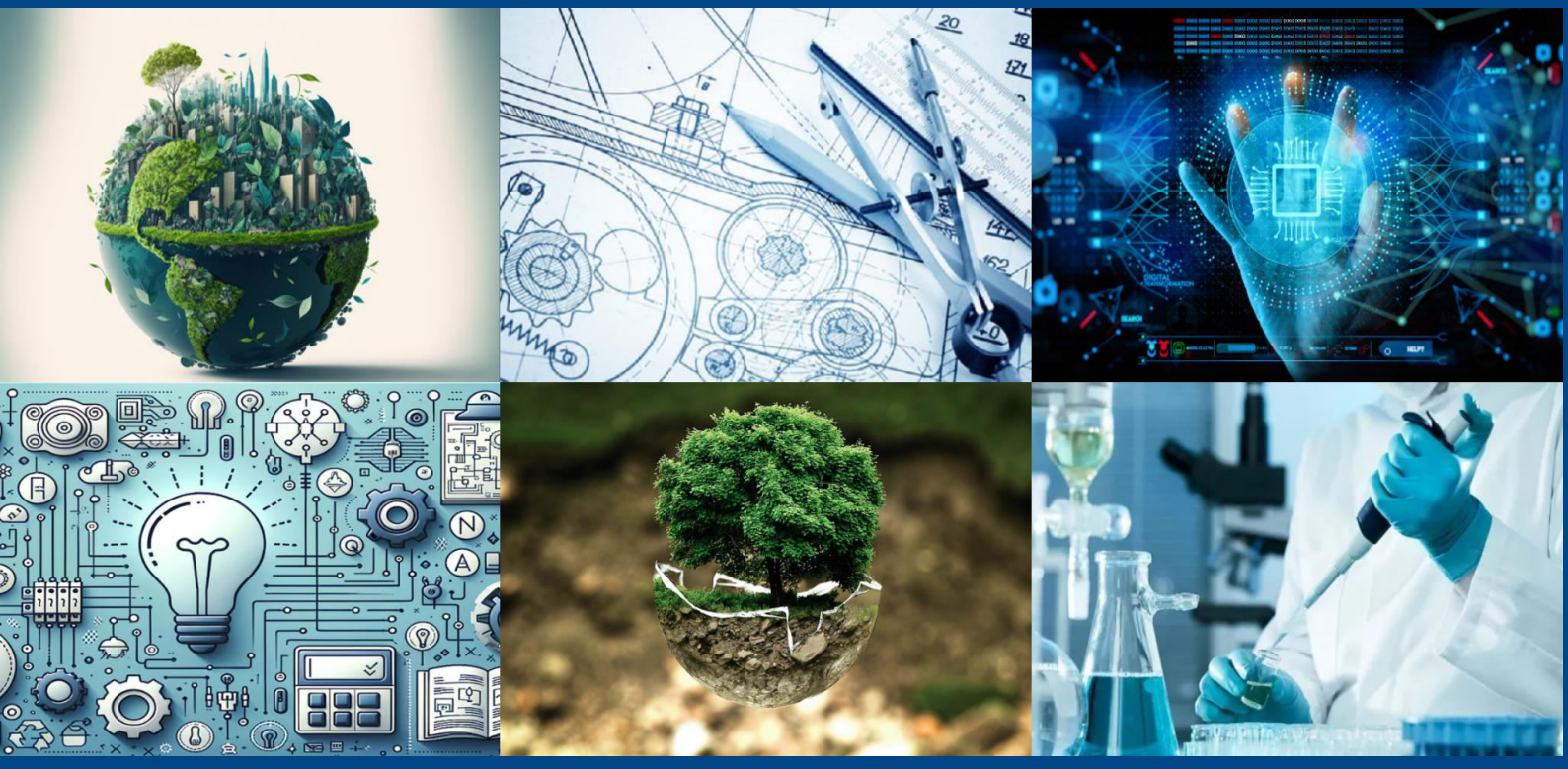
ISSN: 2582-7219

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 5, May 2025**

© 2025 IJMRSET | Volume 8, Issue 5, May 2025| DOI:10.15680/IJMRSET.2025.0805017

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)

Certificate Id Generator Using Blockchain

Saurav Patil, Dr. R.B. Wagh, Mr. V.S. Thakare, Payal Jadhav, Bhagyashri Borse, Vivek Patil

Department of Computer Technology, R.C.Patel Institute of Technology, Shirpur, India

ABSTRACT: In recent years, the demand for secure, tamper-proof, and easily verifiable digital certificates has increased significantly across sectors such as education, healthcare, and legal industries. Traditional systems for issuing and verifying certificates are often prone to forgery, delays in manual verification, and lack of transparency. These inefficiencies undermine trust in the authenticity of certificates and complicate the verification process.

This paper presents a blockchain-based Certificate ID Generator designed to address these issues by leveraging decentralized technologies. Each certificate is assigned a unique identifier, cryptographically secured, and recorded on a blockchain, making it tamper-proof and verifiable in real-time by anyone without relying on intermediaries. Smart contracts on a public blockchain automate the issuance and validation of certificates, while metadata is securely stored off-chain using InterPlanetary File System (IPFS).

The proposed system includes a user-friendly web interface, allowing institutions to issue certificates and recipients to verify them through QR codes. It also ensures scalability, handling high volumes of requests efficiently, as demonstrated by testing results showing fast certificate issuance times and minimal verification delays. This research demonstrates the potential of blockchain to revolutionize the way certificates are issued, validated, and secured, with future enhancements including cross-chain integration and privacy solutions such as zero-knowledge proofs.

This research demonstrates how blockchain can be applied to digital credentials, offering a more efficient, secure, and transparent method of certificate issuance and validation. The approach has far-reaching implications not only for educational institutions but also for industries where the validation of qualifications, skills, and experience is critical.

KEYWORDS: Blockchain, Smart Contracts, Digital Certificates, IPFS, Credential Verification, Decentralized Identity

I. INTRODUCTION

In the modern digital landscape, the issuance and verification of certificates play a pivotal role across academia, professional training, and industry compliance. Digital certificates—ranging from university diplomas to professional licenses—are increasingly prevalent as organizations embrace online learning and remote work. However, existing certificate management systems are typically centralized, relying on institutional databases or third-party services. This centralization introduces multiple vulnerabilities, including single points of failure, susceptibility to data breaches, and opportunities for credential forgery. As a result, verifying the authenticity of digital certificates often involves manual, time-consuming processes that undermine trust and efficiency [1].

Blockchain technology has emerged as a promising foundation for secure, transparent, and tamper-proof credentialing. By recording certificate metadata on a decentralized ledger, blockchain ensures that once issued, a certificate cannot be altered or repudiated [2]. Smart contracts—self-executing programs stored on the blockchain—can automate issuance, validation, and revocation processes according to predefined rules [3]. Off-chain storage solutions such as the InterPlanetary File System (IPFS) complement this approach by housing large data payloads (e.g., PDF certificate files), while the blockchain retains only cryptographic hashes for verification. This combination delivers a scalable, cost-effective platform that supports real-time, trustless certificate verification without reliance on centralized authorities [4].

© 2025 IJMRSET | Volume 8, Issue 5, May 2025| DOI:10.15680/IJMRSET.2025.0805017

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)

Beyond security and immutability, a blockchain-based Certificate ID Generator offers significant operational advantages. Institutions can drastically reduce administrative overhead by automating verification requests and leveraging QR-code scans, while recipients gain immediate, global access to their credentials from any device. Furthermore, the transparent audit trail provided by the blockchain enhances regulatory compliance and simplifies auditing processes [3]. Interoperability with multiple blockchain networks can extend this framework across borders and industries, fostering a universal standard for digital credentialing that bridges disparate systems and jurisdictions [2].

II. LITERATURE REVIEW

Blockchain technology has shown immense potential in various applications beyond cryptocurrency, particularly in ensuring data integrity, security, and decentralization. Several studies and projects have focused on leveraging blockchain for credentialing and certificate verification, highlighting its ability to provide transparent, immutable, and efficient systems for digital identity management.

In one of the most notable implementations, MIT's Blockcerts project aims to provide a solution for issuing and verifying academic certificates using blockchain. The Blockcerts platform allows institutions to issue certificates that can be easily verified by anyone without needing to contact the issuing authority. The use of blockchain ensures the authenticity of the certificates and guarantees that they cannot be altered or falsified once issued [1]. The system leverages public key infrastructure (PKI) and digital signatures to enhance the security of certificates and their verification process.

Similarly, the University of Nicosia has adopted blockchain technology to issue and verify academic diplomas. This adoption demonstrates blockchain's ability to address inefficiencies in the traditional methods of verification, particularly in terms of reducing the time and cost involved in the manual process. Blockchain-based credentials eliminate the need for physical documents and the reliance on third-party verification, providing a faster and more secure method of validating academic qualifications [2].

Furthermore, Kumar and Mehta's research explores the integration of blockchain for tamper-proof credentialing using smart contracts. Their work demonstrates the potential of using blockchain to eliminate fraud in the issuance and validation of digital certificates. The authors highlight the role of smart contracts in automating the certificate issuance process, reducing the need for intermediaries, and ensuring that certificates are issued according to strict and transparent rules. This approach enhances the reliability and trustworthiness of the digital certificate system [3].

While these approaches present promising solutions, they also highlight some of the challenges faced by blockchain implementations, such as scalability and integration with existing systems. Lee and Patel's study investigates these challenges in the context of decentralized identity verification. They emphasize the importance of ensuring interoperability between blockchain systems and traditional platforms to enable widespread adoption in various sectors. Their research suggests that combining blockchain with off-chain storage systems such as IPFS can mitigate scalability issues, providing a more efficient and cost-effective solution for credential management [4].

In comparison to previous work, our approach integrates these concepts into a unified Certificate ID Generator system that not only provides tamper-proof certificates but also offers a user-friendly verification process through QR code scanning. By utilizing Ethereum-based smart contracts for automated issuance and IPFS for secure storage, we aim to overcome scalability limitations and provide a more efficient and accessible solution for digital credentials.

© 2025 IJMRSET | Volume 8, Issue 5, May 2025| DOI:10.15680/IJMRSET.2025.0805017

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)

III.LIMITATIONS OF EXISTING SYSTEM(S)

- Centralized Vulnerabilities: Most institutions store certificates in centralized databases that are susceptible to single points of failure. A server outage, insider threat, or cyberattack on the central repository can render the entire credentialing system unavailable or compromised, leading to potential data loss or unauthorized modifications [1].
- Fraud and Forgery: Paper-based certificates and centralized digital records can be easily forged or tampered with. Malicious actors can alter document details or create counterfeit credentials, making it difficult for employers and third-party verifiers to trust the authenticity of presented certificates [2].
- Manual Verification Overhead: Verifying a certificate often requires contacting the issuing authority via email, phone, or an online portal. This manual process is time-consuming, prone to human error, and cannot scale to support large volumes of
- Verification requests, resulting in delays and increased administrative burden [3].
- Lack of Global Accessibility: Centralized systems typically operate within a single institution or jurisdiction, making cross-border verification cumbersome. Verifiers outside the issuing organization must often rely on intermediaries, which introduces further delays and additional costs [4].
- High Operational Costs: Maintaining secure, centralized infrastructure—including redundancy, backups, and cybersecurity measures—incurs significant expenses. Institutions must allocate resources for server maintenance, database management, and manual support for certificate-related inquiries.

IV. KEY FEATURES

- Blockchain-Based Immutability: Once a certificate is issued, its metadata and hash are recorded on the blockchain, making it immutable and tamper-proof. This eliminates the possibility of certificate forgery or alteration after issuance, ensuring long-term integrity and trust.
- Decentralized Storage via IPFS: Instead of storing the actual certificate files on-chain, which can be costly and inefficient, the system uses the InterPlanetary File System (IPFS) to store the files. The unique Content Identifier (CID) returned by IPFS is then stored on the blockchain, linking the document securely and allowing it to be retrieved at any time.
- Smart Contract Automation: Smart contracts are responsible for automating key tasks such as issuing, verifying, and revoking certificates. These contracts ensure that all operations are executed in a transparent and verifiable manner without requiring manual intervention or centralized approval.
- QR Code Integration for Verification: Each certificate generated by the system contains a unique QR code embedded into the document. This code links to the transaction ID or certificate hash on the blockchain, enabling instant verification simply by scanning it through the web interface.
- User-Friendly Web Interface: A clean and responsive web platform built using modern frameworks allows institutions to issue certificates, and users or employers to verify them. The platform supports real-time interactions and is accessible from both desktop and mobile devices.
- Role-Based Access Control: The system defines clear roles such as Issuer, Verifier, and Administrator, each with specific privileges. Only verified institutions can issue certificates, and access to sensitive functions is strictly restricted through blockchain wallet-based authentication.
- Instant Verification without Intermediaries: Anyone with the certificate's transaction hash or QR code can instantly verify the authenticity of the certificate through the web application, without the need to contact the issuing institution.
- Scalability and Low Cost: The architecture is designed to handle a large number of certificates and verifications with minimal latency. Using efficient blockchain networks and off-chain data handling significantly reduces operational costs and transaction fees.

© 2025 IJMRSET | Volume 8, Issue 5, May 2025| DOI:10.15680/IJMRSET.2025.0805017

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)

V.METHODOLOGY

1) Technical Stack

1.1) Backend:

The backend runs on **Node.js** with **Express.js**, providing a RESTful API layer for interacting with smart contracts and IPFS. It manages user sessions, certificate generation, authentication, and transaction handling. For database management and logging purposes, **MongoDB** can be integrated for off-chain record keeping and analytics.

1.2) Front-end:

The frontend is developed using **Next.js**, a React framework offering server-side rendering and fast performance. **Tailwind CSS** is used for responsive styling, ensuring a smooth user experience across devices. QR code generation is integrated using libraries like qrcode.react, and **MetaMask** is utilized for Ethereum wallet-based login and interaction.

1.3) APIs and Integrations:

Smart contracts are written in **Solidity** and deployed on Ethereum-compatible testnets (like **Polygon Mumbai**). These contracts handle the issuance, validation, and revocation of certificates. Development tools such as **Hardhat**, **Truffle**, and **Remix IDE** are used for compiling, testing, and deploying the contracts. **Web3.js** or **Ethers.js** libraries are used to connect the frontend and backend to the blockchain. These libraries help in signing transactions, reading contract data, and listening to blockchain events like CertificateIssued or CertificateRevoked. **IPFS (InterPlanetary File System)** is used to store certificate documents in a decentralized manner. A CID (Content Identifier) is generated and stored on-chain, while the actual file remains in IPFS. Tools like **Pinata** or **Web3.Storage** are used to facilitate this interaction and ensure file persistence.

2) Implementation

- **Smart Contract Deployment:** Smart contracts include functions like issueCertificate(), revokeCertificate(), and verifyCertificate(). Each certificate's metadata is hashed using SHA-256 and recorded on the blockchain. The issuer's address and timestamp are stored to track who issued what and when.
- **Certificate Generation and IPFS Pinning:** When a certificate is created, the metadata (student name, course, date, issuer info) is stored in a JSON or PDF file. This file is uploaded to IPFS, and the CID is retrieved and sent to the blockchain via the smart contract function. This ensures the certificate can always be retrieved and verified in the future.
- **QR Code and Verification Mechanism:** After issuing a certificate, the system generates a **QR code** embedding the transaction ID or CID. When scanned, it redirects to the verification portal, where the certificate is validated by comparing the metadata hash with the on-chain hash. This enables instant and contactless verification by employers or institutions.
- **Security Measures:** All transactions require MetaMask wallet authentication. Each institution is assigned a unique wallet address that must be whitelisted by the smart contract before they can issue certificates. Role-based permissions restrict unauthorized access to sensitive operations.
- **User Dashboards:** Two dashboards are developed:
    - **Issuer Dashboard** – Allows institutions to manage certificates, track issued records, and revoke documents if needed.
    - **Verification Portal** – Enables anyone to check the validity of a certificate by entering a certificate ID or scanning a QR code.

3) Functional Requirement

- Certificate Issuance: Institutions can upload student or recipient information, which is securely hashed, stored in IPFS, and linked to a blockchain transaction for permanent verification.

© 2025 IJMRSET | Volume 8, Issue 5, May 2025| DOI:10.15680/IJMRSET.2025.0805017

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

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

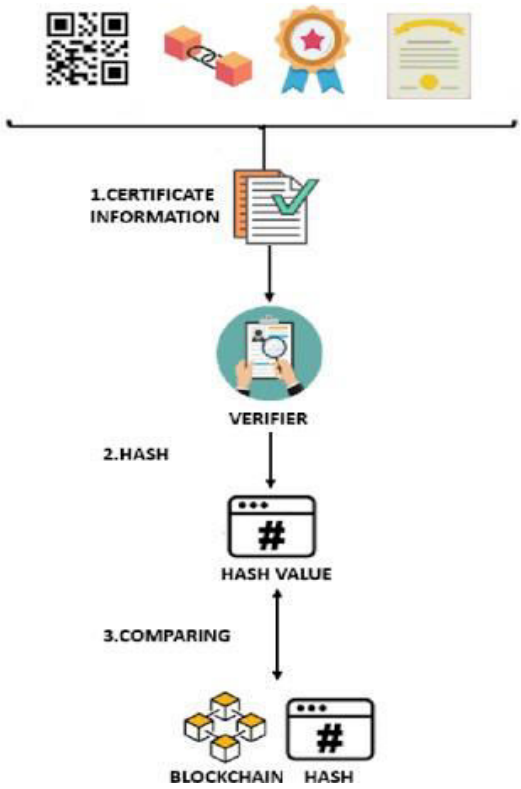
(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

- Tamper-Proof Validation: Each certificate hash is immutable once added to the blockchain. Any attempt to alter the document will result in a mismatch during verification, thus ensuring authenticity.
- Revocation Support: Institutions can revoke any certificate using the revokeCertificate() function. Revoked certificates are flagged in the blockchain and cannot be validated further.
- Decentralized Verification: Users or employers can verify certificates from anywhere without contacting the issuer. The verification tool checks the blockchain for a matching hash and status.
- User Authentication: Users authenticate through MetaMask, which ensures wallet-based identity without the need for traditional passwords, reducing the risk of phishing and unauthorized access.
- Responsive Interface: The application is mobile-friendly and responsive, ensuring smooth access on smartphones, tablets, and desktops.
- Activity Logging and Notifications: Event listeners in the backend capture on-chain actions and provide real-time feedback (e.g., “Certificate Issued”, “Certificate Verified”) to users via notifications.
- High Scalability: The use of IPFS for off-chain storage and efficient smart contract design allows the system to handle thousands of users simultaneously without congestion or delay.

VI. SYSTEM ARCHITECTURE AND DESIGN

1) Use Case Diagrams for Different Modules: The **Issuer Use Case Diagram** illustrates the interactions of an authorized certificate issuer with the system. The issuer logs in via MetaMask, uploads certificate metadata and files, generates a QR code for verification, and submits the information to the blockchain. They can also monitor the status of issued certificates to track their validity and activity.

The **Verifier Use Case Diagram** represents how a third-party verifier (such as an employer or institution) interacts with the system. The verifier can either scan a QR code or manually enter a certificate ID. The system then retrieves metadata from IPFS, compares it with the blockchain-stored hash, and displays the certificate's validity. This ensures instant, secure, and decentralized verification without needing to contact the issuing authority.



© 2025 IJMRSET | Volume 8, Issue 5, May 2025| DOI:10.15680/IJMRSET.2025.0805017

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)

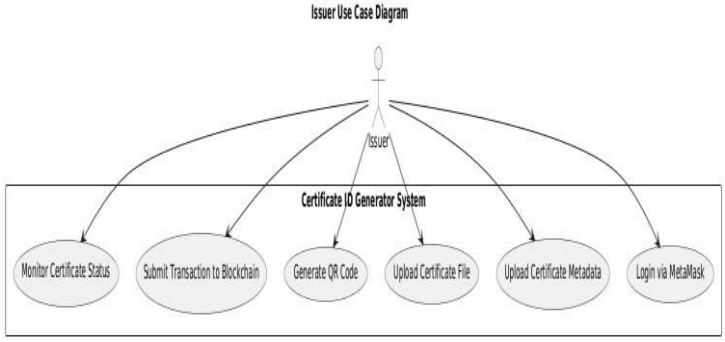


Figure 2. Issuer Use Case Diagram

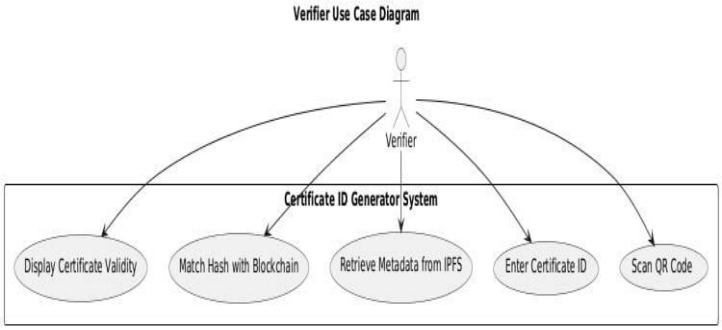


Figure 3. Verifier Use Case Diagram

3. Security Architecture

- **Wallet-based authentication** ensures only authorized institutions issue certificates.
- **Hashing with SHA-256** protects the integrity of certificate content.
- **Smart contract permissions** restrict access to critical operations.
- **IPFS CIDs** prevent direct tampering since files are immutable by nature.

4. Scalability and Fault Tolerance

- Stateless backend services that can be containerized (e.g., Docker + Kubernetes).
- Efficient smart contracts that minimize gas consumption.
- Decentralized file hosting through IPFS nodes.
- Caching mechanisms and rate-limiting APIs to support large-scale institutional use.

5. Design Highlights

- **No Central Authority:** Users can verify certificates without contacting the issuing institution.
- **Cross-Platform Compatibility:** Works on mobile and desktop browsers using Web3 wallets.
- **Modular Integration:** Each layer operates independently, allowing upgrades or migration to other chains or file systems in the future.

VII. CONCLUSION

The Certificate ID Generator using blockchain offers a secure, decentralized, and tamper-proof solution to the long-standing challenges of traditional certificate management systems. By utilizing smart contracts for automated issuance and verification, along with IPFS for decentralized storage, the system ensures data integrity,

global accessibility, and real-time verification without relying on intermediaries. Its QR code integration further simplifies the verification process, making it highly user-friendly. This approach not only enhances trust and transparency but also significantly reduces administrative overhead. Overall, the system represents a scalable and efficient model for modern digital credentialing, with strong potential for adoption across educational institutions, professional certifiers, and regulatory bodies worldwide. Looking ahead, the implementation of advanced features such as multi-chain compatibility, privacy-preserving mechanisms like zero-knowledge proofs, and mobile app integration can further extend the system's utility. These enhancements will not only improve user experience but also ensure compliance with emerging digital identity standards. As credential fraud and administrative complexity continue to pose challenges in the global certification landscape, this blockchain-based solution provides a future-ready framework capable of evolving alongside technological and institutional demands.

REFERENCES

1. S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.
2. M. Swan, *Blockchain: Blueprint for a New Economy*, O’Reilly Media, 2015.
3. R. Kumar and S. Mehta, “Tamper-Proof Digital Credentials with Blockchain,” *IEEE Transactions on Blockchain*, vol. 10, no. 2, 2023.
4. M. Lee and K. Patel, “Decentralized Identity Verification Using Blockchain,” *Journal of Emerging Technologies*, vol. 15, no. 3, 2022.
5. J. Benet, “IPFS – Content Addressed, Versioned, P2P File System,” Protocol Labs, 2014.
6. V. Buterin, “Ethereum White Paper,” Ethereum.org, 2013.
7. D. Tapscott and A. Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*, Penguin, 2016.
8. L. Zhang et al., “Blockchain-Based Credential Management in Education,” *IEEE Access*, vol. 9, pp. 13876-13888, 2021.
9. C. Grech and C. Camilleri, “Blockchain for Education: Lifelong Learning Passport,” *UNESCO Blockchain Report*, 2019.
10. A. Sharples and J. Domingue, “The Open University and Blockchain: Towards a University of the Future,” *Open University Research*, 2017.
11. S. Jagers and P. Moon, “Smart Certificates on Blockchain,” *Blockchain in Education Conference*, 2019.
12. A. Arndt, “A Framework for Blockchain-Based University Diplomas,” *International Journal of Advanced Computer Science*, vol. 10, no. 5, 2020.
13. K. Christidis and M. Devetsikiotis, “Blockchains and Smart Contracts for the Internet of Things,” *IEEE Access*, vol. 4, 2016.
14. D. Yaga et al., “Blockchain Technology Overview,” *NIST Special Publication 800-220*, 2018.
15. M. Alammary et al., “Blockchain-Based Applications in Education: A Systematic Review,” *Applied Sciences*, vol. 9, no. 12, 2019.
16. T. Nguyen et al., “Secure and Transparent Credential Management Using Blockchain,” *Procedia Computer Science*, vol. 177, 2020.
17. A. Hasan and A. Salah, “Blockchain for Document Integrity: Certification Use Case,” *International Journal of Blockchain Applications*, vol. 2, no. 1, 2021.
18. N. Mohan and R. Thomas, “Blockchain for Higher Education Certifications,” *International Journal of Educational Technology*, vol. 8, no. 2, 2020.
19. D. S. Alberts, “Trust and Verification in the Blockchain Era,” *Journal of Digital Trust and Identity*, vol. 4, 2021.
20. M. Rani and V. Singh, “Decentralized Educational Certificate Issuance Using Blockchain,” *International Conference on Computing and Communication*, 2022.
21. K. Sukhwani et al., “Performance Modeling of Hyperledger Fabric,” *IEEE International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems*, 2018.

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