IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

TAMPER PROOF CERTIFICATE VERIFICATION USING BLOCKCHAIN TECHNOLOGY

[1]Vansh Ranawat, [2]Shashank Gole, [3]Shreyas Dhadam, [4]Yash Kokade

[1234]B.Tech Student, Electronics and Computer Engineering

Department of Electronics and Communication Engineering,

School of Engineering and Sciences, MIT ADT University, Pune – 412201, India

Abstract: The increasing number of fake, forged, and tampered academic and professional certificates has become a major concern for universities, employers, and verification authorities. Traditional certificate verification methods rely on centralized databases, manual checking, or physical document validation, all of which are slow, prone to manipulation, and lack transparency. This paper proposes a Tamper Proof Certificate Verification System using Blockchain Technology, designed to provide a secure, decentralized, and immutable platform for issuing and verifying certificates. The system architecture incorporates a web-based portal for certificate generation by authorized institutions, a secure blockchain backend for data storage using SHA-256 cryptographic hashing and smart contracts, and a public verification module that allows users or employers to instantly validate certificates by scanning a QR code or entering a unique blockchain transaction ID. The findings indicate that blockchain-based systems can successfully prevent certificate fraud, streamline verification processes, and provide a scalable solution for academic and professional credential validation.

Index Terms: Blockchain, Certificate Verification, SHA-256, Smart Contracts, QR Code Authentication, Decentralized System, Tamper Detection, Digital Credentials.

I. INTRODUCTION

In the modern digital era, academic institutions, organizations, and government agencies increasingly rely on electronic certificates and digital records for verification purposes. However, the rapid growth of digital documentation has led to a significant rise in certificate forgery, document tampering, and fraudulent credential claims. Traditional certificate verification systems depend on centralized databases, manual verification procedures, and physical document inspection, which are often time-consuming, costly, and vulnerable to manipulation. These limitations create serious challenges for universities, employers, and verification authorities in ensuring the authenticity and integrity of certificates.

Blockchain technology has emerged as a revolutionary solution for secure data storage and transparent verification, offering a decentralized and immutable digital ledger where information, once stored, cannot be altered without network consensus. This makes blockchain highly suitable for applications requiring security, trust, and transparency. By integrating blockchain with certificate verification systems, it becomes possible to create a tamper-proof mechanism for issuing, storing, and validating academic certificates through cryptographic hashing, smart contracts, and QR-code-based authentication.

The proposed project, "Tamper Proof Certificate Verification," focuses on developing a blockchain-based system that ensures secure and transparent validation of certificates. It converts certificate information into a unique cryptographic hash using the SHA-256 algorithm, stores it securely on the blockchain through smart contracts, and incorporates a QR-code-based verification mechanism for instant authentication by employers, institutions, or other stakeholders. The system aims to eliminate dependency on third-party verification agencies, reduce verification time, prevent certificate fraud, and provide a scalable and reliable solution for digital credential management across educational institutions, industries, and government sectors.

II. LITERATURE REVIEW

The review of existing literature reveals that certificate verification and document authentication have attracted growing research attention due to increasing incidents of academic fraud. Traditional certificate verification methods mainly rely on centralized databases, manual verification procedures, and physical document validation. Although these approaches are widely used, they often suffer from problems such as data tampering, unauthorized access, delays in verification, lack of transparency, and dependence on third-party authorities.

Patel and Joshi [1] discussed the increasing prevalence of fake academic certificates in India and emphasized the need for advanced digital verification solutions. Their study highlights that centralized databases are vulnerable to manipulation and unauthorized access, making them unreliable for high-stakes verification. Li, Bahrami, and Singh [2] proposed a blockchain framework for secure document validation, demonstrating how blockchain's immutable structure prevents tampering and ensures data integrity. Smart contracts were utilized to automate certificate issuance, reducing the need for third-party verification authorities.

Rahul and Chakraborty [3] analyzed the use of public blockchain platforms like Ethereum for credential storage and concluded that decentralized verification reduces processing time and enhances transparency. A study by Gupta and Mehta [4] explored QR-code-based verification systems and noted that although QR codes improve accessibility, they remain vulnerable if the backend is centralized and lacks security protections. Therefore, the inclusion of blockchain significantly enhances the trustworthiness of QR-based verification processes. Kim and Park [5] examined various consensus algorithms including Proof of Work and Proof of Authority, concluding that lightweight consensus mechanisms are ideal for certificate storage applications due to low computational requirements.

A. Identification of Gaps

After reviewing the literature, the following gaps were identified: (i) Most existing systems still rely partially on centralized databases. (ii) Limited research focuses on complete end-to-end automated certificate issuance. (iii) Scalability issues remain in public blockchains for large academic institutions. (iv) Few studies address real-time verification using QR codes linked directly to blockchain transactions. (v) Integration of user-friendly web interfaces with blockchain systems is seldom discussed.

B. Problem Statement

The increasing number of fake and tampered academic certificates has become a major challenge for educational institutions, employers, and verification authorities. Traditional certificate verification systems are centralized, slow, vulnerable to manipulation, and dependent on manual validation processes. Therefore, there is a need for a secure, transparent, decentralized, and tamper-proof certificate verification system using blockchain technology.

C. Objectives

The objectives of this project are: (i) To design and develop a blockchain-based certificate verification system. (ii) To ensure secure and tamper-proof storage of certificate data using cryptographic hashing. (iii) To implement smart contracts for automated certificate issuance and verification. (iv) To generate QR codes for instant and user-friendly certificate validation. (v) To reduce verification time and eliminate dependency on third-party verification agencies. (vi) To improve transparency, trust, and security in digital certificate management systems.

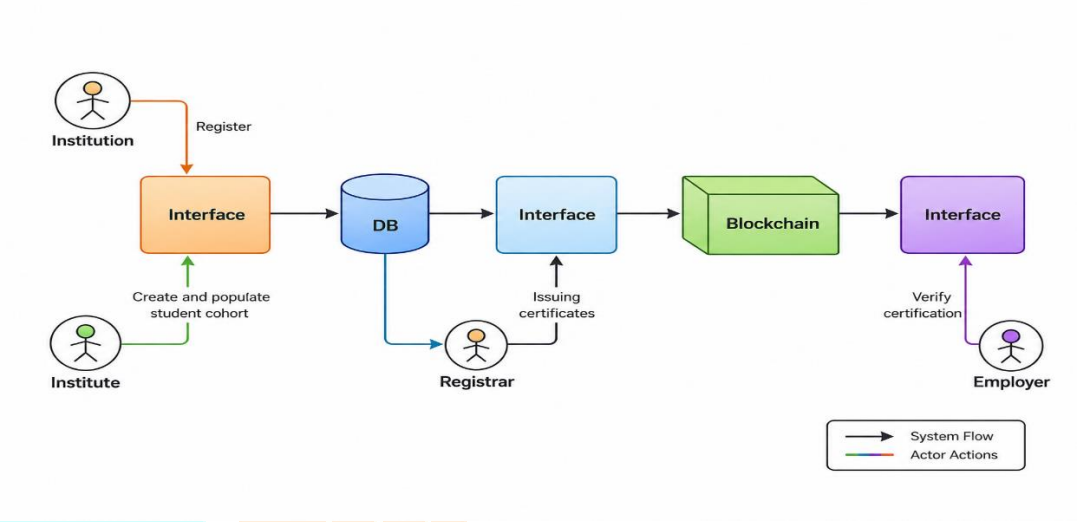
III. METHODOLOGY

This section explains the methodology adopted for the design and development of the Tamper Proof Certificate Verification System using blockchain technology. The methodology describes the overall workflow, system architecture, blockchain integration process, certificate hashing mechanism, QR-code generation, and certificate verification procedure.

The proposed system uses blockchain as a distributed ledger for storing certificate-related information securely. Instead of storing complete certificate files on the blockchain, only the cryptographic hash of the certificate is stored to maintain privacy and reduce storage requirements. Smart contracts are used to automate the process of certificate issuance and verification. Additionally, QR-code-based verification is integrated into the system to enable instant validation of certificates by employers, institutions, and other authorized users.

A. System Architecture

The overall architecture of the proposed system consists of the following components: (i) User Interface — a web-based portal accessible to administrators and verifiers; (ii) Certificate Upload Module — allows authorized institutions to upload and generate certificates; (iii) Hash Generation Module — applies SHA-256 algorithm to generate unique certificate fingerprints; (iv) Blockchain Network — Ethereum or Polygon-based decentralized ledger; (v) Smart Contract — automates certificate storage and verification; (vi) QR Code Generator — creates scannable verification links; (vii) Verification Portal — provides instant authentication results to users.



Block Diagram

B. SHA-256 Hashing Algorithm

SHA-256 (Secure Hash Algorithm 256-bit) is a cryptographic hashing algorithm developed by the National Institute of Standards and Technology (NIST). It belongs to the SHA-2 family and is widely used in blockchain technology, digital signatures, cybersecurity, and data integrity applications. The algorithm converts input data of any size into a fixed 256-bit hash value. In the proposed system, SHA-256 is used to generate a unique hash for each certificate to ensure authenticity and prevent tampering.

The SHA-256 algorithm operates through the following stages: (i) Input Message — the complete certificate data is treated as a binary message; (ii) Message Padding — the input message is padded to make its length a multiple of 512 bits; (iii) Message Parsing — the padded message is divided into multiple 512-bit blocks, each further divided into sixteen 32-bit words; (iv) Initialization of Hash Values — SHA-256 uses eight predefined 32-bit initial hash values derived from the fractional parts of square roots of prime numbers; (v) Compression Function — each message block undergoes 64 rounds of logical operations, modular additions, bitwise rotations, and XOR functions; (vi) Final Hash Generation — a unique 256-bit hash represented as 64 hexadecimal characters is produced.

A critical advantage of SHA-256 is that even a very small change in the input data produces a completely different hash value. This property makes it ideal for detecting forged or modified certificates instantly. The algorithm is collision-resistant, one-way, and ensures data integrity with fast processing.

C. Blockchain Integration

Blockchain technology is integrated into the system to provide secure and decentralized storage of certificate information. The integration process includes: (i) Selection of blockchain platform — Ethereum or Polygon; (ii) Development of smart contracts using Solidity programming language; (iii) Deployment of smart contracts on blockchain test network; (iv) Storage of certificate hash values and transaction details on the distributed ledger. The blockchain ensures immutability of records, decentralization, transparency, and secure verification without any central authority.

D. Smart Contract Implementation

Smart contracts are self-executing programs stored on the blockchain. In the proposed system, smart contracts are responsible for: storing certificate hashes, mapping certificate IDs to hash values, managing certificate verification requests, and maintaining immutable transaction records. The smart contract automatically validates the certificate information without requiring third-party intervention.

E. QR Code Generation and Verification

A unique QR code is generated for each certificate issued through the system. The QR code contains the Certificate ID, Blockchain transaction ID, and Verification URL. When scanned, the QR code redirects the user to the verification portal where the certificate authenticity can be checked instantly by comparing the stored blockchain hash with the hash of the presented certificate.

F. Technologies Used

Table 1: Technologies Used in the Proposed System

Technology	Purpose
Blockchain (Ethereum / Polygon)	Secure decentralized storage
Solidity	Smart contract development
SHA-256	Certificate cryptographic hashing
QR Code Generator	Instant verification link generation
HTML / CSS / JavaScript	Frontend development
Node.js	Backend development
MongoDB / MySQL	Database management

G. System Workflow

The complete workflow of the proposed system is as follows: (i) The authorized institution uploads the certificate through the web interface. (ii) The SHA-256 algorithm generates a unique cryptographic hash value for the certificate. (iii) The generated hash is stored securely on the blockchain through the smart contract. (iv) A unique QR code linked to the blockchain transaction ID is generated. (v) The verifier scans the QR code or enters the certificate ID on the verification portal. (vi) The system retrieves the stored hash from the blockchain, re-computes the hash of the presented certificate, and compares both values to determine authenticity.

IV. RESULTS AND DISCUSSION

This section presents the results obtained from the implementation and testing of the proposed Tamper Proof Certificate Verification System. The implemented system integrates blockchain technology, SHA-256 hashing, smart contracts, and QR-code-based authentication to provide a decentralized and tamper-proof certificate verification mechanism.

A. Certificate Hash Generation

The first stage of implementation involved generating SHA-256 hash values for uploaded certificate files. Each certificate produced a unique 256-bit hash value which acts as a digital fingerprint of the certificate. During testing, it was observed that even a minor modification in the certificate resulted in a completely different hash value, thereby proving the effectiveness of the hashing mechanism in tamper detection. Example generated hash: 3f786850e387550fdab836ed7e6dc881de23001b.

B. Smart Contract Deployment and Blockchain Storage

The smart contract developed using Solidity was successfully deployed on the blockchain test network. The deployed contract was responsible for storing certificate hash values, certificate IDs, and transaction details securely. Each certificate entry generated a unique blockchain transaction ID, enabling transparent and traceable certificate management. The blockchain explorer confirmed that all transactions were recorded successfully and could not be modified after deployment, achieving complete immutability.

C. Testing and Validation Results

Table 2: Test Cases and Verification Results

Test Case	Input Condition	Expected Output	Result
Original Certificate	Valid certificate uploaded	Certificate Verified	Pass
Modified Certificate	Tampered certificate uploaded	Invalid Certificate	Pass
Wrong Certificate ID	Incorrect ID entered	Verification Failed	Pass
QR Verification	QR code scanned correctly	Certificate Verified	Pass

D. System Performance Analysis

Table 3: System Performance Analysis

Parameter	Expected Outcome	Remarks
Verification Speed	< 5 seconds	Faster than manual verification
Security	High	Blockchain ensures immutability
Transparency	High	Publicly verifiable transactions
Tamper Resistance	Excellent	SHA-256 detects any modification
Scalability	Moderate	Can be optimized using private chain
User Accessibility	Easy	QR-based verification

The results demonstrate that blockchain technology effectively solves the challenges associated with traditional certificate verification systems. The proposed system successfully prevented certificate tampering by storing cryptographic hashes on the blockchain. The integration of SHA-256 hashing and smart contracts enhanced system security, while QR-code-based verification simplified the verification process for users and organizations. Compared to traditional manual verification methods, the proposed system provides faster verification, better security, higher transparency, improved reliability, and reduced verification cost.

V. CONCLUSION

This paper proposed a secure, transparent, and tamper-proof certificate verification system using blockchain technology. Traditional verification systems rely heavily on centralized infrastructure, making them vulnerable to manipulation, delays, and unauthorized access. The proposed system addressed these limitations by leveraging the immutability and decentralization characteristics of blockchain.

The methodology introduced key processes including cryptographic hashing of certificate data using SHA-256, blockchain-based storage through smart contracts, and QR-code-enabled instant verification. The results demonstrated that storing certificate hashes on a blockchain eliminates the possibility of tampering, ensuring long-term authenticity. The verification mechanism, which compares uploaded certificate hashes with blockchain-stored hashes, provides a fast, reliable, and user-friendly method for authenticity checks.

The system establishes that blockchain is a powerful technology for mitigating certificate fraud. Future work will focus on full-scale institutional deployment, mobile application development, multi-blockchain support, integration with national platforms such as DigiLocker and NAD, advanced smart contract features for certificate revocation, AI-based fraud detection, and biometric multi-factor authentication for enhanced security.

REFERENCES

[1] A. Patel and M. Joshi, "A Study on Fake Academic Certificates and Need for Digital Verification," International Journal of Computer Applications, vol. 182, no. 25, pp. 1–5, 2020.

[2] Y. Li, M. Bahrami, and S. Singh, "Blockchain-Based Digital Document Verification System," IEEE Access, vol. 9, pp. 122–130, 2021.

[3] S. Rahul and R. Chakraborty, "Secure Credential Verification Using Public Blockchain Networks," Proceedings of the International Conference on Blockchain Technologies, pp. 78–85, 2022.

[4] R. Gupta and S. Mehta, "QR Code Based Certificate Authentication and Its Limitations," Journal of Information Security & Digital Forensics, vol. 7, no. 2, pp. 34–40, 2021.

[5] J. Kim and S. Park, "A Comparative Analysis of Blockchain Consensus Algorithms for Lightweight Applications," IEEE Transactions on Engineering Management, vol. 68, no. 4, pp. 1002–1013, 2021.

[6] K. Sharma and A. Verma, "Blockchain for Educational Certificate Storage," International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 12, pp. 552–556, 2020.

[7] S. Kumar and V. Rathod, "Decentralized Systems for Identity and Document Verification," International Conference on Computing & Information Sciences, pp. 44–50, 2021.

[8] P. Wagh and R. Pawar, "Smart Contract-Based Document Authentication Framework," IEEE International Conference on Emerging Smart Computing & Informatics, pp. 367–372, 2022.

[9] National Institute of Standards and Technology (NIST), SHA-256 Standard. [Online]. Available: https://www.nist.gov

[10] Ethereum Foundation, "Smart Contracts Documentation." [Online]. Available: https://ethereum.org/en/developers/docs/smart-contracts/