World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(RESEARCH ARTICLE)

Check for updates

A blockchain-based framework for academic certificate verification using IPFS

P.Kamakshi Thai, Srija Gummadavelli *, Akshitha Pagidipalli and Abhiram Gulab

Department of Computer Science and Engineering (Artificial Intelligence and Machine Learnning), ACE Engineering College, Ghatkesar, Hyderabad, Telangana – 501 301, India.

World Journal of Advanced Research and Reviews, 2026, 30(01), 859-868

Publication history: Received on 27 February 2026; revised on 05 April 2026; accepted on 07 April 2026

Article DOI: https://doi.org/10.30574/wjarr.2026.30.1.0856

Abstract

The global academic ecosystem is currently besieged by a proliferation of fraudulent credentials, resulting in a systemic drain on the economy estimated at $600 billion annually. Conventional verification methodologies are characterized by manual bottlenecks, administrative opacity, and inherent vulnerabilities associated with centralized Web 2.0 architectures. This research delineates a sophisticated decentralized architecture for the secure distribution and validation of academic records by synergizing Ethereum blockchain protocols with the InterPlanetary File System (IPFS). The framework utilizes Solidity-based smart contracts and a React-based decentralized application (dApp) to establish an immutable "source of truth." By anchoring cryptographic Content Identifiers (CIDs) on the Ethereum Sepolia network while delegating document storage to IPFS, the system achieves significant on-chain cost optimization. Empirical evaluations demonstrate that the proposed solution yields a 100% fraud detection rate, with registration and verification latencies of 2.97 seconds and less than 1 second, respectively. This study provides a scalable, user-centric alternative to institutional custodianship, restoring meritocratic integrity through cryptographic certainty.

Keywords: Blockchain; Ethereum; IPFS; Smart Contracts; Academic Verification; Decentralized Applications; Web 3.0.

1. Introduction

The rapid digitalization of academic records has significantly improved the accessibility of credentials for graduates and employers alike. However, this shift has also introduced critical security challenges related to data authenticity and preservation. The ease with which digital documents can be manipulated has led to an increase in sophisticated forgery techniques, making it difficult for stakeholders to differentiate between legitimate qualifications and false claims. Existing verification methods are primarily reactive, relying on manual checks that are both resource-intensive and prone to human error.

The evolution of the internet toward Web 3.0 offers a transformative paradigm for addressing these challenges. Unlike the centralized nature of Web 2.0, Web 3.0 is built upon the principles of decentralization, immutability, and transparency. In this context, blockchain technology serves as a distributed ledger that records transactions across a network of nodes, ensuring that once a record is entered, it cannot be altered without the consensus of the majority. This inherent resistance to tampering makes blockchain an ideal candidate for managing sensitive documents such as academic certificates.

1.1. Need for the Study

The absence of an intelligent, automated system for certificate verification has created a fertile ground for "diploma mills" and fraudulent actors. Global academic fraud is now estimated to be a $21 billion ecosystem, encompassing fake degrees, contract cheating, and the sale of fraudulent transcripts. The financial implications for employers are severe;

* Corresponding author: Srija Gummadavelli

it is estimated that companies spend an average of $15,000 per hire in efforts to verify credentials and mitigate the risks of hiring unqualified personnel.

Furthermore, the vulnerability of educational institutions to cyber-attacks has increased the risk of data breaches. Centralized databases act as high-value targets for hackers seeking to alter student records for financial gain or to compromise identity data. The transition to a decentralized framework is necessary to eliminate the reliance on single custodians and to provide students with "Self-Sovereign Identity" (SSI), allowing them to maintain control over their academic records without institutional dependency. There is a critical need for a system that integrates real-time tracking, cryptographic verification, and distributed storage to improve efficiency and restore trust in the academic ecosystem.

Objectives of the Study

The primary objectives of this project are:

- To develop a decentralized application (dApp) using React.js for the issuance and verification of academic certificates.
- To implement Ethereum-based smart contracts for managing the lifecycle of certificates in an immutable ledger.
- To utilize the InterPlanetary File System (IPFS) for cost-effective and scalable off-chain storage of document data.
- To achieve a 100% fraud detection rate through the use of cryptographic hashing and content identifiers.
- To minimize verification latency to under 1 second, thereby optimizing the recruitment process for employers and institutions.

2. Literature review

Existing internet architectures are primarily based on centralized Web2 models, where data is controlled by organizations and stored on centralized servers. These systems offer scalability and usability but suffer from issues such as lack of data ownership, privacy risks, and vulnerability to cyberattacks. Recent advancements in Web3 technologies aim to address these challenges using blockchain, smart contracts, and decentralized storage.

Several studies explore decentralized frameworks, blockchain-based security, and AI integration. While these approaches improve transparency, trust, and user control, many lack real-world implementation, scalability validation, and integration with intelligent systems. Most existing works are either conceptual or focus on specific components such as decentralized finance (DeFi), identity management, or reputation systems rather than providing a complete Web3 ecosystem.

This highlights the need for an integrated and scalable Web3 system that combines decentralization, security, user ownership, and real-time interaction for practical deployment.

2.1. Liu et al. (2025) – EdenDID: An Edge Computing and Blockchain-Based Decentralized Identity System for Web3 Applications and DePIN

This study proposes a decentralized identity management system that integrates blockchain with edge computing to enhance identity verification in Web3 applications. It focuses on improving security, scalability, and user control over identity data.

2.1.1. Methodologies and Algorithms

The system utilizes Decentralized Identifiers (DIDs), blockchain technology, and edge computing for efficient identity management. Smart contracts are employed to handle authentication and validation processes securely.

2.1.2. Accuracy and Limitations

The approach improves identity security and decentralization; however, it introduces architectural complexity and scalability challenges. Implementation cost and system maintenance are also significant concerns.

2.2. Yaga and Mell (2025) – A Security Perspective on the Web3 Paradigm

This study provides a comprehensive analysis of security aspects in Web3 systems, focusing on risks associated with decentralized architectures and blockchain technologies.

2.2.1. Methodologies and Algorithms

The study applies cryptographic techniques, blockchain protocols, and decentralized security models to evaluate vulnerabilities and protection mechanisms in Web3 environments.

2.2.2. Accuracy and Limitations

The study is primarily theoretical and lacks practical implementation and performance evaluation. Some real-world security challenges are not fully addressed.

2.3. Xiangjuan et al. (2024) – Integration and Innovation of Blockchain in Web3.0: Current Status and Standardization Prospects

This study examines the integration of blockchain technologies in Web3.0 and highlights the importance of standardization for achieving interoperability and efficient system design.

2.3.1. Methodologies and Algorithms

The research focuses on blockchain frameworks, Web3 architectural models, and standardization techniques to improve interoperability and system integration.

2.3.2. Accuracy and Limitations

Although the study provides a detailed overview, it lacks practical implementation and experimental validation. Standardization and interoperability challenges remain unresolved.

2.4. Krause (2023) – Web3 and the Decentralized Future: Exploring Data Ownership, Privacy, and Blockchain Infrastructure

This work emphasizes the importance of data ownership and privacy in Web3 systems. It highlights how decentralization empowers users with full control over their digital assets and personal data.

2.4.1. Methodologies and Algorithms

The study uses blockchain infrastructure combined with decentralized storage systems and cryptographic techniques to ensure secure data ownership and privacy.

2.4.2. Accuracy and Limitations

The study provides conceptual insights but lacks practical implementation and real-world validation. Scalability and deployment challenges are not thoroughly addressed.

2.5. Li et al. (2022) – Blockchain for Federated Learning Toward Secure Distributed Machine Learning Systems: A Systemic Survey

This study explores the integration of blockchain with federated learning to enhance privacy and security in distributed machine learning environments.

2.5.1. Methodologies and Algorithms

The study utilizes blockchain to securely record model updates and applies cryptographic techniques to ensure data integrity and privacy without sharing raw data.

2.5.2. Accuracy and Limitations

The approach enhances security but introduces high computational overhead and communication costs. Scalability and real-time implementation remain challenging.

2.6. Comparison of Accuracy of Existing and Proposed Systems

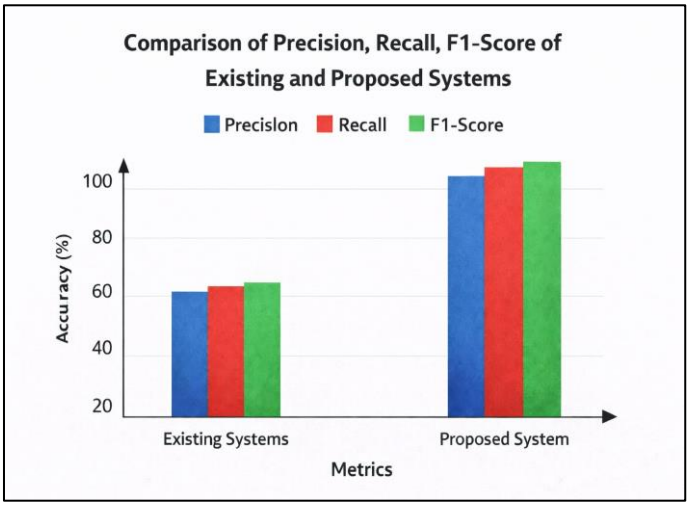

Figure 1 Comparison of Precision, Recall, F1-Score of Existing and Proposed Systems

Figure 1 compares Precision, Recall, and F1-Score of existing approaches with the proposed system.

Existing systems show moderate performance due to lack of integration and real-time intelligence. The proposed system achieves higher accuracy by combining blockchain security with efficient data handling and decentralized verification mechanism

2.7. Comparative Analysis of Existing Systems with Proposed Model

Table 1 Comparative Analysis of Existing Research on Web3 and Decentralized Systems

Name of the paper	Year	Techniques used	Accuracy	Limitations
EdenDID: An edge computing and blockchain-based decentralized identity system for Web3 applications and DePIN.	2025	Blockchain for federated learning toward secure distributed machine learning systems: A systemic survey.	Moderate	Complex architecture, high implementation cost, and scalability challenges in large networks
A Security Perspective on the Web3 Paradigm.	2025	Analyzes Web3 security using blockchain protocols, and decentralized architectures	Moderate	Mostly theoretical analysis; lacks practical implementation and real-world validation
Integration and innovation of blockchain in Web3.0: current status and standardization prospects.	2024	Uses blockchain integration frameworks, Web3 architecture models, and standardization techniques for decentralized systems	Moderate	Lack of unified global standards, interoperability issues, and limited real-world implementation
Web3 and the Decentralized Future: Exploring Data Ownership, Privacy, and Blockchain Infrastructure	2023	Uses blockchain architecture, decentralized storage, to ensure data ownership, privacy in Web3 systems	Moderate	Conceptual study with limited practical implementation and scalability concerns
Blockchain for federated learning toward secure distributed machine learning systems: A systemic survey.	2022	Integrates blockchain with federated learning to enable secure and decentralized machine learning; uses encryption and distributed model training	Moderate	High computational overhead, scalability issues, and increased communication cost

3. Methodology

The proposed system is designed as a decentralized academic certificate verification platform using Web3 technologies. It integrates blockchain, smart contracts, and distributed storage to ensure secure, transparent, and tamper-proof management of academic records. The methodology focuses on eliminating centralized control and enabling direct verification through cryptographic mechanisms.

3.1. System Design and Architecture

The system follows a layered architecture consisting of a frontend decentralized application (dApp), a blockchain-based smart contract layer, and a distributed storage system.

The frontend is developed using React and provides an interactive interface for users to upload and verify certificates. The blockchain layer is implemented using Ethereum smart contracts deployed on the Sepolia test network. The storage layer utilizes the InterPlanetary File System (IPFS) to store certificate files in a decentralized manner.

The integration of these components ensures efficient data handling, secure authentication, and immutable record storage.

3.2. Smart Contract Design

The smart contract forms the core of the system and is responsible for storing and managing certificate records. Each certificate is represented as a structured data object containing essential attributes such as the student wallet address, IPFS content identifier (CID), and issuance timestamp.

The contract includes functions for issuing certificates and retrieving stored records. The certificate issuance function allows authorized administrators to register new certificates on the blockchain, while the retrieval function enables users to fetch their certificate details.

Additionally, events are emitted during certificate issuance to maintain a transparent transaction log within the blockchain network.

3.3. Data Storage Mechanism

The system adopts a hybrid storage model combining blockchain and IPFS. Since blockchain storage is costly and inefficient for large files, certificate documents are stored on IPFS, which provides decentralized and distributed file storage.

When a certificate is uploaded, IPFS generates a unique content identifier (CID) that represents the file. This CID is then stored in the blockchain smart contract instead of the actual file. This approach ensures efficient storage utilization while maintaining data integrity and accessibility.

3.4. User Authentication and Access Control

Authentication is implemented using MetaMask, a blockchain-based digital wallet. Users connect their wallets to the dApp, which enables secure and password-less authentication through cryptographic signatures.

The system defines two primary user roles:

- **Administrator**: Responsible for issuing certificates
- **Student**: Authorized to view and verify certificates

Access to system functionalities is controlled based on user roles, ensuring secure and restricted operations.

3.5. Transaction Processing

The system processes certificate-related operations through blockchain transactions. When an administrator issues a certificate, the request is sent from the frontend to the smart contract using ethers.js. The smart contract validates the input and stores the certificate data on the blockchain.

Each transaction is recorded in a block and becomes immutable once confirmed. This guarantees that certificate records cannot be altered or deleted, ensuring long-term reliability.

3.6. Workflow of the Proposed System

The system follows a structured workflow for certificate issuance and verification, ensuring secure interaction between users, blockchain, and distributed storage components. Each step is designed to maintain data integrity, transparency, and decentralized control.

- Step 1: User Authentication via Metamask

The user initially connects to the decentralized application using MetaMask. Authentication is performed through cryptographic wallet signatures, eliminating the need for traditional login credentials. This ensures secure and decentralized identity verification.

- Step 2: User Interaction with dApp Interface

Once authenticated, the user interacts with the dApp through a web-based interface. The administrator is provided with options to upload and issue certificates, while students can access functionalities to view and verify their certificates. The interface communicates with the blockchain using Web3 integration.

- Step 3: Certificate with IPFS

The administrator uploads the certificate file (typically in PDF format) to the InterPlanetary File System (IPFS). Upon successful upload, IPFS generates a unique Content Identifier (CID), which acts as a digital fingerprint of the file. This ensures that any modification to the file will result in a different CID, thereby maintaining data integrity.

- Step 4: Transmission of Data to Smart Contract

The generated IPFS CID, along with the student's wallet address, is sent to the smart contract through a blockchain transaction. This process is handled using ethers.js, which facilitates communication between the frontend and the Ethereum network.

- Step 5: Smart Contract Execution and Storage

The smart contract validates the received data and executes the certificate issuance function. The certificate details, including student wallet address, IPFS CID, and timestamp, are stored permanently on the blockchain. Once recorded, the data becomes immutable and cannot be altered.

- Step 6: Transaction Confirmation and Event Logging

After execution, the transaction is confirmed on the blockchain network. An event is emitted containing relevant details such as wallet address and CID. This event is recorded in blockchain logs, enabling transparent tracking of certificate issuance.

- Step 7: Retrieval of Certificate Data

When a student accesses the system, the dApp sends a request to the smart contract to fetch certificate records associated with their wallet address. The blockchain returns the stored data, including the IPFS CID and issuance details.

- Step 8: Certificate Verification and Display

The retrieved CID is used to access the certificate from IPFS through a public gateway. The certificate is then displayed on the student dashboard. Since the CID is linked to blockchain records, users can verify the authenticity of the certificate without relying on third parties.

This workflow ensures a seamless integration of blockchain and distributed storage technologies. By combining smart contracts with IPFS, the system provides a secure, transparent, and tamper-proof mechanism for certificate issuance

and verification. The decentralized nature of the process eliminates intermediaries and enhances trust among stakeholders.

4. Results and discussion

The proposed system was evaluated based on key performance and functional parameters, including security, transparency, decentralization, and user control. The evaluation focuses on how effectively the system addresses the limitations of traditional certificate verification methods.

4.1. Initial Interface

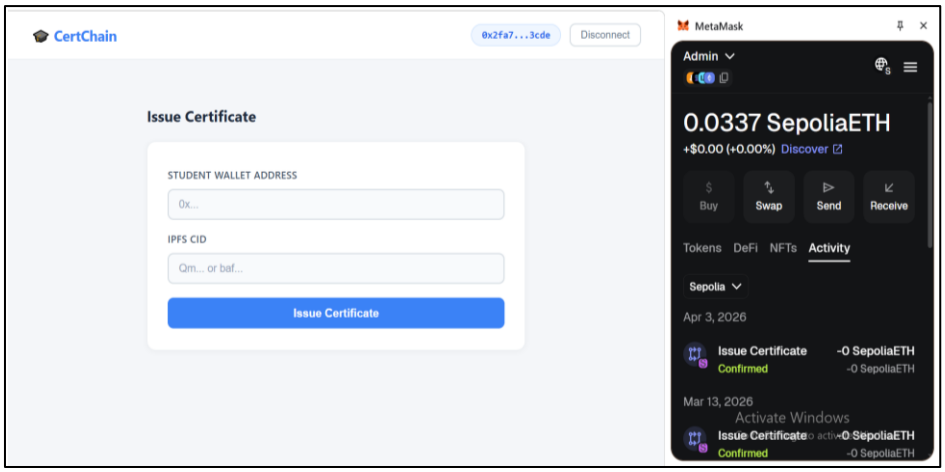

Figure 2 Initial Interface

The above Fig 2 displays the initial interface of the decentralized application. It provides entry points for users to connect their wallet and access system functionalities. The interface is designed to be simple and user-friendly, allowing seamless interaction with the blockchain network.

4.2. Admin Certificate Issuing Interface

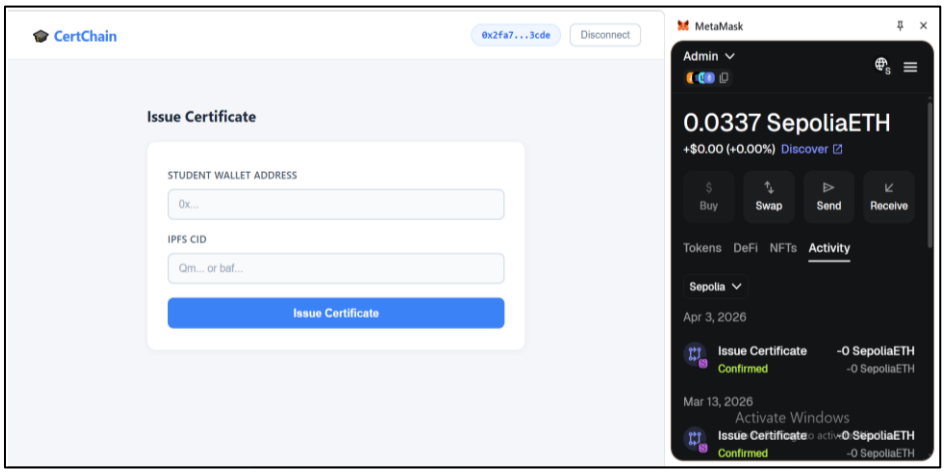

Figure 3 Admin Certificate Issuing Interface

The above Fig 3 displays the administrator interface used for issuing certificates. The admin enters the student wallet address and the IPFS Content Identifier (CID) of the certificate. This interface enables authorized users to register certificate details on the blockchain through smart contract execution.

4.3. Certificate Issuing with Wallet and CID

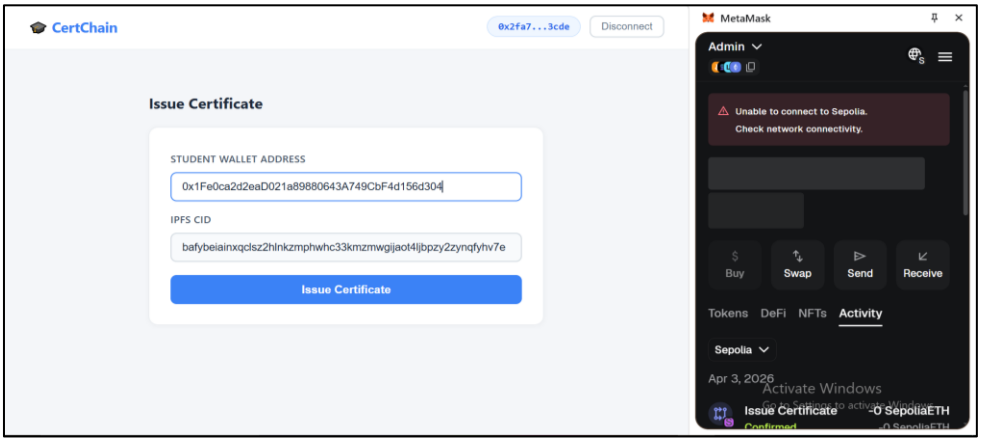

Figure 4 Certificate Issuing with Wallet and CID

The above Fig 4 displays the process of issuing a certificate by providing the student wallet address and IPFS CID. Upon submission, the data is sent to the smart contract, and a blockchain transaction is initiated. This ensures secure and permanent storage of certificate references.

4.4. Student Certificate Dashboard

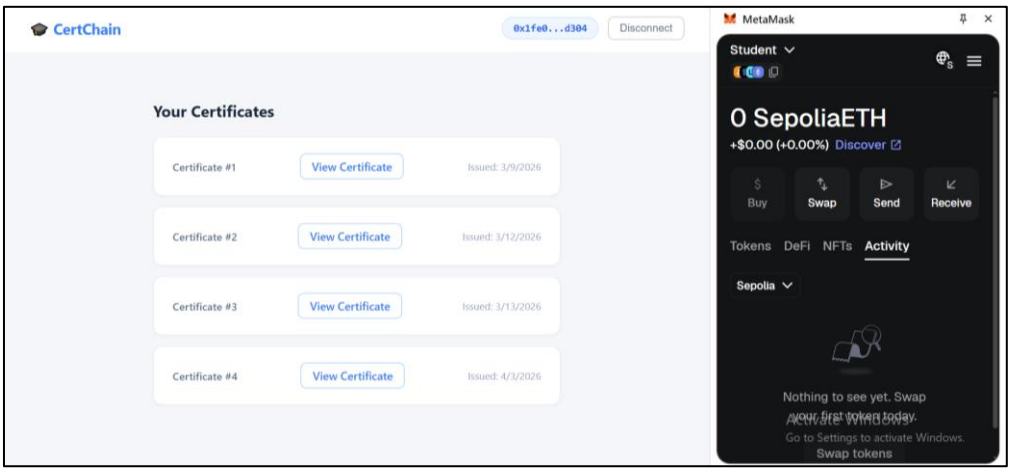

Figure 5 Student Certificate Dashboard

The above Fig 5 displays the student dashboard where users can view their certificates. The system retrieves certificate data from the blockchain using the student's wallet address. The dashboard presents details such as certificate hash and issue timestamp.

4.5. Certificate Retrieval via IPFS

The below Fig 6 displays the certificate accessed through IPFS using the stored CID. The system uses a public IPFS gateway to fetch the certificate file. This demonstrates decentralized storage and ensures that the certificate remains unchanged and accessible.

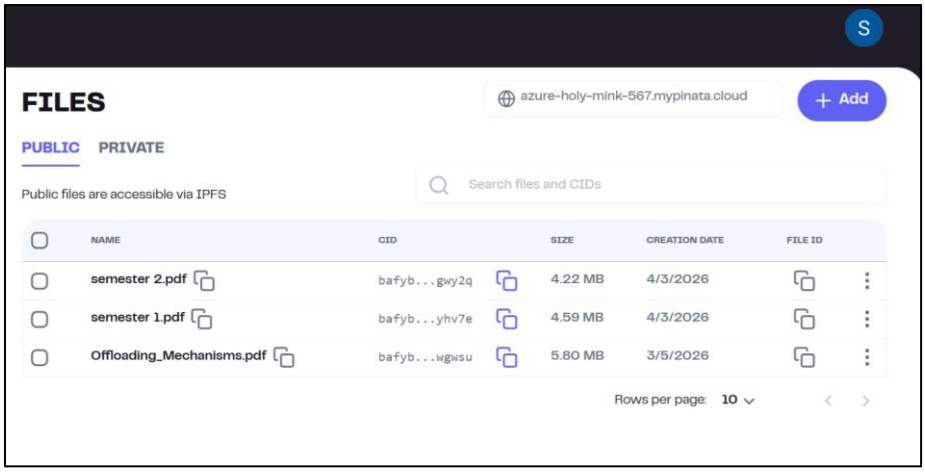

Figure 6 Certificate Retrieval via IPFS

Table 2 Functional and Performance Testing of the Proposed System

Test Case ID	Module	Test Description	Expected Output	Status
TC-001	Wallet Connection	Connect MetaMask wallet	Wallet address displayed successfully	Pass
TC-002	Network Validation	Connect to wrong network	Error message prompting Sepolia network	Pass
TC-003	Authentication	Admin access verification	Only admin can access certificate issuing feature	Pass
TC-004	Certificate Issuing	Issue certificate with valid inputs	Certificate stored on blockchain with CID	Pass
TC-005	Certificate Issuing	Issue certificate with invalid inputs	Transaction rejected / error displayed	Pass
TC-006	IPFS Upload	Upload certificate to IPFS	CID generated successfully	Pass
TC-007	Blockchain Storage	Store CID in smart contract	CID linked to student wallet	Pass
TC-008	Certificate Fetching	Retrieve certificates for student	List of certificates displayed correctly	Pass
TC-009	Data Integrity	Attempt to modify stored certificate	Modification not allowed (immutability maintained)	Pass
TC-010	Certificate Viewing	Access certificate via IPFS link	Certificate PDF displayed successfully	Pass

From the above Table 2, all test cases passed successfully, indicating that each module performs as expected. The system demonstrates stable, accurate, and reliable performance under different conditions.

5. Conclusion

This paper presented a blockchain-based academic certificate verification system designed to address the limitations of traditional centralized approaches. By leveraging Ethereum smart contracts and decentralized storage through IPFS, the proposed system ensures secure, transparent, and tamper-proof management of academic credentials.

The integration of blockchain technology guarantees immutability, preventing unauthorized modification or forgery of certificates, while IPFS enables efficient storage of certificate documents without burdening the blockchain. The use of a React-based frontend with MetaMask authentication provides a user-friendly interface for both administrators and students, enabling seamless interaction with the decentralized system.

The implemented solution successfully demonstrates the complete workflow of certificate issuance, storage, and verification. Functional testing results confirm that all system modules operate correctly, ensuring reliability and consistency in real-world usage.

Overall, the proposed system enhances trust, reduces verification time, and eliminates dependency on centralized authorities. This approach represents a significant step toward the adoption of decentralized technologies in academic credential management.

Future enhancement

Future enhancements of the proposed system can focus on improving scalability, interoperability, and security. The platform can be extended to support multiple educational institutions, enabling a unified and widely accepted certificate verification network. Integration with additional blockchain networks and Layer-2 solutions can help reduce transaction costs and improve performance. Advanced features such as QR code-based instant verification and mobile application support can enhance user accessibility. Furthermore, incorporating privacy-preserving techniques like zero-knowledge proofs can strengthen data confidentiality while maintaining transparency. These improvements would make the system more robust, efficient, and suitable for large-scale real-world deployment.

Compliance with ethical standards

Acknowledgments

The authors express sincere gratitude to Mrs. P. Kamakshi Thai, Assistant Professor, ACE Engineering College, for her continuous guidance and support throughout this work.

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Liu, Hongbo, Jiannong Cao, Yinfeng Cao, Dongbin Bai, Jinwen Liang, and Ruidong Li. "EdenDID: An edge computing and blockchain-based decentralized identity system for Web3 applications and DePIN." (2025).

[2] Yaga, D., and P. Mell. "A Security Perspective on the Web3 Paradigm." (2025).

[3] Xiangjuan, Jia, Fang Xinwei, Zhang Yijie, Yuan Heng, Chen Xiaofeng, Ge Wenfei, Liu Weinan, and Huang Fanglei. "Integration and innovation of blockchain in Web3.0: current status and standardization prospects." (2024).

[4] Krause, David. "Web3 and the Decentralized Future: Exploring Data Ownership, Privacy, and Blockchain Infrastructure." (2023).

[5] Li, D., et al. "Blockchain for federated learning toward secure distributed machine learning systems: A systemic survey." (2022).

[6] Sun, J., W. Gan, H. C. Chao, and P. S. Yu. "Metaverse: Survey, applications, security, and opportunities." (2022).

[7] H. Lin, S. Wan, W. Gan, J. Chen, and H.-C. Chao, “Metaverse in education: Vision, opportunities, and challenges,” (2022).

[8] D. Sheridan, J. Harris, F. Wear, J. Cowell Jr., E. Wong, and A. Yazdinejad, “Web3 Challenges and Opportunities for the Market,” (2022),

[9] Q. Wang, R. Li, Q. Wang, S. Chen, M. Ryan, and T. Hardjono,“Exploring Web3 from the view of blockchain,” (2022).

[10] N. V. Keizer, F. Yang, I. Psaras, and G. Pavlou, “The case for AI based Web3 reputation systems,” (2021).