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 5, Issue 11, April 2025
Impact Factor: 7.67

# Securing Academic Credentials: A Systematic Literature Review of Blockchain-Based Verification Systems

**Stuti Bhajipale[1], Prof. Shubhkirti Bodkhe[2], Prof. Mrunali Jadhav[3]**
U.G. Student, Department of Computer Science and Engineering[1]
Professor, Department of Computer Science and Engineering[2,3]
Tulsiramji Gaikwad-Patil Institute of Engineering & Technology, Mohgaon, Nagpur, Maharashtra, India
stutibhajipale@gmail.com, shubhkirtibodkhe@gmail.com, mrunalijadhav2018@gmail.com

**Abstract:** *In this paper, we present a blockchain-based certificate verification system for academic and professional certificates. Current methods of certificate verification are slow, centralized, and vulnerable to forgery. Utilizing blockchain technology, our system guarantees data permanence, decentralization, and openness, enabling employers, universities, and certification agencies to verify the validity of certificates in real-time. We implement a smart contract-based system on Ethereum and compare its performance. Our solution cuts verification time, does away with third-party dependencies, and provides a tamper-proof way to store digital credentials.*

*Through the use of smart contracts, our solution enables trusted institutions to issue tamper-proof certificates stored on a public blockchain, allowing for instant and trustworthy verification by employers and other third parties. The system reduces the need for manual verification, greatly minimizes the risk of forgery, and maintains data integrity by storing immutable certificate records. We design and test our system based on Ethereum and smart contracts and prove that it is a highly secure, efficient, and scalable replacement for common verification procedures. The method also unveils the groundbreaking potential of blockchain in reengineering credential validation within educational, business, and government institutions.*

**Keywords:** Block Chain, Digital Certificates, Confidentiality, Reliability, Availability

## I. INTRODUCTION

The authentication of academic qualifications, professional certifications, and other types of credentials has been an essential process in various industries like education, healthcare, finance, and government services. With the world rapidly shifting towards digital communication and globalization, fast, secure, and efficient verification mechanisms are more important than ever. Most traditional methods of certificate verification are manual, centralized, time-consuming, and vulnerable to errors or tampering. Such systems are usually based on direct contact with the issuing organization or third-party verification solutions, adding associated costs, latency, and failure points. In addition, certificate forgery, falsification, and document tampering cases have been increasing steadily, causing severe repercussions like the employment of unqualified staff, financial scams, and loss of institutional reputation.

Blockchain technology provides an optimistic solution to the above problems. Utilizing its inherent properties — decentralization, immutability, transparency, and security — blockchain has the potential to develop a reliable and efficient system for certificate issuance and verification. Blockchain-issued certificates are recorded on a permanent, distributed ledger and can be verified at any point without reliance on the availability or presence of the issuer. This decentralized system eliminates the requirement for intermediaries, cuts verification time from days to seconds, and guarantees that credentials cannot be tampered with or forged once they are recorded.

This work introduces a blockchain certificate validation system that employs smart contracts to mechanize certificate issuance and verification. Institutions will issue certificates in a digital form by putting them on the blockchain, where a

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 5, Issue 11, April 2025
Impact Factor: 7.67

secure storage of each unique hash of every certificate is kept. Verifiers like employers or educational institutions can verify instantly the genuineness of any certificate by inquiring with the blockchain. Our system seeks to upgrade security, simplify the verification process, and construct a more reliable digital credentials ecosystem.

The remainder of the paper is structured as follows: Section II presents related work in blockchain-based credential systems. Section III describes the system architecture and components proposed. Section IV describes the system design and functionality of smart contracts. Section V offers the implementation and results of experiments. Lastly, Section VI concludes the paper and presents directions for future work.

## II. LITERATURE SURVEY

Certificate verification is an essential process across different industries, especially in education and employment. The traditional method of verification of credentials has been through centralized systems that are slow, inefficient, and vulnerable to security breaches. These types of systems are based on direct communication with the issuing institution or a third-party verification agency, which tends to cause huge delays and is costly. Additionally, centralized systems can be accessed through cyber-attacks, tampered with, and forged, questioning the integrity of the data being verified. With blockchain technology coming to the forefront, new avenues have opened up for offering secure, transparent, and decentralized solutions for overcoming these issues.

In [Koutroumpouchos et al., 2020], the authors suggested a blockchain-based smart contract system specific to the healthcare sector for verifying credentials. The system enables healthcare practitioners to digitally validate their qualifications, e.g., medical degrees or certifications, to employers or regulatory bodies. The research illustrates that the blockchain-based system minimizes administrative burden and accelerates hiring since verifiers can immediately authenticate the credentials. In addition, utilizing smart contracts guarantees that the validity of the certificate is verified automatically, without the necessity of manual verification.

In [Zohdy et al., 2019], the authors implemented a decentralized application (DApp) for management of academic certificates using Ethereum. The DApp enables educational institutions to issue certificates via smart contracts and gives students an effortless means to present their authenticated credentials to employers or other institutions. The authors explained how certificate issuance, verification, and checks for expiration are automated through smart contracts, making the certification process more efficient and reliable.

Smart contracts also have a huge contribution in automating the process of verification so that they only accept valid certificates. By incorporating business logic into the smart contracts, the system is able to undertake complex operations such as ensuring that the certificate's validity date is in effect, ensuring the identity of the issuer, and even ensuring that certain conditions are met, such as whether the certificate has been suspended or revoked.

## III. METHODOLOGY

The approach to creating a blockchain-based certificate verification system is centered on the design, development, integration, and testing of the system. This involves choosing the right blockchain platform, designing the system architecture, developing the smart contracts, providing privacy protection mechanisms, deploying the system in phases, and thoroughly testing the system prior to its deployment in a real-world environment.

### 1. System Design and Architecture

The initial task in designing the blockchain-based certificate authentication system is to create the overall architecture and know the components, requirements, and functions of the system. It determines the high-level design of the system as well as communication between the components.

### A. System Requirements

The system should facilitate the issuance, verification, and management of certificates in a decentralized, secure, and transparent way. It should be capable of:

- Enabling educational institutions and certification bodies to issue certificates to individuals.

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 5, Issue 11, April 2025
Impact Factor: 7.67

- Storing certificate information securely and immutably on the blockchain.
- Facilitating verifiers (e.g., employers or educational institutions) to verify certificates efficiently and reliably.
- Offering an interface for users to query certificate information without sacrificing privacy or security.

**B. Data Storage Strategy:**

Since blockchain does not have much storage capacity for big datasets, sensitive data pertaining to certificates (such as personal information, grades, or contents of certificates) will not be stored on the blockchain. However, the hash of the certificate data (e.g., the certificate ID and other metadata) will be stored on the blockchain. The complete certificate information will be kept safely in an off-chain decentralized storage solution, like Interplanetary File System (IPFS) or a proprietary cloud-based system. The IPFS links (which are hashed cryptographically) will be kept on the blockchain to guarantee the integrity of the certificate.

System Components: The most important system components are:

- Certificate Issuance Interface: A UI for certified staff in institutions to issue certificates.
- Blockchain Network: A distributed network (Ethereum in our context) where the data of certificates (hashes) and transactions are kept.
- Certificate Verification Interface: A UI for verifiers to inquire from the blockchain to confirm the legitimacy of certificates.
- Off-Chain Storage: An incentivized storage solution (e.g., IPFS) where certificate data is deposited in detail and linked to its blockchain hash.

**2. Smart Contract Development**

Smart contracts are self-executing pieces of code run on the blockchain that automate, verify, and enforce the terms of a contract. In this system, smart contracts will oversee every aspect of the life cycle of a certificate, from creation to verification and cancellation.

**A. Smart Contract for Certificate Issuance:**

The initial smart contract to be built will issue certificates. The contract will have the following functions:

Register information about a certificate, including certificate ID, recipient information, issuer information, issuance date, and other data as required.

Compute a cryptographic hash of the certificate content

Store the certificate hash on the blockchain along with metadata like the certificate issuer and timestamp.

Enable certificate holders to provide their certificate information to employers or institutions by pointing to the hash of the certificate on the blockchain.

**B. Smart Contract for Certificate Validation:**

The second smart contract will enable third-party verifiers (employers, other institutions) to verify the validity of a certificate. The contract will:

Accept a query with the public key of the holder or the certificate ID.

Get the hash of the certificate from the blockchain.

Compare the given certificate's hash with the stored blockchain hash.

Return the verification result to the verifier, stating whether the certificate is valid or not.

## IV. SYSTEM ARCHITECTURE

**A. Overall Architecture Overview**

The architecture relies on a client-server model with the blockchain acting as the infrastructural core. The infrastructure consists of three major modules:

- Certificate Issuance Module: The module is responsible for the creation, storage, and issuance of certificates by qualified institutions.

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 5, Issue 11, April 2025
Impact Factor: 7.67

- Certificate Verification Module: The module is utilized by the verifiers (e.g., employers or other educational institutions) to verify whether a certificate is valid.
- Blockchain Layer: The blockchain offers a decentralized, transparent, and immutable ledger for managing and verifying certificates

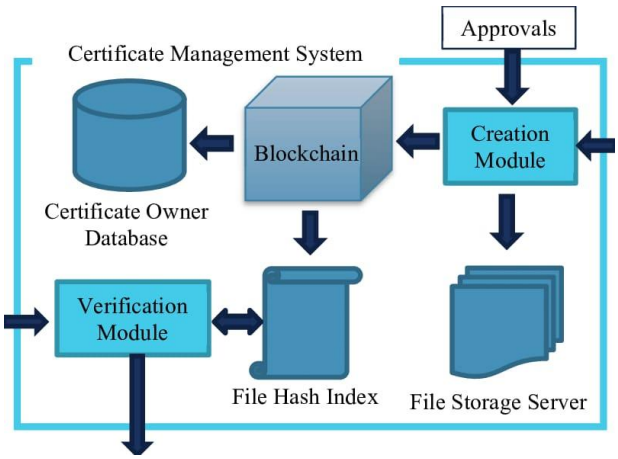


Fig.01 Architecture

.

**B. Blockchain Layer**

The blockchain layer is the foundation of the system. The Ethereum blockchain is applied in this architecture given its strong capability in processing smart contracts and its popularity in being utilized for decentralized applications (DApps). The blockchain serves the following purposes:

- Certificate Storage: The blockchain only stores the hashes of the certificates and metadata like the certificate ID, issuer information, and timestamp. It is transparent, as any certificate's hash is publicly verifiable and tamper-proof.
- Smart Contracts: The smart contracts on the Ethereum blockchain manage the logic for certificate issuance, validation, revocation, and expiration. The smart contracts:

Process the issuance of certificates by registering them on the blockchain along with attached metadata.

Provide facilities for verifiers to query the blockchain and verify the validity of certificates by matching the stored hash on the blockchain with the certificate hash presented by the holder.

Provide facilities for revocation and expiration of certificates so that invalid or expired certificates cannot be verified.

## V. CONCLUSION

The conventional certificate verification processes tend to be slow, expensive, and prone to forgery. The suggested blockchain-based certificate verification system overcomes these challenges by providing a secure, transparent, and tamper-evident solution. Utilizing the decentralized and immutable properties of blockchain technology, certificates can be issued, verified, and controlled with high trust and efficiency.

The system architecture makes use of smart contracts on the Ethereum blockchain to self-automate the issuance and verification processes, with sensitive certificate information being safely stored off-chain with the use of decentralized storage systems such as IPFS. The combination of these two architectures keeps the system transparent as well as private. Extra security mechanisms such as cryptographic hashing, role-based access control, and zero-knowledge proofs further add robustness and confidentiality to the system.

With this system, institutions and certifying agencies can issue credentials that can be easily verified by employers and other stakeholders without the possibility of forgery. Blockchain also eliminates the use of intermediaries, thus saving on costs and verification time.


DOI: 10.48175/IJARSCT-25804

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 5, Issue 11, April 2025
Impact Factor: 7.67

In summary, the blockchain certificate verification system offers an innovative solution that not only updates credential management but also sets a new standard for trust, security, and accessibility in educational and professional settings. Enhancements in the future, including the integration of more efficient blockchain platforms and linking with national education data banks, would further enhance the system's acceptance and influence.

## VI. FUTURE SCOPE

The blockchain certificate verification system is a revolutionary way of securing academic and professional qualifications. Nevertheless, there is tremendous scope for expansion and extension in the future. One of the key areas of development is linking the system to national and global education and professional databases. By forging alliances with universities, government agencies, and accrediting agencies worldwide, the system could emerge as a global platform for validating educational qualifications. Such unification would not only make the verification process uniform across borders but also much more rapid and secure for employers, institutions, and students.

Another significant area of future research is the use of more scalable and energy-efficient blockchain platforms. With advancing technology, newer blockchain networks like Ethereum 2.0, Polygon, or even private blockchains optimized for academic purposes could be utilized to increase transaction speed, lower operational costs, and enhance environmental sustainability. These enhancements would be essential in processing large numbers of certificate transactions while preserving the decentralized and secure aspect of the system.

## VII. ACKNOWLEDGMENT

I would like to express my heartfelt gratitude to my guide, Prof. Shubhkirti Bodkhe and Prof.Mrunali Jadhav for his invaluable guidance and support incompleting my project. I also extend my sincere thanks to the Head of the Department, Dr.Lawlesh N. Yadav and all the professors for providing me with the necessary facilities and support throughout this endeavor.

Miss Stuti Bhajipale

## REFERENCES

**[1].** Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from https://bitcoin.org/bitcoin.pdf

**[2].** Wood, G. (2014). Ethereum: A Secure Decentralised Generalised Transaction Ledger. Ethereum Project Yellow Paper.

**[3].** Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain Technology: Beyond Bitcoin. Applied Innovation Review, 2, 6–10.

**[4].** Zyskind, G., & Nathan, O. (2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data. In 2015 IEEE Security and Privacy Workshops (SPW), 180–184.

**[5].** Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2018). A Survey on the Security of Blockchain Systems. Future Generation Computer Systems, 107, 841–853.

**[6].** Shahaab, A., Lidgey, B., Hewage, C., & Khan, I. (2020). Blockchain-Based Smart Contracts: Applications and Challenges. Journal of Network and Computer Applications, 149, 102454.

**[7].** Benet, J. (2014). IPFS - Content Addressed, Versioned, P2P File System. arXiv preprint arXiv:1407.3561.

**[8].** Zhang, P., White, J., Schmidt, D. C., Lenz, G., & Rosenbloom, S. T. (2018). FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data. Computational and Structural Biotechnology Journal, 16, 267–278.

**[9].** Swan, M. (2015). Blockchain: Blueprint for a New Economy. O'Reilly Media, Inc.

**[10].** Christidis, K., & Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. IEEE Access, 4, 2292–2303.

**[11].** Tapscott, D., & Tapscott, A. (2016). Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World. Penguin.

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 5, Issue 11, April 2025
Impact Factor: 7.67

**[12].** Lin, I. C., & Liao, T. C. (2017). A Survey of Blockchain Security Issues and Challenges. International Journal of Network Security, 19(5), 653–659.

**[13].** Jha, S., Rajput, S., & Tiwari, P. (2019). Blockchain Technology for Certification and Digital Diploma Validation. International Journal of Recent Technology and Engineering (IJRTE), 8(4S2), 750–754.

**[14].** Alammary, A., Alhazmi, S., Almasri, M., & Gillani, S. (2019). Blockchain-Based Applications in Education: A Systematic Review. Applied Sciences, 9(12), 2400.

**[15].** Rouhani, S., & Deters, R. (2019). Security, Performance, and Applications of Smart Contracts: A Systematic Survey. IEEE Access, 7, 50759–50779.

**[16].** Bhaskaran, S., & Chang, V. (2020). Blockchain for Higher Education Certifications. In Handbook of Research on Blockchain Technology (pp. 270–284). IGI Global.

**[17].** Ferrag, M. A., Maglaras, L., Derhab, A., & Janicke, H. (2019). Blockchain Technologies for the Internet of Things: Research Issues and Challenges. IEEE Internet of Things Journal, 6(2), 2188–2204.

**[18].** Omar, A. A., Jayaraman, R., Salah, K., Simsekler, M. C. E., Yaqoob, I., & Ellahham, S. (2019). Trustworthy Smart Contracts for Healthcare Systems on the Blockchain. Journal of Healthcare Engineering, 2019

**[19].** Chen, S., Shi, R., Ren, Z., & Yan, J. (2018). A Blockchain-Based Certificate Authentication System. Proceedings of the 2018 27th International Conference on Computer Communication and Networks (ICCCN), 1–7