International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

Certifichain:Blockchain-Based Credential Verification System

Mr. Rohan.R.Bhale
Assistant Professor of Information Technology
MGI-COET,Shegaon

Vaishnavi Itkhede
Dept. Information Technology
MGI-COET,Shegaon

Snehal Badgujar
Dept. Information Technology
MGI-COET,Shegaon

Rachit Sharma
Dept. Information Technology
MGI-COET,Shegaon

Lavkesh Dongre
Dept. Information Technology
MGI-COET,Shegaon

***Abstract* - Credential fraud and inefficient verification processes remain major challenges in academic and professional environments. Traditional methods of credential verification rely on manual communication between institutions and organizations, which is time-consuming, costly, and vulnerable to document forgery. To address these challenges, this paper proposes CertifiChain, a blockchain-based universal credential verification platform designed to provide a secure, transparent, and tamper-resistant mechanism for issuing and verifying digital certificates. The proposed system leverages blockchain technology to store cryptographic hashes of credentials, ensuring that once a certificate is recorded, it cannot be altered or falsified. Educational institutions can issue digitally signed certificates, while employers and other stakeholders can verify their authenticity instantly through the platform without relying on intermediaries. By integrating decentralized ledger technology, secure hashing algorithms, and smart contracts, CertifiChain enhances trust, reduces verification time, and minimizes administrative overhead. The platform aims to create a reliable and scalable infrastructure for global credential validation, thereby improving transparency and security in academic and professional credential management systems.**

Keywords: Blockchain, Credential Verification, Digital Certificates, Smart Contract, SHA-256, Decentralized Identity

I. INTRODUCTION

In the digital age, academic and professional certificates serve as essential proof of an individual's qualifications and achievements. However, the rapid growth of digital documentation has also increased the risk of fake and forged certificates, creating significant challenges for organizations attempting to verify credentials. Traditional certificate verification systems are largely manual and rely on centralized databases, making them time-consuming, inefficient, and vulnerable to data tampering or unauthorized modifications.
Credential verification is critical for maintaining trust between educational institutions, employers, and other stakeholders. The lack of a secure and globally accessible verification mechanism often results in delays and administrative overhead during the validation process.
To address these issues, blockchain technology offers a decentralized and tamper-proof platform for managing digital records. This project proposes a blockchain-based digital certificate verification system that enables secure issuance, storage, and instant verification of certificates, thereby enhancing transparency, reducing fraud, and improving the overall reliability of credential management.

II. LITERATURE REVIEW

CertifiChain is a blockchain-based system designed to securely issue, store, and verify academic or professional credentials. Traditional certificate verification methods rely on centralized databases and manual verification processes, which can be slow, costly, and vulnerable to document forgery. CertifiChain addresses these issues by using blockchain technology to create a decentralized and tamper-proof system for managing digital certificates.In CertifiChain, educational institutions or authorized organizations issue digital certificates to students or professionals. The certificate data or its cryptographic hash is stored on a blockchain network. Because blockchain records are immutable, once the certificate information is recorded, it cannot be altered or deleted, ensuring the authenticity and integrity of the credentials.The system typically uses smart contracts to automate the certificate issuance and verification process. Students receive a digital certificate with a QR code or unique identifier that links to the blockchain record. When employers or institutions need to verify the credential, they can scan the QR code or enter the certificate ID, and the system checks the blockchain ledger to confirm whether the certificate is valid.CertifiChain may also integrate technologies such as cryptographic hashing, digital signatures, and decentralized storage (e.g., IPFS) to enhance security and efficiency. By removing intermediaries and enabling instant verification, the system reduces administrative workload, prevents certificate

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

fraud, and increases trust in digital credentials.Overall, CertifiChain provides a secure, transparent, and efficient solution for credential verification in education, recruitment, and professional certification.

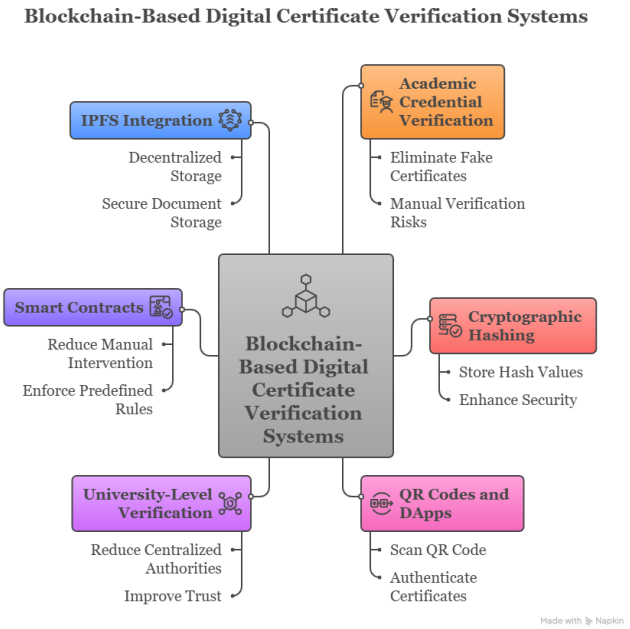

Fig 1:Blockchain-Based Digital Certificate Verification Systems

III. OBJECTIVE OF THE PROPOSED SYSTEM

The main objective of the proposed system, CertifiChain – a Blockchain-Based Credential Verification System, is to develop a secure and reliable platform for issuing, storing, and verifying digital credentials. The system uses blockchain technology to ensure that certificates cannot be altered or forged once they are recorded on the network. It also aims to simplify and speed up the verification process by allowing employers or institutions to verify certificates instantly using a unique ID or QR code. In addition, the system promotes transparency and reduces manual effort by providing a decentralized and automated method for managing and validating academic or professional credentials.

- To Provide Secure Credential Storage: The system aims to store academic and professional certificates securely using blockchain technology. Since blockchain records are immutable, the stored credential information cannot be modified or tampered with.
- To Prevent Certificate Fraud and Forgery: One of the major objectives of CertifiChain is to eliminate fake certificates. By recording certificate data or its hash on the blockchain, the authenticity of credentials can be easily verified.
- To Enable Fast and Easy Verification: The proposed system allows employers, universities, or organizations to verify certificates instantly using a unique ID or QR code linked to the blockchain record.
- To Create a Decentralized Verification System: Unlike traditional systems that depend on centralized databases, the proposed system uses blockchain's decentralized architecture, which increases transparency and reliability.
- To Reduce Manual Verification Effort: The system automates certificate verification using smart contracts, reducing the need for manual checks by institutions and saving time and administrative costs.
- To Ensure Data Integrity and Transparency: By using cryptographic techniques and blockchain technology, the system ensures that certificate data remains accurate, trustworthy, and transparent for all authorized users.
- To Provide Easy Access to Digital Credentials: Students and professionals can securely store and share their digital certificates with organizations whenever required.

IV. PROPOSED SYSTEM

A. System Architecture and Design

The proposed system is designed to establish a secure, decentralized, and efficient framework for the issuance and verification of digital certificates using blockchain technology. Initially, authorized educational institutions register within the system and submit certificate-related data of students through a secure interface. The submitted data undergoes validation and is systematically stored within the application environment. Each certificate is associated with a unique identifier, such as a Quick Response (QR) code or certificate identification number, to facilitate seamless retrieval and verification.

Subsequently, a cryptographic hash of the certificate data is generated and recorded on the blockchain ledger. Owing to the immutable nature of blockchain, once the data is stored, it cannot be altered or deleted, thereby ensuring data integrity and authenticity.

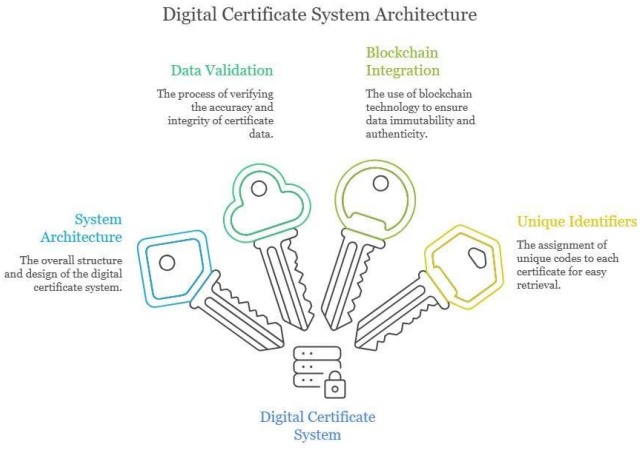

Fig 2:Digital Certificates Systems Architecture

B. Digital Certificate Issuance

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

The digital certificate issuance process follows a structured and standardized approach. The issuing authority provides essential information, including student details, course information, institutional identity, and issuance date. The system processes this data to generate a digital certificate in a predefined format.

A hash value corresponding to the certificate data is computed and stored on the blockchain network. Additionally, smart contracts are employed to automate the issuance process, enforce predefined rules, and ensure consistency and reliability in certificate management.

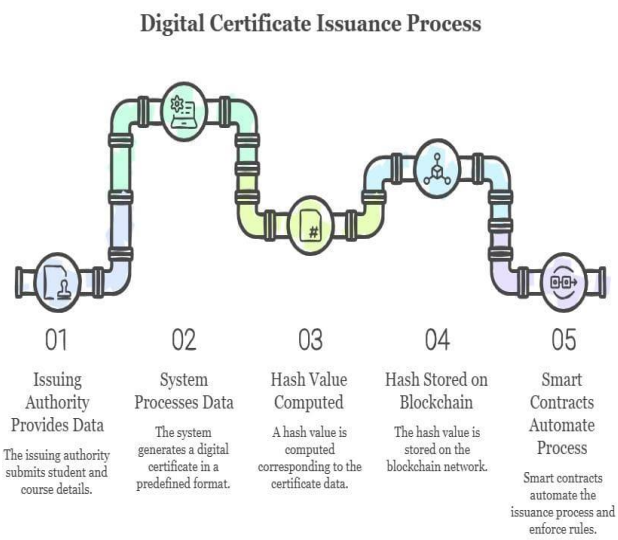

Fig 3:Digital Certificates Issuance

C. Hash Generation and Security Mechanism

To ensure data security and integrity, the system utilizes cryptographic hashing techniques, specifically algorithms such as SHA-256. The hashing process transforms certificate data into a fixed-length alphanumeric string that uniquely represents the original data.

A minor alteration in the input data results in a significantly different hash value, thereby enabling efficient detection of data tampering. The generated hash is permanently stored on the blockchain, serving as a trusted reference for subsequent verification processes.

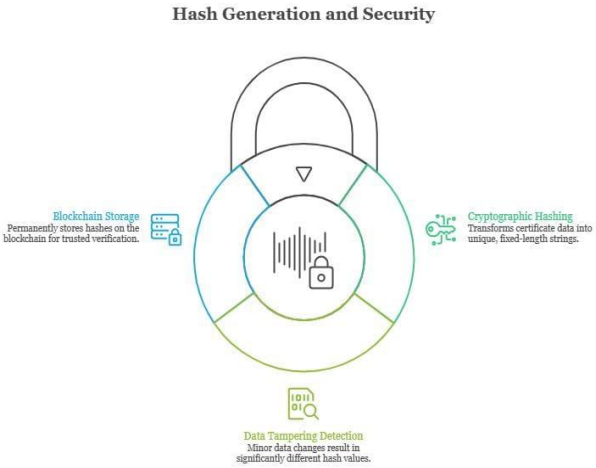

Fig 4:Hash Generation and Security

D. Certificate Verification Mechanism

The verification mechanism is designed to provide a reliable and automated approach for validating digital certificates. Users initiate the verification process by entering the certificate identification number or scanning the associated QR code. The system retrieves the corresponding certificate data and recomputes its hash value.

This computed hash is then compared with the hash stored on the blockchain ledger. A successful match confirms the authenticity and integrity of the certificate, whereas a mismatch indicates potential tampering or forgery. This mechanism eliminates the need for manual verification and enhances system efficiency.

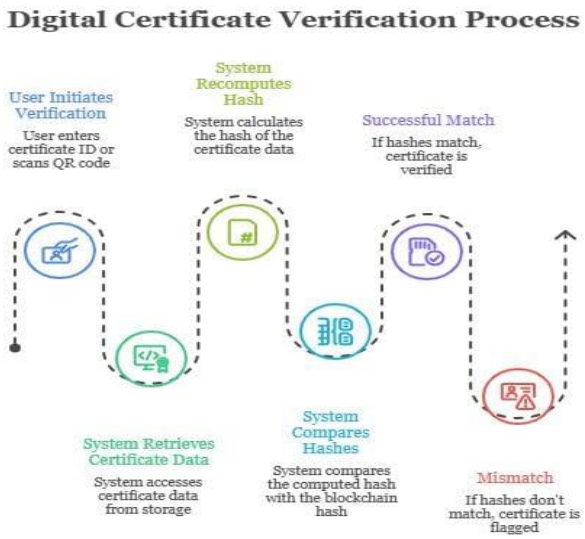

Fig 5:Certificate Verification Mechanism

E. Operational Workflow of the System

The overall operation of the system is facilitated through an intuitive and user-friendly interface. Educational institutions can upload and manage certificate data via a dedicated dashboard, while the backend system processes the data and interacts with the blockchain network for secure storage.

Upon successful issuance, students receive digital certificates embedded with a QR code or verification link. Verifiers can access the system to authenticate certificates in real time by utilizing these identifiers. This streamlined workflow ensures transparency, minimizes verification time, and enhances the overall reliability of digital credential management.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

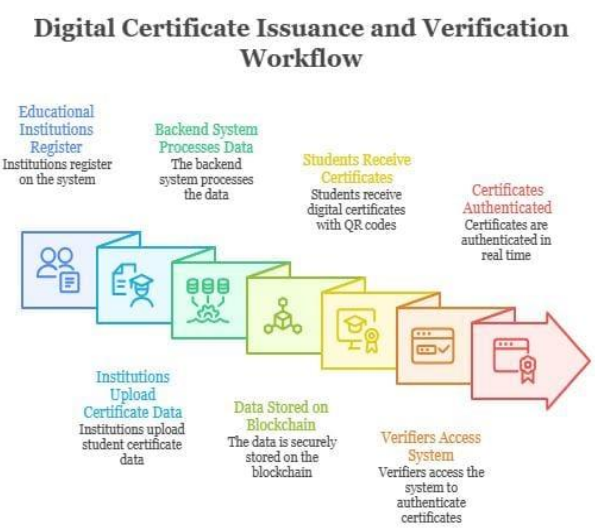

Fig 6:Operational Workflow of System

V. ALGORITHM

i. Start
ii. Input certificate ID or scan QR code
iii. Retrieve certificate details from system
iv. Generate hash value using certificate data
v. Fetch stored hash from blockchain
vi. Compare generated hash with stored hash
vii. If both hashes are equal

Display “Certificate is Valid”

Else

Display “Certificate is Invalid”

viii. End

The algorithm verifies a digital certificate by taking input in the form of a certificate ID or QR code. The system retrieves the certificate details and generates a hash value from the data. It then fetches the original hash stored on the blockchain and compares both values. If the hashes match, the certificate is valid; otherwise, it is invalid. This process ensures secure and tamper-proof verification.

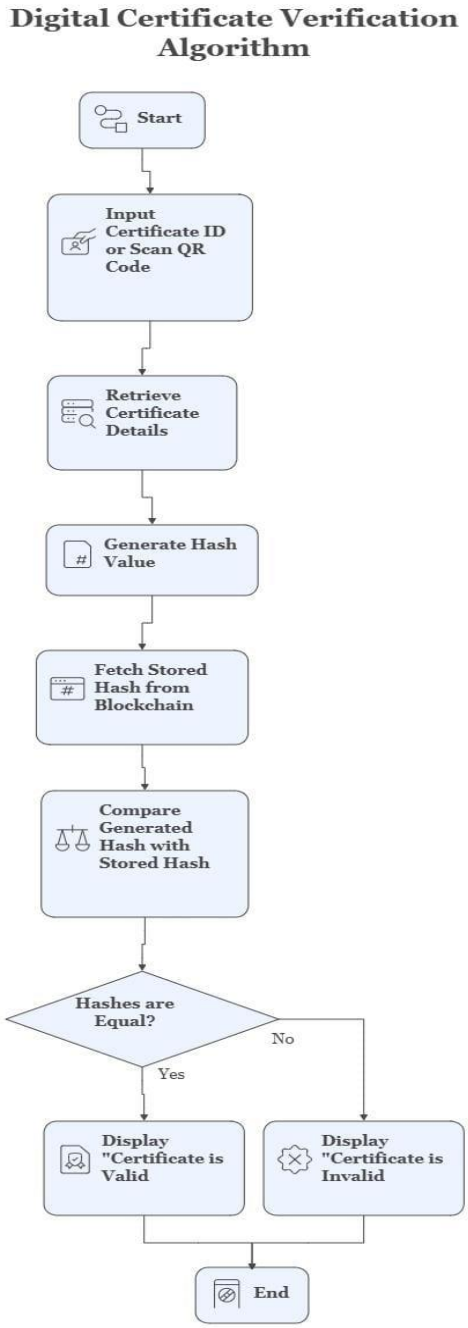

Fig 7:Certificate Verification Algorithm

VI. CONCLUSION

This paper presents a secure and efficient approach for digital certificate issuance and verification using blockchain technology. The proposed system addresses the limitations of traditional certificate management systems, such as susceptibility to fraud, lack of transparency, and dependency on manual verification processes. By leveraging the decentralized and immutable characteristics of blockchain, the system ensures that certificate data remains tamper-proof and reliable.

The integration of cryptographic hashing techniques enhances data integrity by enabling accurate detection of any

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

unauthorized modifications. Furthermore, the use of QR codes and unique certificate identifiers facilitates quick and user-friendly verification. The implementation of smart contracts automates key processes, thereby reducing administrative overhead and improving operational efficiency.

Overall, the proposed solution provides a robust framework for secure credential management, minimizing the risk of certificate forgery while ensuring transparency and trust among stakeholders. The system can be further extended to support large-scale deployment across multiple institutions, contributing to the development of a reliable and globally accessible digital verification ecosystem.

VII. REFERENCES

[1] D. Shukla et al., "A Blockchain-Based System for Digital Certificate Verification," 2024. ResearchGate

[2] S. Gangwar et al., "Blockchain-based Authentication and Verification System for Academic Certificate using QR Code and Decentralized Applications," International Journal of Computer Applications, 2024. ResearchGate

[3] O. S. Oluwaseyi et al., "Utilizing Blockchain Technology for University Certificate Verification System," International Journal of Applied Information Systems, 2024. ijais.org

[4] S. H. D. et al., "Secure Academic Certificate Authentication Using Blockchain Technology," 2025. SSRN

[5] K. Dongare et al., "Verification and Validation of Certificate Using Blockchain," IJRASET, 2025. IJRASET

[6] T. R. Sree et al., "Decentralized Certificate Issuing and Verification System Based on Ethereum Blockchain," 2025. ScienceDirect

[7] S. K. Patel et al., "Secure Digital Academic Certificate Verification Using Blockchain and Cryptographic Techniques," 2024. inderscience.com

[8] S. H. Said et al., "Blockchain-Based Conceptual Model for Certificate Verification," Engineering, Technology & Applied Science Research, 2023. ETASR

[9] T. Rahman et al., "Verifi-Chain: A Credentials Verifier using Blockchain and IPFS," 2023. arXiv