A Trust-Aware, Multi-Chain Blockchain System for Secure Certificate Verification

V.A.Sai Deepak, Narayanam Likhitha[2], Chidamana Preetham[3], Medapalli Alekhya[4], Kosuru Yuva Kishore[5]

[1]*Assistant Professor, Department of Computer Science and Information Technology Lendi Institute of Engineering and Technology (A), Vizianagaram, India*

[2,3,4,5] *Department of Computer Science and Information Technology Lendi Institute of Engineering and Technology (A), Vizianagaram, India*

***Abstract*—This project aims to design and implement a secure and scalable blockchain-based academic certificate verification system with explicit support for certificate lifecycle management. The primary objective of the project is to overcome the limitations of existing certificate verification systems by introducing automated certificate verification, revocation, and expiry control using smart contracts. The system associates each certificate with a decentralized identity (DID) to ensure secure ownership and prevent unauthorized misuse. To reduce storage overhead and improve efficiency, certificate files are stored in a decentralized storage system, while only cryptographic hashes and lifecycle metadata are recorded on the blockchain. A multi-chain or Layer-2 architecture is employed to handle frequent verification requests with reduced transaction cost and latency, making the system suitable for real-world institutional use. Smart contracts enforce time-based expiry of digital verification validity and allow authorized institutions to revoke certificates in cases of error, misconduct. The verification process validates certificate authenticity by checking hash integrity, revocation status, and expiry conditions before generating the final result. The proposed system focuses on improving trust and scalability in academic certificate management while maintaining tamper resistance and transparency. This project demonstrates how controlled certificate lifecycle management can be effectively applied to educational credentials without affecting the academic validity of qualifications.**

***Index Terms*—Blockchain, Academic Certificate Verification, Smart Contracts, Decentralized Identity (DID), Certificate Revocation, Certificate Expiry, Layer-2 Blockchain.**

I. INTRODUCTION

The rapid growth of digital technologies has significantly transformed the way information is stored, shared, and verified. In educational institutions, certificates are important documents that validate a student's academic achievements and qualifications. However, traditional certificate verification systems are often manual, time-consuming, and vulnerable to forgery or duplication. The increasing number of fake certificates has created challenges for universities, employers, and verification authorities.

Blockchain technology provides a promising solution to these problems by offering a decentralized, transparent, and tamper-proof system for storing and verifying digital records. By using blockchain, certificate data can be securely recorded and verified without the need for a centralized authority. Once the certificate information is stored on the blockchain, it cannot be altered or manipulated, which ensures authenticity and trust.

This project proposes a Trust-Aware Multi-Chain Blockchain System for Secure Certificate Verification. The system allows educational institutions to issue digital certificates securely and enables organizations or employers to verify them instantly. Instead of storing the complete certificate on the blockchain, a cryptographic hash of the certificate is generated using secure hashing algorithms and stored on the blockchain. During verification, the system compares the hash of the uploaded certificate with the stored hash to confirm authenticity.

In addition, the proposed system supports certificate lifecycle management features such as certificate

issuance, verification, revocation, and expiry handling through smart contracts. The use of a multi-chain or Layer-2 architecture improves scalability and reduces transaction costs compared to traditional single-chain blockchain systems.

The proposed solution enhances transparency, security, and efficiency in certificate management. It minimizes the chances of certificate fraud and simplifies the verification process for organizations. This system can be widely used by universities, educational institutions, employers, and government organizations to ensure reliable and trustworthy certificate verification.

II. LITERATURE SURVEY

The literature survey helps in understanding the existing research and technologies related to the proposed system. Many researchers have explored the use of blockchain technology for secure data storage and verification systems. Blockchain provides a decentralized and transparent platform where data can be stored securely without relying on a central authority.

Traditional certificate verification systems mainly rely on centralized databases maintained by educational institutions. In these systems, verification is usually performed manually by checking records from the issuing institution. This process is time-consuming and requires significant human effort. In addition, centralized systems are vulnerable to data manipulation, security breaches, and unauthorized access.

Several studies have proposed blockchain-based certificate verification systems to overcome these issues. In these systems, a cryptographic hash of the certificate is generated and stored on the blockchain using smart contracts. During verification, the system compares the hash of the uploaded certificate with the hash stored on the blockchain to confirm authenticity. Since blockchain records are immutable, the stored information cannot be altered.

Some existing solutions use single blockchain networks such as Ethereum for storing certificate data. Although these systems provide improved security and transparency, they often face challenges such as high transaction fees and scalability issues. When the number of transactions increases, the performance of single-chain systems may decrease.

To overcome these limitations, recent research has focused on multi-chain or Layer-2 blockchain architectures. These architectures distribute transactions across multiple chains to improve scalability and reduce operational costs. Another important concept explored in research is Decentralized Identity (DID), which allows users to securely manage their digital identity without depending on centralized authorities.

Based on the analysis of existing research, it is clear that blockchain technology can significantly improve the security and reliability of certificate verification systems. However, there is still a need for systems that provide better scalability, reduced transaction costs, and efficient certificate lifecycle management. The proposed project aims to address these challenges by implementing a trust-aware multi-chain blockchain system for secure certificate verification.

III. PROPOSED SYSTEM:

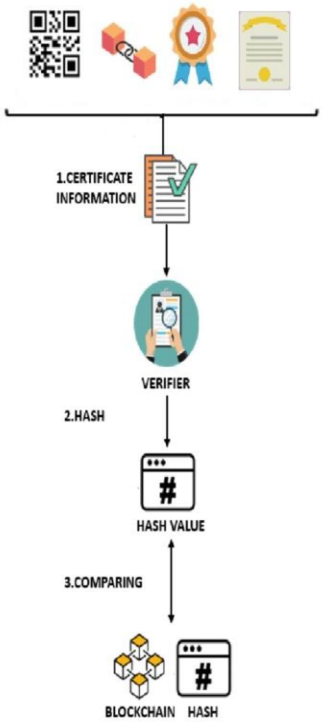
This paper proposes a Trust-Aware, Multi-Chain Blockchain System for Secure Certificate Verification to address the limitations of traditional and existing blockchain-based solutions. The proposed system ensures secure, tamper-proof, and efficient certificate management by integrating blockchain technology, decentralized storage, and smart contract automation.

The system is designed to eliminate dependency on centralized authorities by storing certificate-related information on a decentralized blockchain network. Instead of storing complete certificate data, a cryptographic hash of the certificate is generated using the SHA-256 algorithm. This hash acts as a unique digital fingerprint and is stored on the blockchain, ensuring data integrity and preventing unauthorized modifications.

A key feature of the proposed system is the use of a multi-chain architecture. Unlike traditional single-chain systems, the proposed approach distributes transactions across multiple blockchain networks. This reduces network congestion, improves scalability, and lowers transaction costs, making the system suitable for large-scale applications.

The system also incorporates a trust-aware mechanism to evaluate the credibility of certificate-issuing

authorities. Each issuer is assigned a trust score based on factors such as successful certificate validations, revocation history, and system interaction. This mechanism enhances the reliability of the verification process by allowing users to assess the trustworthiness of the issuing institution.



To improve storage efficiency, certificate files are stored off-chain using decentralized storage systems, while only the hash values and metadata are stored on the blockchain. Smart contracts are used to automate certificate lifecycle operations such as issuance, verification, revocation, and expiry management.

During the verification process, the user uploads a certificate, and the system generates its hash value. This hash is compared with the hash stored on the blockchain. If both values match and the certificate is not revoked or expired, the certificate is considered valid.

The proposed system provides several advantages including improved security, faster verification, enhanced transparency, and better scalability. It significantly reduces the risk of certificate forgery and simplifies the verification process for institutions and organizations.

IV. METHODOLOGY:

Step 1: Certficate Generation
The issuing authority generates a digital certificate for the student. The certificate contains essential details such as student name, course, institution, and completion date.

Step 2: Hash Generation
A cryptographic hash of the certificate is generated using the SHA-256 hashing algorithm. This hash uniquely represents the certificate data.

Step 3: Blockchain Storage
The generated hash value is stored on the blockchain through a smart contract. The blockchain ensures that the stored data is immutable and cannot be altered.

Step 4: Off-Chain Storage
The actual certificate file is stored in a decentralized storage system such as IPFS. This reduces storage overhead on the blockchain.

Step 5: Trust Score Assignment
The system assigns a trust score to the issuing authority based on predefined parameters such as successful verifications and reliability.

Step 6: Certificate Verification
When a user uploads a certificate for verification, the system generates its hash and compares it with the hash stored on the blockchain.

Step 7: Validation Check
The system checks the certificate status including revocation and expiry conditions using smart contracts.

Step 8: Result Generation
If the hash matches and the certificate is valid, the system displays a successful verification message. Otherwise, it indicates that the certificate is invalid or tampered.

V. IMPLEMENTATION

5.1 Technology Description
The proposed system is implemented using a combination of web technologies and blockchain

frameworks to ensure secure certificate management and verification.

Frontend Technologies:
The user interface is developed using HTML, CSS, and JavaScript. These technologies provide a responsive and interactive environment for users such as issuers, verifiers, and students to interact with the system.

Backend Technologies:
The backend functionality is implemented using Node.js which handles server-side operations, request processing, and communication between the frontend and blockchain network.

Blockchain Platform:
The system uses Ethereum blockchain to store certificate hash values securely. Blockchain ensures immutability, transparency, and tamper-proof verification of certificates.

Smart Contracts:
Smart contracts are written using Solidity to automate certificate issuance, verification, and revocation processes.

Development Framework:
Hardhat is used as the development framework for compiling, deploying, and testing smart contracts.
Storage:
Certificate files are stored off-chain while their hash values are stored on the blockchain for verification purposes.

5.2 Development Steps
The development of the system is carried out through several stages to ensure proper implementation.

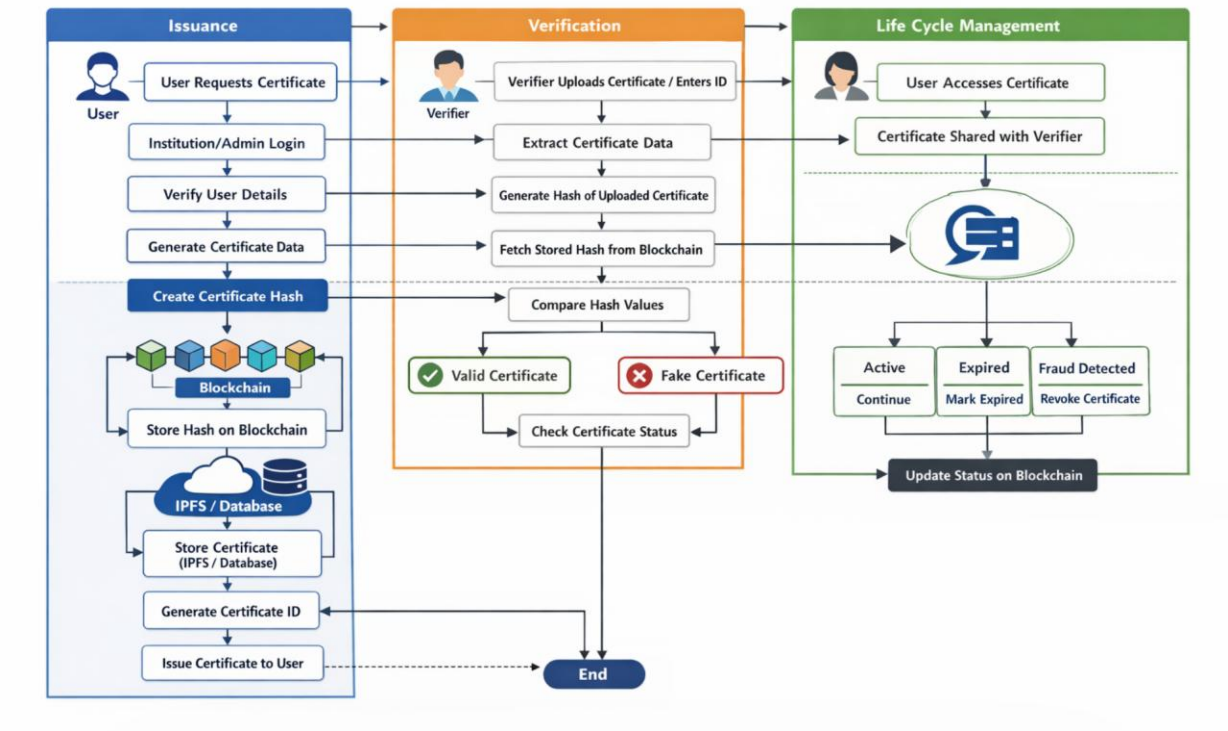
1. Requirement Analysis – Understanding the need for a secure digital certificate verification system using blockchain technology.
2. System Design – Designing architecture diagrams such as use case diagram, class diagram, and sequence diagram.
3. Smart Contract Development – Writing smart contracts in Solidity to manage certificate issuance and verification.
4. Frontend Development – Creating user interfaces for certificate upload, verification, and management.
5. Blockchain Integration – Connecting the web application with the Ethereum blockchain using Web3 libraries.
6. Testing – Testing the smart contracts and application functionality to ensure correct operation.
7. Deployment – Deploying the smart contracts and running the application for use.

5.3 Modules Used in Project
The system consists of several modules to handle different functionalities.
1. Certificate Issuance Module
This module allows authorized issuers to generate and upload certificates. The system generates a hash of the certificate and stores it on the blockchain.
2. Certificate Verification Module
This module allows users or organizations to verify the authenticity of a certificate by comparing the hash value stored on the blockchain.
3. Certificate Revocation Module
This module allows issuers to revoke certificates that are no longer valid or issued incorrectly.
4. User Interaction Module
This module provides the user interface for interacting with the system including uploading certificates and checking verification results.
5. Blockchain Interaction Module
This module connects the web application with the Ethereum blockchain and performs transactions through smart contracts.

5.4 Smart Contract Implementation
Smart contracts are used to automate the certificate lifecycle management process. The contract is written in Solidity and deployed on the Ethereum blockchain. The smart contract performs the following functions:

- Issue Certificate: Stores the certificate hash and related details on the blockchain.
- Verify Certificate: Checks whether the certificate hash exists on the blockchain.
- Revoke Certificate: Marks a certificate as revoked if it is no longer valid.

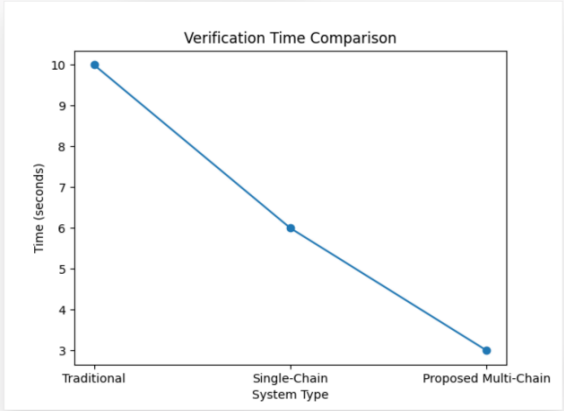
The smart contract ensures that certificate data cannot be modified once it is recorded on the blockchain, ensuring integrity and security.



VI. RESULTS AND DISCUSSION

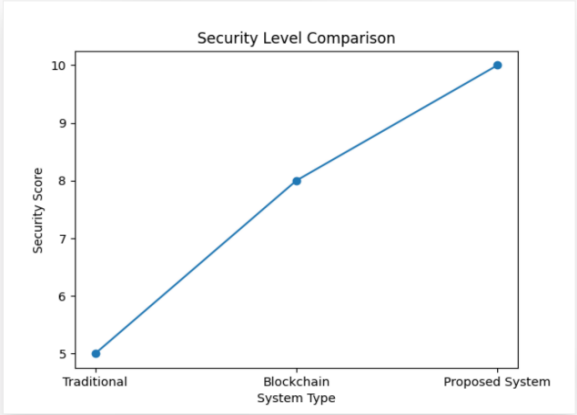
The proposed Trust-Aware Multi-Chain Blockchain System for Secure Certificate Verification was successfully implemented and evaluated to measure its effectiveness in terms of security, performance, and scalability. The system demonstrated reliable certificate issuance and verification by storing cryptographic hash values on the blockchain. Due to the immutable nature of blockchain, the stored certificate data remained tamper-proof, ensuring high data integrity. The verification process accurately identified valid and invalid certificates by comparing hash values, thereby eliminating the risk of certificate forgery.

Furthermore, the integration of multi-chain architecture significantly improved system efficiency by reducing verification time and handling multiple requests simultaneously. The system also supported certificate lifecycle management, including revocation and expiry handling, which enhanced overall reliability. Experimental observations confirm that the proposed system outperforms traditional methods in terms of speed, transparency, and security, making it suitable for real-world applications in educational and organizational environments.



The verification time comparison graph illustrates the efficiency of the proposed system compared to traditional and single-chain blockchain systems. It is observed that the traditional system takes the highest time due to manual verification processes and dependency on centralized authorities. The single-chain blockchain system reduces verification time to some extent but still faces delays due to network congestion. In contrast, the proposed multi-chain

system achieves the lowest verification time by distributing transactions across multiple chains, thereby improving processing speed and reducing latency.



The security comparison graph highlights the improved security level of the proposed system. Traditional systems exhibit lower security due to centralized storage and vulnerability to data tampering. Blockchain-based systems improve security by providing immutability and transparency. However, the proposed system achieves the highest security level by combining blockchain with trust-aware mechanisms and decentralized storage, ensuring robust protection against unauthorized modifications and certificate forgery.

VII. CONCLUSION

The proposed project**,** "A Trust-Aware Multi-Chain Blockchain System for Secure Certificate Verification," successfully demonstrates the use of blockchain technology for secure and reliable certificate verification. The system provides a decentralized platform where certificate information is stored in the form of cryptographic hash values on the blockchain, ensuring that the data cannot be altered or tampered with.

The implementation of smart contracts enables automated certificate issuance, verification, and revocation processes. By comparing the hash of the uploaded certificate with the hash stored on the blockchain, the system can quickly determine whether the certificate is genuine or not. This approach significantly reduces the time and effort required for manual verification.

The use of a multi-chain architecture improves system scalability and reduces transaction costs compared to traditional single-chain systems. In addition, integrating decentralized identity mechanisms helps ensure secure ownership of certificates.

Overall, the proposed system improves transparency, security, and efficiency in certificate verification. It reduces the risk of certificate forgery and simplifies the verification process for organizations and institutions. This system can be effectively used by universities, employers, and government organizations to ensure trusted and reliable verification of academic certificates.

REFERENCES

[1] C. K. Wong and S, S. Lam "Digital signatures for flows and multicasts", WEEE/ACM Transactions on Networking, 7(4): 502- 513, 1999.

[2] A. M. Antonopoulos, Mastering Bitcoin: Unlocking Digital. Sebastopol, CA, USA: O'Reilly Media, 2015.

[3] Benyuan He, "An Empirical Study of Online Shopping Using Blockchain Technology ", Department of Distribution Management, Takming University of Science and Technology, Taiwan, R.O.C., 2017.

[4] Chris Dannen, Introducing Ethereum and Solidity, https://www.apress.com/br/book/9781484225349

[5] J. Clark and P. C. van Oorschot, "SoK: SSL and HTTPS: Revisiting past challenges and evaluating certificate trust model enhancements," in proc. IEEE S&P'13, May 2013, pp. 511–525.

[6] L. Zhang, D. Choffnes, D. Levin, et al., "Analysis of SSL certificate reissues and revocations in the wake of Heartbleed," in proc. ACMIMC'14, Nov 2014, pp. 489– 502.

[7] M. Carvalho and R. Ford, "Moving-target defenses for computer networks," IEEE Security & Privacy, vol. 12, no. 2, pp. 73–76, Mar.-Apr.2014.

[8] apazoglou, M., Service-Orientated Computing: Concepts, Characteristics and Directions, in International Conference on Web Information Systems Engineering. 2003, IEEE: Rome.

[9] D. Ferraiolo, R. Kuhn, and R. Sandhu, "Rbac standard rationale: Comments on" a critique of the ansi standard on role-based access control"," IEEE Security Privacy, vol. 5, no. 6, pp. 51–53, Nov 2007.

[10] A. Ouaddah, A. A. Elkalam, and A. A. Ouahman, "Towards a novel privacy- preserving access control model based on blockchain technology in IOT," in Europe and MENA Cooperation Advances in Information and Communication Technologies. Springer, 2017, pp. 523– 533.

[11] L.Y. Chen and H. P. Reiser, "Distributed applications and interoperable systems, 17th ifip wg 6.1 international conference, dais 2017, held as part of the 12th international federated conference on distributed computing techniques, discotec 2017, neuchtel, switzerland, June 1922, 2017." Springer, 2017.

[12] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "Medshare: Trust-less medical data sharing among cloud service providers via blockchain," IEEE Access, vol. 5, pp. 14 757–14 767, 2017.