Certificate Verification using Blockchain Technology

Deeksha Satish[1], Aayush Goyal[2], Aditya Kr. Thakur[3], Ankit Kr. Gope[4], Suman Kr. Singh[5]

[1]Assitant Professor, Dept. of Computer Science and Engineering, Acharya Institute Of Technology
[2]Computer Science and Engineering, Acharya Institute Of Technology
[3]Computer Science and Engineering, Acharya Institute Of Technology
[4]Computer Science and Engineering, Acharya Institute Of Technology
[5]Computer Science and Engineering, Acharya Institute Of Technology

---***---

Abstract - Certificate verification processes are often slow, fragmented, and vulnerable to forgery due to reliance on centralized storage systems. This paper presents Certify-Chain, a decentralized certificate verification system built on the Ethereum blockchain to ensure authenticity, transparency, and trust. The proposed system uses Solidity smart contracts to immutably record certificate hashes, issuer identities, and verification events on-chain. A React-based frontend interacts with the blockchain through Ethers.js, while MetaMask enables secure and user-controlled transaction signing. The system removes dependence on centralized authorities, prevents unauthorized data modification, and enables real-time certificate verification. Experimental evaluation of core operations, including certificate issuance, registration, ownership validation, and verification, demonstrates improved reliability and robustness. The results indicate that blockchain-based architectures provide an effective approach for strengthening the integrity and trustworthiness of digital credential verification systems.

Key Words: Blockchain, Ethereum, Smart contracts, Certificate Verification, Web-3, Metamask

1. INTRODUCTION

Academic and professional institutions issue certificates across domains such as education, training, licensing, and employment. Conventional certificate verification systems rely on isolated databases and manual validation procedures, resulting in fragmented records, limited transparency, and vulnerability to forgery. The absence of a shared and trusted verification mechanism often leads to delays and disputes during authenticity validation.

Blockchain technology provides a decentralized and tamper-resistant framework for secure data management without reliance on a central authority. In this paper, an Ethereum-based certificate verification system is proposed, in which Solidity smart contracts immutably record certificate issuance, registration, and verification events on the blockchain. A React-based frontend communicates with the smart contract using Ethers.js, while MetaMask enables secure transaction signing on the Sepolia test network. The proposed system establishes a single trusted source of certificate data, enabling real-time verification while improving traceability, accountability, and resistance to document forgery.

2. RELATED WORK

The adoption of blockchain for certificate verification has increased due to the limitations of centralized authentication systems, particularly their vulnerability to data tampering. Early studies demonstrated that blockchain immutability provides an effective mechanism for preserving certificate integrity by recording issuance and verification events as on-chain transactions, validated through timestamps, digital signatures, and cryptographic hashes.

Subsequent research modeled certificate verification as a state-based workflow rather than isolated events, enabling detection of invalid transitions and missing updates. The integration of smart contracts further automated certificate issuance, status management, and validation, reducing human intervention and ensuring deterministic enforcement of verification rules on public blockchains.

Other studies emphasized secure user authentication using blockchain wallets such as MetaMask to restrict certificate issuance to authorized entities. Hybrid approaches combining blockchain with QR codes, off-chain storage systems like IPFS, and digital repositories were proposed to maintain cryptographic linkage while improving scalability. Performance challenges related to gas costs, latency, and throughput were addressed through layer-2 solutions and lightweight decentralized applications.

Recent work extends blockchain-based credential systems by incorporating decentralized identity frameworks, access control mechanisms, and interoperable platforms such as Hyperledger Fabric and Corda to enhance privacy and data sharing. These studies collectively demonstrate the feasibility and effectiveness of decentralized, tamper-resistant certificate verification systems, motivating the Ethereum-based approach adopted in this work.

3. PROPOSED METHODOLOGY

The proposed system presents a decentralized blockchain-based architecture for transparent, tamper-proof, and verifiable certificate authentication in a multi-institution environment. Conventional certificate verification systems rely on siloed databases and manual processes, which lead to data manipulation, inconsistent verification, and delayed dispute resolution. To address these challenges, the proposed model integrates Ethereum smart contracts, Web3-based middleware, and a responsive frontend into a unified end-to-end verification framework. All certificate-related operations, including issuance, validation, and authenticity confirmation, are immutably recorded on the blockchain, ensuring trust, auditability, and verification efficiency.

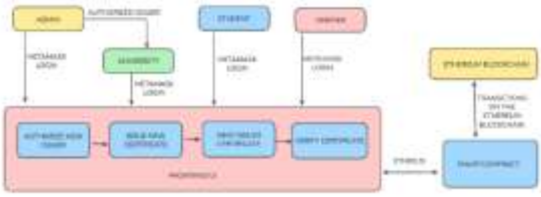


Fig 1: System architecture of the proposed Ethereum-based certificate verification system.

The system architecture, shown in **Fig. 1**, is organized into three layers. The **Blockchain Layer** consists of Solidity smart contracts deployed on the Ethereum network that manage certificate data, issuer details, status transitions, and timestamps. On-chain records are immutable and eliminate reliance on centralized authorities. The **Interaction Layer** handles secure communication between the frontend and the blockchain using Ethers.js and MetaMask, supporting wallet authentication, transaction signing, state queries, and event monitoring. The **Application Layer** is implemented using React and provides user interfaces for certificate issuance, verification, confirmation, and history tracking, with real-time updates triggered by blockchain events.

The functional workflow ensures that once certificate data is recorded, it cannot be altered or deleted, preventing forgery and unauthorized modification. Cryptographic signatures are required for all operations, while verified timestamps and status logs preserve a complete and permanent certificate history. The decentralized design removes single points of failure and enables reliable, real-time certificate verification across all participants.

4. Implementations and Results

The proposed Ethereum-based certificate verification system was implemented using Solidity smart contracts, a React-based frontend, and MetaMask for wallet interaction. Development and testing were carried out in a local Hardhat environment, followed by deployment on the Sepolia Ethereum test network. The evaluation focused on verification accuracy, transaction latency, operational cost, and functional correctness across all certificate-related operations.

A. User Interface Performance

The user interface demonstrated high responsiveness during real-time blockchain interactions. Average response times remained below two seconds during certificate issuance and verification workflows. Transaction confirmations required approximately 5 - 6 s, after which the interface was updated using blockchain event listeners. A unified dashboard design enabled efficient navigation for administrators, issuers, students, and verifiers, minimizing operational complexity.

An overview of the unified frontend dashboard is shown in Fig. 2, which presents role-based access for different system participants - Student, University and Verifier.

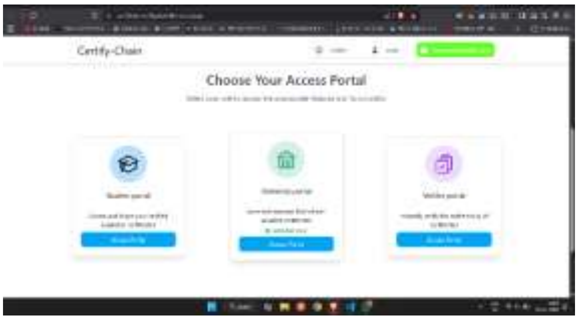
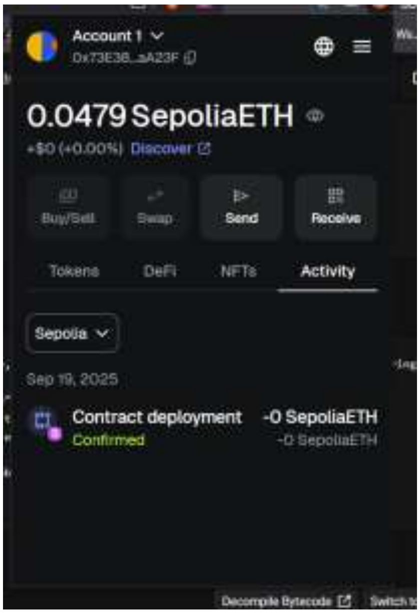


Fig 2: Unified frontend dashboard providing role-based access for system participants.

B. Wallet Interaction and Transaction Validation

MetaMask was used as the primary wallet for user authentication and transaction signing. All certificate issuance, verification, and authorization operations resulted in confirmed on-chain transactions, with accurate gas usage and timestamp records. This demonstrates seamless integration between the React frontend, Ethers.js provider, and the Ethereum network



Sep 19, 2025

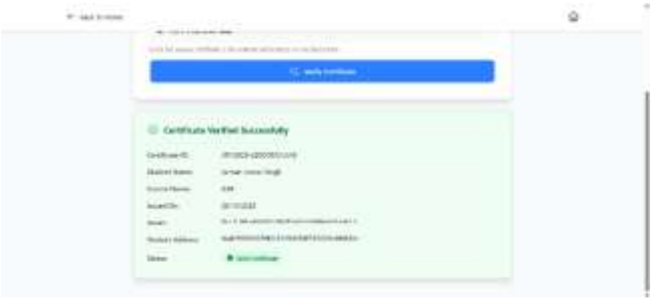
Contract deployment -0 SepoliaETH
Confirmed -0 SepoliaETH

Fig 3: MetaMask wallet displaying confirmed smart contract transactions.

Confirmed smart contract interactions recorded in the MetaMask wallet are illustrated in **Fig. 3**, validating successful transaction execution and blockchain-level transparency.

C. Access Control and Certificate Verification

Access control was enforced through smart contract authorization mechanisms, ensuring that only admin-approved issuers could generate certificates. Issued certificates were immutably stored on-chain and could be retrieved in real time by students. Third-party verifiers were able to independently validate certificate authenticity using unique certificate identifiers, without relying on centralized databases.



Certificate Verified Successfully

Fig 4: Certificate verification result displayed to a third-party verifier.

The certificate verification output displayed to third-party verifiers is shown in **Fig. 4**, demonstrating successful retrieval of certificate details and validation status directly from the blockchain.

These results confirm that the proposed system provides a secure, tamper-resistant, and reliable certificate verification mechanism with real-time validation and decentralized trust.

4. Conclusion

This paper presented an Ethereum-based decentralized certificate verification system designed to improve the authenticity, reliability, and transparency of digital credentials. The proposed solution integrates Solidity smart contracts with a React-based frontend and MetaMask wallet authentication to enable secure, real-time certificate issuance and verification using on-chain authorization. By eliminating dependence on centralized databases and manual validation processes, the system effectively mitigates certificate forgery and unauthorized modification. Experimental results demonstrate that the proposed approach provides efficient verification, strong access control, and reliable performance. Overall, the work confirms that blockchain technology offers a practical and scalable solution for secure and transparent certificate management in academic and professional environments.

Acknowledgment

The authors express their sincere gratitude to their project mentor, Ms. Deeksha Satish, for her continuous guidance, constructive feedback, and encouragement throughout the course of this work. Her support was instrumental in completing this research successfully.

REFERENCES

[1] Ethereum smart contract documentation by Ethereum Foundation in 2024.

[2] Hardhat: Ethereum development framework documentation by Nomic Foundation in 2024.

[3] A next-generation smart contract and decentralized application platform by Vitalik Buterin in 2014.

[4] MetaMask developer documentation: Web3 wallet and DApp integration by ConsenSys in 2024.

[5] Ethereum: a secure decentralised generalised transaction ledger (Yellow Paper) by Gavin Wood in 2023.

[6] R. Moore, "Ethers.js: A Complete Ethereum Wallet Implementation and Utilities in JavaScript," *Ethers.js Documentation*, 2024. [Online]. Available: https://docs.ethers.org/

[7] J. Mora, A. Sánchez, and M. García, "Blockchain Ensuring Academic Integrity with a Degree Traceability Prototype," *Procedia Computer Science*, vol. 214, pp. 1234–1245, 2022.

[8] T. R. Sree, "Decentralized Certificate Issuance and Verification System," *ScienceDirect*, 2025.