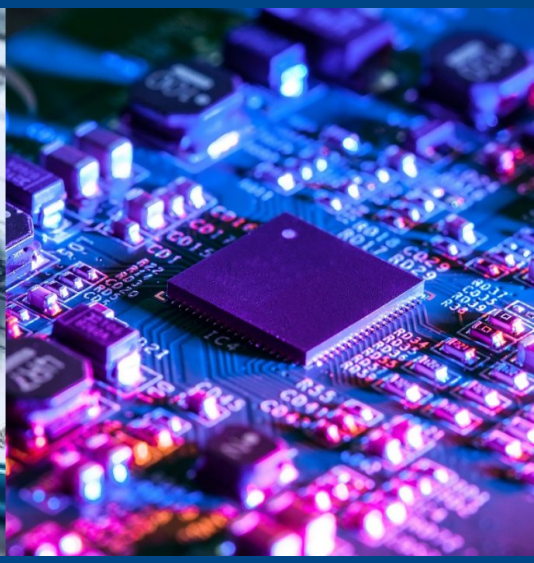
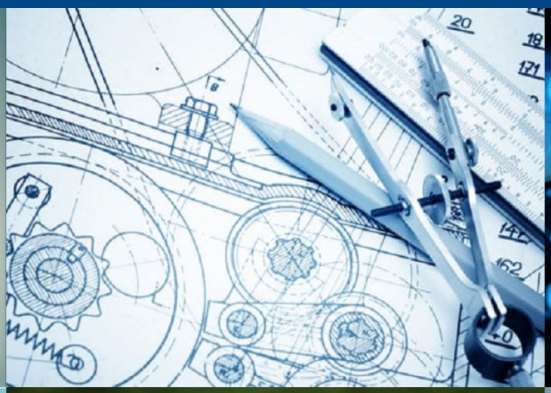
ISSN: 2582-7219

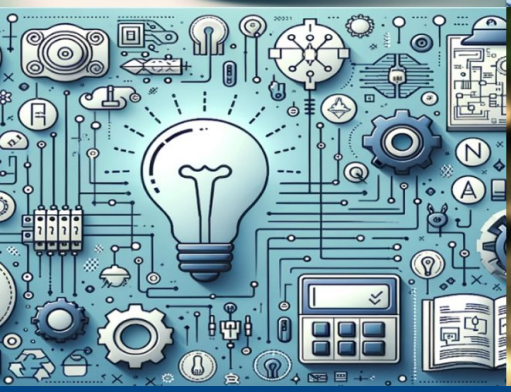




International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206 **Volume 9, Issue 4, April 2026**

© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904279

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Decentralized Certificate Verification System Using Blockchain Technology Authors

Muzamil J [1], Najmudeen Sait M [2], Syed Thahir Ahamed S H[3], Muhammed Abid I [4], Faritha Banu A[5]

Fourth Year B.E. Student, Department of Computer Science and Engineering, Aalim Muhammed Salegh College of Engineering, Chennai, Tamil Nadu,India[1]

Fourth Year B.E. Student, Department of Computer Science and Engineering, Aalim Muhammed Salegh College of Engineering, Chennai, Tamil Nadu, India[2]

Fourth Year B.E. Student, Department of Computer Science and Engineering, Aalim Muhammed Salegh College of Engineering, Chennai, Tamil Nadu, India[3]

Fourth Year B.E. Student, Department of Computer Science and Engineering, Aalim Muhammed Salegh College of Engineering, Chennai, Tamil Nadu, India[4]

Assistant Professor, Department of Computer Science and Engineering, Aalim Muhammed Salegh College of Engineering, Chennai, Tamil Nadu, India[5]

ABSTRACT: The rapid growth of digital education and online certification has raised serious concerns regarding academic certificate forgery, data tampering, and inefficient verification mechanisms. Traditional centralized systems are vulnerable to cyberattacks, unauthorized modifications, and single-point failures. This paper proposes a Decentralized Certificate Verification System using blockchain technology to ensure secure, transparent, and tamper-proof certificate management. The system enables institutions to issue certificates through smart contracts, stores cryptographic hashes on the blockchain, and allows instant verification using QR codes. Additional features such as digital signatures, certificate status tracking, and revocation mechanisms enhance system reliability. The proposed system significantly reduces verification time, improves security, and provides a scalable solution for modern digital certification.

KEYWORDS: Blockchain, Certificate Verification, Smart Contracts, QRCode,CryptographicHashing, Decentralization

I. INTRODUCTION

Academic certificates play a crucial role in validating a student's qualifications for employment and higher education. However, traditional certificate management systems rely heavily on centralized storage and manual verification processes, making them vulnerable to forgery, duplication, and unauthorized modification.

With the increasing demand for fast and secure verification, existing systems fail to provide real-time authentication and data integrity. Blockchain technology offers a decentralized andimmutable platform that ensures transparency and security. This paper presents a blockchain-based system to address these limitations and provide a reliable verification mechanism.

II. PROBLEM STATEMENT

Traditional certificate verification systems suffer from several limitations:
Vulnerability to certificate forgery and manipulation
Dependence on centralized databases
Time-consuming manual verification
Lack of real-time validation

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Absence of tamper detection mechanisms
These issues create inefficiencies and reduce trust in academic credentials.

III. REVIEW OF LITERATURE

Several studies have explored blockchain applications in education. Early research highlights the use of blockchain for secure credential storage and verification. Smart contracts have been widely used to automate certificate issuance and validation processes.

Existing solutions demonstrate improved security and transparency but face challenges such as scalability, cost, and user adoption. This paper builds upon these concepts by integrating QR-based verification and enhanced security features.

IV. OBJECTIVES OF THE STUDY

To develop a secure and tamper-proof certificate system
To eliminate certificate forgery using blockchain
To enable instant verification using QR codes
To ensure transparency and data integrity
To provide certificate status tracking and revocation

V. EXISTING SYSTEM

The current system relies on centralized databases and manual verification processes. Institutions store certificates either physically or digitally, and verification requires direct communication with issuing authorities.
This approach is:
Time-consuming
Prone to human error
Vulnerable to hacking and data breaches
Inefficient in detecting fake certificates

VI. PROPOSED SYSTEM

The proposed system uses blockchain technology to securely issue and verify certificates.
Key Features:
Certificates issued using smart contracts
Data stored as cryptographic hashes on blockchain
QR code-based instant verification
Tamper detection mechanism
Certificate revocation support
This ensures a decentralized, transparent, and secure system.

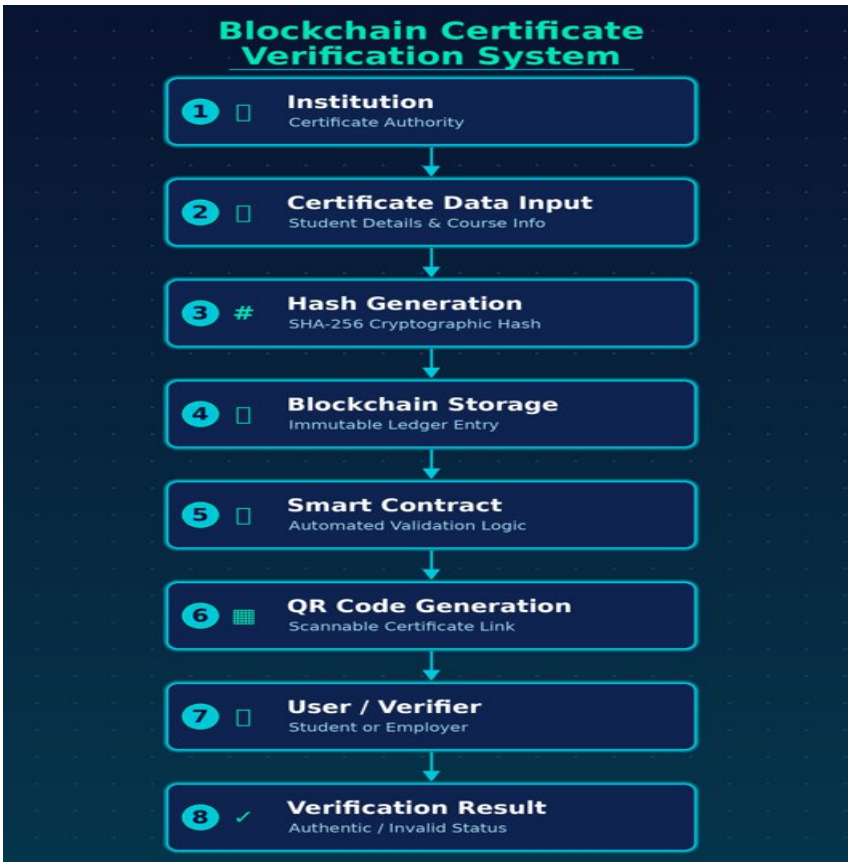
© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904279

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

VII. SYSTEM ARCHITECTURE



The system consists of three main components:
Institution Module – Issues certificates
Blockchain Layer – Stores certificate hash
User/Verifier Module – Verifies certificates
Workflow:
Institution uploads certificate details
Data is converted into a hash
Hash is stored on blockchain
QR code generated for certificate
Verifier scans QR → instant validation

VIII. METHODOLOGY

a. Technology Stack
Blockchain: Ethereum
Smart Contracts: Solidity
Frontend: HTML, CSS, JavaScript
Backend: Node.js

b. Algorithm Steps
Register institution
Input certificate data
Generate cryptographic hash (SHA-256)
Store hash on blockchain

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Generate QR code
Verify using QR scan

IX. RESULTS AND DISCUSSION

The system successfully demonstrates:
Secure certificate issuance
Instant verification through QR codes
Prevention of data tampering
Reduced verification time
Improved transparency
Compared to traditional systems, the proposed solution offers significantly higher security and efficiency.

X. ADVANTAGES

Tamper-proof data storage
Faster verification process
Reduced administrative workload
Enhanced trust and transparency
Secure and decentralized architecture

XI. APPLICATIONS

Educational institutions
Recruitment agencies
Online learning platforms
Government certification systems

XII. CONCLUSION

The proposed Decentralized Certificate Verification System effectively addresses the limitations of traditional verification methods. By leveraging blockchain technology, the system ensures data integrity, transparency, and real-time verification. It reduces fraud, improves efficiency, and provides a scalable solution for modern digital certification systems.

© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904279

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

XIII. FUTURE ENHANCEMENTS

Integration with mobile applications
Multi-chain support for scalability
AI-based fraud detection
Decentralized identity (DID) integration

XIV. LIMITATIONS

Blockchain transaction cost
Requires technical knowledge
Scalability challenges in large-scale systems

REFERENCES

1. Sharples, M., & Domingue, J. (2016). Blockchain in Education
2. Grech, A., & Camilleri, A. (2017). Blockchain for Education
3. Turkanović, M. et al. (2019). EduCTX Blockchain System
4. Ethereum Whitepaper
5. Recent IEEE papers on Blockchain Applications

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com