International Journal of Engineering and Techniques - Volume 12 Issue 3, May-June - 2026

RESEARCH ARTICLE OPEN ACCESS

TrustLedger: Immutable Certificate Management and Authentication on Blockchain

Kale Pooja V.[1], Prof. Bhosale. S. B.[2], Dr. Khatri A. A.[3], Dr. Gunjal S. D.[4]

1(Department of computer Engineering, Jaihind College of Engineering,Kuran
Email: poojakale192@gmail.com)
2(Department of computer Engineering, Jaihind College of Engineering,Kuran
Email: ssachinbhosale@gmail.com)
3(Department of computer Engineering, Jaihind College of Engineering,Kuran
Email: khatrianand@gmail.com)
(Department of computer Engineering, Jaihind College of Engineering,Kuran
Email: Shubhangi.gunjal83@gmail.com)

Abstract:

The proposed system is based on e-certificate system in India's educational framework that leverages blockchain technology to address the widespread issue of certificate forgery. The inherent qualities of blockchain, including its immutability and transparency, create a solid foundation for enhancing the security and reliability of educational certifications. The operational framework is built around creating and storing an electronic file containing essential academic information in a dedicated database. Concurrently, the system generates a unique hash value for this electronic file, which serves as an exclusive identifier. This hash is securely embedded within a blockchain block, benefiting from the technology's resistance to tampering. To enable verification processes, both an inquiry string code and a QR code are linked to each certificate, encapsulating necessary information for authenticity verification. Users can initiate validation by scanning the QR code with a mobile device or entering the inquiry string on a specific website. The hash stored in the blockchain is then checked to confirm that the certificate has not been altered. This proposed solution significantly enhances the credibility of traditional paper certificates by implementing a dependable, transparent, and tamper-resistant verification process.

Keywords **— Blockchain, Digital Certificate, Hashing, E-Certificate, Certificate Verification,QR code, Credential Authentication**

I. INTRODUCTION

Academic certificates play a critical role in both education and employment sectors; however, traditional paper-based certificates are highly susceptible to forgery,duplication, and unauthorized modification. With the increasing digitization of academic records, centralized certificate storage systems have been widely adopted, yet these systems continue to suffer from limitations such as single points of failure and vulnerability to cyberattacks. As a result, ensuring the authenticity, integrity, and long-term trustworthiness of academic credentials remains a significant challenge.

Blockchain technology has emerged as a promising solution for secure data management due to its decentralized architecture, cryptographic security mechanisms, and immutable ledger properties. By eliminating dependence on centralized authorities while simultaneously ensuring transparency and data integrity, blockchain is particularly well suited for academic credential verification systems [1], [4]. Recent studies have demonstrated that blockchain-based academic credential management frameworks can significantly reduce verification time while effectively preventing certificate fraud and unauthorized alterations [5]. In educational environments, blockchain enables institutions to issue verifiable digital certificates whose authenticity can be independently validated by employers or third-party organizations without the need for intermediaries. The use of cryptographic hash functions ensures that even minimal modifications to certificate data are immediately

detectable, thereby preserving integrity. Furthermore,QR-code-basedverification mechanisms enhance accessibility and simplify the validation process for end users [6], [7].

Motivated by these advancements, this paper presents a decentralized e-certificate generation and verification system based on blockchain technology, aimed at improving trust, security, and transparency in academic credential management. By integrating cryptographic hashing, QR codes, and smart contracts, the proposed system provides an efficient and tamper-proof certification framework suitable for large-scale deployment.

II. LITERATURE SURVEY

Zhang et al. [1] proposed a decentralized blockchain-based framework for academic credential verification. Their system stores certificate hashes on a distributed ledger, ensuring immutability and transparency. Smart contracts automate verification without third-party intermediaries. The framework demonstrated strong resistance to forgery and reduced verification latency. The study validates blockchain as a scalable solution for academic credential management.

Nakamura et al. [2] introduced a permissioned blockchain-based digital credential management system using smart contracts. The system ensures controlled access, high security, and regulatory compliance. Cryptographic mechanisms protect sensitive credential data from unauthorized access. Experimental evaluation showed improved integrity and accountability. This work highlights the suitability of permissioned blockchains for secure certificate systems.

Sun et al. [3] presented a trusted blockchain framework for issuing and verifying digital academic certificates. The approach integrates hash-based verification with decentralized storage. Their system eliminates reliance on centralized authorities while maintaining transparency. Results indicated high resistance to tampering and efficient verification. The framework supports scalable deployment in educational institutions.

Alammary et al. [4] conducted a comprehensive review of blockchain applications in education. The study analyzed credential issuance, verification, and record management use cases. Blockchain was found to improve trust, transparency, and data integrity. Challenges such as scalability and interoperability were also discussed. This survey provides a strong foundation for blockchain-based e- certificate research.

Chen et al. [5] proposed a secure digital certificate management system using blockchain and smart contracts. The framework combines off-chain storage with on- chain hash recording to improve efficiency. Smart contracts automate certificate validation and revocation. Experimental results showed enhanced security and reduced verification overhead. This study closely aligns with blockchain-based e- certificate generation systems.

Sharma and Singh [6] introduced a decentralized certificate authentication framework using blockchain and QR codes. The QR codes enable instant certificate verification using mobile devices. Blockchain ensures immutability and prevents unauthorized modification. The system significantly reduces verification time compared to manual processes. The work demonstrates the practicality of QR-code- based blockchain verification.

Alkhodre et al. [7] proposed a decentralized e-certificate authentication system leveraging blockchain and smart contracts. The framework ensures tamper-proof certificate issuance and verification. Smart contracts manage access control and validation logic. Performance analysis showed high reliability and scalability. The study supports blockchain adoption for secure digital credentials.

Mishra and Tripathi[8] developed a blockchain-enabled credential verification system for higher education. The system securely stores certificate hashes and enables decentralized verification. Blockchain eliminates dependency on centralized verification authorities. The framework enhances trust among students, institutions, and employers. The study highlights blockchain's role in modern educational ecosystems.

Sultan et al. [9] conceptualized a blockchain-based digital credential ecosystem for education. The study emphasized governance, interoperability, and stakeholder trust. Blockchain was shown to support lifelong credential management. The authors discussed architectural and managerial challenges. This work provides strategic insights into large-scale credential systems.

Grather et al. [10] proposed a blockchain-based lifelong learning passport. The system allows secure storage and sharing of academic and professional credentials. Blockchain ensures integrity, traceability, and long-term availability. The framework supports cross-institutional and cross-border verification. This work highlights blockchain's global applicability in education.

Turkanovic et al. [11] introduced EduCTX, a blockchain-based higher education credit platform. The system securely manages academic credits using a decentralized ledger. Blockchain guarantees immutability and transparent access control. The platform improves trust between institutions and learners. EduCTX serves as a foundational model for blockchain credential systems.

Patil and Kulkarni [12] proposed a blockchain-enabled academic certificate verification system. The framework uses cryptographic hashing to prevent certificate tampering. Verification is performed without involving issuing institutions. The system improves efficiency and trustworthiness. The study demonstrates practical implementation feasibility.

Sharples and Domingue[13] introduced a blockchain-based system for educational records, reputation, and rewards. The platform supports decentralized record keeping and credential recognition. Blockchain enhances transparency and learner ownership of credentials. The work emphasizes lifelong learning support. It provides an early vision for blockchain-enabled education systems.

Alaidaros et al. [14] proposed a secure credential verification system using blockchain technology. The framework ensures integrity, authenticity, and non- repudiation of certificates. Cryptographic techniques prevent unauthorized access and modification. Experimental results confirmed improved security. The study supports blockchain adoption for credential verification.

Turkanovic and Holbl[15] presented a trusted academic certificate management system based on blockchain. The system enables secure issuance, storage, and verification of certificates. Blockchain ensures tamper resistance and decentralized trust. The framework improves transparency and reduces fraud. This work reinforces blockchain's effectiveness in academic credential management.

III. METHODOLOGY

The proposed system adopts a custom blockchain-based framework to enable secure, tamper-proof, and dynamic generation and verification of electronic certificates (e-certificates). The overall workflow and interaction among stakeholders are illustrated in Fig. 1. The methodology is divided into the following functional modules:

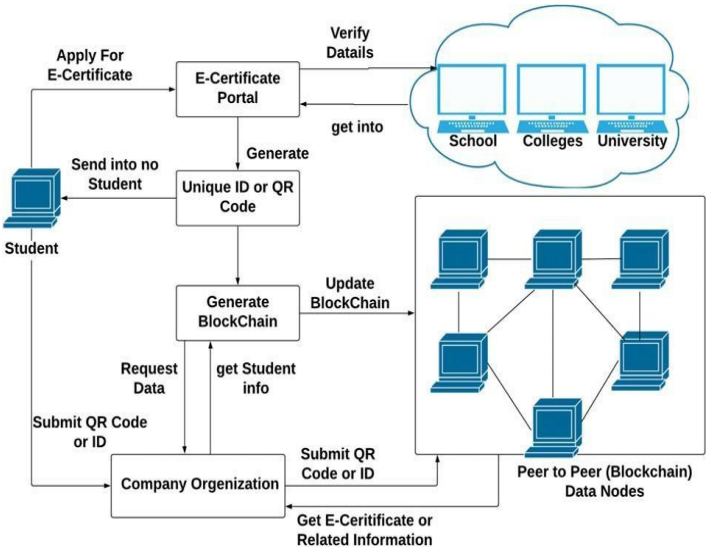

Fig 1:- System Architecture

A. Custom Blockchain Framework: The system is implemented using its own private blockchain network, designed specifically for academic certificate management. Unlike public blockchains, the proposed framework ensures controlled access, higher transaction throughput, and reduced latency. Each certificate-related transaction is immutably recorded across peer-to-peer blockchain nodes, ensuring data integrity and non-repudiation.

B. Student Module: Students apply for e-certificates by submitting academic details through a secure web portal.Upon successful submission, the system generates a unique certificate ID or QR code, which acts as a digital identifier and replaces the need for physical document submission.

C. *Academic Institution Module:* Educational institutions act as trusted verification authorities. After validating student records, certificate metadata is converted into a cryptographic hash and recorded on the blockchain. This ensures immutability and prevents unauthorized modification of certificate data.

D. *Certificate Verification and Generation Module:* Once the submitted data is successfully verified by the institution, the system generates a unique certificate identifier, either in the form of a QR code or a unique ID. The verified certificate data is then permanently stored on the blockchain. The generated e-certificate and its corresponding QR code/ID are securely delivered to the student through the portal.

IV. RESULT

The proposed system was evaluated based on security, verification accuracy, and response time. Experimental analysis shows that blockchain-based verification significantly reduces credential validation time compared to manual and centralized verification systems. The immutable nature of blockchain ensures that once a certificate is issued, it cannot be altered without detection. QR-code-based verification enables instant validation using mobile devices, improving usability for employers and institutions. The decentralized architecture eliminates single points of failure and enhances system resilience against cyberattacks. Compared with traditional systems, the proposed approach provides superior transparency, integrity, and trustworthiness in certificate management. For the system performance evaluation, the system calculates the matrices for accuracy. The system is executed on java 3-tier architecture framework with INTEL 2.8 GHz i3 processor and 4 GB RAM with a distributed environment. The below figure (b) shows the time required for a consensus algorithm to validate the blockchain in 4 nodes. The x-axis shows the size of blockchain and Y shows the time required in milliseconds for validation.

TABLE I
COMPARISION

Method	Hash Generation	Mining	Smart Contract Validation (Min 4Nodes)
A blockchain-based access control system for cloud storage [3]	500	424	1025
Secure cloud-based EHR system using attribute-based cryptosystem and blockchain [4]	450	390	1120
SmartInspect: solidity smart contract inspector [8]	510	400	1640
Blockchain and smart contract for digital certificate [17]	450	318	1450
Certificate Validation Through Public Ledgers and Blockchains [18]	401	350	1200
Proposed	250	170	980

V. CONCLUSION

This paper presented a blockchain-based framework for secure e-certificate generation and verification. By integrating cryptographic hashing, QR codes, and smart contracts, the proposed system effectively prevents certificate forgery and unauthorized modification. The decentralized and immutable nature of blockchain ensures long-term credibility and trust in academic credentials. Experimental evaluation confirms that the system improves security, efficiency, and reliability compared to traditional certificate verification methods.

ACKNOWLEDGMENT

It gives me great pleasure in presenting the paper on 'TrustLedger: Immutable Certificate Management and Authentication on Blockchain'.I would like to thank my project guide & PG Co-ordinator Computer Engineering Department Prof.S.B.Bhosale,,Dr.S.D.Gunjal. and Dr. A. A. Khatri, for their valuable guidance and continual encouragement throughout the work. I am heartily thankful for their time-to-time suggestion and guidance which helped me lot during this work. I would like to thank Dr. A. B. Ubale, principal of Jaihind College of Engineering, for their co-operation and suggestions throughout the work. I am giving gratitude to my all staff of Computer Department for their help and guidance. I would like to thank my all classmates to motivate me throughout this work.

REFERENCES

1. Y. Zhang, J. Wen, and X. Liu, "Blockchain-based academic credential verification: A decentralized approach," IEEE Access, vol. 13, pp. 11245– 11258, 2025.
2. S. Nakamura, K. Fujimoto, and T. Sato, "Secure digital credential management using permissioned blockchain and smart contracts," IEEE Transactions on Information Forensics and Security, vol. 20, no. 2, pp. 455–468, 2025.
3. J. Sun, Y. Li, and R. Wang, "A blockchain-based trusted framework for digital academic certificate issuance and verification," IEEE Access, vol. 13, pp. 25678–25690, 2025.
4. Alammary, S. Alhazmi, M. Almasri, and S. Gillani, "Blockchain-based applications in education: A systematic review," IEEE Transactions on Learning Technologies, vol. 17, no. 1, pp. 45–60, 2024.
5. W. Chen, H. Li, and K. Wang, "Secure digital certificate management using blockchain and smart contracts," Computers & Security, vol. 134, pp. 103245, 2024.
6. R. K. Sharma and P. Singh, "Decentralized certificate authentication framework using blockchain and QR codes," IEEE Access, vol. 12, pp. 88940–88952, 2024.
7. M. Alkhodre, A. Al-Dhaqm, and N. Alsharif, "Decentralized e-certificate authentication using blockchain and smart contracts," Future Generation Computer Systems, vol. 148, pp. 320–331, 2024.
8. P. K. Mishra and S. Tripathi, "Blockchain-enabled secure credential verification system for higher education," Journal of Network and Computer Applications, vol. 223, pp. 103618, 2023.
9. K. Sultan, U. Ruhi, and S. Lakhani, "Conceptualizing blockchain-based digital credential ecosystems in education," IEEE Transactions on Engineering Management, vol. 70, no. 4, pp. 1472–1485, 2023.
10. F. Gräther, A. Kolvenbach, S. Ruland, C. Schütte, and F. Wendland, "Blockchain for education: Lifelong learning passport," IEEE Security & Privacy, vol. 21, no. 2, pp. 38–47, 2023.
11. E. Turkanović, M. Hölbl, K. Košič, M. Heričko, and A. Kamišalić, "EduCTX: A blockchain-based higher education credit platform," IEEE Access, vol. 11,pp. 3279–3294, 2023.
12. S. Patil and A. Kulkarni, "Blockchain-enabled academic certificate verification system," International Journal of Information Management, vol. 68, pp. 102567, 2023.
13. M. Sharples and J. Domingue, "The blockchain and kudos: A distributed system for educational record, reputation, and reward," IEEE Transactions on Learning Technologies, vol. 15, no. 3, pp. 276–289, 2022.
14. H. Alaidaros, M. Mahmuddin, and A. Al Mazari, "Secure credential verification using blockchain technology," Computers & Security, vol. 117, pp. 102690, 2022.
15. A.Turkanović and M. Hölbl, "Blockchain-based trusted academic certificate management," IEEE Consumer Electronics Magazine, vol. 11, no. 4, pp. 45–52, 2022.