# Digital Certificate Verification System by Blockchain Technology

Bhagyashri Bhoyar[1], Kalyani Pal[2], Sakshi Nikhade[3], Sayali Gotefode[4], Muskan Bankar[5], Prof. Rakesh Jambhulkar[6]

[1'2'3'4'5] *UG Student, Department of Computer Engineering, Manoharbhai Patel Institute of Engineering and Technology, Shahapur*

[6] *Project Guide, Department of Computer Engineering, Manoharbhai Patel Institute of Engineering and Technology, Shahapur*

***Abstract*—The digital certificate verification system is a blockchain-based solution designed to provide a secure, efficient and transparent way to verify digital certificates. Traditional certificate verification methods are plagued by security risks, inefficiencies and lack of transparency, leading to loss of trust, financial losses and reputational damage. This paper leverages blockchain technology to address these challenges, ensuring the authenticity and integrity of digital certificates. The digital certificate verification system enhances security, improves efficiency and increases transparency, providing a reliable solution for industries and organizations to manage digital certificates. By eliminating intermediaries and enabling real-time verification, the system reduces costs and enhances trust and credibility in digital certificates.**

***Index Terms*—Blockchain, Document Verification, Digital Certificate, Smart Contract, SHA256, QR Code.**

## I. INTRODUCTION

In today's digital age, the use of digital certificates has become increasingly prevalent across various industries, including education, healthcare, finance and government. These certificates serve as a crucial means of verifying identity, authenticity and qualifications. However, traditional certificate verification methods are often plagued by security risks, inefficiencies and lack of transparency. The digital certificate verification system, built on blockchain technology, offers a robust solution to these challenges, ensuring secure, efficient and transparent verification of digital certificates. By utilizing smart contracts, we automate the verification process, ensuring the authenticity and integrity of certificates. This solution eliminates intermediaries, reduces administrative overhead and enables real-time verification.

## II. LITERATURE REVIEW

Jiin-Chiou Chen et al. [1] proposed a digital certificate system based on blockchain technology using unmodifiable blockchain properties to create anti-counterfeit and verifiable digital certificates with QR-code and inquiry string codes. Austin Draper et al. [2] studied popular security applications in Blockchain, presenting major problems and emerging challenges for future research. Marco Baldi et al. [3] proposed a solution using public ledgers based on blockchain where multiple certificate authorities share a public, decentralized ledger for certificate revocation lists. Santosh Pandey et al. [4] introduced BlockSIM, a comprehensive open-source blockchain system simulation tool. Christopher Ehmke et al. [5] proposed a lightweight and scalable blockchain protocol enabling transaction validation without downloading the whole blockchain. S. Sunitha Kumara and D. Saveetha [6] proposed a system for uploading degree certificates and behavior activities using personal ID to blockchain. Further works [7–15] extended blockchain-based certificate verification to decentralized identity management, IPFS integration, and smart contract-based authenticity checks.

## III. PROPOSED SYSTEM

### Problem Definition

In the existing system, the problem of fake certificates is a significant issue. Companies hiring thousands of freshers spend large amounts of money to get the educational certificates and transcripts of applicants verified. To address this problem, the implementation of a Digital Certificate System for verification of educational certificates using blockchain technology is proposed.

### Objectives

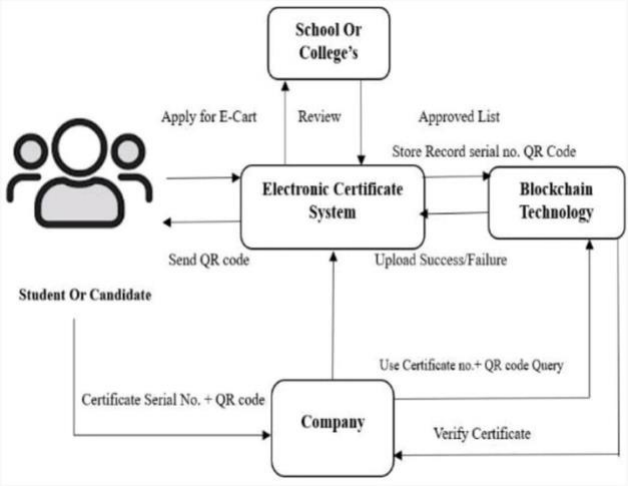
- To enhance security, improve efficiency, increase transparency, and reduce cost.
- To create a secure and efficient certificate verification system that combats certificate forgery in the education sector.
- To store certificate data securely using blockchain technology, with digital signatures and QR codes stored in an immutable manner.

### Algorithms

Smart Contract: Smart contracts are programs stored on a blockchain that run when predetermined conditions are met. They typically are used to automate the execution of an agreement so that all participants can be immediately certain of the outcome. SHA-256 Hash Generation: SHA-256 stands for Secure Hash Algorithm 256-bit and is used for cryptographic security. Cryptographic hash algorithms produce irreversible and unique hashes, minimizing the chance that two values will create the same hash.

**Architecture**

The Digital Certificate Verification System is designed using a blockchain-based decentralized architecture that ensures secure issuance, storage, and verification of digital certificates. The system architecture consists of multiple interacting components including educational institutions, blockchain network, certificate storage, verification module, and end users. Certificates issued by educational institutions are converted into digital




records and stored securely using blockchain technology. Each certificate is associated with a unique cryptographic hash and QR code that enables instant verification by employers or other organizations.

*Fig. 1: Architecture of System*

## IV. RESULT

To implement a decentralized application and designed a certificate system based on custom blockchain. The system addresses features of incorruptibility, encryption, and trackability, and permits data synchronization. The implementation improves operational efficiency by 85–90% at each stage. The proposed system saves on paper, cuts management costs, prevents document forgery, and provides accurate and reliable information on digital certificates.

## V. CONCLUSION

The Digital Certificate Verification System based on blockchain technology provides a secure, transparent, and efficient solution for managing and verifying digital certificates. Traditional certificate verification methods are often slow, expensive, and vulnerable to fraud. By leveraging blockchain technology, the proposed system eliminates many of these limitations. The decentralized architecture of blockchain ensures that certificate records remain secure, immutable, and accessible for verification at any time. The integration of smart contracts automates the verification process, significantly reducing administrative effort and verification time. Additionally, the use of cryptographic hashing and QR code technology enhances the usability and reliability of the system. In the future, the system can be further enhanced by integrating advanced technologies such as artificial intelligence, decentralized identity management, and distributed storage solutions.

## REFERENCES

[1] J.-C. Chen, N.-Y. Lee, C. Chi, and Y.-H. Chen, "Blockchain and Smart Contract for Digital Certificate," Proc. IEEE ICASI, 2018.

[2] A. Draper et al., "Security Applications and Challenges in Blockchain," IEEE ICCE, 2019.

[3] M. Baldi et al., "Certificate Validation through Public Ledgers and Blockchains," ITASEC17, 2017.

[4] S. Pandey et al., "BlockSIM: A practical simulation tool for optimal network design," IEEE ICBC, 2019.

[5] C. Ehmke, F. Wessling, and C. M. Friedrich, "Proof-of-Property – A Lightweight and Scalable Blockchain Protocol," IEEE WETSEB, 2018.

[6] S. Sunitha Kumara and D. Saveetha, "Blockchain and Smart Contract for Digital Document Verification," 2020.

[7] M. Aldwairi, M. Badra, and R. Borghol, "DocCert: Nostrification, Document Verification and Authenticity Blockchain Solution," 2023.

[8] T. Rahman et al., "Verifi-Chain: A Credentials Verifier Using Blockchain and IPFS," 2023.

[9] M. Rahman et al., "Blockchain-based certificate authentication system with enabling correction," 2023.

[10] Y. Abu Hammoudeh et al., "Digital Certificate Validation Using Blockchain: A Survey," Proc. ICIT, 2023.

[11] A. Geethakumari and C. Sweethapreethi, "Educational Certificate Verification Using Blockchain Based Framework," Int. J. Adv. Comput. Sci. Appl., vol. 12, no. 4, 2021.

[12] M. Toorani and C. Gehrmann, “A Decentralized Dynamic PKI based on Blockchain,” arXiv:2012.15351, 2020.

[13] H. Kinkelin et al., “Hardening X.509 Certificate Issuance using Distributed Ledger Technology,” arXiv:2004.07063, 2020.

[14] J.-C. Cheng, N.-Y. Lee, C. Chi, and Y.-H. Chen, “Blockchain and Smart Contract for Digital Certificate,” IEEE ICASI, 2018, pp. 1046–1051.

[15] L. S. B. S. Hossain, M. I. Ali, and D. S. R. Ghosh, “Blockchain-Based Digital Certificate Management System,” IJCSNS, vol. 18, no. 7, pp. 121–127, 2018.