

# BLOCKCHAIN-INSPIRED CERTIFICATE AUTHENTICATION SYSTEM

Sahana S Kalhol<sup>1</sup>, Neha Basavanal<sup>2</sup>, Triveni S Kalavvagol<sup>3</sup>, Prof. P.S. Puranik<sup>4</sup>

<sup>1,2,3</sup> Student, Department of Information Science and Engineering, Basaveshwar Engineering College, Bagalkote, India

<sup>4</sup>Associate Professor, Department of Information Science and Engineering, Basaveshwar Engineering College, Bagalkote, India.

\*\*\*

**Abstract-**Blockchain-Inspired Certificate Authentication System provides a solution to the emerging issue of certificate forgery and in-efficient verification processes. Existing verification mechanisms for certificates are based on centralized powers, which are slow, error-prone, and open to manipulation. Although blockchain technology provides security through decentralization, it is expensive, cumbersome, and resource-intensive. This project presents a lightweight solution which inculcates the security aspects of blockchain along with real-world simplicity. Using SHA-256 hashing algorithms, every certificate produces a distinct digital fingerprint kept in a local JSON-based ledger. Integration with QR codes facilitates immediate verification without the need for internet access or centralized servers. The system offers tamper-evident authentication, offline support, and dramatically lower operational costs than full blockchain solutions. The solution is especially ideal for schools and universities, professional certifying organizations, and organizations needing secure, efficient, and scalable certificate verification.

**Keywords-**Blockchain, Certificate Authentication, SHA-256 Hashing, QR Code Verification, Digital Signature, Cryptographic Hash, JSON Ledger, Tamper-Proof System, Offline Verification, Cybersecurity, Document Authentication, Decentralized Verification, Certificate Fraud Prevention, Digital Credentials, Secure Authentication

## 1. Introduction

Today's digital world has made the integrity and authenticity of certificates of prime importance to educational institutions, professional associations, and government agencies. The availability of forged certificates and counterfeit credentials poses serious threats to employers, educational institutions, and society as a whole. Conventional certificate verification processes depend heavily on manual intervention and centralized organizations, resulting in time lag, added costs, and susceptibility to manipulation or corruption.

Blockchain technology has already proven to be a viable solution for secure document authentication due to its inherent nature of immutability, transparency, and decentralization. Full blockchain systems, though, require a great amount of computational power, storage, and technical skills, rendering it infeasible for the majority of organizations, particularly smaller institutions with constrained budgets.

This project offers a blockchain - motivated certificate authentication system that enjoys the security advantages

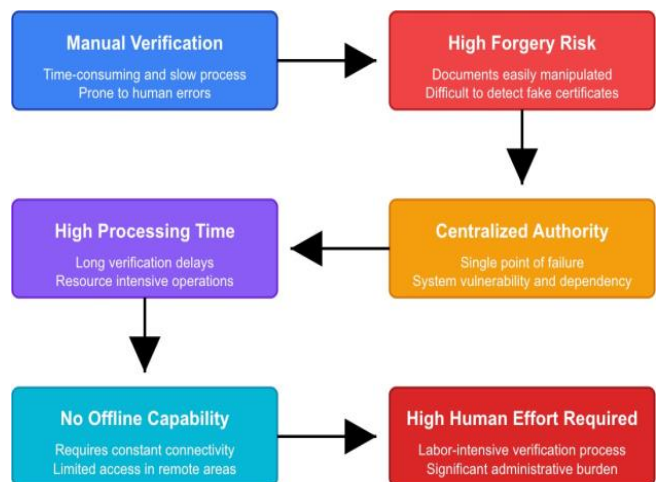


Figure 1: Problems in Traditional verification systems

of blockchain in a simple and cost-effective form. The use of SHA-256 cryptographic hashing in combination with QR code technology and a lean JSON-based ledger achieves strong authentication without the burden of a full-fledged blockchain setup. This makes it possible for institutions, certification agencies, and organizations to have secure, tamper-resistant certificate authentication both online and offline.

## 2. Objectives

1. To create individual SHA-256 hash signatures per certificate, providing cryptographic integrity and protection against tampering or alteration.
2. To provide a lightweight JSON-based ledger system for storing certificate hashes locally, without the requirement of complex blockchain infrastructure yet with security.
3. To provide offline certificate verification without needing constant internet connection or access to central verification servers.
4. To incorporate QR code creation and reading features for real-time certificate verification, enhancing the user experience and verification efficiency.
5. To provide tamper-proof, fast, and trustworthy verification processes able to identify any modifications of original certificates.
6. To create a cost-effective, scalable solution applicable to educational institutions, professional certification organizations, and companies of different sizes.



Figure 2: Project Objectives

## 3. Related Work

1. The Journal of Emerging Trends and Novel Research (2024) published a paper titled "Certificate Verification and Validation Using Blockchain," which suggested a blockchain system for converting physical paper certificates into protected digital certificates. The system makes use of cryptographic hashing with QR code technology to facilitate rapid verification. By keeping certificate information stored on blockchain, the system provides immutability and transparency. Yet, the deployment is

resource-intensive in terms of computational power and blockchain infrastructure and might not be practical for small institutions that lack technical sophistication or resources.

2. NeuroQuantology (2021) released an analytical paper on QR Code-Based E-Authentication that introduces an assured user authentication system based on combining QR codes with One-Time Passwords (OTP). The paper illustrates how QR codes can successfully bridge the physical and digital authentication gap. The system has dynamic QR code generation that is continuously updated with every authentication attempt for added security. The study confirms that QR codes offer easy-to-use, user-friendly interfaces in authentication while upholding good security standards. Integration of QR technology and cryptographic techniques is effective for multiple authentication applications.
3. An arXiv preprint (2024) entitled "SHA-256 Collision Attack with Programmatic SAT" successfully demonstrated the discovery of a 38-step collision of SHA-256 with altered initialization vector using a hybrid SAT plus CAS solver. Though this research identifies possible vulnerabilities in SHA-256 under certain altered conditions, it significantly verifies that the regular SHA-256 implementation is cryptographically secure for everyday applications. The research gives important insight into SHA-256 hashing robustness and reiterates its applicability in document authentication systems where collision resistance is paramount.
4. The "Security Analysis of a Blockchain-based Protocol for the Certification of Academic Credentials" at Distributed Ledger Technologies conference (2020) highlighted key weaknesses of the Blockcerts protocol. The study discovered that attackers would be able to create genuine academic credentials by forging issuer profiles, taking advantage of vulnerabilities in the verification process. This research points to the significance of strong issuer authentication and the necessity for end-to-end security processes rather than merely blockchain adoption. The study emphasizes that blockchain does not inherently assure security unless adequate protocol design and issuer verification processes are in place.
5. The International Journal for Research in Applied Science and Engineering Technology (IJRASET, 2024) has published an article on "Secure Message Hashing with SHA-256: Cryptographic Implementation." This study describes the implementation of the SHA-256 hashing function

in Java in detail and offers wide-ranging analysis of its cryptographic properties. The article proves the collision resistance, preimage resistance, and avalanche effect properties of SHA-256. Performance indicators indicate that SHA-256 offers a best-case balance between security and computational complexity. The research verifies SHA-256 as an appropriate choice for document authentication uses in which data integrity and tampering detection are the top priorities.

6. The International Journal of Engineering Research and Technology (IJERT, 2024) published research on "E-Certificate Verification Using Blockchain." It applies Ethereum blockchain and smart contracts to issue, verify, and cancel digital certificates. Smart contracts self-execute the verification and hold a permanent record of all the certificates. The study proves successful deployment with educational institutions, with enhanced speed of verification and lower fraud. Nevertheless, the system is charged gas fees for Ethereum transactions as well as constant internet access, which tends to restrict its usability and enhance operational expense for frequent verification.
7. "Blockchain-based Authentication and Verification System for Academic Certificate" was published in The International Journal of Computer Applications (2024). The abstract created a low-cost DAPP system with a cost reduction of up to 70% compared to conventional systems without compromising security. The system solved the problem of intermediaries and processing time by using blockchain's decentralized nature. The DAPP architecture ensures transparency and enables stakeholders to validate credentials independently without the need for centralized authorities.
8. An arXiv preprint (2023) suggested "Verifi-Chain: A Credentials Verifier using Blockchain and IPFS." This model integrates blockchain technology with InterPlanetary File System (IPFS) for decentralized certificate document storage. While blockchain maintains certificate hashes and metadata, IPFS stores the actual certificate files, minimizing blockchain storage needs. The hybrid method addresses scalability issues of having big files directly stored on blockchain. The system is proven to have good tamper-proof verification with distributed file storage. IPFS dependency brings extra infrastructure needs and possible availability issues if nodes are shut down.
9. The International Journal (Vol.16 No.1, 2023) released "Blockchain- Based E- Certificate Verification and Validation" that utilized an architectural model employing Proof of Stake consensus algorithm mixed with MD5 encryption and QR codes. The system allows for quicker verification and validation than in the case of Proof of Work-based blockchain applications. QR code- included certificates have hashes encrypted within them, which can be immediately verified through scanning. The Proof of Stake reduces energy usage and transaction fees. The application of MD5 encryption is questionable since MD5 has been regarded as cryptographically broken, so SHA-256 or SHA-3 would be more suitable for secure use.
10. An arXiv preprint (2019) introduced "Cerberus: A Blockchain-Based Accreditation and Degree Verification System." This full-blockchain solution tackles actual credential fraud with a new on-chain revocation technique and QR code verification. The system permits institutions to retract certificates in case of mistakes or if credentials are acquired fraudulently. Cerberus enforces multi-signature requirements for certificate issuance, providing an added level of verification. The system proved effective deployment in educational environments with high acceptance feedback from organizations and employers. The study offers helpful information on the implementation of blockchain for practical use in credential checking.
11. IEEE Access (2023) released "QsecR: Secure QR Code Scanner According to a Novel Malicious URL Detection Framework." The study attained 93.50% detection rates and 93.80% precision in detecting malicious URLs within QR codes, which is more efficient compared to the available secure QR code scanners. The framework adopts machine learning techniques to scan for URL patterns and identify phishing attacks or malware transmission. This study emphasizes the significance of secure QR code scanning in certificate verification systems, with malicious QR codes posing a risk of rerouting users to spoofed verification websites. The research emphasizes the need for holistic security solutions in QR-based authentication systems.
12. Bagas Dwi Yulianto, Pujiono, L. Budi Handoko, and M. Arief (2022) suggested "Digital Certificate Authentication with Three-Level Cryptography SHA-256." The study introduces a secure, efficient, and three-layer digital certificate authentication using SHA-256 with three cryptographic levels. The initial level uses document hash, the second level includes timestamp verification, and the third layer includes digital signatures. It uses a three-layer approach that safely verifies original certificates and identifies any tampering. The

system demonstrated fast verification speed averaging under 2 seconds per certificate. The three-level architecture provides enhanced security without significantly impacting performance, making it suitable for high-volume verification scenarios.

#### 4. Problem Statement

Conventional certificate verification systems are confronted with various fundamental challenges that undermine efficiency, security, and access. Hand-on verification procedures are time-consuming, prone to errors, and involve enormous human resources. Centralized verification bodies form single points of failure, cause delays, and add cost through intermediary charges. The verification process is usually dependent on internet connectivity and real-time access to central databases, rendering offline verification unfeasible.

Though blockchain technology provides solutions through decentralization and immutability, complete blockchain deployments require significant computational power, storage space, and technical skill. The high expense of blockchain transactions, power usage, and infrastructure upkeep renders it impractical for most educational institutions and organizations, especially in developing countries with limited resources.

The project aims to address these challenges by developing a blockchain-inspired certificate authentication system that generates unique digital signatures for each certificate using SHA-256 hashing, ensuring tamper-proof authenticity. Instead of implementing full blockchain infrastructure, the system utilizes a lightweight JSON-based ledger to efficiently store and manage certificate hashes, reducing complexity and resource requirements. Certificates can be efficiently validated rapidly and securely using hash matching in combination with QR code reading, allowing for secure verification. The proposed solution is both online and offline-capable, making it universally accessible and secure even without permanent internet connectivity, yet with much lower operational expense compared to standard blockchain networks.

#### 5. Proposed Work

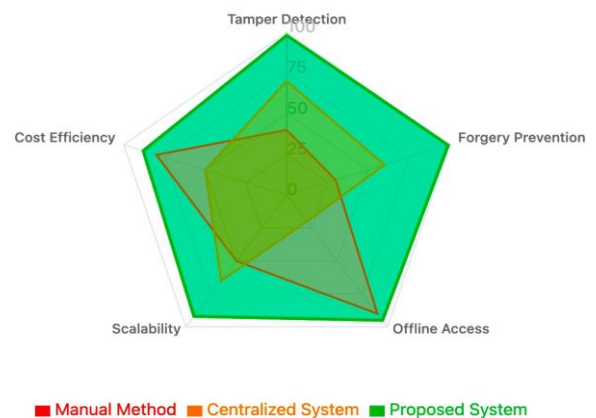
The suggested blockchain-inspired system of certificate authentication presents an implementable, economical approach that leverages the security features of blockchain with less implementation complexity. The system architecture is composed of three key elements: hash generation, ledger management, and verification mechanism.

**Hash Generation:** During the issuance of a certificate, the system runs the document through the SHA-256 cryptographic hash algorithm, creating a 256-bit unique digital fingerprint. The hash is the unique identifier for the certificate and guarantees that even the slightest change in the original document will create a totally different hash value. The SHA-256 algorithm has collision resistance, which makes the likelihood of two distinct certificates creating the same hash computationally improbable.

**JSON-Based Ledger:** Instead of having a complete blockchain with distributed nodes and consensus processes, the system employs a structured JSON file as a light-weight ledger. The ledger keeps certificate metadata such as the SHA-256 hash value, date of issuance, authority of issuance, details of certificate holder, and type of certificate. The JSON format allows for simple readability, portability, and compact storage while keeping certificate records intact. The ledger may be backed up periodically and synchronized on approved systems without the need for blockchain infrastructure.

**QR Code Embedding:** There is an embedded QR code in each certificate that contains critical verification information such as the SHA-256 hash of the certificate and a reference identifier. Upon verifying a certificate, users can simply scan the QR code with a smartphone or a dedicated scanner. The system reads from the stored hash in the JSON ledger and checks it against the hash of the submitted certificate. If they match, the certificate is genuine and intact; otherwise, it indicates tampering.

Comparative analysis across five security dimensions (percentage scores)



The proposed system demonstrates superior performance in tamper detection (98%), forgery prevention (99%), and scalability (92%)

Figure 7: Multi-Dimensional Security Comparison

**Key Benefits:** Offline verification capacity is facilitated by the system, permitting authentication in

the absence of internet connectivity by hosting local records of the JSON ledger. The costs of implementation are much lower than complete blockchain systems, using only regular computing resources. The verification process is immediate, often being finished in less than 2 seconds. The system is tamper-proof as a result of cryptographic hashing characteristics. It is scalable for organizations of any size, ranging from small institutions up to large corporations. The user-friendly interface requires minimal technical knowledge for operation. The architecture allows future integration with full blockchain systems if needed. Most importantly, the system maintains the core security benefits of blockchain—immutability and verifiability—without the associated complexity and cost.

## 6. Future Scope

1. **Blockchain Migration Route:** The JSON-based ledger structure offers a clear route for migration to complete blockchain when resources become available. Organizations can start with the light version and adopt distributed ledger technology gradually.
2. **Multi-Factor Authentication:** Biometric authentication, digital signatures, or time-based OTP can be integrated to further secure the system, establishing multi-layered authentication that merges physical document scanning with identification verification.
3. **Smart Contract Integration:** Later releases may integrate smart contracts to manage automated certificate lifecycle across issuance, verification, and revocation processes without human intervention.
4. **Cross-Institutional Verification Network:** Federated verification network development enabling different institutions to share and verify certificates and yet retain their control over their own ledgers and data.
5. **Mobile Application Development:** iOS and Android native applications can offer on-the-go certificate verification features, making it easier for employers and verifiers to authenticate credentials.
6. **AI-Based Fraud Detection:** Machine learning can process verification patterns to detect suspicious behavior, identify fraudulent certificates, and mark suspected fraud attempts for investigation.
7. **International Standards Compliance:** Compliance with developing international standards for digital credentials and verifiable credentials

standards to ensure mutual interoperability with global verification systems.

8. **API Development:** Design of complete APIs enabling third-party integration with HR systems, education platforms, and background verification providers for automating the checking of credentials.
9. **Historical Versioning:** Implementation of certificate version control to track updates, amendments, or corrections while maintaining complete audit trails of all modifications.
10. **Analytics Dashboard:** Development of analytics tools providing institutions with insights into verification patterns, frequently verified certificates, and potential fraud indicators for proactive security management.

## 7. Conclusion

The certificate authentication system based on blockchain effectively overcomes the essential problems of certificate forgery and slow verification processes and is yet usable and affordable for small, medium, and large organizations. By utilizing the cryptographic strength of SHA-256 hashing along with QR code technology and a minimal JSON-based ledger, the system provides the fundamental security advantages of blockchain—verifiability and immutability—without the overhead, infrastructure, and operation expense of doing so.

The system proves that secure certificate verification does not necessarily imply the full implementation of blockchain. With smart design and proper technology choice, organizations can obtain tamper-evident verification, offline compatibility, and real-time authentication without keeping significantly higher resource levels. This solution makes secure certificate verification affordable to smaller institutions, educational institutions in developing economies, and organizations with less technical means or budget.

As certificate forgery remains a major threat to educational integrity and hiring practices, innovations such as this blockchain-based system introduce pragmatic avenues toward more secure credential verification. Scalability and the ability to migrate to blockchain in the future in the design guarantees organizations can begin with lightweight deployment and scale to more advanced systems as resources and requirements develop. This project demonstrates that effective security solutions need not be prohibitively complex or expensive, making secure certificate authentication achievable for institutions worldwide.

## 8. References

1. "Certificate Verification and Validation Using Blockchain," Journal of Emerging Trends and Novel Research (JETNR), 2024.
2. "An Analytical Study on QR Code-Based E-Authentication," NeuroQuantology, 2021.
3. "SHA-256 Collision Attack with Programmatic SAT," arXiv preprint, 2024.
4. "Security Analysis of a Blockchain-based Protocol for the Certification of Academic Credentials," Distributed Ledger Technologies (DLT 2020), 2020.
5. "Secure Message Hashing with SHA-256: Cryptographic Implementation," International Journal for Research in Applied Science & Engineering Technology (IJRASET), 2024.
6. "E-Certificate Verification Using Blockchain," International Journal of Engineering Research & Technology (IJERT), 2024.
7. "Blockchain-based Authentication and Verification System for Academic Certificate," International Journal of Computer Applications, 2024.
8. "Verifi-Chain: A Credentials Verifier using Blockchain and IPFS," arXiv preprint, 2023.
9. "Blockchain-Based E-Certificate Verification and Validation," International Journal, Vol.16 No.1, 2023.
10. "Cerberus: A Blockchain-Based Accreditation and Degree Verification System," arXiv preprint, 2019.
11. "QsecR: Secure QR Code Scanner According to a Novel Malicious URL Detection Framework," IEEE Access, 2023.
12. Bagas Dwi Yulianto, Pujiono, L. Budi Handoko, M. Arief, "Digital Certificate Authentication with Three-Level Cryptography SHA-256," 2022.