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 8, Issue 11, November 2025

© 2025 IJMRSET | Volume 8, Issue 11, November 2025| DOI:10.15680/IJMRSET.2025.0811029

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)

BlockCertify: A Blockchain Based Certificate Generation and Verification System

Ritesh Ishwar Patil[1], Harshal Suresh Patil[2], Swapnil Hemant Chavhan[3], Kalpesh Prabhakar Khairnar[4], Prof. G P. Mohole[5]

Department of Computer Engineering, Jawahar Education Society' Institute of Technology and Research, Nashik, India[1]

Department of Computer Engineering, Jawahar Education Society' Institute of Technology and Research, Nashik, India[2]

Department of Computer Engineering, Jawahar Education Society' Institute of Technology and Research, Nashik, India[3]

Department of Computer Engineering, Jawahar Education Society' Institute of Technology and Research, Nashik, India[4]

Department of Computer Engineering, Jawahar Education Society' Institute of Technology and Research, Nashik, India[5]

ABSTRACT: The proliferation of digital documents and academic credentials in today's interconnected world has created both opportunities and vulnerabilities. Traditional certificate issuance and storage mechanisms are highly susceptible to forgery, duplication, and unauthorized manipulation, undermining the trustworthiness of academic and professional qualifications. To address these challenges, this research proposes a blockchain-based certificate generation and verification system that ensures transparency, immutability, and trust across stakeholders. Leveraging distributed ledger technology, the system securely records certificate metadata and unique identifiers, enabling real-time, tamper-proof validation without reliance on intermediaries. The architecture integrates modern web technologies such as Next.js for frontend and backend services, MongoDB for scalable storage, JWT for authentication, and cryptographic techniques including bcrypt for enhanced security. Additionally, smart contracts deployed on Ethereum/Ganache enable decentralized storage and validation, while certificate data is simultaneously linked with non-fungible tokens (NFTs) to provide verifiable ownership and authenticity. This integration not only eliminates certificate fraud but also facilitates seamless verification across institutions, employers, and regulatory authorities. By combining blockchain's decentralized security with user-friendly web applications, the proposed approach aims to create a globally interoperable, cost-effective, and future-ready framework for academic and professional certification systems.

KEYWORDS: *Blockchain, Certificate Verification, Fake Certificate Detection, Smart Contracts, Non-Fungible Tokens (NFTs), Digital Credentialing, Next.js, MongoDB, Cryptographic Security, Immutable Ledger*

I. INTRODUCTION

In the modern digital era, certificates and credentials serve as a fundamental trust mechanism across industries, academic institutions, and organizations. Whether it is a university degree, a professional training certificate, or a compliance credential, these documents represent proof of knowledge, skills, or legal entitlement. However, the reliance on traditional, paper-based, and even centralized digital systems for certificate issuance has led to a surge in fraud cases, including forged certificates, duplicate records, and unauthorized alterations. Such vulnerabilities not only damage institutional reputation but also erode trust among employers, regulators, and stakeholders. Addressing these issues requires a system that is not only secure but also transparent, verifiable, and resistant to manipulation.

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)

Blockchain technology has emerged as a powerful solution to address these long-standing challenges in credential management. By design, blockchain offers decentralization, immutability, and transparency, ensuring that once data is recorded, it cannot be altered without detection. For certificate management, this means that every issued certificate can be stored as a permanent, verifiable entry on the blockchain ledger. This tamper-proof nature makes blockchain an ideal backbone for combating certificate fraud and enabling real-time authentication. Moreover, the distributed nature of blockchain eliminates dependency on a single authority, creating a trustless environment where certificates can be independently verified by anyone with access to the ledger.

The proposed system builds on this foundation by integrating blockchain technology with modern web application frameworks and cryptographic mechanisms. Instead of relying solely on centralized university portals or third-party verification agencies, the system allows institutions to issue certificates directly onto a blockchain. Each certificate is assigned a unique identifier and bound with cryptographic security features, ensuring that forgery becomes practically impossible. Furthermore, the integration of Non-Fungible Tokens (NFTs) provides an additional layer of ownership verification, as each certificate is tokenized and linked uniquely to its rightful holder, making certificates not only secure but also digitally transferable and globally verifiable.

From a technical standpoint, the system leverages a combination of technologies to achieve robustness, usability, and scalability. Next.js serves as both the frontend and backend framework, enabling a seamless user experience for students, administrators, and verifiers. MongoDB provides a scalable database solution to manage user details and certificate metadata, while JSON Web Tokens (JWT) ensure secure authentication and controlled access to the platform. For certificate rendering and storage, tools such as docxrender and docxtopdf are employed to automate the generation of professional digital certificates in multiple formats. Blockchain integration is achieved using Ethereum's Ganache test network, where smart contracts handle certificate creation, validation, and binding with NFTs.

Beyond technical implementation, the adoption of such a system holds significant socio-economic impact. Employers, academic institutions, and even governments can benefit from a secure, efficient, and universally verifiable certificate verification mechanism. This reduces hiring risks, minimizes bureaucratic delays, and strengthens global collaboration in education and workforce mobility. Moreover, the scalability of blockchain ensures that the solution can grow across institutions, countries, and even industries without sacrificing security or interoperability. By providing a unified, tamper-proof verification framework, the system not only enhances trust but also addresses global challenges in education and credential management.

II. LITERATURE REVIEW

1. Immutable Digital Recognition via Blockchain (2025).
This recent work addresses the heterogeneity in certification systems by introducing a hybrid model that combines NFTs, RSA blind signatures, and distributed storage to balance uniqueness, authority, and regulatory compliance. The authors argue that fully decentralized certificate frameworks often conflict with legal requirements, so their hybrid approach retains certain centralized oversight functions while preserving blockchain's immutability. Their system demonstrates practical pathways for global adoption, offering tamper-proof credentialing with auditability and compliance, making it a forward-looking solution for next-generation academic certification systems.[1]

2. Decentralized Certificate Issuance and Verification System (2025).
TR Sree proposes an Ethereum-based framework for decentralized issuance and validation of certificates, focusing on lifecycle management including creation, verification, and revocation. The paper highlights how smart contracts can automate interactions between issuers, holders, and verifiers, reducing reliance on intermediaries. Empirical analysis of gas fees, scalability, and latency provides insights into the trade-offs of blockchain deployment in real-world education contexts. This contribution demonstrates how practical blockchain implementations are maturing and becoming cost-competitive with traditional centralized solutions.[2]

3. Blockchain-based Authentication and Verification System for Academic Certificates using QR Code and DApps (2024).
This study introduces a user-friendly approach where certificates are linked to QR codes, enabling verifiers to scan and confirm authenticity through a decentralized application (DApp). By combining blockchain immutability with mobile accessibility, the system bridges the gap between technical robustness and usability. The work emphasizes integration

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)

into institutional workflows and highlights challenges in adoption, such as network costs and end-user awareness. Its novelty lies in merging blockchain verification with an intuitive, low-barrier verification mechanism.[3]

4. Verifi-Chain: A Credentials Verifier using Blockchain and IPFS (2023).
Verifi-Chain presents a cost-effective hybrid solution where certificates are stored in IPFS while blockchain records only the metadata hash, ensuring tamper-proof validation with reduced storage overhead. The architecture enables efficient large-scale deployments by addressing blockchain's scalability issues. The authors showcase a prototype where verifiers can independently fetch and validate certificates, proving both technical feasibility and economic sustainability. This work is significant for institutions seeking affordable yet secure verification solutions.[4]

5. Student Certificate Sharing System Using Blockchain and NFTs (2023).
This paper explores the use of NFTs for certificate storage and selective sharing, positioning students as the ultimate custodians of their credentials. Certificates are minted as tokens, allowing secure, transparent, and transferable proof of ownership. The authors highlight advantages such as student autonomy, prevention of duplication, and simplified cross-border validation. However, they acknowledge challenges in adoption due to regulatory uncertainties and limited institutional readiness. This research reflects the growing trend of blending blockchain with tokenization to empower learners.[5]

6. DocCert: Nostrification, Document Verification and Authenticity Blockchain Solution (2023).
DocCert broadens the scope of blockchain credentialing by addressing verification of foreign academic and professional documents, also known as "nostrification." The system leverages permissioned blockchain to allow trusted authorities to register verifiable documents while ensuring privacy and controlled access. The authors focus on legal and interoperability concerns, showing how blockchain can streamline international credential validation. This work contributes significantly to solving cross-border verification, a pressing issue in globalized education and employment.[6]

7. EduChain: A Blockchain-based Education Data Management System (2023).
EduChain proposes a two-layer blockchain framework that separates private institutional records from public verification functions, striking a balance between confidentiality and transparency. The system introduces secondary consensus mechanisms to ensure data consistency between off-chain databases and blockchain states. Evaluations highlight how this hybrid model improves traceability and scalability. By addressing data integrity and interoperability, EduChain provides a strong foundation for building large-scale, secure educational ecosystems.[7,16]

8. Blockchain Based Certificate Authentication System with Enabling Correction (2023).
This paper tackles a practical issue often ignored in blockchain systems certificate corrections. Instead of rewriting blockchain records, the authors propose generating new blocks that reference original entries, maintaining audit trails while allowing corrections. This innovative approach provides flexibility for institutions while preserving blockchain's tamper-evident nature. The system represents a pragmatic adaptation of immutability, aligning technology with real-world academic requirements.[8]

9. Blockchain Based Certificate Verification System (Management) (2023).
This research focuses on enhancing certificate revocation management using blockchain to overcome limitations in conventional PKI mechanisms like CRLs and OCSP. By decentralizing revocation processes, the proposed framework ensures higher resilience against fraud and downtime. The authors extend metadata fields in certificates to support efficient status checks and demonstrate improved reliability. This work is especially relevant for developing dynamic verification systems that need to adapt to changing validity statuses.[9]

10. Singh & Kim – Blockchain-Based Academic Certificate Verification System (2019).
This foundational work highlights how blockchain can secure academic certificate issuance by ensuring immutability and decentralized verification. Through Ethereum smart contracts, the system enables automated certificate creation and querying, reducing risks of forgery and administrative overhead. Although the paper identifies scalability and cost limitations in public blockchains, it set a significant benchmark for subsequent innovations.[10-14]

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)

II. FINDINGS OF LITERATURE REVIEW

The literature reviewed highlights a consistent trend toward adopting blockchain as a secure, tamper-proof mechanism for managing academic and professional certificates. Across recent works (2023–2025), researchers increasingly focus on hybrid models that combine blockchain with decentralized storage (e.g., IPFS) or tokenization (NFTs) to improve scalability, reduce cost, and enhance user control. For instance, studies such as Verifi-Chain and EduChain demonstrate how off-chain storage reduces blockchain overhead, while NFT-based solutions emphasize student autonomy and global certificate portability. At the same time, newer works like Immutable Digital Recognition (2025) and DocCert (2023) address practical challenges such as regulatory compliance, international verification (nostrification), and controlled corrections to immutable data. These modern innovations reveal a shift from proof-of-concept systems to more deployable, standards-driven frameworks.

Earlier studies (2016–2019) primarily established blockchain's feasibility for credentialing by focusing on immutability, smart contracts, and decentralization [1]. Foundational works such as Singh & Kim (2019), Pokhrel & Choi (2019), and EduCTX (2018) [15] proved blockchain's ability to eliminate forgery and reduce verification delays, but also identified key challenges including high gas costs, scalability limitations, and lack of interoperability. Surveys and conceptual works, including Gill et al. (2019) and Sharples & Domingue (2016) [16-18], broadened the scope by exploring applications like plagiarism detection, academic reputation, and lifelong learning passports. Collectively, the findings confirm blockchain's effectiveness in securing academic records while also underscoring unresolved gaps such as global standardization, interoperability, legal frameworks, and energy-efficient consensus mechanisms that must be addressed for widespread adoption.[19-20]

III. PROPOSED SYSTEM

A. Detailed Proposed System

The proposed system is a blockchain-based certificate generation and verification platform that ensures tamper-proof, transparent, and verifiable academic credentials. Institutions issue certificates through a web application (Next.js) that automatically generates documents (DOCX/PDF), computes cryptographic hashes (SHA-256), and stores essential metadata on a blockchain. Smart contracts manage certificate issuance, ownership, and revocation, while large files are stored off-chain (MongoDB or IPFS) to reduce blockchain overhead. Each certificate is linked to a unique identifier and optionally tokenized as an NFT for verifiable ownership. Verification is achieved by matching certificate hashes with blockchain records, allowing employers or third parties to instantly validate authenticity. The system also supports revocation and corrections via append-only records, ensuring auditability. This design reduces fraud, enhances trust, and provides a scalable solution adaptable to universities, online courses, and professional organizations.

B. Software Requirements

- **Frontend/Backend**: Next.js, Node.js
- **Database**: MongoDB
- **Blockchain**: Ethereum (Solidity smart contracts), Ganache for testing
- **Storage**: IPFS for decentralized files, docxrender + docxtopdf for certificate generation
- **Authentication**: JWT, bcrypt
- **Other Tools**: Ethers.js/Web3.js, Docker, Nginx, GitHub Actions (CI/CD), QR code generator

C. Hardware Requirements

- **Development/Test**: Intel i5 or higher, 8 GB RAM, 250 GB SSD, Windows/Linux/Mac
- **Production**:
  - Application server: 4–8 vCPU, 16–32 GB RAM
  - Database: MongoDB replica set, 1 TB SSD
  - Blockchain nodes: 4 validators, each 8 vCPU, 32 GB RAM
  - IPFS cluster or S3-compatible storage for certificates
  - Optional HSM or cloud KMS for secure key storage

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)

D. Stakeholders and System Objectives

To address the described problems, the system is designed to serve the needs of several key stakeholders based on its core capabilities.

Key Stakeholders

- **Institutions (Issuers):** These are the universities, online course providers, and professional organizations that issue certificates through the web application.
- **Students (Holders):** These are the recipients who are provided with "verifiable academic credentials" and "verifiable ownership," optionally through NFTs.
- **Employers & Verifiers:** These are the third parties who can "instantly validate authenticity" by matching certificate hashes with the immutable blockchain records.

System Objectives

Based on the design, the system's primary objectives are to:

- **Reduce Fraud:** Create "tamper-proof" credentials using cryptographic hashes (SHA-256) and blockchain storage.
- **Enhance Trust:** Ensure a "transparent" and "verifiable" system for all parties.
- **Improve Efficiency:** Provide instant validation without intermediaries and support an "auditable" process for corrections via append-only records.
- **Ensure Scalability:** Deliver a "scalable solution" that reduces blockchain overhead by storing large files off-chain (in MongoDB or IPFS).

III. METHODOLOGY

A. System Architecture

The methodology follows a layered architecture where each layer has a distinct responsibility to ensure scalability, security, and modularity. At the top, the User Interface Layer (Next.js frontend) enables students, administrators, and verifiers to interact with the platform. The Application Layer manages authentication, certificate requests, document generation, and communication with blockchain smart contracts. The Blockchain Layer (Ethereum network or Ganache testnet) records certificate metadata, ownership, and revocation status. The Data Layer uses MongoDB for user details, certificate metadata, and off-chain storage references, while IPFS or S3 handles larger documents. Together, these layers form a secure and transparent ecosystem that enables issuance, verification, and lifecycle management of certificates.

- **Client Layer**
- **Tools:** Next.js
- **Function:** User actions (login, request, verify)
- **Application Layer**
- **Tools:** Next.js, JWT, bcrypt
- **Function:** Authentication & API handling
- **Data Layer**
- **Tools:** MongoDB
- **Function:** Store user data & certificate metadata
- **Processing Layer**
- **Tools:** docxrender, docxtopdf
- **Function:** Generate and convert certificates
- **Blockchain Layer**
- **Tools:** Ganache, Smart Contract, NFT
- **Function:** On-chain certificate storage & verification
- **Infrastructure Layer**
- **Tools:** Node.js, Python, Hosting
- **Function:** Runtime environment & deployment

© 2025 IJMRSET | Volume 8, Issue 11, November 2025| DOI:10.15680/IJMRSET.2025.0811029

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)

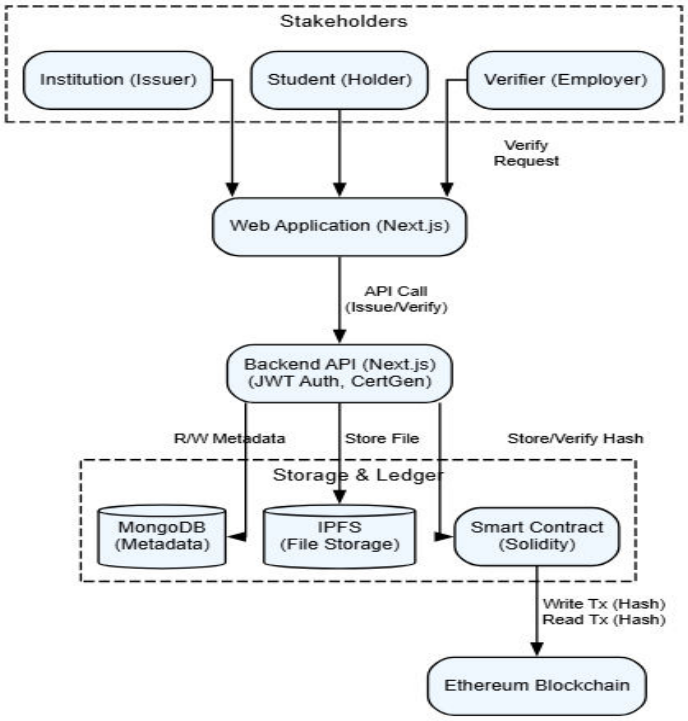
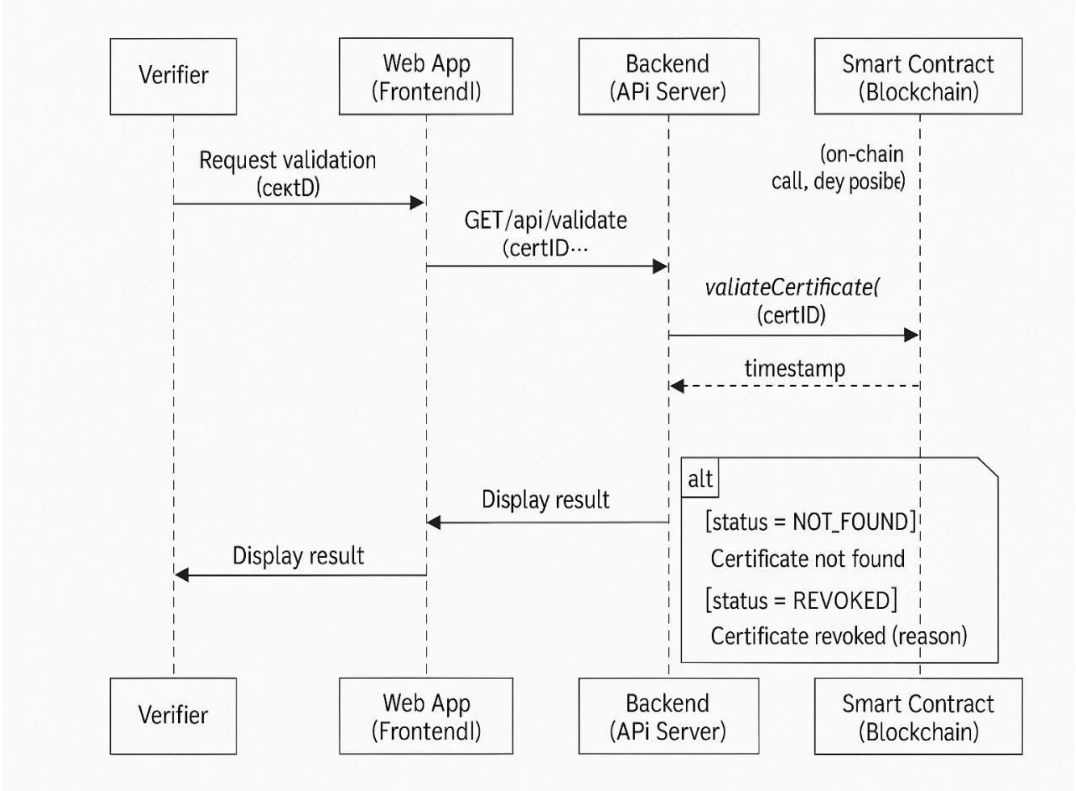


FIGURE.I: System Architecture



B. Sequence diagram

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)

Modules of the Project

1. **User Management Module**

Handles registration, login, role assignment (student, admin, verifier) with secure authentication using JWT and bcrypt.

2. **Certificate Generation Module**

Enables administrators to design and issue certificates. Templates are generated via docxrender and converted into PDFs with docxtopdf.

3. **Blockchain Module**

Implements smart contracts to store certificate IDs, hashes, and metadata. Handles minting, revocation, and correction of certificates.

4. **Verification Module**

Verifiers can scan a QR code or input a certificate ID to instantly validate its authenticity against blockchain records.

5. **Database & Storage Module**

Stores user data and certificate metadata in MongoDB. Full certificate files are stored in IPFS or S3, linked by content hashes.

6. **Revocation & Correction Module**

Provides a mechanism for revoking certificates and linking correction records without altering original blockchain entries.

V. FUTURE SCOPE

While this research establishes a robust proof-of-concept, future work will focus on enhancing deployment readiness and interoperability.

- **Interoperability & Standardization:** Future iterations will integrate **W3C Verifiable Credentials (VCs)** and **Decentralized Identifiers (DIDs)**. This is essential to move beyond a proprietary system and ensure credentials are globally interoperable with other compliant verification platforms.
- **Mainnet Deployment & Scaling:** The system will be migrated from the Ganache testnet to a public **Layer 2 scaling solution (e.g., Polygon or Arbitrum)**. This is a critical step to manage real-world gas costs and transaction latency, ensuring the system is economically viable for institutions.
- **Persistent Decentralized Storage:** To guarantee long-term certificate availability beyond local pinning, the system will be integrated with a persistent storage network like **Filecoin** or a decentralized pinning service.

VI. CONCLUSION

This research demonstrates that blockchain can provide a robust and tamper-proof framework for certificate generation and verification, addressing the long-standing problems of forgery, duplication, and administrative inefficiencies in traditional systems. By leveraging smart contracts, cryptographic hashing, and off-chain storage, the proposed system ensures certificates remain secure, transparent, and verifiable in real time without reliance on third-party verifiers. The design also supports revocation and corrections, balancing blockchain's immutability with the flexibility required in academic and professional contexts.

Beyond technical advantages, the proposed solution carries significant implications for institutions, employers, and students. It enables faster verification, reduces operational costs, and enhances global trust in academic credentials. With interoperability features such as NFT integration and potential alignment with W3C Verifiable Credentials, the system can scale internationally, supporting cross-border recognition of qualifications. As blockchain adoption continues to expand, this work positions decentralized credentialing as a practical and future-ready standard for education and professional certification.

REFERENCES

[1] "Immutable Digital Recognition via Blockchain," *arXiv preprint*, 2025.
[2] TR. Sree, "Decentralized Certificate Issuance and Verification System," *Journal of Network and Computer Applications*, vol. 240, 2025.
[3] S. Ahmed et al., "Blockchain-based Authentication and Verification System for Academic Certificates using QR Code and DApps," *International Journal of Advanced Computer Science*, 2024.
[4] K. Sharma et al., "Verifi-Chain: A Credentials Verifier using Blockchain and IPFS," *arXiv preprint*, 2023

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)

[5] R. Karthik et al., "Student Certificate Sharing System Using Blockchain and NFTs," *arXiv preprint*, 2023.
[6] A. Malik et al., "DocCert: Nostrification, Document Verification and Authenticity Blockchain Solution," *arXiv preprint*, 2023.
[7] L. Zhang et al., "EduChain: A Blockchain-based Education Data Management System," *arXiv preprint*, 2023.
[8] S. Verma et al., "Blockchain Based Certificate Authentication System with Enabling Correction," *Journal of Information Security*, vol. 14, no. 4, pp. 125–139, 2023
[9] A. Gupta et al., "Blockchain Based Certificate Verification System (Management)," *International Journal of Computer Applications*, vol. 185, no. 38, pp. 10–17, 2023.
[10] M. Singh and S. Kim, "Blockchain-Based Academic Certificate Verification System," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 10, no. 8, pp. 351–355, 2019.
[11] S. S. Gill, I. Chana, and R. Buyya, "Blockchain-Based Smart Education: A Comprehensive Survey," *IEEE Access*, vol. 7, pp. 128451–128471, 2019.
[12] S. R. Pokhrel and J. Choi, "A Decentralized Certificate Management System Using Blockchain," *IEEE Access*, vol. 7, pp. 150073–150084, 2019.
[13] N. Alammary, S. Alhazmi, M. Almasri, and S. Gillani, "Blockchain-Based Applications in Education: A Systematic Review," *Applied Sciences*, vol. 9, no. 2400, pp. 1–23, 2019.
[14] H. Li, L. Pei, Y. Liao, Y. Gao, and W. Xu, "Design of an Electronic Diploma System Based on Blockchain and Smart Contracts," *2019 IEEE International Conference on Smart Internet of Things (SmartIoT)*, pp. 384–389, 2019.
[15] M. Turkanović, M. Hölbl, K. Košič, M. Heričko, and A. Kamišalić, "EduCTX: A Blockchain-Based Higher Education Credit Platform," *IEEE Access*, vol. 6, pp. 5112–5127, 2018.
[16] P. Gräther, A. Kolvenbach, M. Ruland, A. Schütte, and U. Tönjes, "Blockchain for Education: Lifelong Learning Passport," *Proceedings of the 1st ERCIM Blockchain Workshop*, pp. 1–7, 2017.
[17] N. Al-Bassam, "SCPKI: A Smart Contract-Based PKI and Identity System," *Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts (BCC '17)*, pp. 35–40, 2017.

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