12493-6.

[8] M. M. Rahman, M. T. K. Tonmoy, S. R. Shihab, and R. Farhana, "Blockchain-Based Certificate Authentication System with Enabling Correction," Journal of Computer and Communications, vol. 11, no. 3, pp. 73–82, 2023.

[9] M. Dattatreya Goud, "A Student–Teacher Network Approach for Detecting and Defending Against

Adversarial Attacks," European Journal of Analytics and Artificial Intelligence (EJAAI), 2025.
[10] N. Vikhankar, A. Andhare, and I. Barne, "E-Certificate Verification Using Blockchain," International Journal of Engineering Research and Technology, vol. 13, no. 5, pp. 188–193, 2024.
[11] R. Priyadarshini, R. Pandey, A. K. C., D. Bhandari, B. Khadka, R. K. Barik, and M. J. Saikia, "A Faster, Integrated and Trusted Certificate Authentication and Issuer Validation System Based on Blockchain," IEEE Access, vol. 13, pp. 1–18, 2025.
[12] M. Fartitchou, I. Lamaakal, K. El Makkaoui, Z. El Allali, and Y. Maleh, "BlockMEDC: Blockchain Smart Contracts System for Securing Higher Education Digital Certificates," IEEE Access, vol. 13, pp. 39152–39175, 2025.
[13] A. S. Yadav, "ECertChain: A Blockchain-Based Educational Certificates and Degree Verification Management System," in Proc. IEEE ICCCA, 2025, pp. 1–6.
[14] 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, no. 1, Art. no. e70030, 2026. doi: 10.1049/blc2.70030.
[15] M. Dattatreya Goud, "A Student–Teacher Network Approach for Detecting and Defending Against Adversarial Attacks," EJAAI, vol. 3, no. 3, 2025. https://ejai.com/index.php/ejai/article/view/21
[16] S. K. Sharma, P. Verma, and R. Gupta, "Smart Certificate Validation and Fraud Detection Framework Using Blockchain and CNN-OCR," in Proc. 2026 International Conference on Visual Analytics and Data Visualization (ICVADV), 2026, pp. 1–6. doi: 10.1109/ICVADV67766.2026.11470562.
[17] A. De, G. Pal, A. Mukherjee, S. Das, and K. Roy, "Blockchain-Based Hybrid Academic Certificate Management System," in Proc. IEEE IATMSI, 2026. doi: 10.1109/IATMSI68868.2026.11465908.
[18] P. S. Gupta, M. A. Shabur, and P. Barua, "Blockchain-Enabled Academic Certificate Validation Using Hyperledger Fabric and IPFS," 2026. doi: 10.5281/zenodo.18254296.
[19] 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, no. 1, 2026.
[20] M. Dattatreya Goud, "URL-Based Phishing Detection Using Hybrid Machine Learning," AAJED, vol. 3, no. 3, 2025. https://aajed.com/index.php/aajed/article/view/21
[21] A. Kumar and S. Patel, "Blockchain-Enabled Educational Credential Verification Using Ethereum Smart Contracts," International Journal of Advanced Computer Science and Applications, vol. 11, no. 8, pp. 320–328, 2020.
[22] V. Sharma and P. Singh, "Secure Digital Certificate Verification Framework Based on Blockchain Technology," International Journal of Information Technology, vol. 13, no. 4, pp. 1547–1555, 2021.
[23] M. Alharbi, A. Alzahrani, and S. Alghamdi, "Blockchain-Based Educational Document Authentication System," Sensors, vol. 22, no. 17, pp. 1–20, 2022.
[24] Y. Zhang, H. Liu, and J. Wang, "Decentralized Academic Credential Management Using Blockchain and IPFS," Future Internet, vol. 15, no. 3, pp. 1–18, 2023.
[25] S. Ahmed and M. Khan, "Blockchain and Smart Contracts for Secure Academic Records Management," Journal of King Saud University–Computer and Information Sciences, vol. 36, no. 2, pp. 1–12, 2024.
[26] P. R. Nair, A. Joseph, and V. Thomas, "Secure Verification of Educational Credentials Through Decentralized Identity and Blockchain," IEEE Access, vol. 13, pp. 1–14, 2025.
[27] T. Nguyen and L. Tran, "Privacy-Preserving Academic Certificate Verification Using Blockchain and Zero-Knowledge Proofs," Computers & Security, vol. 141, Art. no. 103845, 2025.
[28] S. Verma, R. Kapoor, and N. Bansal, "Blockchain-Driven Digital Credential Ecosystem for Higher Education Institutions," International Journal of Information Management Data Insights, vol. 6, no. 1, Art. no. 100310, 2026.
[29] M. Dattatreya Goud, "Automated Fraud Detection in Banking Transactions Using AI Techniques," European Data Science Journal (EDSJ), vol. 3, no. 3, 2025. https://doi.org/10.5281/zenodo.15868373