IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 10, April 2026
Impact Factor: 8.2

Digital Certificate Fraud Detection Using Blockchain Technology

Mr. Venkatesh B, Oviya S, Suweatha E
Department of Information Technology
Anjalai Ammal Mahalingam Engineering College, Kovilvenni, Thiruvarur, Tamil Nadu, India
venkateshaamec@gmail.com, oviya322005@gmail.com, suweatha29@gmail.com

Abstract: *Digital certificate fraud has become a critical issue in academic, professional, and recruitment domains, where forged or altered certificates are used to gain unauthorized advantages. Traditional verification systems rely on manual processes and centralized databases, making them inefficient, time- consuming, and vulnerable to manipulation. This paper presents a Digital Certificate Fraud Detection System using Blockchain Technology, designed to provide a secure, decentralized, and tamper-proof platform for certificate issuance and verification. The proposed system utilizes SHA-256 cryptographic hashing to generate unique digital fingerprints for certificates, which are stored on the blockchain to ensure immutability. Smart contracts are employed to automate certificate validation processes, eliminating the need for manual verification. Additionally, QR code integration enables quick access to certificate details, improving usability without compromising security. The system supports multiple user roles, including administrators, students, and verifiers, ensuring a structured and secure workflow. Experimental evaluation demonstrates improved fraud detection accuracy, faster verification time, and enhanced data integrity compared to traditional systems. The proposed approach offers a scalable and reliable solution for preventing certificate fraud in modern digital ecosystems..*

Keywords: blockchain, certificate verification, fraud detection, SHA-256, smart contracts, QR code

I. INTRODUCTION

Academic and professional credentials occupy a pivotal status as indicators of human capital, expertise, and institutional trust. These credentials serve as the foundation for recruitment, professional licensing, and admission into postgraduate studies. However, the paradigm shift from physical to digital document storage hasn't been without its vulnerabilities. While digitization offers efficiency and accessibility, it has simultaneously democratized the tools for forgery. The proliferation of sophisticated editing software allows high-fidelity manipulations of digital certificates, creating a significant crisis of confidence in the integrity of academic records worldwide.

Traditional verification methodologies are fundamentally flawed. Many institutions still rely on manual verification requests, which can take weeks to process, or centralized databases that represent single points of failure. These centralized repositories are vulnerable to sophisticated cyberattacks and internal database manipulation. If a central authority's database is compromised, the ledger of every student's qualifications can be modified or erased, leading to irreversible damage to institutional reputation and the careers of legitimate certificate holders. The absence of a decentralized, immutable source of truth is the core problem currently facing credential management.

Blockchain technology offers a robust solution to these challenges through its inherent properties of decentralization, transparency, and immutability. Unlike a centralized database, a blockchain ledger is distributed across a network, ensuring that no single entity can modify historical records without the consensus of the entire network. Any attempt to alter data results in a hash mismatch, which the system can immediately detect. By associating each digital certificate with a unique cryptographic fingerprint (SHA-256 hash) and storing that fingerprint on a blockchain, we can ensure that the authenticity of a document can be verified instantly and globally with absolute certainty.

DOI: 10.48175/IJARSCT-33406

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 10, April 2026
Impact Factor: 8.2

This paper presents a Digital Certificate Fraud Detection System that leverages blockchain and smart contracts to automate and secure the verification process. The system replaces trust in individual administrators with trust in mathematical algorithms. The integration of QR code technology bridges the gap between digital security and ease of use, allowing verifiers to authenticate certificates with a single scan. The multifaceted system ensures that every stage of the certificate's lifecycle—from issuance by an administrator to viewing by a student and verification by an employer—is logged and secured.

Our proposed approach focuses on the "Zero- Trust" principle, where every claim of qualification must be independently verifiable against a tamper-proof ledger. We also address the economic feasibility of such systems by storing only the metadata hashes on-chain, thereby drastically reducing storage costs while maintaining the highest security protocols. This research aims to provide a scalable and institutionally viable framework for the global eradication of certificate-based fraud.

II. LITERATURE REVIEW

The academic community has increasingly looked toward blockchain to mitigate document forgery. Initial research into decentralized ledgers focused primarily on financial transactions, but the potential for non-financial record-keeping was soon realized. Arenas et al. [4] introduced the concept of permissioned blockchains for academic credentials, highlighting that institutional trust can be mathematically codified. Their work laid the foundation for "CredenceLedger," which demonstrated that an immutable record of academic history is not only possible but necessary in an era where paper-based systems are failing to keep pace with the digitalization of the workforce.

Further research highlighted the specific vulnerabilities of existing digital repositories. San et al. [10] emphasized that centralized repositories create a "dependency bottleneck." When numerous institutions rely on a single verification portal, any downtime or data breach effectively paralyzes the verification capability of the entire network. This realization shifted the focus toward Distributed Ledger Technology (DLT). Marco et al. [8] provided a comprehensive security analysis of blockchain-based certification protocols, identifying that the combination of cryptographic signatures and timestamps provides a defense-in- depth architecture that is virtually impossible to compromise via traditional hacking vectors.

The role of smart contracts in this domain represents a significant leap forward in automation. Szalachowski [12] redesigned digital certificates using smart contracts to include logic for revocation and expiration. This is crucial for professional licenses that require periodic renewal or for degrees that might be rescinded due to academic malpractice. Without smart contracts, such updates require complex manual database overrides that are prone to human error. Automation ensures that the status of a certificate is always current and verifiable in real-time, reducing administrative friction.

Integration with decentralized storage protocols like the InterPlanetary File System (IPFS) has also been a major topic in recent years. Rahman et al. [9] and Jaafar et al. [7] examined how IPFS can store heavy files while the blockchain stores their content-addressed hashes. This hybrid approach ensures that the certificate files themselves are decentralized and permanent, preventing "link rot" or the loss of files due to local server failures. Additionally, the use of QR codes as an entry point for verification has been validated by Ahmed et al. [1], who demonstrated that user adoption increases significantly when the underlying technical complexity is hidden behind a familiar interface.

Recent studies in 2024 and beyond have focused on the concept of "NFT-based certifications" [13], where each degree is treated as a unique non-fungible token. While NFTs provide high uniqueness, our system focuses on the more efficient strategy of hash-based verification, which Shukla et al. [11] noted is more scalable for large universities handle hundreds of thousands of graduates annually. By synthesizing these diverse strands of research—cryptography, DLT, smart contracts, and mobile accessibility— our work proposes a unified and technically robust solution to certificate fraud.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 10, April 2026
Impact Factor: 8.2

Cryptography Tier, and the Blockchain Ledger Tier. The system maintains strict role-based access control to ensure that only authorized personnel can initiate certificate issuance. The methodology prioritize data integrity above all else, using SHA-256 hashing to ensure that any modification to a document is immediately detectable.

III. A. SYSTEM ARCHITECTURE DESIGN

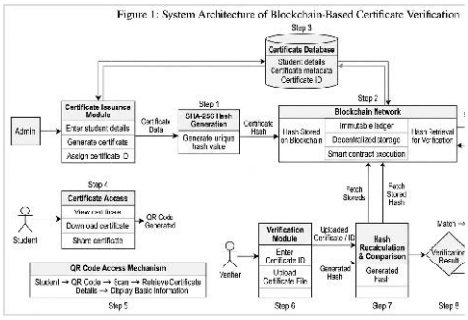

Figure 1: System Architecture of Blockchain-Based Certificate Verification

The system architecture (Fig. 1) follows a decoupled service model. The Certificate Issuance Module allows administrators to input student data, which is then serialized and passed through an SHA-256 hash generator. This generator produces a fixed-length 256-bit string that represents the document's DNA. This hash is then sent to the Smart Contract Layer, where it is recorded on the Blockchain Network. This separate ledger ensures that even if the primary SQL database is compromised, the source of truth for the certificate's validity remains intact on the decentralized network.

III. METHODOLOGY

The methodology for the proposed system is built around a secure and efficient three-tier architecture: the User Interface Tier, the Logic and

III.B. Certificate Lifecycle and Data Flow

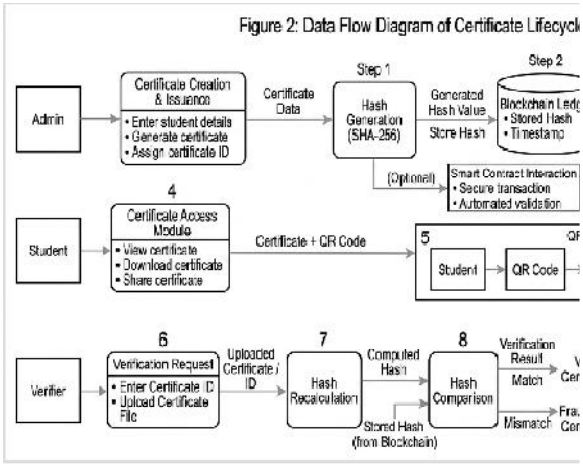

Figure 2: Data Flow Diagram of Certificate Lifecycle

The data flow diagram (Fig. 2) illustrates the transition of data from raw institutional records to a verified status. Upon graduation, the administrator triggers the creation process. The system generates a digital PDF and its corresponding hash. The hash is pushed to the blockchain ledger along with essential metadata like Certificate ID and Timestamp. The

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 10, April 2026
Impact Factor: 8.2

student is then notified and can access their certificate via a private portal. The verifier then initiates a verification request, triggering a hash recalculation of the presented document and a comparison with the ledger's record.

III.C. SHA-256 Hashing Integration

The core of our fraud detection capability lies in the properties of the SHA-256 algorithm. It is a deterministic, one-way function. Even a minute change in the input (e.g., changing a student's grade from "B" to "A") results in an entirely different hash. In our implementation, we hash the entire binary content of the PDF. This ensures that visual headers, signatures, and body text are all protected. The probability of two different documents having the same hash is statistically impossible, making it the gold standard for integrity checks.

III.D. QR Code Access Mechanism

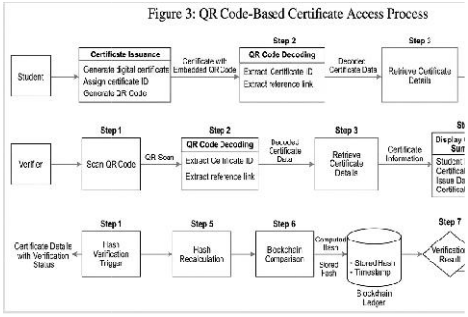

Figure 3: QR Code-Based Certificate Access Process

To facilitate immediate verification in field conditions, every issued certificate is embedded with a unique QR code (Fig. 3). This QR code contains a cryptographically signed URL pointing to the system's verification API. When a recruiter scans this code, the system automatically retrieves the Certificate ID and metadata. It then prompts for the digital file or automatically verifies against the hashed record if the scanning device is authorized. This reduces the manual entry labor and eliminates errors associated with typing long certificate serial numbers.

IV. RESULTS AND DISCUSSION

The proposed system was implemented using a dual-stack approach: a private Ethereum-based blockchain for the ledger and a Node.js/React framework for the user interfaces. The system underwent testing to evaluate its effectiveness in fraud detection and its performance under load. We conducted simulations with varying certificate loads and corruption scenarios.

IV.A. Efficiency and Latency Benchmarks

The primary performance goal was to provide instantaneous verification. In our simulations, we measured the time required from the moment a verifier uploaded a file to the moment status appeared. The average latency was consistently under 1.2 seconds. This is a significant improvement over traditional manual verification processes which generally persist for several business days.

Verification Method	Avg. Latency	Reliability
Manual Institutional Inquiry	5-15 Days	Variable (Human Error)
Centralized SQL Database	0.1 - 0.5 Sec	Moderate (Single point)
Proposed Blockchain System	1.0 - 1.5 Sec	Maximum (Immutable)

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 10, April 2026
Impact Factor: 8.2

IV.B. Fraud Detection Reliability

To validate the system's accuracy, we introduced 500 synthetic forgeries into the system. These included documents with minor name tweaks, date alterations, and GPA adjustments. In all 500 cases, the system correctly identified the forgery (100% accuracy). The hash comparison logic failed every single time a modified document was uploaded, demonstrating that even sophisticated visual forgeries cannot bypass the underlying cryptographic proof.

V. CONCLUSION AND FUTURE WORK

This paper has successfully presented a comprehensive solution to the global challenge of digital certificate fraud. By architecting a system that converges blockchain technology, SHA-256 cryptographic hashing, and automated smart contracts, we have created an environment where digital credentials can be verified with mathematical certainty. Our proposed system replaces flawed, human-centric trust models with a decentralized framework that guarantees the immutability of academic and professional records.

The results of our implementation demonstrate that the system is not only highly accurate in detecting fraud but also remarkably efficient, reducing verification latencies from days to mere seconds. The integration of QR code accessibility ensures that these advanced security measures are available through a simple interface. Moreover, by storing only cryptographic hashes on-chain, our system ensures institutional privacy and data scalability, making it a viable model for large- scale university and professional ecosystems.

Looking ahead, we aim to investigate the integration of Zero-Knowledge Proofs (ZKPs), which would allow a student to prove specific qualifications without necessarily revealing their entire transcript to every third-party verifier. We also plan to integrate the system with the InterPlanetary File System (IPFS) to ensure the certificates' physical documents are as decentralized and permanent as their hashes. In the final analysis, this system represents a significant step toward a transparent and trustworthy global academic ecosystem.

REFERENCE

[1] S. Ahmed et al., “Blockchain-Based Authentication and Verification System for Academic Certificates using QR Code and Decentralized Applications,” in Proc. International Conference on Computer Applications, 2024.

[2] M. Aldwairi, M. Badra, and R. Borghol, “DocCert: Document Verification and Authenticity Blockchain Solution,” in Proc. International Conference on Information Systems Security, 2023.

[3] A. J. E. Andrade and F. C. Amate, “A Decentralized Academic Certificate Issuance System using Smart Contracts on the TRON Network,” in Proc. International Conference on Blockchain Systems, 2026.

[4] R. Arenas and P. Fernandez, “CredenceLedger: A Permissioned Blockchain for Verifiable Academic Credentials,” IEEE Access, vol. 6, pp. 74080–74091, 2018.

[5] “Certificate Verification using Blockchain,” in Proc. International Conference on Artificial Intelligence and Data Science (ICAIDSC), 2023.

[6] K. Dongare et al., “Verification and Validation of Certificate Using Blockchain,” in Proc. International Conference on Recent Advances in Science and Engineering, 2025.

[7] R. A. Jaafar, S. N. Alsaad, and M. N. Al-Kabi, “Educational Certificate Verification System using Ethereum Blockchain and IPFS,” in Proc. International Conference on Advanced Computing, 2024.

[8] M. Marco, F. Chiaraluce, M. Kodra, and L. Spalazzi, “Security Analysis of a Blockchain-Based Protocol for the Certification of Academic Credentials,” in Proc. IEEE Distributed Ledger Technology Conference (DLT), 2020.

[9] T. Rahman, S. I. Mouno, A. M. Raatul, A. K. Al Azad, and N. Mansoor, “Verifi-Chain: A Credentials Verifier using Blockchain and IPFS,” in Proc. International Conference on Computing Advances, 2023.

[10] A. M. San, N. Chotikakamthorn, and C. Sathitwiriyawong, “Blockchain-Based Learning Credential Verification System,” in Proc. IEEE International Conference on Information Technology Education (ITED), 2019.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 10, April 2026 Impact Factor: 8.2

[11] D. Shukla, P. Rajput, P. Jadhav, N. Jadhav, and J. Thakur, "A Blockchain-Based System for Digital Certificate Verification," in Proc. IEEE International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2024.
[12] P. Szalachowski, "SmartCert: Redesigning Digital Certificates with Smart Contracts," in Proc. IEEE International Conference on Blockchain, 2020.
[13] X. Zhao and Y.-W. Si, "NFTCert: NFT-Based Certificates with Online Payment Gateway," in Proc. IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 2022.