Blockchain and MFA: A Hybrid System for Secure Digital Credentials

Mr. Rokade. P.P[1], Mr. Abhale. B.A[2], Miss. Kalyani Jadhav[3], Miss. Shraddha Sonawane[4], Miss. Rutuja Dumbre[5], Miss. Nilesha Dhivar[6]
S.N.D College of engineering and research center yeola Savitribai Phule Pune University

***Abstract*—Traditional credential systems are often expensive, inefficient, and susceptible to forgery and security breaches, which undermine public trust. This survey paper explores how Decentralized Ledger Technology (DLT), commonly known as blockchain, can address these challenges through its core features—immutability, cryptographic hashing, and smart contracts—which enhance data integrity and reduce administrative costs. A key focus is the Blockchain-Enabled Two-Factor Honeytoken Authentication (B2FHA) system, designed to actively detect credential misuse and prevent phishing attacks. The study concludes that this hybrid, tamper- resistant approach offers significantly greater security and efficiency compared to traditional non-blockchain and standard multi-factor authentication systems, highlighting its potential for adoption in critical sectors such as finance, healthcare, and e-commerce.**

***Index Terms*—Blockchain, Decentralized Identifiers (DIDs), Smart Contracts, Cryptographic Hash Function (or Hashing), Immutability, Tamper-proof, Forgery Prevention, Data Integrity, Authentication, Two-Factor Authentication, QR Code, Digital Identity.**

I. INTRODUCTION

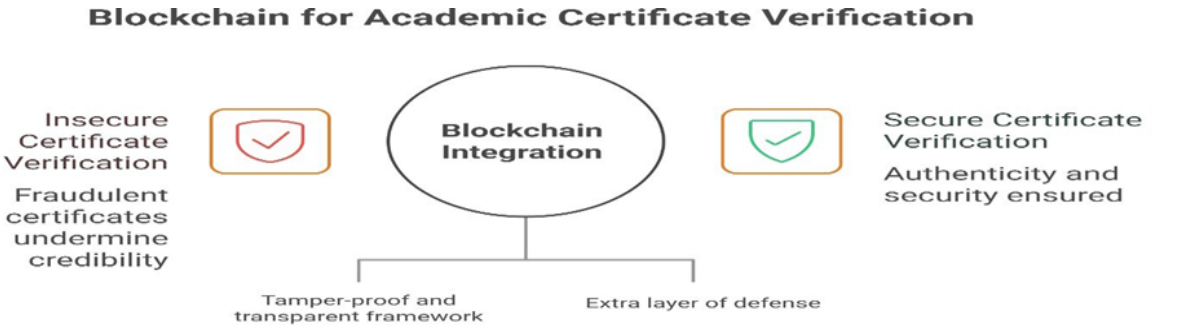


Fig 1: Tamper-Proof Verification

The growing issue of fake academic certificates has become a major concern in the education sector, as it weakens the credibility of institutions and reduces the value of genuine qualifications. Traditional systems for verifying certificates often depend on centralized databases, which are prone to fraud, inefficiency, and heavy administrative work. These limitations lead to delays, higher costs, and a lack of transparency in the verification process. Moreover, since these systems usually require significant manual effort, they are more susceptible to human error. In contrast, blockchain technology provides a decentralized, tamper-proof, and transparent framework that can overcome these challenges, ensuring the authenticity and security of academic credentials while making verification faster and more efficient.

This paper investigates the integration of blockchain technology into academic certificate verification systems, emphasizing its potential to revolutionize the management and authentication of educational credentials. To strengthen security and build user trust, the incorporation of a multi-factor

authentication (MFA) mechanism adds an extra layer of defense, protecting sensitive information and preventing unauthorized access during the verification process. The study provides a detailed review of existing literature, examines the major challenges in current verification systems, and assesses the advantages and limitations of blockchain-based approaches.

II. PROBLEM DEFINITION

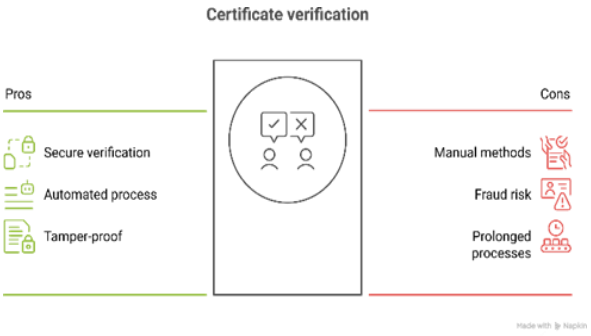


Fig 2: Overview of the Blockchain-Based Certificate Verification Process

In traditional academic systems, the verification of student certificates is largely a manual process that – involves direct communication between the verifying authority and the issuing institution. This process often requires physical submission of documents, postal correspondence, or email-based confirmation, which leads to delays, inefficiency, and administrative overhead. Educational institutions must dedicate time and staff to respond to verification requests, while employers and universities face extended waiting periods before confirming an applicant's credentials. These manual methods are not only time-consuming but also prone to human error, miscommunication, and document misplacement.

Furthermore, the existing digital systems used for certificate storage and validation are not fully secure. Many institutions rely on centralized databases or easily editable digital documents, making them vulnerable to cyberattacks, unauthorized access, and data manipulation. Fraudsters can easily forge certificates or alter information using basic editing tools, which severely undermines the authenticity and trustworthiness of academic qualifications. Such incidents compromise institutional reputation and make it difficult for employers to rely on digital credentials. As a result of these inefficiencies and vulnerabilities, hiring processes and academic admissions become significantly prolonged.

Employers must spend additional time and resources to verify the legitimacy of submitted certificates, and students face delays in admission or recruitment due to slow verification procedures. This situation emphasizes the urgent need for a secure, automated, and tamper-proof verification mechanism that eliminates human dependency, prevents forgery, and provides instant verification using technologies such as blockchain and cryptographic hashing.

III. LITERATURE SURVEY

Sr no	Paper title	Author name	year
1	Blockchain-based Authentication and Verification System for Academic Certificate using QR Code and Decentralized Applications	Shivam Gangwar, Anushka chaurasia	2024
2	Blockchain Based Certificate Verification System Management	Qurotul Aini; Eka Purnama Harahap; Nuke Puji Lestari Santoso	2022
3	Blockchain Based Certificate Validation System	Mrs. R. Suganthalakshmi, Mrs. G. Chandra Praba, Mrs. K. Abhirami, Mrs. S. Puvaneswari	2022
4	Verification and Validation of Certificate Using Blockchain	Rohan Hargude, Ghule Ashutosh, Abhijit Nawale	2021

5	Certificate Verification And Validation Using Blockchain	Anne Dhatri, Dr. A. Kalavathi	2024
6	E-Certificate Verification Using Blockchain	Nupur Vikhankar,Ankita Andhare, Ishwari Barne	2024
7	Blockchain Enabled Certificate Verification And Validation	Dr. K. Palani, Naseema Tabassum	2024
8	Utilizing Blockchain Technology for University Certificate Verification System	Olaiya Samuel Oluwaseyi	2024
9	Detecting and Preventing Credential Misuse in OTP-Based Two and Half Factor Authentication Toward Centralized Services Utilizing Blockchain-Based Identity Management	Jozef Drga, Ivan Homoliak, Juraj Van	2022
10	A Blockchain-based two Factor Honeytoken Authentication System	Vasilis Papaspirou, Leandros Maglaras, Ioanna Kantzavelou	2023

IV. OBJECTIVES

This objective focuses on replacing traditional paper-based certificates with digitally signed, blockchain-backed certificates. Each certificate is generated by an authorized institution (issuer) and secured using cryptographic algorithms like SHA-256. Once issued, the digital certificate cannot be modified or falsified because it carries a unique hash linked to the blockchain. This ensures the authenticity and originality of each document. Such a system minimizes human error, reduces administrative work, and eliminates risks of duplication or manipulation, making the certificates truly tamper- proof and verifiable for life.

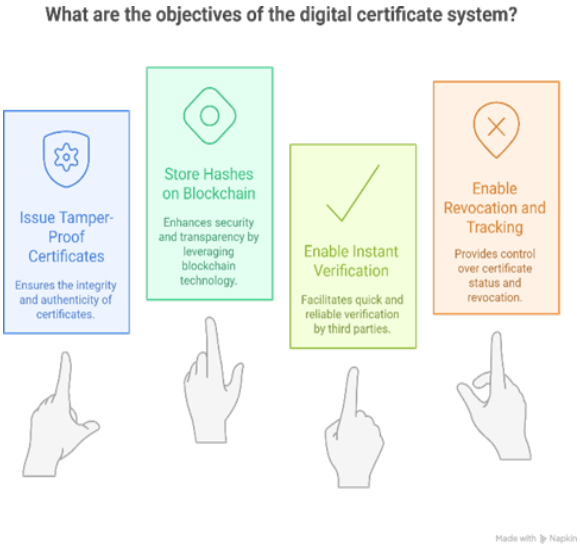


Fig 3: Objectives of the Blockchain-Based Digital Certificate System

Instead of storing the actual certificate files, only their hashed values (digital fingerprints) are recorded on the blockchain.

A hash is a short, fixed-length string generated using a cryptographic function (like SHA-256) that uniquely represents the certificate's contents. When any certificate is altered, even slightly, the hash changes

completely — allowing instant detection of forgery or modification. Because blockchain records are immutable and transparent, storing these hashes ensures permanent, decentralized, and secure proof of authenticity without revealing private or sensitive data.

Employers, universities, or government agencies (verifiers) can instantly verify any certificate's authenticity by comparing the uploaded document's hash with the one stored on the blockchain. If both hashes match, the certificate is verified as genuine and unaltered. This removes the need for time-consuming manual checks or contacting the issuing institution, thus providing fast, trustless, and transparent verification. This objective enhances trust among all stakeholders—issuers, students, and verifiers—by enabling real-time validation without intermediaries.

Sometimes certificates may need to be revoked or updated, for example, due to administrative errors or misconduct.

The system includes a revocation mechanism where the issuer can change the status of a certificate (e.g., *valid*, *revoked*, *expired*, *under review*) directly on the blockchain. Verifiers can then check not only if a certificate is genuine but also whether it is currently valid or revoked. This feature ensures lifecycle management of digital credentials and keeps all records up-to-date, transparent, and trustworthy.

V. PROPOSED SYSTEM

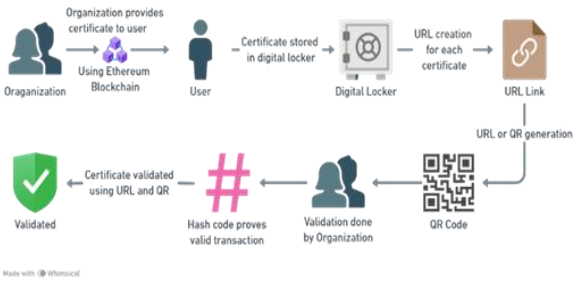


Fig 4: Workflow of Certificate Issuance and Verification Using Blockchain

The proposed system introduces a blockchain-based framework for the secure issuance, verification, and revocation of academic certificates. It integrates multi-factor authentication (MFA) for both the issuer and verifier, ensuring that only authorized individuals can issue or validate credentials. Through the combined use of SHA-256 hashing, smart contracts, and a revocation mechanism, the system enhances transparency, trust, and control over digital certificates.

The process begins when an authorized university or organization initiates the certificate creation. To prevent unauthorized access, the issuer logs in securely using MFA, which provides an additional security layer beyond standard credentials. After successful authentication, the issuer enters the student's details, including academic information and course records. The system then automatically generates a unique Certificate ID for each record.

All certificate data are subsequently processed using the SHA-256 hashing algorithm, generating a unique cryptographic hash that represents the certificate's content. This hash, along with the Certificate ID, is securely stored on the blockchain network through a smart contract, ensuring that the data are immutable and publicly verifiable.

Once stored, the system generates a digital PDF certificate that includes the student's details, Certificate ID, and a QR code or secure verification link. This QR code enables third parties to easily validate the certificate's authenticity by referencing its blockchain record.

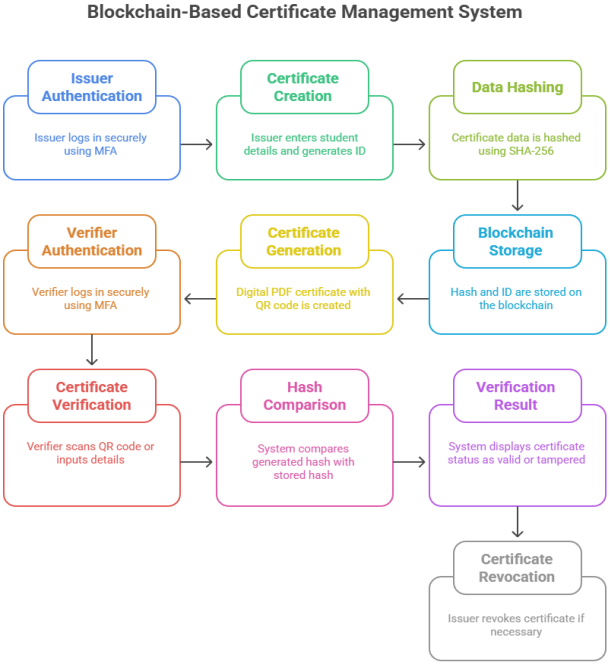


Fig 5: Workflow of Blockchain-Enabled Certificate Issuance and Verification

During the verification stage, a verifier, such as an employer or academic institution, logs in securely using MFA to access the verification portal. The verifier scans the QR code or inputs the certificate details, allowing the system to regenerate the hash value from the provided data. This hash is compared with the hash stored on the blockchain. A match confirms the certificate as "VALID", while a mismatch indicates it has been "TAMPERED" or "FAKE."

To handle cases where a certificate must be invalidated—such as errors, disciplinary actions, or withdrawal—the system includes a certificate revocation mechanism. The issuer, after MFA authentication, can trigger the revocation through a smart contract function, marking the certificate's blockchain record as "REVOKED." Any subsequent verification attempt automatically reflects this status, preventing misuse of invalid credentials.

By combining blockchain immutability, MFA-based security, SHA-256 hashing, and revocation control, the proposed system establishes a robust, transparent, and trustworthy approach to digital certificate management. It ensures end-to-end integrity from issuance to verification and provides the flexibility to revoke compromised or outdated certificates when necessary.

ARCHITECTURE:

The architecture of the proposed blockchain-based certificate verification system is designed to provide a secure, transparent, and tamper-proof environment for issuing, verifying, and revoking academic certificates. It is structured into three main layers — the User Layer, the Application Layer, and the Blockchain Layer — each performing distinct yet interconnected functions to ensure the reliability and integrity of the overall process.

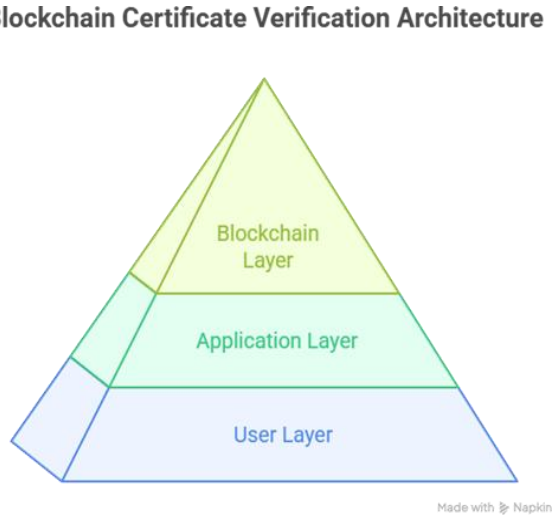


Fig 6: Three-Tier Blockchain Certificate Verification Architecture

1. User Layer

The User Layer represents the external entities interacting with the system, including issuers, students, and verifiers.

- The issuer, typically a university or organization, initiates the process of certificate creation and storage on the blockchain.
- The student receives the issued digital certificate, which contains a unique Certificate ID and a QR code or verification link.
- The verifier, such as an employer or another academic institution, validates the authenticity of the certificate using the verification portal. Both the issuer and verifier are required to authenticate through Multi-Factor Authentication (MFA) to ensure secure access and prevent unauthorized actions, whereas students can freely access their certificates for sharing or submission.

2. Application Layer

The Application Layer serves as the middleware that connects users with the blockchain network. It manages the logical flow of operations and provides interfaces for certificate issuance, verification, and revocation. This layer includes several modules:

- Authentication Module: Implements MFA for issuers and verifiers to enhance system security.
- Certificate Management Module: Handles certificate creation, assigns a unique Certificate ID, and generates the corresponding digital PDF with a QR code.
- Hashing Module: Applies the SHA-256

algorithm to the certificate data, producing a unique digital fingerprint.

- Verification Module: Recomputes hashes during verification and compares them with stored values on the blockchain to confirm validity.
- Revocation Module: Allows authorized issuers to revoke previously issued certificates, updating their status on the blockchain.

The Application Layer acts as a bridge between the user interface and the blockchain, ensuring data consistency and secure communication through smart contract functions.

3. Blockchain Layer

The Blockchain Layer forms the core of the system, ensuring immutability, transparency, and decentralized recordkeeping. It stores critical data such as the certificate's SHA-256 hash, Certificate ID, and revocation status using smart contracts.

- Smart Contracts automate certificate storage, verification, and revocation without requiring a centralized authority.
- Distributed Ledger ensures that all transactions — including certificate issuance, verification, and revocation — are permanently recorded, preventing tampering or deletion.

By separating system responsibilities across these three layers, the architecture achieves scalability, reliability, and enhanced security. The layered design also allows easy integration of additional features such as analytics dashboards, interoperability with other academic systems, and future upgrades to support emerging blockchain platforms.

WORKING:

The working of the proposed blockchain-based certificate verification system follows a structured sequence of operations that ensures secure certificate issuance, transparent verification, and controlled revocation. The entire process involves three major participants — Issuer, Student, and Verifier — and operates through the interaction of the Application
Layer and Blockchain Layer described in the system architecture

Fig 7: Life Cycle of Blockchain-Enabled Certificate Verification System

The workflow begins with the Issuer, typically a university or authorized institution, who securely logs into the system using Multi-Factor Authentication (MFA). This step verifies the issuer's identity and prevents unauthorized access to the certificate management interface. Once authenticated, the issuer enters the necessary student and course details into the system. The Application Layer then generates a unique Certificate ID for each record to ensure distinct identification.

After the data entry, the system applies the SHA-256 hashing algorithm to the complete certificate information, producing a unique cryptographic hash that represents the digital fingerprint of that certificate. This hash, along with the Certificate ID, is transmitted to the Blockchain Layer, where it is recorded through a smart contract. This process ensures that the certificate data are stored immutably and can be verified publicly without exposing sensitive personal details.

Upon successful blockchain storage, the system automatically generates a digital PDF certificate containing the student's details, Certificate ID, and a QR code or secure verification URL linked to the

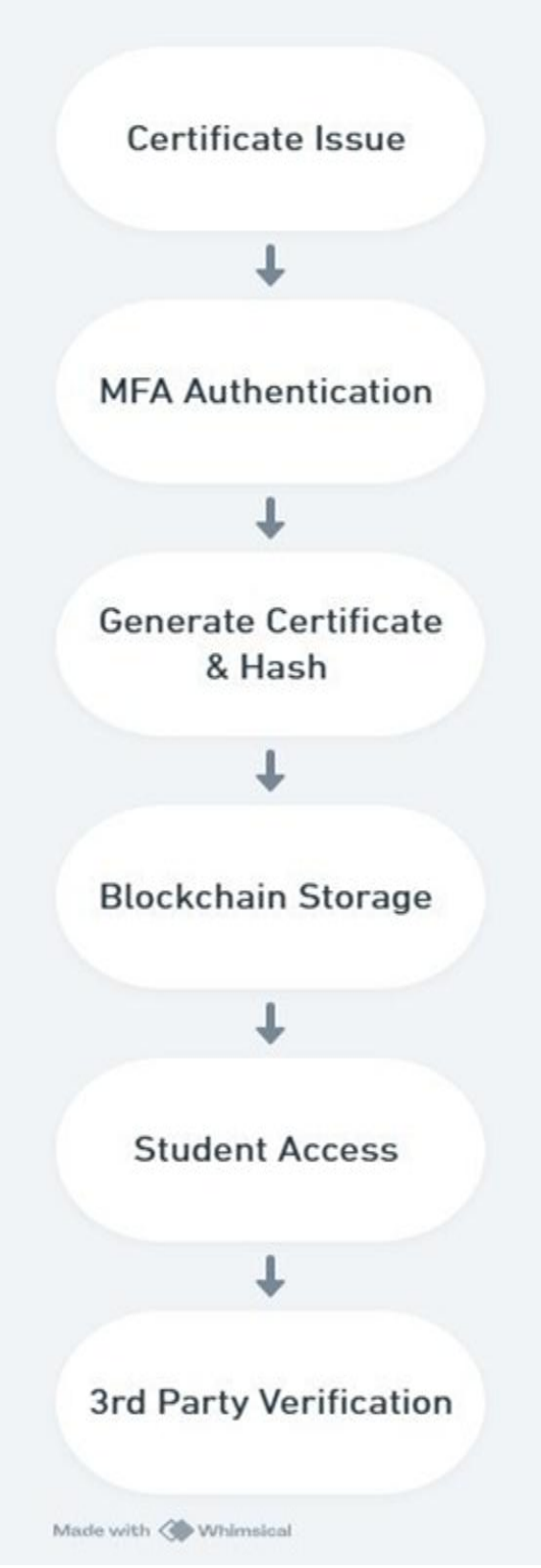
blockchain record. The digital certificate is then issued to the student, who can access it through their digital wallet, email, or institutional portal.
When a Verifier—such as an employer, recruiter, or academic body—needs to validate the certificate, they log in securely using MFA to ensure authorized access. The verifier can either scan the QR code on the certificate or manually enter the Certificate ID in the verification portal. The system retrieves the certificate details, regenerates the hash value, and compares it with the hash stored on the blockchain. If both values match, the system confirms the certificate as "VALID". If any discrepancy is detected, it flags the certificate as "FAKE" or "TAMPERED."

In cases where a certificate needs to be invalidated due to correction, cancellation, or misconduct, the issuer can initiate the revocation process. After MFA authentication, the issuer triggers the revocation function through the smart contract, which updates the certificate's status on the blockchain as "REVOKED." Any subsequent verification attempt will display the updated status, preventing further misuse of that certificate.

This sequential workflow ensures end-to-end transparency and security across the entire certificate lifecycle—from issuance to verification and revocation. By integrating MFA, blockchain immutability, cryptographic hashing, and automated smart contracts, the system minimizes manual intervention, prevents forgery, and fosters trust among academic institutions, students, and employers.

FLOWCHART:

1. System Block Diagram:



2. Certification Verification Workflow:

VI. CONCLUSION

This paper presents a blockchain-based framework for academic certificate issuance, verification, and revocation, designed to enhance security, transparency, and trust in digital credential management. By integrating Multi-Factor Authentication (MFA) for issuers and verifiers, SHA-256 hashing for data integrity, smart contracts for automated verification, and a revocation mechanism for certificate control, the system effectively addresses challenges such as certificate forgery, tampering, and inefficiencies present in traditional centralized systems. The layered architecture, comprising User, Application, and Blockchain layers, ensures secure and seamless interactions between issuers, students, and verifiers, while the workflow and algorithmic approach provide a clear, step-by-step procedure for managing certificates. Leveraging blockchain's immutability and decentralization, the system allows stakeholders to independently and reliably validate certificates, fostering trust among educational institutions, students, and employers. Overall, the proposed framework demonstrates the potential of blockchain technology to modernize academic credential management, reduce fraud, and streamline administrative processes, with future enhancements such as cross-institution interoperability, integration with decentralized identity systems, and advanced analytics promising further improvements in scalability, usability, and robustness.

REFERENCES

[1] S. Gangwar and A. Chaurasia, "Blockchain-based Authentication and Verification System for Academic Certificate using QR Code and Decentralized Applications," *International Journal of Computer Applications*, vol. 186, no. 26, pp. 1–7, June 2024. doi: 10.5120/ijca2024923722.

[2] Q. Aini, E. P. Harahap, N. P. L. Santoso, S. N. Sari, and P. A. Sunarya, "Blockchain Based Certificate Verification System Management," *APTISI Transactions on Management (ATM)*, vol. 7, no. 3, pp. 1–10, 2023. doi: 10.34306.

[3] R. Suganthalakshmi, G. C. Praba, K. Abhirami, and S. Puvaneswari, "Blockchain Based

Certificate Validation System," *International Research Journal of Modernization in Engineering, Technology and Science (IRJMETS)*, vol. 4, no. 7, pp. 3816–3819, July 202

[4] R. Hargude, G. Ashutosh, A. Nawale, and S. Adsure, "Verification and Validation of Certificate Using Blockchain," International Journal of Creative Research Thoughts (IJCRT), vol. 9, no. 6, Jun. 2021.

[5] C. Saranya et al., "Certificate Verification and Validation Using Blockchain," Journal of Emerging Trends and Novel Research (JETNR), vol. 2, no. 4, Apr. 2024.

[6] N. Vikhankar, A. Andhare, I. Barne, A. Dhawale, and S. Kauchali, "E-Certificate Verification Using Blockchain," International Journal of Engineering Research & Technology (IJERT), vol. 13, no. 5, May 2024.

[7] K. Palani and N. Tabassum, "Blockchain Enabled Certificate Verification and Validation," Journal of Engineering Sciences, vol. 15, no. 9, 2024.

[8] O. S. Oluwaseyi, "Utilizing Blockchain Technology for University Certificate Verification System," International Journal of Applied Information Systems (IJAIS), vol. 12, no. 45, Aug. 2024.

[9] J. Drga et al., "Detecting and Preventing Credential Misuse in OTP-Based Two and Half Factor Authentication Toward Centralized Services Utilizing Blockchain-Based Identity Management," arXiv preprint arXiv:2211.03490v1, Nov. 2022.

[10] L. Maglaras, V. Papaspirou, and N. Moradpoor, "A Blockchain-based Two Factor Honeytoken Authentication System," arXiv preprint arXiv:2307.05047v2, Jul. 2023.