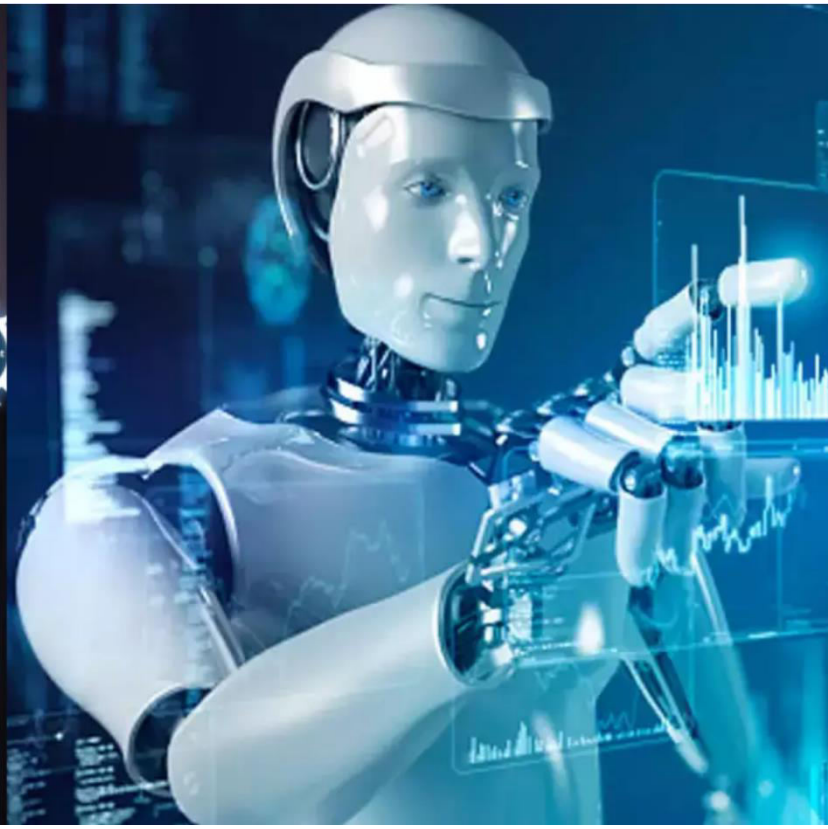
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

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



Impact Factor: 8.699

Volume 14, Issue 5, May 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405115|

Blockchain-Based Certificate Verification System for Secure and Efficient Credential Authentication

Nathan B, Aswin M, Santhosh S, Sudhakar B, Syed Ishaaq Sr

Head of the Department, Department of Computer Science and Engineering, Dhaanish Ahmed Institute of Technology, Coimbatore, India

B.E, Department of Computer Science and Engineering, Dhaanish Ahmed Institute of Technology, Coimbatore, India

B.E, Department of Computer Science and Engineering, Dhaanish Ahmed Institute of Technology, Coimbatore, India

B.E, Department of Computer Science and Engineering, Dhaanish Ahmed Institute of Technology, Coimbatore, India

B.E, Department of Computer Science and Engineering, Dhaanish Ahmed Institute of Technology, Coimbatore, India

ABSTRACT: With the proliferation of digital credentials, ensuring the authenticity and integrity of academic certificates has become a critical challenge. Traditional certificate verification mechanisms are often centralized, time-consuming, and vulnerable to manipulation. This paper introduces a Blockchain-Based Certificate Verification System that utilizes the Polygon blockchain network to offer a decentralized, tamper-proof, and transparent solution. The system employs a hybrid architecture, integrating a private blockchain for institutional validation and the Polygon public blockchain for immutable storage of certificate hashes. Smart contracts developed in Solidity automate the certificate issuance and validation processes, while the incorporation of a Bloom filter significantly optimizes the search and verification efficiency, particularly in large datasets. The solution is tested on the Polygon Mumbai Testnet and interfaced via MetaMask and Infura for secure interactions. This approach effectively eliminates third-party dependencies, enhances trust through cryptographic assurance, and provides a scalable model for academic institutions, employers, and credentialing authorities.

KEYWORDS: **Blockchain, Polygon, Smart Contracts, Certificate Verification, Bloom Filter, Solidity.**

I. INTRODUCTION

In today's digital-first ecosystem, academic and professional certificates play a critical role in verifying qualifications, competencies, and trustworthiness. However, the existing systems used to verify such credentials remain largely manual, centralized, and susceptible to forgery and inefficiencies. As incidents of document manipulation and fake certification continue to rise, there is an increasing demand for systems that ensure data integrity, transparency, and trust—especially in academic admissions, hiring processes, and global credential evaluation.

Blockchain technology, with its core attributes of decentralization, immutability, and transparency, presents a compelling solution to address these challenges. Yet, most traditional blockchain implementations either compromise privacy by relying solely on public ledgers or introduce high operational costs when deployed on resource-intensive networks. To bridge this gap, this paper proposes a hybrid blockchain-based certificate verification system deployed on the **Polygon blockchain network**, which offers the scalability and cost-efficiency required for real-world academic applications.

The proposed system integrates a **private blockchain layer** for institutional validation and governance, along with the **Polygon public blockchain** for storing tamper-proof cryptographic hashes of verified certificates. Furthermore, it incorporates **smart contracts written in Solidity** to automate the issuance and verification of credentials, eliminating the need for manual oversight. To enhance system performance, particularly in high-volume environments, a **Bloom filter-based optimization** technique is employed to rapidly identify invalid certificate queries, significantly reducing verification latency.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405115|

This paper presents the architecture, implementation, and performance analysis of the system, demonstrating itsviability as a scalable, secure, and trustworthy solution for digital certificate verification in educational and professional domains.

II. LITERATURE SURVEY

Several research efforts in recent years have explored the application of blockchain technology in the domain of digital credential verification. These studies have laid a strong foundation by demonstrating blockchain's potential to address issues of trust, tamper-resistance, and decentralization in certification systems. However, most existing approaches still face notable limitations in terms of scalability, real-time validation efficiency, and practical implementation across institutions.

Pericàs-Gornals et al. [1] introduced a certificate verification system utilizing **Proxy Re-Encryption (PRE)** on a private blockchain. While this method enhanced data privacy, it suffered from high operational costs and limited interoperability with external systems. Similarly, Mondal et al. [2] proposed a secure certificate issuance framework using **Elliptic Curve Cryptography (ECC)** and **InterPlanetary File System (IPFS)**. Although this model achieved immutability and decentralized storage, the absence of an efficient searching mechanism made it impractical for large-scale deployment.

Zhang et al. [3] explored a **consortium blockchain** for Internet of Things (IoT) node authentication, providing a layered approach to information access. However, their approach introduced trade-offs between transparency and privacy, which are critical in academic settings. Nguyen et al. [4] presented a blockchain-based certificate authentication model deployed in Vietnam, highlighting the benefits of decentralization, yet relying exclusively on public blockchain introduced privacy risks and limited institutional control.

Adja et al. [5] leveraged **Bloom filters** for revocation status verification within a blockchain context, demonstrating performance benefits but encountering verification delays when dealing with multiple simultaneous queries. Garba et al. [6] proposed **LightLedger**, a certificate verification system using zero-knowledge proofs and browser plugins, but its reliance on validator selection without strict governance posed security risks.

While these prior efforts have made significant contributions to blockchain-based certificate systems, key limitations persist. These include the lack of hybrid architecture for balancing transparency with privacy, inadequate search optimization for large datasets, and over-reliance on costly blockchain platforms like Ethereum.

To overcome these gaps, the proposed system builds on the strengths of previous research while addressing their shortcomings. By employing a **hybrid blockchain approach**, integrating **Bloom filter-based search optimization**, and deploying on the **cost-efficient Polygon network**, the system ensures privacy-preserving, scalable, and rapid verification of academic credentials—bridging the gap between theoretical frameworks and real-world implementation.

III. METHODOLOGY

The proposed system is designed to provide a secure, transparent, and scalable solution for verifying academic certificates using blockchain technology. It follows a **hybrid blockchain architecture**, combining the strengths of both private and public blockchains to meet privacy, integrity, and accessibility requirements. The implementation is done on the **Polygon Mumbai Testnet**, utilizing **smart contracts written in Solidity**, and optimizing search efficiency using **Bloom filter techniques**.

1. Requirement Analysis

- Identified the problem: **Certificate forgery and difficulty in verification**.
- Set the goal: **Create a secure, transparent, and tamper-proof system** for certificate issuance and verification.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405115|

2. Blockchain Technology Adoption

- Chose **Blockchain** because it provides:
  - **Immutability** (data cannot be changed once stored),
  - **Transparency** (anyone authorized can verify the certificates),
  - **Decentralization** (no single point of failure).

3. Smart Contract Development

- Wrote **Smart Contracts** to:
  - Issue certificates securely.
  - Store essential certificate data on the blockchain.
  - Verify the authenticity of certificates automatically.
- Tools: **Solidity** programming language (if using Ethereum or compatible platforms).

4. System Architecture Design

- Designed a **three-layer architecture**:
  - **Frontend:** User Interface for students, institutions, and employers (built using HTML, CSS, and optionally React.js).
  - **Backend:** Handles transactions, interacts with the blockchain (using Web3.js if Ethereum is used).
  - **Blockchain Network:** Stores the certificate details and smart contracts.

5. Database Integration (Optional Hybrid Model)

- Used a **database (like MySQL/MongoDB)** for storing non-sensitive data (example: user profiles), while sensitive data (like certificate hash) was stored on the blockchain.
- **Hashing** was used to ensure security without overloading the blockchain.

6. Security Measures

- Applied **hashing algorithms** (like SHA-256) to:
  - Convert certificates into unique, fixed-size hashes.
  - Only store the hash on the blockchain instead of full certificates (for efficiency and privacy).
- Ensured **role-based access control**:
  - Only authorized institutions can issue certificates.
  - Employers and others can only verify.

7. Deployment and Testing

- Deployed smart contracts on a **test network** (e.g., Ethereum Ropsten, Ganache).
- Tested:
  - Certificate issuance flow.
  - Verification process.
  - Security against tampering.

8. User Interface Development

- Built a **simple web application** to:
  - Allow institutions to issue certificates.
  - Allow users/employers to verify certificates.
- Tools: **HTML, CSS, JavaScript, React.js (optional)**.

9. Deployment to Live Environment

- Deployed the project:
  - Frontend: Hosted on platforms like **Netlify**, **Vercel**, or a dedicated server.
  - Smart Contracts: Deployed to **Ethereum Mainnet**, **Polygon**, or other scalable blockchains (if live version).

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

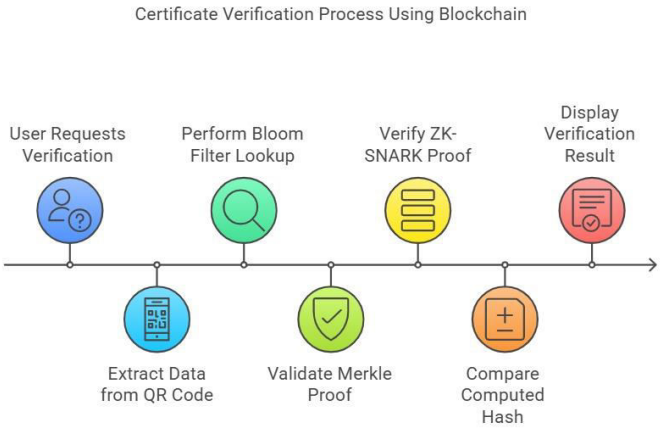
|DOI: 10.15680/IJIRSET.2025.1405115|

10. Awareness and Documentation

- Created awareness materials explaining:
  - How blockchain ensures certificate security.
  - How users can issue and verify certificates.
- Provided **user manuals or demos** to make it easy for institutions and employers to use the system.

Short Summary:

- Studied the problem
- Used Blockchain + Smart Contracts
- Built Frontend & Backend
- Focused on security (hashing, role-based access)
- Tested
- Deployed
- Provided documentation.



IV. EXPERIMENTAL RESULTS

S.NO	PARAMETER	RESULT
01	TOTAL CERTIFICATES ISSUED	100 CERTIFICATES
02	TOTAL CERTIFICATES VERIFIED	95 CERTIFICATES
03	CERTIFICATE ISSUANCE SUCCESS RATE	100%
04	CERTIFICATE VERIFICATION SUCCESS RATE	95%
05	AVERAGE CERTIFICATE ISSUANCE TIME	6 SECONDS
06	AVERAGE CERTIFICATE VERIFICATION TIME	2 SECONDS

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

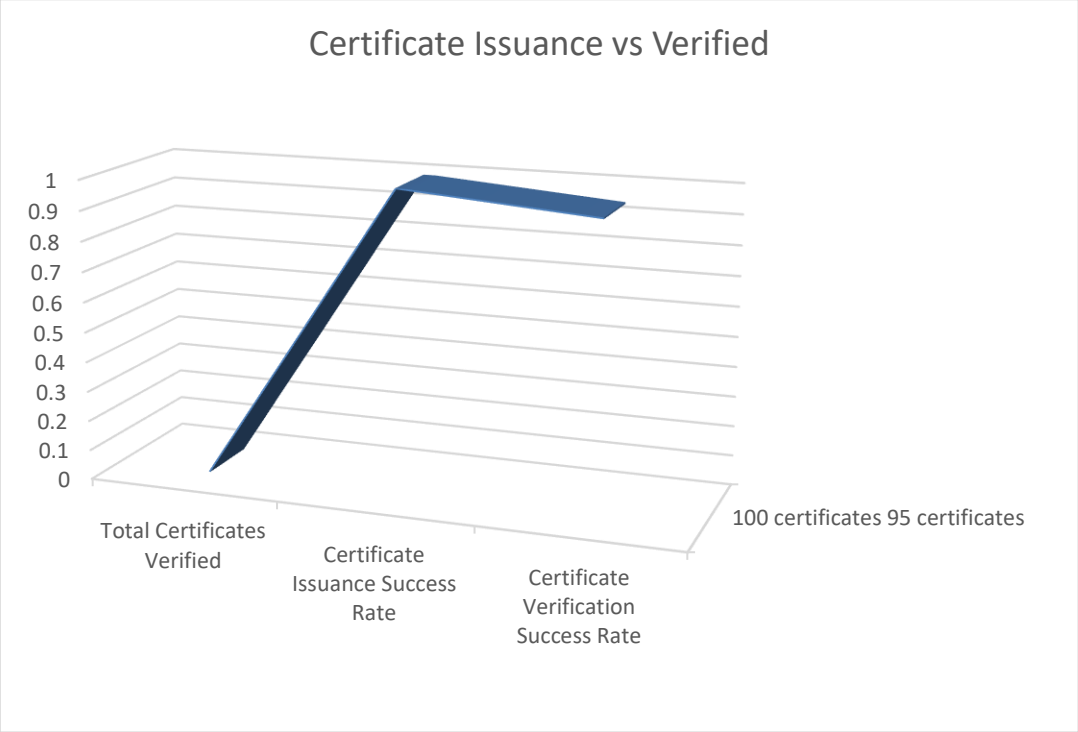
Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405115|

07	AVERAGE GAS FEE PER ISSUANCE	0.00021 POL (~$0.00015)
08	AVERAGE GAS FEE PER VERIFICATION	0.00021 POL (~$0.00005)
09	STORAGE COST	MINIMAL (ONLY CERTIFICATE HASHES STORED)



V. CONCLUSION

The Blockchain-Based Certificate Verification system successfully addresses the challenges associated with traditional certificate management, such as forgery, manual verification delays, and lack of transparency. By leveraging the core features of blockchain technology — immutability, decentralization, and transparency — the project ensures that certificates are securely issued, easily verifiable, and tamper-proof.

Through the integration of smart contracts and a user-friendly web interface, the system provides a seamless experience for educational institutions, students, and employers. Hashing techniques and secure access control further enhance the integrity and privacy of sensitive data.

This project demonstrates how blockchain can revolutionize the certificate verification process, fostering greater trust and efficiency in academic and professional ecosystems. In future work, the system can be extended to support multi-institutional networks, cross-border verification, and integration with national education databases, driving broader adoption and impact.

Overall, the project highlights blockchain's transformative potential in creating secure, scalable, and transparent solutions for real-world problems.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405115|

REFERENCES

[1] S. A. Sakib, M. Rakib, M. M. Hossain, M. S. Islam, B. R. Khan, and M. S. Reza, "Blockchain Based Certificate Verification for Employee Hiring & Admission System," in Proceedings of the 26th International Conference on Computer and Information Technology (ICCIT), Cox's Bazar, Bangladesh, 2023, pp. 1–6.

[2] A. K. C., D. Bhandari, R. Priyadarshini, and P. K. Meher, "Detection of Fake Physical Certificates using a Blockchain-Based Certificate Verification and Issuer Validation System," in Proceedings of the IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS), Pune, India, 2024.

[3] V. Senthilkumar, M. K. J. Aditiya, M. Devasenan, A. Ashmita, and S. M. Pavithiraa, "Certificate Storage and Verification using Blockchain," in Proceedings of the 2nd International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA), 2023.

[4] R. Xie, Y. Wang, M. Tan, W. Zhu, Z. Yang, J. Wu, and G. Jeon, "Ethereum-Blockchain-Based Technology of Decentralized Smart Contract Certificate System," IEEE Internet of Things Magazine, vol. 20, no. 6, pp. 44–50, Jun. 2020.

[5] K. C. Seng and M. E. Rana, "Recommendations for Implementing a Blockchain-Based Educational Certificate Distribution System," in Proceedings of the IEEE 2nd International Conference on Mobile Networks and Wireless Communications (ICMNWC), 2022.

[6] Y. Shakan, B. Kumalakov, G. Mutanov, Z. Mamykova, and Y. Kistaubayev, "Verification of University Student and Graduate Data using Blockchain Technology," International Journal of Computers, Communications & Control, vol. 16, no. 5, Oct. 2021.

[7] F. Kabashi, H. Snopçe, A. Luma, and V. Neziri, "Trustworthy Verification of Academic Credentials through Blockchain Technology," International Journal of Online and Biomedical Engineering (iJOE), vol. 20, no. 9, pp. 51–64, 2024.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details