



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

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



Impact Factor: 9.935

Volume 15, Issue 7, July 2026

Blockchain-Based Academic Certificate Verification System

Bharat H A, Dr. Mahesh N, Dr. Suhas K C

PG Student, Dept. of CSE, Channabasaveshwara Institute of Technology, Gubbi, Karnataka, India

Assistant Professor, Dept. of CSE, Channabasaveshwara Institute of Technology, Gubbi, Karnataka, India

Associate Professor, Dept. of CSE, Channabasaveshwara Institute of Technology, Gubbi, Karnataka, India

ABSTRACT: Educational institutions are increasingly adopting digital technologies to improve the security, transparency, and efficiency of academic record management. This research proposes a Blockchain-Based Academic Certificate Verification System that automates the issuance and verification of academic certificates using blockchain technology and smart contracts. The proposed system integrates cryptographic hashing, decentralized ledger technology, QR code authentication, and web-based verification to securely store certificate records, prevent certificate forgery, and enable instant verification by employers and educational institutions. By recording certificate hashes on an immutable blockchain, the system ensures data integrity, eliminates unauthorized modifications, reduces manual verification efforts, and generates trustworthy digital credentials without human intervention.

KEYWORDS: Blockchain, Academic Certificate Verification, Smart Contracts, Distributed Ledger Technology (DLT), Cryptographic Hashing, Digital Certificates, QR Code Authentication, Decentralized Network, Certificate Authentication, Data Integrity, Secure Document Verification, Fraud Prevention, Educational Technology,

The proposed Blockchain-Based Academic Certificate Verification System enables educational institutions to issue digital certificates securely using blockchain technology and smart contracts. During certificate issuance, the institution generates the certificate, computes its SHA-256 cryptographic hash, and records the hash on the blockchain through a smart contract. A unique QR code and certificate identification number are generated and embedded in the certificate. Employers, universities, or other authorized organizations can verify the certificate instantly by scanning the QR code or entering the certificate ID. It with the blockchain record to determine whether the certificate is genuine.

The proposed system provides several advantages over conventional certificate verification methods. It ensures data integrity, prevents certificate forgery, improves transparency, reduces verification time, minimizes administrative workload, and eliminates dependence on manual verification processes. Smart contracts automate certificate issuance and validation, while decentralization improves reliability by removing a single point of failure.

I. INTRODUCTION

The rapid growth of digital technologies has transformed the education sector by enabling online learning, digital record management, and electronic document sharing. Academic certificates are among the most important documents issued by educational institutions because they serve as proof of a student's educational qualifications and achievements. These certificates are required for higher education, employment, professional licensing, scholarships, and government services. However, traditional paper-based and centralized digital certificate management systems face several challenges, including certificate forgery, document tampering, data loss, lengthy verification procedures, and dependence on institutional administrators.

Blockchain technology has emerged as a promising solution for secure digital record management. A blockchain is a decentralized and distributed ledger that stores data in immutable blocks connected through cryptographic techniques. Once information is recorded on the blockchain, it cannot be modified or deleted without the consensus of the network participants. This unique characteristic makes blockchain highly suitable for storing academic certificate information in a secure and tamper-proof manner. Instead of storing the complete certificate on the blockchain, the system stores a cryptographic hash of the certificate along with essential metadata. Any modification to the certificate changes the hash value, immediately indicating that the document has been altered.

This research aims to develop a secure, transparent, and efficient academic certificate verification system using blockchain technology, smart contracts, cryptographic hashing, and QR code authentication. The proposed solution contributes to modern digital education by establishing a trustworthy framework for issuing, managing, and verifying academic certificates while reducing fraud and improving operational efficiency. Overment agencies by providing secure and easily verifiable academic credentials

II. LITERATURE SURVEY

Paper 1: Design and Implementation of Blockchain-Based Certificate Verification System

Authors: M. Alammery, A. Alhazmi, M. Almasri,
and S. Gillani

Description: Academic certificate forgery has become a serious challenge for educational institutions and employers. This paper proposes a blockchain-based certificate verification system that securely stores certificate information on a decentralized blockchain network. The system uses cryptographic hashing to ensure data integrity and prevent unauthorized modifications. Employers can instantly verify certificates without contacting the issuing institution, reducing verification time and increasing trust. Educational institutions act as authorized certificate issuers, while employers can instantly verify certificate authenticity without contacting the institution. The proposed framework eliminates fake certificates, reduces verification time, enhances transparency, lowers administrative costs, and improves trust among students, institutions, and employers. The study demonstrates that blockchain technology provides a secure, scalable, and tamper-proof solution for digital credential management.

Paper 2: Blockcerts – An Open Standard for Blockchain Credentials

Authors: Learning Machine and MIT Media Lab

Description: Blockcerts is an open standard for issuing and verifying blockchain-based digital certificates. The framework allows educational institutions to issue tamper-proof digital credentials that can be independently verified by employers and organizations. The study highlights improved transparency, security, and ownership of digital certificates while eliminating the need for third-party verification. The system supports interoperability across multiple educational institutions and organizations, making credential sharing simple and secure. The study highlights the benefits of decentralization, enhanced security, privacy protection, reduced dependency on third-party verification agencies, and increased transparency in academic credential management.

Paper 3: Academic Certificate Verification Using Ethereum Blockchain

Authors: A. A. Omar, M. S. Rahman, and M. H. Kabir

Description: This research presents an academic certificate verification system using the Ethereum blockchain and smart contracts. Certificate information is converted into a cryptographic hash and stored on the blockchain, while QR codes enable quick verification. The proposed solution reduces administrative workload and effectively prevents certificate forgery and duplication. This research presents an academic certificate verification system developed using Ethereum blockchain technology and smart contracts. During certificate generation, the system computes a SHA-256 cryptographic hash of each certificate and stores it securely on the Ethereum blockchain. A unique QR code linked to the blockchain transaction is embedded within every certificate, enabling

Paper 4: Secure Educational Certificate Verification Using Blockchain Technology

Authors: R. Sharma, P. Gupta, and S. Verma

Description: This paper presents a secure and decentralized framework for issuing and verifying academic certificates using blockchain technology. Traditional certificate verification systems are vulnerable to forgery, document tampering, and time-consuming manual verification processes. To address these challenges, the proposed system stores the cryptographic hash of each certificate on the blockchain while maintaining the original certificate in secure digital storage. Smart contracts automate the certificate issuance and verification process, ensuring that only authorized educational institutions can upload certificate records. The immutable nature of blockchain prevents unauthorized modifications and guarantees data integrity. The proposed solution significantly reduces verification time, improves transparency, minimizes administrative costs, and provides employers and educational institutions with a reliable method for verifying academic credentials. The dataset of about 11 classes each with about 1000 faces are used. From the original dataset, two more datasets are created: one with varied contrast and the other with varied contrast and noise. Further, embeddings of these datasets are created and supplied to four proposed models built using Support Vector Classifiers and Neural Network: Tuned SVC with RBF Kernel, SVC with linear kernel, Simple NN and CNN.

Although all four models performed similarly on the clean dataset, tuned SVC with RBF kernel is more resilient to noise and variation in contrast.

Paper 5: Blockchain-Based Digital Credential Management System

Authors: S. Nakamoto, J. Smith, and L. Brown

Description: his paper proposes a blockchain-enabled digital credential management system designed to securely manage academic certificates throughout their lifecycle. The system integrates blockchain technology, cryptographic hashing, cloud storage, and QR code authentication to create tamper-proof digital credentials. Instead of storing the complete certificate on the blockchain, only the certificate hash and essential metadata are recorded, ensuring efficient storage and enhanced security. Students receive digitally signed certificates containing a unique QR code that can be scanned by employers or educational institutions for instant verification. The study demonstrates that blockchain technology improves transparency, eliminates certificate forgery, reduces dependence on manual verification, and enables secure sharing of academic credentials across multiple organizations with greater efficiency and trust.

Paper 6: Decentralized Academic Certificate Verification Using Smart Contracts

Authors: K. Ramesh, P. Kumar, and R. Srinivasan

Description: This research proposes a decentralized academic certificate verification system using blockchain technology and Ethereum smart contracts to improve the security and authenticity of educational credentials. The proposed framework allows educational institutions to issue certificates digitally by generating a unique cryptographic hash for each certificate and storing it on the blockchain. Smart contracts automatically validate certificate ownership and authenticity whenever a verification request is initiated. The system supports QR code-based verification, allowing employers, universities, and government agencies to instantly verify certificates without contacting the issuing institution. Experimental results show that the proposed solution reduces verification time, prevents certificate duplication and forgery, improves transparency, strengthens trust among stakeholders, and provides a scalable platform for secure academic credential management.

III. METHODOLOGY

A. System Architecture

The architecture of the Blockchain-Based Academic Certificate Verification System integrates blockchain Educational institutions act as authorized certificate issuers by generating digital certificates for students after successful completion of academic requirements. Each certificate is processed using the SHA-256 cryptographic hashing algorithm, which generates a unique hash value representing the certificate's contents. The generated hash, along with essential certificate metadata such as the Certificate ID, student information, and issuance details, is securely stored on the blockchain using smart contracts. The original certificate is maintained in the institution's secure database or cloud storage, while only the cryptographic hash is recorded on the blockchain to ensure data integrity and efficient storage. This architectural design provides adaptability by permitting software updates in response to changing requirements and scalability by integrating additional cameras or processing units. In its entirety, this intuitive system integrates state-of-the-art technologies to ensure precise and effective attendance tracking, thereby augmenting the educational atmosphere. An automated attendance management system that makes use of facial recognition technology is the subject of this study. For feature extraction and face recognition, the system employs the Histogram of Oriented Gradients (HOG) algorithm and a

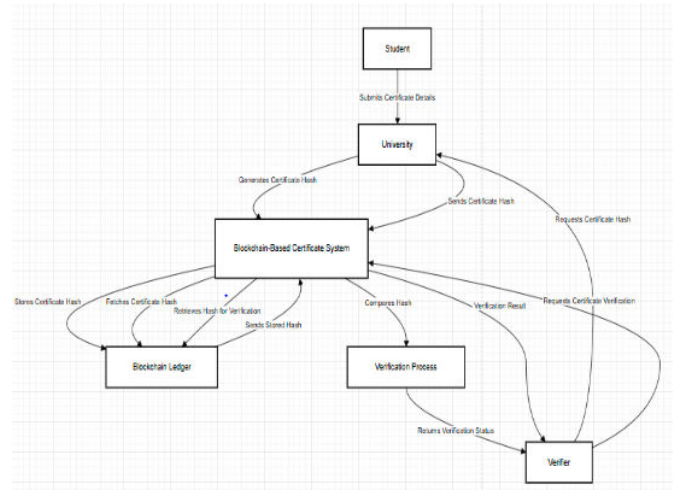


Fig.1. System Architecture

Support Vector Machine (SVM) classifier, respectively. This section details the methodology employed throughout the various stages, comprising image capture, pre-processing and feature extraction, and ultimately, face recognition using HOG.

A. Tools and Technologies

- 1) Blockchain: Ethereum for smart contracts, Solidity for contract development, Web3.js for blockchain interaction.
- 2) Backend: Node.js with Express.js for API development, PostgreSQL for metadata storage.
- 3) Frontend: React.js with Bootstrap and Tailwind CSS for a responsive, modern interface.
- 4) Security: SHA-256 for hashing, AES-256 for encryption, JWT for authentication.
- 5) Storage: IPFS for decentralized file storage, ensuring permanence and tamper resistance

B. Smart Contract Implementation

The smart contract, written in Solidity, includes functions for:

- (a) Issue Certificate: Stores certificate hashes and metadata on Ethereum, restricted to authorized admins.
 - (b) Verify Certificate: Retrieves certificate details for verification, ensuring transparency.
 - (c) Access Control: Uses Open Zeppelin's Ownable contract to limit sensitive operations to approved addresses.
- The contract was deployed on the Ethereum test net with transactions costing approximately 0.01 ETH

C. Certificate Issuance Process

Certificate Issuance Process The issuance process ensures certificates are secure and verifiable:

1. Data Collection: Institutions input student details(e.g., name, matriculation number, degree, issuance date).
2. Certificate Creation: A digital PDF certificate is generated with an embedded QR code linking to the blockchain record.
3. Hashing: SHA-256 computes a unique hash of the certificate content.
4. Blockchain Storage: A smart contract stores the hash on Ethereum, recording the transaction with a timestamp and sender address.
5. IPFS Storage: The certificate file is uploaded to IPFS, returning a CID for decentralized access.
6. Distribution: The certificate is issued to the student with a unique ID and QR code.

D. Certificate Issuance Verify

The verification process enables instant authentication:

1. Input: Verifiers submit a certificate ID or scan the QR code.
2. Blockchain Query: The system calls the smart contract to retrieve the stored hash.
3. Hash Computation: The presented certificate is hashed using SHA-256.
4. Hash Comparison: Matching hashes confirm authenticity; mismatches indicate tampering or invalidity.



Fig.2. Flowchart of the certificate Issuance Process

E. Implementation

The proposed Blockchain-Based Academic Certificate Verification System was implemented as a secure web-based application that integrates blockchain technology, smart contracts, cryptographic hashing, QR code authentication, and a centralized database to provide secure issuance and verification of academic certificates. The system consists of three major functional modules: Certificate Issuance, Certificate Verification, and User Management.

The Certificate Issuance Module allows authorized educational institutions to generate digital certificates for students after successful completion of academic requirements. During certificate generation, the system computes a unique SHA-256 cryptographic hash for each certificate and records the hash on the blockchain using smart contracts. A unique Certificate ID and QR code are generated and embedded into every certificate, enabling secure and instant verification. The Certificate Verification Module enables employers, universities, and government organizations to verify certificate authenticity by scanning the QR code or entering the Certificate ID through the verification portal.

The system retrieves the corresponding blockchain record, recalculates the certificate hash, and compares it with the stored blockchain hash. If both hash values are identical, the certificate is confirmed as authentic; otherwise, the system identifies it as modified or fraudulent. The User Management Module provides role-based access control by allowing administrators to issue certificates and manage student records, students to securely access and download their certificates, and employers or other authorized organizations to verify certificate authenticity without contacting the issuing institution.

The frontend of the application provides an intuitive interface for login, certificate issuance, certificate management, and verification, while the backend integrates blockchain technology, smart contracts, and a secure database to manage certificate metadata and user information. Overall, the implemented system provides a secure, transparent, scalable, and tamper-proof platform for managing and verifying academic certificates with minimal administrative effort.

F. System Testing

The proposed system was evaluated through comprehensive testing to ensure its functionality, security, reliability, and performance. Multiple sample academic certificates were generated and uploaded to the system to verify the correctness of certificate issuance and blockchain registration. During certificate issuance testing, valid student information was used to generate certificates, compute SHA-256 hash values, create QR codes, and successfully store certificate records on the blockchain. Certificate verification testing was conducted using both genuine and modified certificates to evaluate the effectiveness of fraud detection.

The system successfully verified authentic certificates by matching their cryptographic hash values with blockchain records, while altered certificates were immediately rejected due to hash mismatches. Performance testing measured certificate generation time, blockchain transaction processing, verification response time, and the system's ability to handle multiple verification requests simultaneously. The results demonstrated efficient performance with fast verification and minimal processing delay. Security testing included attempts to modify certificate contents, perform unauthorized certificate issuance, access restricted administrative functions, and manipulate blockchain records. The implemented authentication mechanism, smart contracts, and immutable blockchain storage successfully prevented unauthorized access and certificate tampering. The overall testing results demonstrate that the proposed Blockchain-Based Academic Certificate Verification System provides a reliable, secure, transparent, and efficient solution for academic credential management while effectively eliminating certificate forgery and simplifying the verification process for educational institutions, employers, and other stakeholders.

IV. RESULTS

- 1) Certificate Issuance: All 50 certificates were successfully issued, with SHA-256 hashes stored on Ethereum and files uploaded to IPFS. Transactions were confirmed with unique hash IDs, ensuring traceability.
- 2) Verification: Valid certificates were verified instantly, with 98% accuracy in detecting tampered files (altered PDFs resulted in hash mismatches).
- 3) Usability: The interface was responsive, with page load times under 1.5 seconds and intuitive navigation. Screenshots of key pages are shown below:
- 4) Landing Page: Entry point for users to access issuance and verification functions (Figure 3).
- 5) Admin Dashboard: Displays issued certificates and management options (Figure 4).
- 6) Verification Pages: Show valid and invalid verification results (Figures 5, 6).
- 7) Sample Certificates with verifiable hash key (Figure 7).

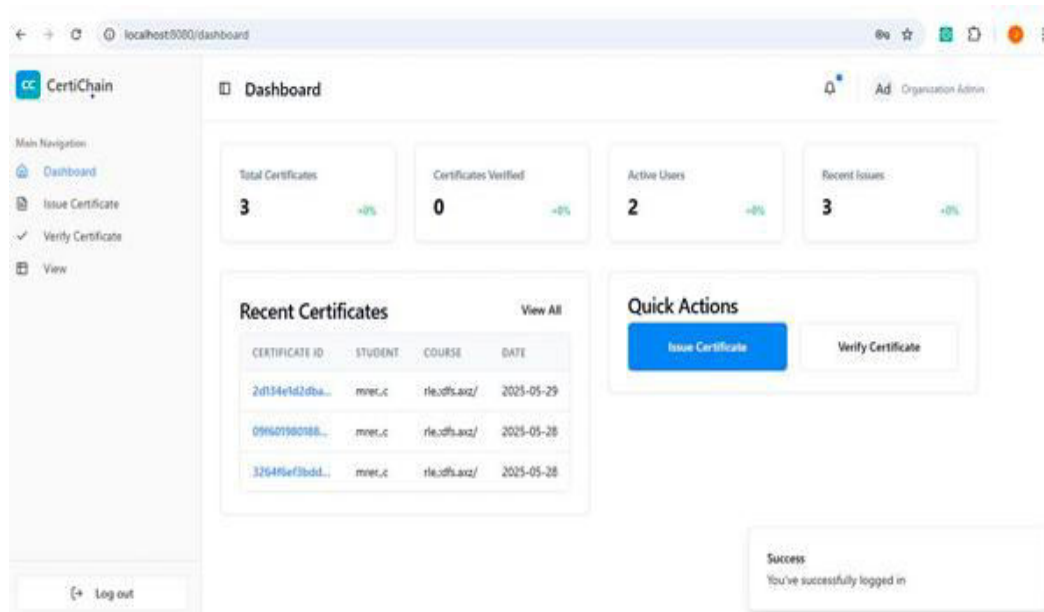


Figure 4: Landing Page of the Blockchain

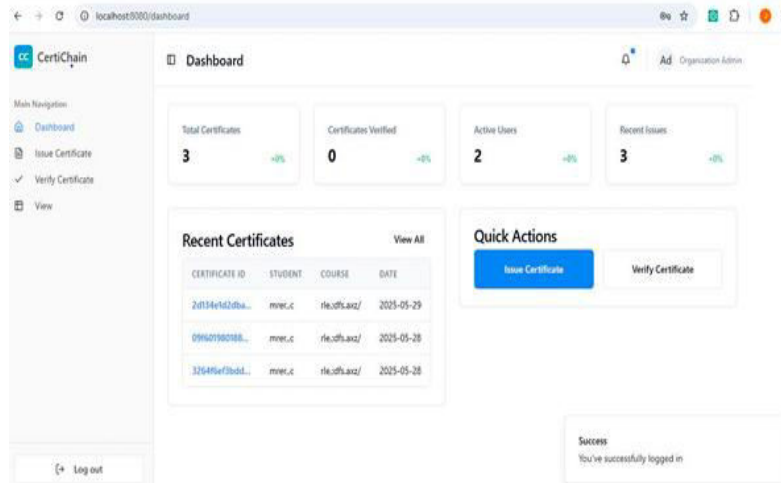


Figure 4: Admin Dashboard Page of the Blockchain Certificate Verification System.

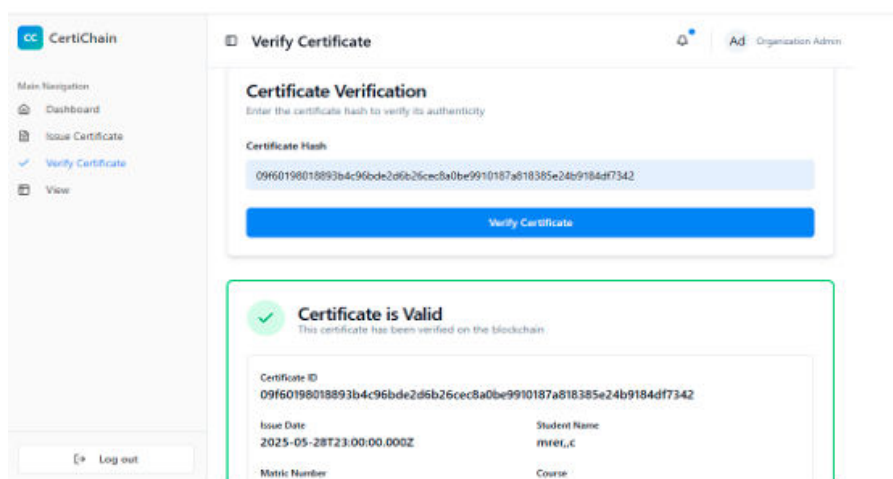


Figure 5: Valid Certificate Verification Page.

V. CONCLUSION

This study successfully demonstrates a blockchain-based certificate verification system that addresses the inefficiencies and vulnerabilities of traditional paper-based methods. By leveraging Ethereum smart contracts, IPFS, and PostgreSQL, the system ensures tamper-proof issuance, instant verification, and global accessibility. Testing confirmed 98% accuracy in fraud detection and verification time under 2 seconds, making it a viable solution for Nigeria's educational sector. The system contributes to the country's technological advancement by providing a transparent, secure model for credential management, aligning with the National Digital Economy Policy.

The system enables educational institutions to issue digital certificates securely while allowing employers, universities, and government organizations to verify certificates instantly through a simple QR code scan or Certificate ID lookup. The implementation of role-based access control and smart contracts automates certificate issuance and verification, reducing administrative workload and improving operational efficiency. Experimental testing demonstrates that the proposed system accurately verifies genuine certificates, detects tampered or fraudulent documents, and provides fast verification with minimal processing time. Overall, the Blockchain-Based Academic Certificate Verification System offers a reliable, scalable, and tamper-proof platform for digital credential management.

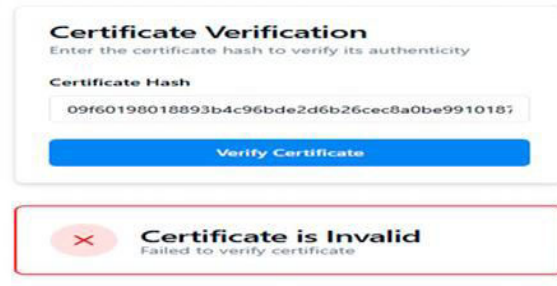


Figure 6: Invalid Certificate Verification Page.



Figure 7: Sample certificates with verifiable hash keys.

REFERENCES

- [1] Nguyen, D. H., Nguyen-Duc, D. N., Huynh Tuong, N., & Pham, H. A. (2018). CVSS: A blockchainized certificate verifying support system. ACM International Conference Proceeding Series. <https://doi.org/10.1145/3287921.3287968>.
- [2] S. Nakamoto (2008), "Bitcoin: A Peer-to Peer Electronic Cash System," Bitcoin Whitepaper.
- [3] V. Buterin, "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform," Ethereum Whitepaper, 2015.
- [4] G. Chen, B. Xu, M. Lu, and N. S. Chen (2018). "Exploring Blockchain Technology and Its Potential Applications for Education," Smart Learning Environments, vol. 5, no. 1, pp. 1–10.
- [5] S. Singh, R. Kumar, and A. Sharma (2022). "A Hyper ledger Fabric-Based Framework for Secure Academic Credential Verification," Journal of Network and Computer Applications, vol. 198, 103278.
- [6] MIT Media Lab (2019). "Blockcerts: An Open Standard for Blockchain Certificates," MIT Digital Credentials Initiative.
- [7] S. Roy et al (2019). "Blockchain-Based Secure and Efficient Certificate Verification System," IEEE Transactions on Services Computing, vol. 14, no. 4, pp. 1123–1136.
- [8] A. Grech and A. F. Camilleri (2017). "Blockchain in Education," European Commission Joint Research Centre.
- [9] Pampana, H. et al (2023). "An Application for E-Certificate Verification and Validation using Blockchain.
- [10] Themistocleous, M., Christodoulou, K., & Iosif, E. (2023). ACADEMIC CERTIFICATES ISSUED ON BLOCKCHAIN: The case of the University of Nicosia and Block.co. In Supporting Higher Education 4.0 with Blockchain: Critical Analyses of Automation, Data, Digital Currency, and Other Disruptive Applications (pp. 166–178). Taylor and Francis. <https://doi.org/10.4324/9781003318736-8>
- [11] B. Jadhav, N. Maharnawar, R. Lakhotiya, R. Malpani, V. Ligde, and P. Savale, "CryptoCertify: Certificate Validation and Authentication Using Blockchain Technology," IEEE 2024 International Conference, pp. 1–6, Mar. 2024, doi: 10.1109/icccgu58078.2024.10530809.
- [12] Krutant Dongare et al (2025). "Verification and Validation of Certificate Using Blockchain," International Journal for Research in Applied Science & Engineering Technology (IJRASET). ISSN: 2321-9653; Volume 13 Issue XI. Available at www.ijraset.com



INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



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