Certchain: Decentralized Certificate Verification System

Hrithik Singh[1], Sairaj Khot[2], Jaykumar Sathe[3], Sahil Dhabhekar[4], Dr. Vanitha Soman[5]
[1,2,3,4] *Computer Science and Engineering (Data Science) Mahatma Gandhi Mission's College of Engineering and Technology, Navi Mumbai, India*
[5] *Dept. Computer Science and Engineering (Artificial Intelligence and Machine Learning) Mahatma Gandhi Mission's College of Engineering and Technology Navi Mumbai, India*

***Abstract*—Certificate fraud and the limitations of centralized verification systems have made secure and tamper-proof solutions essential. Traditional certificate validation methods rely on intermediaries and are prone to forgery and delays. This paper introduces CertChain, a decentralized application designed to provide a reliable and cost-efficient framework for issuing and verifying academic certificates using blockchain technology.**

The system adopts a hybrid architecture where cryptographic hashes of certificates are stored on the Ethereum blockchain, while actual files are maintained on cloud-based off-chain storage to reduce storage cost, improve scalability, and enable better accessibility. Smart contracts ensure data integrity and immutability, while MetaMask enables secure authentication and controlled access. The platform supports dual verification using certificate IDs and hash-based validation, providing transparency and flexibility. The system also includes a user-friendly interface for certificate management and verification.

***Index Terms*—Blockchain, Certificate Verification, Smart Contracts, Decentralized Applications (DApps), SHA-256, Hybrid Storage, Ethereum, MetaMask, Cloud Storage**

I. INTRODUCTION

1.1 Context and Motivation

With the rapid growth of digital education and online certifications, ensuring the authenticity of academic credentials has become a major challenge. Traditional certificate verification systems rely on centralized authorities, making them vulnerable to forgery, manipulation, and delays in validation. These systems often require manual verification processes, which are time-consuming and inefficient.

Blockchain technology offers a promising solution by providing a decentralized, transparent, and tamper-proof environment for storing and verifying data [1], [6]. However, directly storing certificate files on blockchain is expensive and inefficient due to high storage costs. This creates a need for a system that ensures security while maintaining cost efficiency.

1.2 Research Gap and Challenges

Existing certificate verification systems are either fully centralized or entirely blockchain-based. Centralized systems lack transparency and are prone to data tampering, while fully decentralized solutions suffer from high storage costs and scalability issues.

Although several blockchain-based solutions have been proposed, many of them store large amounts of data on-chain, leading to increased transaction costs. Additionally, such systems often require technical expertise, limiting their usability for general users. Another challenge is ensuring secure yet efficient verification without compromising performance or user experience.

1.3 Research Objectives and Key Contributions

The primary objectives and contributions of this research work are as follows:

- To design and develop CertChain, a decentralized application for secure certificate issuance and verification.
- To implement a hybrid architecture combining on-chain hash storage with off-chain file storage for cost optimization.
- To enable dual verification mechanisms using blockchain-based certificate IDs and hash-based validation.
- To provide a user-friendly interface with secure authentication using MetaMask.
- To ensure data integrity, transparency, and scalability in certificate management systems.

II. LITERATURE REVIEW

1. Blockchain-Based Certificate Verification Systems

Several blockchain-based solutions have been proposed to address certificate fraud and verification challenges. Systems such as Blockcerts utilize blockchain technology to provide tamper-proof digital certificates, ensuring authenticity and transparency [9]. These systems leverage cryptographic hashing and decentralized storage to prevent data manipulation [8]. However, many existing approaches store large amounts of certificate data directly on-chain, leading to high transaction costs and scalability issues [6].

2. Smart Contracts and Data Integrity

Smart contracts play a crucial role in ensuring secure and automated certificate verification using Ethereum-based frameworks [2], [3]. Studies highlight the use of Ethereum-based smart contracts to store and validate certificate data through immutable records. Cryptographic techniques such as SHA-256 hashing are widely used to ensure data integrity and prevent tampering, supported by secure smart contract models [10]. While these approaches provide strong security guarantees, they often lack cost optimization and efficient data handling mechanisms.

3. Decentralized Applications (DApps) and Blockchain Integration

Decentralized applications (DApps) have been widely adopted for building transparent and trustless systems. Research shows that integrating blockchain with web technologies such as React and Node.js enables the development of user-friendly and scalable platforms. Wallet-based authentication systems like MetaMask provide secure access control and transaction management. However, many DApps face challenges related to usability, scalability, and dependency on blockchain networks.

4. Hybrid On-Chain and Off-Chain Architectures

To overcome the limitations of full on-chain storage, hybrid architectures have been proposed. These systems store only essential data, such as hashes, on the blockchain while keeping large files off-chain using cloud-based storage solutions. This approach significantly reduces storage costs while maintaining data integrity through hash verification. Despite its advantages, maintaining synchronization between on-chain and off-chain data remains a key challenge.

III. PROPOSED METHOD

3.1 Architecture of the System

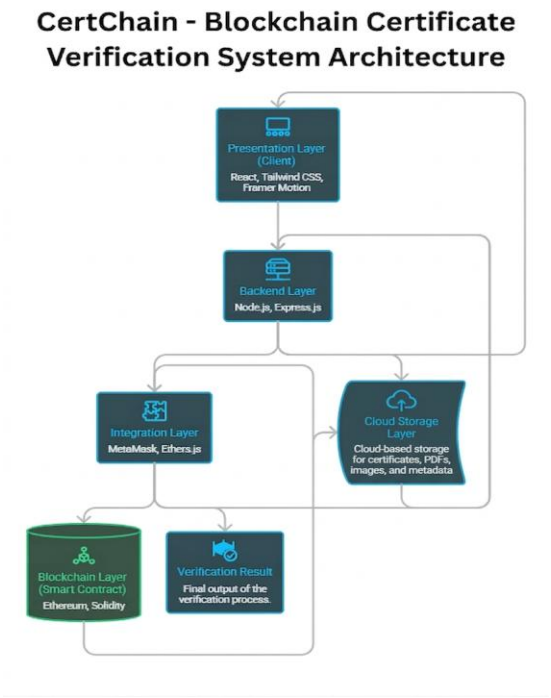

Fig. 1: Certchain - Blockchain Certificate Verification System Architecture

As shown in Figure 1, the CertChain architecture follows a layered design that integrates user interaction, backend processing, blockchain verification, and off-chain storage into a unified system.

The presentation layer provides a user-friendly interface for certificate issuance and verification. The backend layer handles file processing, hash generation, and API communication. The blockchain layer ensures secure and tamper-proof storage of certificate hashes using smart contracts. The off-chain storage layer maintains certificate files and metadata using cloud storage services, ensuring scalable, reliable, and globally accessible data management while reducing blockchain storage costs. The integration layer connects the system with MetaMask for secure authentication and transaction handling.

3.2 Data Handling Framework

The system processes certificate data through a structured workflow to ensure integrity and efficiency. It handles certificate details such as student information, course data, and uploaded files including PDFs and images, which are stored securely in cloud storage.

3.2.1 Data Acquisition

Certificate data is collected through the frontend interface, where authorized users upload certificate details along with supporting documents. The backend receives this data, uploads the files to cloud storage, and prepares the metadata for further processing.

3.2.2 Data Processing

The backend processes the uploaded data by generating a cryptographic hash using the SHA-256 algorithm, a widely used method for ensuring data integrity in blockchain systems [5]. This ensures that each certificate has a unique digital fingerprint.

The processing includes:

- Validating input data and uploaded files
- Generating SHA-256 hash for certificate data
- Structuring metadata for storage

The system also stores the generated file URLs from cloud storage as part of the certificate metadata.

3.2.3 Hash-Based Integrity Mechanism

To ensure data integrity, the system stores only the generated hash on the blockchain while keeping actual files off-chain.

Hash = SHA-256 (Certificate Data)

Where:

- Certificate Data includes student details, course information, and file references
- The generated hash uniquely represents the certificate

Any modification in the original data results in a different hash, enabling tamper detection during verification.

3.3 Implementation Details

The CertChain system integrates multiple components into a single framework that supports secure certificate issuance and verification using Solidity smart contracts and blockchain development frameworks:

(1) Blockchain-based hash storage
(2) Backend-based file management
(3) Dual verification mechanism

3.3.1 Certificate Issuance Module

The issuance module allows authorized users to upload certificate data through the frontend. The backend generates a hash and stores it on the blockchain using the smart contract. The actual files are stored in cloud-based off-chain storage, and their corresponding URLs are maintained in the backend.

3.3.2 Verification Module

The verification module allows users to validate certificates using two approaches:

- Blockchain-based verification using certificate ID
- Hash-based verification using backend data

The system compares the retrieved hash values to confirm authenticity.

3.3.3 Hybrid Storage Framework

The system adopts a hybrid approach by combining on-chain and off-chain storage. The blockchain ensures immutability and security, while cloud-based off-chain storage improves scalability, accessibility, and reduces storage cost.

This approach balances performance, cost-efficiency, and data integrity in certificate verification systems.

IV. EVALUATION

4.1 System Evaluation

To evaluate the effectiveness of the CertChain system, three approaches were considered: traditional centralized verification systems, fully blockchain-based storage systems, and the proposed hybrid architecture with cloud-based off-chain storage.

Traditional systems rely on centralized databases, making them vulnerable to data tampering and lacking transparency. Fully blockchain-based systems provide strong immutability but suffer from high storage costs and limited scalability due to the large size of certificate files.

The proposed CertChain system adopts a hybrid approach, where certificate hashes are stored on the blockchain while certificate files are stored in cloud-based off-chain storage. This significantly reduces blockchain storage costs while ensuring data integrity and global accessibility.

4.2 Functional Evaluation

The system was evaluated based on its core functionalities, including certificate issuance and verification. The issuance module successfully uploads certificate data, stores files in cloud storage, and records the corresponding hash on the blockchain.

The verification module supports dual validation methods:

• Blockchain-based verification using certificate ID

• Hash-based verification using backend and cloud data

The system accurately detects any data modification through hash mismatch, ensuring tamper-proof validation.

4.3 Performance and Cost Analysis

The performance of the system was analyzed in terms of storage efficiency and operational cost. By storing only hashes on the blockchain and moving certificate files to cloud storage, the system significantly reduces gas costs compared to fully on-chain storage models, aligning with scalable blockchain practices [6].

Cloud storage enables efficient file handling, faster retrieval, and improved scalability without increasing blockchain load. This makes the system suitable for handling large volumes of certificate data.

4.4 Security Analysis

The security of the CertChain system is ensured through multiple mechanisms. The use of SHA-256 hashing guarantees data integrity, while blockchain immutability prevents unauthorized modifications.

Even though certificate files are stored off-chain in the cloud, their authenticity is verified by matching hashes stored on the blockchain. Any alteration in the file results in a hash mismatch, ensuring reliable tamper detection.

Additionally, MetaMask-based authentication ensures secure access control and transaction validation.

4.5 Scalability and Practical Deployment

The integration of cloud storage significantly improves system scalability and availability. Unlike local storage, cloud-based storage allows access from any location and supports large-scale deployment.

This enhancement removes dependency on local infrastructure and makes the system more suitable for real-world applications such as educational institutions, recruitment platforms, and certification authorities.

V. RESULTS AND DISCUSSIONS

The CertChain system provides a secure and efficient solution for certificate management using blockchain and cloud storage. Certificate integrity is ensured through blockchain-stored hashes, preventing any modification after issuance.

The hybrid architecture reduces storage cost by storing only hashes on-chain while maintaining files in cloud storage, improving scalability and performance.

The dual verification mechanism enables reliable validation using both blockchain-based ID lookup and hash comparison. Overall, the system offers a secure, cost-effective, and scalable approach for digital certificate verification.

Fig. 2: CertChain Home Dashboard

As shown in Figure 2, the CertChain home dashboard provides an overview of the platform, enabling users to navigate between certificate issuance and verification modules. It highlights the blockchain-based functionality and serves as the primary interface for user interaction.

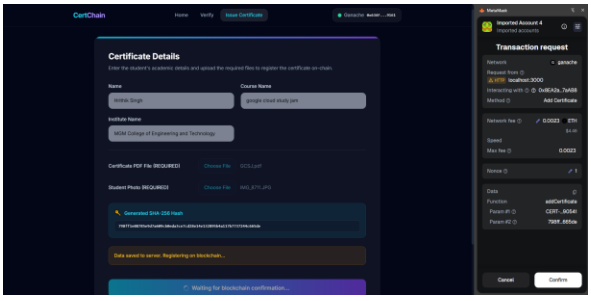

Fig. 3: Certificate Issuance and Blockchain Transaction

As shown in Figure 3, the certificate issuance process involves uploading user details and files, followed by the generation of a SHA-256 hash. The generated data

is then registered on the blockchain through a MetaMask transaction, ensuring secure and tamper-proof storage.

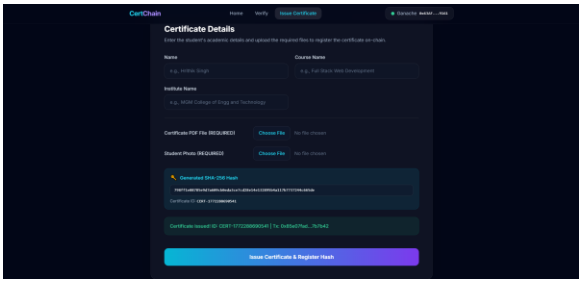

Fig. 4: SHA-256 Hash Generation and Certificate Registration

As shown in Figure 4, a unique SHA-256 hash is generated for the uploaded certificate data, which serves as a digital fingerprint to ensure data integrity and enable secure registration on the blockchain.

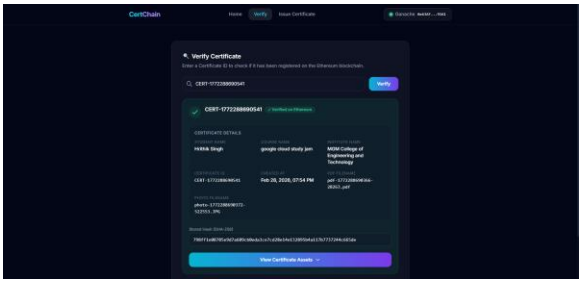

Fig. 5: Certificate Verification Interface

As shown in Figure 5, the certificate verification interface allows users to enter a certificate ID to validate its authenticity. The system retrieves the corresponding hash from the blockchain and processes the verification request to ensure data integrity.

VI. CONCLUSION AND FUTURE SCOPE

The CertChain system provides a secure and efficient solution for certificate issuance and verification using blockchain technology. By combining cryptographic hashing, smart contracts, and cloud-based storage, the system ensures data integrity, transparency, and cost efficiency. The hybrid architecture reduces storage overhead while maintaining tamper-proof verification. Future work can focus on integrating decentralized storage solutions such as IPFS and enhancing authentication mechanisms during certificate issuance. Further improvements may include multi-chain support and increased scalability for real-world deployment.

REFERENCES

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.
[2] V. Buterin, “Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform,” 2014.
[3] G. Wood, “Ethereum: A Secure Decentralised Generalised Transaction Ledger,” Ethereum Project Yellow Paper, 2014.
[4] M. Swan, “Blockchain: Blueprint for a New Economy”, O’Reilly Media, 2015.
[5] K. Christidis and M. Devetsikiotis, “Blockchains and Smart Contracts for the Internet of Things,” IEEE Access, vol. 4, pp. 2292–2303, 2016.
[6] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends,” IEEE International Congress on Big Data, 2017.
[7] A. Dorri, S. S. Kanhere, and R. Jurdak, “Blockchain in Internet of Things: Challenges and Solutions,” IEEE, 2017.
[8] M. Sharples and J. Domingue, “The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward,” European Conference on Technology Enhanced Learning, 2016.
[9] MIT Media Lab, “Blockcerts – An Open Infrastructure for Academic Credentials on the Blockchain,” 2016.
[10] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, “Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts,” IEEE Symposium on Security and Privacy, 2016.