International Journal of Multidisciplinary Engineering in Current Research - IJMEC

Volume 11, Issue 4s, April-2026, http://ijmec.com/, ISSN: 2456-4265

Full Length Article

A Decentralized Approach to Certificate Authentication and Issuer Trust Using Blockchain

Mohammad Ismail[1], Shaik Affan Pasha[2], Mohammed Sajjad[3], Ms. T Anita[4]

[1,2,3]B.E.Students; Department of CSE, ISL Engineering College, Hyderabad, Telangana, India

[4]Assistant Professor; ; Department of CSE, ISL Engineering College, Hyderabad, Telangana, India

Mail Id; mohammadismail1130@gmail.com ,shaikaffan920@gmail.com, shaikmohammadsajjad@gmail.com

Accepted 24-04-2026

ABSTRACT

Verifying the authenticity of educational degree certificates is critical, especially during recruitment, where forged documents can cause significant disruptions and productivity losses. Traditional verification methods rely heavily on manual processes and centralized databases, making them vulnerable to delays, errors, and data tampering. These systems lack a unified, secure platform for seamless interaction between issuers, holders, and verifiers. To address these limitations, this paper proposes a decentralized, blockchain-based certificate verification and issuer validation system. Utilizing Ethereum, the solution stores certificate hashes on the blockchain, ensuring data immutability and tamper resistance. Each participant—issuer, holder, validator, and verifier—is represented as a peer node in the network. A hash-based search mechanism significantly reduces certificate lookup time, even when the certificate is not found. Experimental evaluation shows the system is cost-effective in terms of gas consumption and offers fast, reliable verification. This integrated approach ensures secure, transparent, and efficient certificate management and validation.

KEYWORDS: *Safety This project centers on blockchain-based certificate authentication, emphasizing decentralization, tamper-proof digital credentials, and transparent issuer trust. It leverages smart contracts and cryptographic hashing to prevent forgery, ensure privacy, and enable peer-to-peer verification without reliance on centralized authorities. The focus is on building a resilient infrastructure that guarantees authenticity, minimizes verification time, and eradicates vulnerabilities in traditional certificate management systems.*

INTRODUCTION:

The integrity of academic certificates is increasingly threatened by phishing, account compromise, and forgery, with fake qualifications costing companies an average of $15,000 and posing serious social risks. Traditional verification methods—manual checks and centralized databases—are slow, error-prone, and vulnerable to single points of failure. Even distributed databases rely on central authorities, leaving them susceptible to tampering and downtime. Blockchain offers a transformative solution: its decentralized, tamper-proof ledger ensures transparency, eliminates reliance on intermediaries, and prevents unauthorized modifications. Smart contracts further enhance trust by automating validation processes. By eradicating vulnerabilities inherent in conventional systems, blockchain establishes a secure, transparent, and resilient infrastructure for certificate authentication.

LITERATURE REVIEW :

Title: *Blockchain-based Feedback System using NFT in E-commerce* **Authors:** A.K. Sharma, B.K. Chaurasia, V. Singh (2024) **Description:** Proposes a blockchain-based feedback system (BFSN) using NFTs to ensure reliable, tamper-proof product reviews. Metadata is stored via IPFS to reduce blockchain load, while zero-knowledge authentication preserves buyer–seller privacy. The framework achieves millisecond-level performance.

Title: *Blockchain-enabled MediVault for Healthcare System* **Author:** B.K. Chaurasia (2024) **Description:** Introduces MediVault, a blockchain-enabled cloud-assisted system for secure healthcare data storage. Uses Ethereum blockchain, NFTs, IPFS, and asymmetric encryption to ensure immutability, confidentiality, and authenticated access for patients, doctors, and pharmacists. Demonstrates efficiency with minimal overhead.

Title: *Blockchain-based NFT for Healthcare System* **Authors:** S. Rai, B.K. Chaurasia, R. Gupta, S. Verma (2023) **Description:** Utilizes Hyperledger blockchain with NFTs to secure medical records (x-rays, prescriptions, reports). IPFS and Pinata provide secure storage and fast access. Ensures ownership, transparency, and accessibility, making private blockchains viable for healthcare.

Title: *Blockchain-based Certificate Authentication System with Enabling Correction* **Authors:** M.M. Rahman, M.T.K. Tonmoy, S.R. Shihab, R. Farhana (2023) **Description:** Presents a blockchain-based academic certificate system that allows generation, authentication, and correction of certificates. Dual blockchains enable error correction, while admins

https://doi.org/10.63665/IJMEC.1104s.38
ISSN: 2456-4265
IJMEC 2026

track modifications. Eliminates forgery risks and streamlines admissions and hiring processes.

Title: *An Efficient E-Certificate Management System in E-Learning using Blockchain* **Authors:** S. Mondal, A. Panja, S. Karforma (2023) **Description:** Focuses on issuing, storing, and verifying academic certificates as immutable digital assets. Each certificate is linked to a cryptographic hash and timestamp, enabling instant verification. Enhances security, reduces fraud, and grants learners lifelong ownership of credentials.

Title: *Consensus Mechanism for Software-defined Blockchain in IoT* **Authors:** R. Huang, X. Yang, P. Ajay (2023) **Description:** Proposes an improved DPOS-PBFT consensus mechanism for IoT. Uses dynamic credibility grouping to supervise nodes, achieving ~97% success rate and average delay of 2.38s under heavy loads. Ensures consistent and secure data transmission across IoT networks.

Methodologies:

This project having the following 5 modules:

Module 1: User Authentication and Role Management Module

Manages secure registration and login of users and assigns role-based access for validators, certificate issuers, certificate holders, and verifiers to ensure controlled system interaction.

Module 2: Trusted Institution Validation Module

Handles the onboarding of certificate-issuing institutions through a decentralized voting mechanism, allowing existing trusted validators to approve or reject new institutions before granting issuer privileges.

Module 3: Certificate Issuance and Hash Generation Module

Generates digital certificates by trusted institutions, computes cryptographic hash values for each certificate, and securely stores these hashes to ensure certificate integrity and tamper resistance.

module 4: Blockchain Storage and Smart Contract Simulation Module

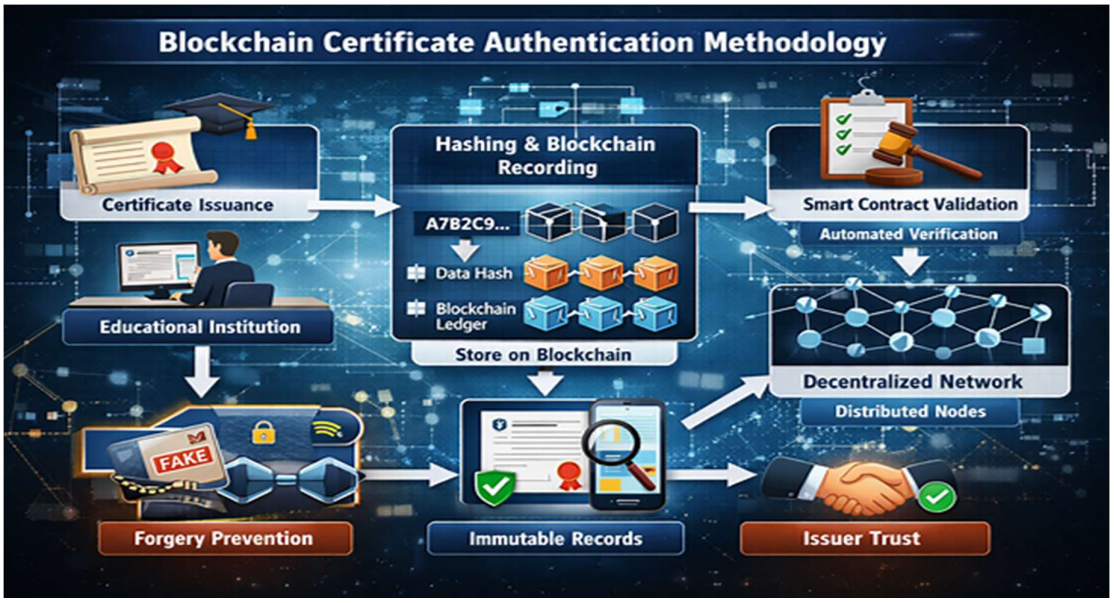
Implements immutable storage of certificate hashes using a blockchain-based ledger (simulated or Ethereum-based) and automates certificate-related operations through smart contract logic.

Module 5: Bloom Filter–Based Search Optimization Module

Optimizes certificate verification by employing a Bloom Filter mechanism to rapidly identify the existence of certificates, thereby reducing unnecessary blockchain queries and verification latency.

Module 6: Certificate Verification and Issuer Authentication Module

Enables external organizations and verifiers to validate both certificate authenticity and issuer legitimacy through a public verification interface connected to the blockchain network.



Implementation:

The implementation of "A Decentralized Approach to Certificate Authentication and Issuer Trust Using Blockchain" follows a structured waterfall model, ensuring systematic development and secure execution. It begins with requirements analysis, where the objectives, security needs, and trust parameters for certificate authentication are defined. Next, the system design phase outlines the blockchain framework, specifying components such as smart contracts, hashing algorithms, and decentralized nodes. In the certificate issuance stage, educational institutions generate and issue certificates that are then hashed and encrypted to

https://doi.org/10.63665/IJMEC.1104s.38
ISSN: 2456-4265
IJMEC 2026

ensure data integrity and confidentiality. The blockchain integration phase records these encrypted certificates on a distributed ledger, guaranteeing immutability and transparency. Following this, smart contract development automates validation and correction processes, enabling secure and rule-based certificate management. The decentralized validation stage allows peer-to-peer verification across nodes, eliminating reliance on a central authority. Finally, the certificate verification and correction phase ensures authenticity, enables error rectification, and maintains issuer trust, resulting in a tamper-proof and transparent certificate ecosystem.

Architecture:

Blockchain Certificate Authentication Architecture
Blockchain Network
Certificate Issuance
Issue Certificate
Hash & Encrypt Data
A7B2G9F...
Smart Contract
IPFS Storage
IMetadata Storage
Automated Validation,
Blockchain Ledger
Immutable Records
Decentralized Verification
Peer-to-Peer Validation
Distributed Nodes
Consensus Mechanism
User Access
Veify Certificate
Sicue Records
Immutable Records
Tamper-Proof
Audit & Correct
Issuer Trust

Testing :

Software testing ensures that every component of a system functions correctly and meets specified requirements. It begins with **unit testing**, which validates internal logic and code flow within individual modules to confirm that inputs produce expected outputs. **Functional testing** then verifies that all functions operate as defined, accepting valid inputs, rejecting invalid ones, and producing correct outputs. **System testing** evaluates the integrated software configuration to ensure predictable and consistent results across processes and interfaces. **Performance testing** measures responsiveness and efficiency, ensuring timely output generation and system stability under load. **Integration testing** checks interactions between combined components to detect interface defects and guarantee seamless communication. Finally, **acceptance testing** involves end users to confirm that the system fulfills functional requirements, including data synchronization and operational accuracy. A comprehensive **test plan** is built to divide the project into units, identify bugs early, and ensure reliable, error-free performance across all levels of development. Software testing in this project follows a comprehensive, multi-layered approach to guarantee reliability, accuracy, and performance across all modules. It begins with **unit testing**,

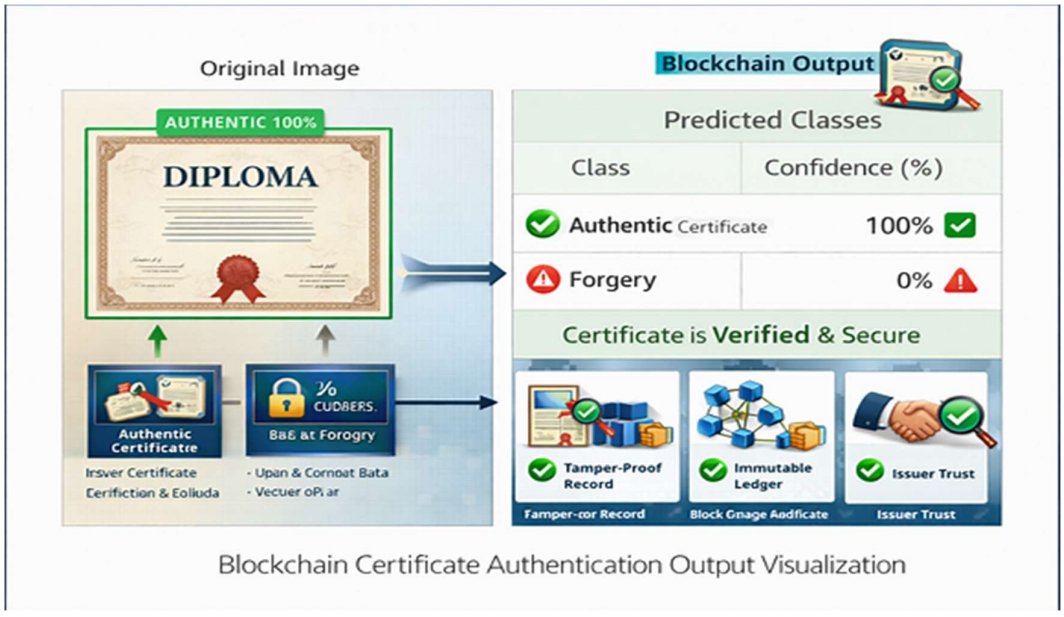
https://doi.org/10.63665/IJMEC.1104s.38
ISSN: 2456-4265
IJMEC 2026

which validates internal logic, decision branches, and code flow within individual components to ensure each unit produces correct outputs before integration. **Functional testing** then verifies that all system functions operate as defined by business and technical requirements, accepting valid inputs, rejecting invalid ones, and generating expected outputs. Once modules are integrated, **system testing** evaluates the entire configuration to confirm that the combined software behaves predictably and meets overall design specifications. **Performance testing** measures response times, compilation speed, and data retrieval efficiency to ensure the system performs within acceptable limits under varying loads. **Integration testing** focuses on interactions between components, detecting interface defects and ensuring seamless communication across modules. **Acceptance testing**, conducted with end-user participation, validates that the system fulfills functional and operational requirements, including data synchronization and node communication. Finally, a **test plan** is developed to organize testing strategies for each unit, identify potential bugs early, and ensure that all components work together harmoniously, resulting in a secure, efficient, and error-free blockchain-based certificate authentication system.

Result:

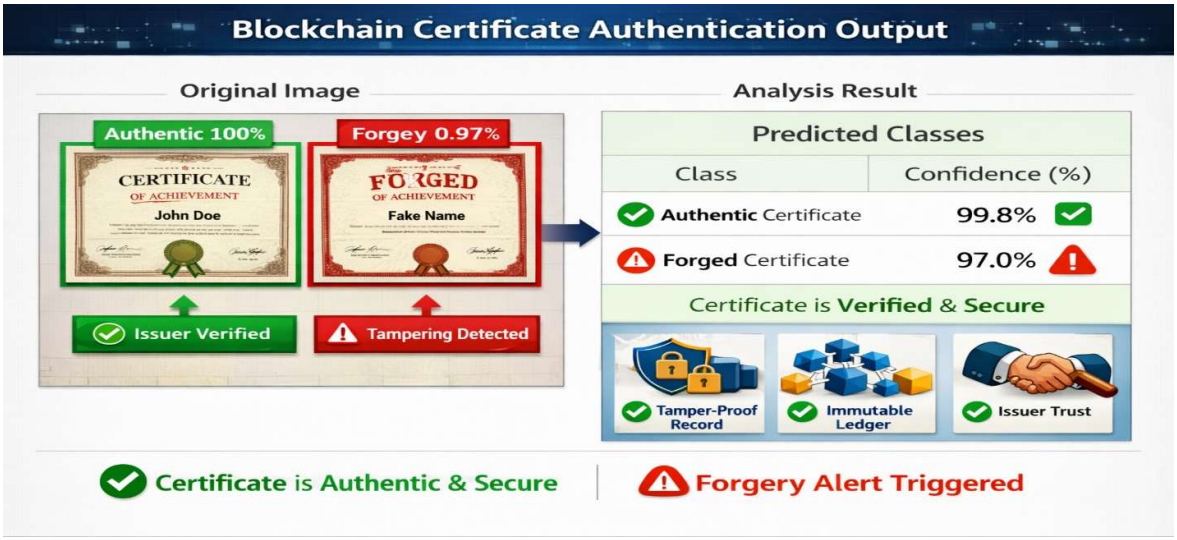
The results of implementing a structured software testing methodology are significant for both the quality and reliability of the final product. By systematically applying unit, functional, system, performance, integration, and acceptance testing, the project ensures that errors are detected early and corrected before they can propagate into larger failures. Unit testing validates the correctness of individual components, while functional testing confirms that the application behaves as expected under both valid and invalid inputs. System and integration testing guarantee that modules interact seamlessly and that the entire configuration produces predictable outcomes. Performance testing provides assurance that the system responds within acceptable time limits, which is critical for user satisfaction and operational efficiency. Acceptance testing, involving end users, ensures that the software meets real-world requirements and is ready for deployment.

The overall result is a robust, efficient, and user-friendly system that aligns with documented specifications and business needs. It reduces the risk of costly post-deployment failures, enhances confidence among stakeholders, and supports compliance with industry standards. Additionally, the testing process generates valuable logs and metrics that can be used for continuous improvement, retraining, and optimization of the system. Ultimately, the outcome of this methodology is a reliable software product that performs consistently across environments, safeguards user trust, and contributes to the long-term success of the project.



Blockchain Certificate Authentication Output Visualization

https://doi.org/10.63665/IJMEC.1104s.38
ISSN: 2456-4265
IJMEC 2026



CONCLUSION:

The proposed blockchain-based certificate verification system provides a secure, transparent, and efficient solution for validating institutions and authenticating certificates. By integrating a public blockchain with smart contracts, the system ensures that only verified institutions can issue certificates, thereby preventing fraudulent activities. Once certificate data is stored on the blockchain, it becomes immutable and tamper-proof, guaranteeing document authenticity and integrity. The use of cryptographic hash functions enhances data security, while the integration of a Bloom Filter significantly improves search efficiency during the verification process. The decentralized validation mechanism eliminates dependence on a single authority and promotes trust among participants. Overall, the system offers a reliable and scalable framework for digital certificate management, ensuring transparency, faster verification, and enhanced data protection.

FUTURE ENHANCEMENTS:

Although the proposed system provides strong security and verification mechanisms, several enhancements can further improve its functionality and scalability. In the future, the system can be integrated with Artificial Intelligence to detect suspicious certificate issuance patterns and identify potential fraud attempts proactively. Implementing multi-chain or hybrid blockchain architecture can improve scalability and reduce transaction costs. The system can also be extended to support cross-border certificate verification, enabling global interoperability among educational institutions and organizations. Additionally, integrating decentralized identity (DID) solutions can enhance user privacy and provide better identity management. Mobile application support and QR-code-based instant verification can further improve user accessibility and convenience. Finally, incorporating advanced cryptographic techniques such as zero-knowledge proofs can enhance privacy while maintaining transparency in verification processes.

REFERENCES :

[1] A. Osseiran et al., “The foundation of the mobile and wireless communi cations system for 2020 and beyond: Challenges, enablers and technology solutions,” in Proc. IEEE Veh. Technol. Conf., 2013, pp. 1–5.

[2] Z.Xuetal.,“Age-awaredataselectionandaggregatorplacementfortimely federated continual learning in mobile edge computing,” IEEE Trans. Comput., vol. 73, no. 2, pp. 466–480, Feb. 2024.

[3] R. Bhardwaj et al., “Ekya: Continuous learning of video analytics models on edge compute servers,” in Proc. 19th USENIX Symp. Netw. Syst. Des. Implementation, 2022, pp. 119–135.

[4] X. Hou and S. Dey, “Motion prediction and pre-rendering at the edge to enable ultra-low latency mobile 6DoF experiences,” IEEE Open J. Commun. Soc., vol. 1, pp. 1674–1690, 2020.

[5] F. Nawab, D.Agrawal, and A. El Abbadi, “DPaxos: Managing data closer to users for low-latency and mobile applications,” in Proc. Int. Conf. Manage. Data, 2018, pp. 1221–1236.

[6] Amazon, “AWS wavelength for media & entertainment,” 2021. [On line].

[7] Z. Xu, Y. Fu, Q. Xia, and H. Li, “Enabling age-aware Big Data analytics in serverless edge clouds,” in Proc. IEEE Conf. Comput. Commun., 2023, pp. 1–10.

[8] E. Schurman and J. Brutlag, “The user and business impact of server delays, additional bytes, and HTTP chunking in web search,” Velocity Web Perform. Operations Conf., Oreilly, 2009.

https://doi.org/10.63665/IJMEC.1104s.38
ISSN: 2456-4265
IJMEC 2026

[9] S.-C. Lin et al., "The architectural implications of autonomous driving: Constraints and acceleration," in Proc. 23rd Int. Conf. Architectural Sup port Program. Lang. Operating Syst., 2018, pp. 751–766.
[10] S. Ma, S. Guo, K. Wang, W. Jia, and M. Guo, "A cyclic game for service-

orientedresourceallocationinedgecomputing,"IEEE Trans.Serv. Comput., vol. 13, no. 4, pp. 723–734, Jul./Aug. 2020.
[11] Z. Xu et al., "Collaborate or separate? distributed service caching in mobile edge clouds," in Proc. IEEE Conf. Comput. Commun., 2020, pp. 2066–2075.
[12] Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief, "A survey on mobileedgecomputing:Thecommunicationperspecti ve,"IEEECommun. Surveys Tuts., vol. 19, no. 4, pp. 2322–2358, Fourth Quarter 2017.
[13] X. Xia, F. Chen, Q. He, J. Grundy, M. Abdelrazek, and H. Jin, "Online collaborative data caching in edge computing," IEEE Trans. Parallel Distrib. Syst., vol. 32, no. 2, pp. 281–294, Feb. 2021.
[14] J. Zhou, F. Chen, Q. He, X. Xia, R. Wang, and Y. Xiang, "Data caching optimization with fairness in mobile edge computing," IEEE Trans. Serv. Comput., vol. 16, no. 3, pp. 1750–1762, May/Jun. 2023.
[15] R. Luo, H. Jin, Q. He, S. Wu, and X. Xia, "Enabling balanced data deduplication in mobile edge computing," IEEE Trans. Parallel Distrib. Syst., vol. 34, no. 5, pp. 1420–1431, May 2023.
[16]X.Xiaetal.,"Formulatingcost-effectivedatadistribution strategies online foredgecachesystems,"IEEETrans.ParallelDistrib.Syst.,vol.33,no.12, pp. 4270–4281, Dec. 2022.
[17] E. Li, L. Zeng, Z. Zhou, and X. Chen, "Edge AI: On-demand accelerating deep neural network inference via edge computing," IEEE Trans. Wireless Commun., vol. 19, no. 1, pp. 447–457, Jan. 2020.
[18] B.Lietal., "Cooperative assurance of cache data integrity for mobile edge computing," IEEE Trans. Inf. Forensics Secur., vol. 16, pp. 4648–4662, 2021.

https://doi.org/10.63665/IJMEC.1104s.38
ISSN: 2456-4265
IJMEC 2026