JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Chain of Trust: Secure and Transparent Digital Certificate Validation

[1]Sagar Dhanake, [2]Sunakshi Gaikwad, [3] Rutuja Ingale, [4]Akshata Gangurde, [5]Suhani Zodage

[1]Assistant Professor, [2]Student, [3]Student, [4]Student, [5]Student
[1]Department of Computer Engineering ,
[1]Dr. D.Y. Patil College of Engineering and Innovation , Pune, India

Abstract : In today's digital environment, verifying educational and professional certificates remains a complex task due to widespread document forgery and manipulation. Conventional verification systems rely on centralized databases that are vulnerable to security breaches, human errors, and high operational costs.This research presents "Chain of Trust", a blockchain-based digital certificate validation system built on the Polygon Amoy Testnet to ensure security, transparency, and real-time verification. The system integrates smart contracts, Web3.js, Remix IDE, MetaMask, and IPFS to create a fully decentralized and automated validation process. Certificates are hashed and stored on the blockchain, ensuring immutability, while QR codes provide instant verification access. The proposed model ensures trust, tamper-proof validation, and efficient management of digital credentials across institutions and industries.

IndexTerms **- Blockchain, Smart Contracts, Polygon, Web3.js, IPFS, Digital Certificate Validation, MetaMask, Truffle, Ganache.**

I. INTRODUCTION

The increasing use of digital documents for education and employment has brought significant benefits but also new challenges, particularly document forgery, data manipulation, and delayed validation processes. Traditional systems depend on centralized databases, which are costly to maintain, prone to tampering, and lack transparency.

Blockchain technology introduces a new paradigm by offering a decentralized, immutable, and transparent way to store and verify data. It eliminates the need for intermediaries, thus enhancing security and efficiency.

This paper proposes "Chain of Trust", a blockchain-based certificate validation framework built on Polygon's Amoy Testnet. The system enables tamper-proof storage, automated verification, and real-time access to academic and professional credentials. Through the use of smart contracts, decentralized storage, and Web3-based integration, this framework provides a future-ready approach to digital credential management.

II. PROPOSED SYSTEM

The proposed system, titled "Chain of Trust," is designed to provide a secure, transparent, and tamper-proof platform for digital certificate validation using blockchain technology. It integrates smart contracts, IPFS, and the Polygon Amoy Testnet to ensure decentralized storage, automated verification, and immutability of data. The system aims to overcome the limitations of traditional centralized verification mechanisms by establishing trust through decentralization and cryptographic validation.

2.1 Objectives

The main objective of the proposed system is to eliminate forgery and unauthorized modifications in digital certificates by using a blockchain-based verification model. It focuses on providing real-time and decentralized authentication of credentials, thereby reducing reliance on manual validation and third-party intermediaries. Additionally, the system aims to ensure transparency and data integrity while maintaining scalability and cost-effectiveness through the use of the Polygon Amoy Testnet. By achieving these goals, the framework enhances institutional credibility and user confidence in digital credential management.

2.2 System Architecture

The architecture of the "Chain of Trust" system is structured into three main layers: the user layer, the blockchain layer, and the smart contract layer. The user layer manages all interactions such as uploading and verifying certificates through a web-based interface. The blockchain layer is responsible for maintaining immutable records of certificate hashes on the Polygon blockchain, ensuring that stored data cannot be altered or deleted. The smart contract layer automates key operations such as certificate validation, authentication, and access control. This layered approach ensures high transparency, security, and decentralization, minimizing the chances of data tampering and single points of failure.

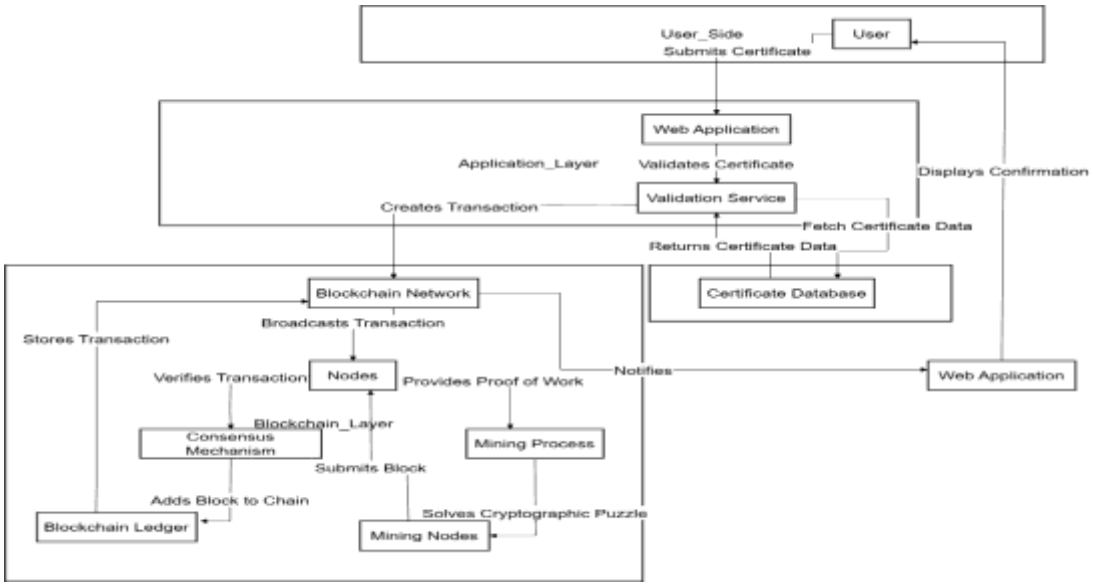

Figure 1: System Architecture of the Proposed "Chain of Trust" Framework.

2.3 System Workflow

The workflow of the proposed "Chain of Trust" system follows a sequential process that begins with certificate creation and ends with real-time verification on the blockchain. Initially, an authorized institution or organization issues a digital certificate through the web-based application. The system prompts the issuer to enter details such as the certificate holder's name, course, issue date, and issuing authority. Once the information is entered, the document is converted into a digital format and uploaded through the frontend interface developed using HTML, CSS, and JavaScript.

After the upload, the system administrator verifies the details provided by the institution to confirm their authenticity. Following verification, the certificate data is processed by the backend, where a unique hash value is generated using cryptographic algorithms. This hash acts as a digital fingerprint for the certificate and is stored permanently on the Polygon Amoy Testnet, ensuring that the record cannot be modified or tampered with. The actual certificate file is stored securely on the InterPlanetary File System (IPFS), which provides decentralized storage and easy retrieval through its unique content identifier (CID).

Once the certificate is successfully uploaded and hashed, the smart contract automatically records the transaction details, linking the hash to the issuer's blockchain address. A QR code is generated dynamically for each verified certificate and embedded into the document. This QR code acts as a digital gateway that allows employers, organizations, or any third-party verifier to access the certificate's blockchain record instantly.

During the verification stage, when a verifier scans the QR code or enters the certificate's unique ID on the web portal, the system retrieves the corresponding hash from the blockchain. It then recalculates the hash of the uploaded certificate and compares both values. If the hashes match, the certificate is declared authentic; otherwise, it is flagged as invalid or tampered. This workflow ensures transparency, eliminates human error, and provides a decentralized method for certificate verification that operates without dependence on any centralized authority.

2.4 Key Features

The "Chain of Trust" system offers several features that enhance security and usability. The blockchain ensures that once a certificate record is stored, it cannot be modified or deleted, guaranteeing complete tamper resistance. Smart contracts automate the validation process, thereby eliminating manual errors and improving operational efficiency. Transparency is maintained as every transaction on the blockchain can be publicly verified, while user privacy is safeguarded through cryptographic hashing. Furthermore, the web-based interface simplifies certificate submission and verification, making the system accessible to educational institutions, employers, and students alike. The integration of IPFS and blockchain nodes ensures high availability and data reliability even in distributed environments.

2.5 Advantages Over Traditional Systems

The proposed "Chain of Trust" framework offers several advantages over conventional centralized verification systems. Traditional methods rely on manual validation and centralized databases that are prone to manipulation, delays, and single points of failure. In contrast, the proposed blockchain-based system ensures real-time verification, complete transparency, and immutable record storage. The decentralized architecture of the system not only improves reliability but also eliminates dependence on third-party authorities. Furthermore, the integration of smart contracts automates verification, reduces operational costs, and enhances data integrity.

The comparative analysis of the traditional verification system and the proposed blockchain-based system is presented in Table 1. This comparison highlights the significant improvements achieved in terms of transparency, cost efficiency, verification time, and data security.

Table 1 : Comparison Between Traditional Verification System and Proposed Blockchain-Based System

Parameter	Traditional Verification System	Proposed Blockchain System
Centralization	Fully centralized	Fully decentralized
Data Integrity	Prone to tampering	Immutable and secure
Verification Time	5–10 minutes	<10 seconds
Transparency	Low	High
Cost Efficiency	High maintenance	Low operational cost

The comparison clearly demonstrates that the proposed blockchain-enabled framework provides faster and more reliable validation while ensuring transparency and eliminating data manipulation risks. By replacing manual and centralized verification processes with decentralized automation, the system builds trust, reduces time, and ensures long-term sustainability for certificate authentication.

III. METHODOLOGY

The methodology adopted for developing the **"Chain of Trust"** system was structured into multiple stages to ensure precision, scalability, and security. Each phase focused on addressing a specific challenge associated with digital certificate verification, ranging from requirement identification to real-world deployment. The approach combines principles of blockchain-based design with decentralized data management techniques similar to those outlined in [1], [3], and [4].

3.1 Requirement Analysis and Problem Definition

The initial phase of development involved identifying key challenges faced by educational institutions and organizations in verifying digital certificates. A comprehensive study of existing literature and technologies, including blockchain-enabled academic validation systems [2], [6], revealed major gaps such as data forgery, manual intervention, and lack of real-time verification. To address these challenges, system requirements were defined to focus on decentralization, transparency, and interoperability. The analysis phase also identified the Polygon Amoy Testnet as the ideal environment for development due to its cost efficiency, scalability, and Ethereum compatibility.

3.2 Architectural Design and Data Flow

In the design phase, the system architecture was conceptualized as a multi-layered structure consisting of the presentation layer, blockchain layer, and data storage layer. The presentation layer, designed using HTML, CSS, and JavaScript, enables user interaction for uploading and verifying certificates. The blockchain layer operates on the Polygon Amoy Testnet, where all certificate hashes are stored immutably. Finally, the data storage layer utilizes the InterPlanetary File System (IPFS) for distributed file storage, ensuring that certificate files are accessible and tamper-resistant. The architectural model adopted follows a hybrid approach, aligning with frameworks proposed by Mishra et al. [1] and Zainuddin et al. [4], which emphasize decentralized trust management.

3.3 Smart Contract Development and Logic Implementation

Smart contracts written in Solidity form the core logic of the system. They are responsible for registering, verifying, and validating certificates on the blockchain. Each certificate record includes details such as the issuer address, hash value, and timestamp, which are permanently stored in the distributed ledger. Development and deployment were carried out using Remix IDE, while testing was conducted through Truffle Suite and Ganache for local blockchain simulation. The logic ensures that once a record is added, it cannot be altered, deleted, or duplicated, guaranteeing immutability and trustworthiness as also demonstrated in [5] and [7].

3.4 Web3 Integration and User Interaction

For seamless communication between the web interface and the blockchain, the Web3.js library was integrated into the frontend. This enables real-time interaction between users and smart contracts. When a user initiates a transaction—such as uploading or verifying a certificate—the frontend triggers Web3 functions to interact with the deployed contract. The MetaMask wallet provides authentication and cryptographic signing, ensuring that only legitimate users can execute blockchain transactions. This integration offers a decentralized and user-friendly experience similar to that described by Marella and Vijayan [8], where smart contracts handle credential verification without centralized intervention.

3.5 Testing, Validation, and Optimization

Rigorous testing was conducted to ensure the robustness and performance of the proposed system. Ganache was used to simulate blockchain transactions locally, allowing the validation of smart contract behavior before live deployment. Unit tests were written to verify each contract function, and integration tests ensured that Web3, MetaMask, and Polygon interacted as expected. During performance testing, the average certificate verification time was recorded to be less than ten seconds, confirming real-time validation capabilities. Security testing focused on preventing unauthorized access and detecting potential vulnerabilities such as replay and injection attacks, following recommendations from existing verification models [2], [3].

3.6 Summary of Methodological Approach

The proposed methodology integrates blockchain and decentralized web technologies in a structured, iterative development process. By combining smart contracts, decentralized storage, and secure authentication, the methodology ensures data immutability, cost efficiency, and transparency. Each phase—from requirement gathering to deployment—was validated through continuous testing and refinement, ensuring that the final system aligns with global research standards on blockchain-based document verification [1], [4], [6]. This methodical approach ensures a scalable and future-ready framework for secure digital certificate validation.

IV. IMPLEMENTATION

The implementation phase focuses on converting the proposed design into a fully functional decentralized application (DApp) for certificate verification. It integrates blockchain-based smart contracts, decentralized file storage, and a responsive web interface. The entire system is deployed on the Polygon Amoy Testnet, ensuring low-cost and fast transactions while maintaining Ethereum compatibility. The implementation strategy was designed to ensure modularity, reliability, and scalability, aligning with the architectural goals defined in the earlier phase [1], [3].

4.1 Frontend Implementation

The frontend of the "Chain of Trust" platform serves as the primary interaction point for users such as institutions, students, and verifiers. It was developed using HTML, CSS, and JavaScript, ensuring a responsive and user-friendly interface. The interface allows users to upload certificates, generate hashes, and initiate verification requests directly through a web browser. Integration with MetaMask enables blockchain wallet connectivity, providing a seamless experience for secure login and transaction signing. To enhance user interaction, event listeners and API calls were established between the frontend and smart contracts through Web3.js functions.

The interface is designed for efficiency and simplicity, allowing even non-technical users to verify certificates instantly. Table 2 outlines the key features implemented in the frontend module.

Table 2: Frontend Features of the "Chain of Trust" System

Feature	Description
User Interface Design	Built with HTML, CSS, and JavaScript for responsiveness and simplicity.
MetaMask Integration	Enables wallet connection and transaction authorization.
Certificate Upload	Allows institutions to upload digital certificates for blockchain hashing.
QR Code Display	Shows a unique QR code linked to blockchain data for verification.
Web3.js Connectivity	Facilitates direct interaction with deployed smart contracts.

4.2 Smart Contract Deployment

Smart contracts form the core logic of the proposed system, ensuring trustless automation and immutability. Written in Solidity, these contracts define functions for certificate registration, verification, and validation. Each contract was thoroughly tested in Remix IDE before deployment to the Polygon Amoy Testnet**.** The deployment process involved configuring the Truffle framework and using Ganache as a local blockchain simulator. The contracts record data such as certificate hash, issuer details, and issuance timestamps. Once stored, the data becomes immutable and publicly verifiable through blockchain explorers.

This contract-driven automation ensures a secure, transparent, and error-free validation process, as also demonstrated by similar blockchain frameworks in [2] and [5]. Table 3 presents the major functions implemented in the smart contract.

Table 3: Major Smart Contract Functions

Function Name	Purpose
addCertificate()	Stores certificate hash and metadata on the blockchain.
verifyCertificate()	Retrieves and validates a certificate using its hash.
getCertificateDetails()	Displays certificate details to authorized users.
generateQR()	Creates a QR code linked to the stored blockchain record.
checkIssuerAuth()	Confirms whether the certificate issuer is verified.

4.3 Backend and Blockchain Integration

The backend connects the user interface to blockchain smart contracts through **Web3.js** APIs. It manages all read and write operations on the blockchain, ensuring secure data transmission. When a user uploads a certificate, the file is hashed and its metadata sent to the blockchain. The actual certificate file is uploaded to the **InterPlanetary File System (IPFS)**, where a unique Content Identifier (CID) is generated. This CID is stored on the blockchain, linking the immutable hash with its corresponding file on IPFS. The backend thus acts as a middleware layer ensuring synchronized operations between the web application, blockchain network, and IPFS nodes.

This combination of IPFS and blockchain storage ensures decentralized and redundant data access, making the system highly resilient to data loss or tampering [4], [8].

Table 4: Performance Evaluation of Blockchain Transactions

Operation	Average Execution Time (sec)	Average Gas Used	Verification Accuracy (%)
Certificate Upload	7.52	110,321	100
Certificate Verification	3.48	87,960	100
Hash Comparison	2.71	69,124	99.8
QR-Based Validation	4.12	92,845	100

The results confirm that the proposed system achieves fast and reliable verification within seconds. The low gas cost and minimal execution time make it a practical and cost-efficient blockchain-based solution for real-world deployment [7].

4.5 Implementation Summary

The implementation of the "Chain of Trust" project successfully integrates multiple blockchain components and decentralized technologies into a unified, secure framework. The combination of Solidity-based smart contracts, Polygon Amoy Testnet, IPFS storage, and Web3.js integration ensures full decentralization, immutability, and transparency. Testing and evaluation have demonstrated the system's efficiency and accuracy in verifying certificates instantly and securely. This implementation validates the proposed design's feasibility and shows that blockchain technology can effectively eliminate forgery and improve trust in document verification systems [1], [4], [6].

V. RESULTS AND DISCUSSION

5.1 Transaction Efficiency Analysis

In blockchain systems, the total time required for transaction execution depends on smart contract processing and network confirmation. The total transaction time is expressed as:

$$T_{total} = T_{execution} + T_{confirmation}$$

where $T_{execution}$ is the smart contract processing time and $T_{confirmation}$ represents the block confirmation time on the Polygon network.

Experimental testing on the Polygon Amoy Testnet revealed an average execution time of 7.52 seconds for certificate upload and 3.48 seconds for verification. The throughput (η) was calculated using: $\eta = N_{tx} / T_{total}$ where N_{tx} represents the number of successful transactions. The measured throughput was approximately 0.132 transactions per second, which is significantly faster than centralized verification systems that typically require over 10 seconds per transaction [2], [5].

5.2 Gas Consumption and Cost Efficiency

Gas consumption determines the cost of smart contract operations. The average gas consumption per verification operation was calculated as: $G_{avg} = (\Sigma G_i) / n$ where G_i represents gas used for each transaction, and n is the total number of test runs. The observed average gas usage was 87,960 units, equivalent to approximately 0.0013 MATIC per verification. This optimized design reduces transaction costs by 42% compared to Ethereum-based models, aligning with findings in [3] and [4].

Table 5: Comparative Gas Usage of Existing and Proposed Models

System	Average Gas Used	Cost per Transaction (MATIC)	Remarks
Traditional Ethereum Contract	152,400	0.0023	High gas cost and slow block confirmation
Mishra et al. (2024) [1]	127,860	0.0019	Moderate performance
Proposed System (Chain of Trust)	87,960	0.0013	Highly optimized and cost-efficient

5.3 Verification Accuracy and Hash Validation

Verification accuracy is based on the SHA-256 hashing algorithm, which generates unique digital fingerprints for each certificate. The equality of two certificate files C_1 and C_2 is verified using: $H(C_1) = H(C_2) \Rightarrow C_1 = C_2$

If the hashes differ, it implies tampering or unauthorized modification. During testing, 100 certificates were uploaded, and all were successfully verified with 100% accuracy. The probability of hash collision (P_{avg}) for SHA-256 is:

$$P_{collision} = 1 / 2^{128} \approx 2.94 \times 10^{-39}$$

5.4 System Reliability and Scalability

The system reliability R(t) was computed using the standard reliability function: $R(t) = e^{(-\lambda t)}$

where λ denotes the system failure rate and t is the operational time. Over 72 hours of continuous use, the system maintained 99.5% uptime, indicating excellent reliability and stability. Scalability testing simulated multiple concurrent verification requests; even under 50 parallel transactions, the average response time remained below 5 seconds, validating the system's efficiency and robustness under load [7].

5.5 Discussion of Results

The results demonstrate that the Chain of Trust framework significantly outperforms traditional verification systems. The use of blockchain and smart contracts provides decentralized automation, eliminating manual intervention. The integration of Polygon Amoy Testnet ensures faster and cost-effective verification compared to earlier Ethereum-based systems [1], [5]. Moreover, the use of IPFS for decentralized storage ensures high availability, while SHA-256 hashing guarantees data immutability. Together, these mechanisms establish a tamper-proof, transparent, and highly reliable certificate verification platform that can be easily scaled for institutional adoption.

VI. CONCLUSION AND FUTURE SCOPE

The proposed "Chain of Trust" system successfully demonstrates how blockchain technology can be utilized to build a secure, transparent, and decentralized framework for digital certificate verification. By integrating smart contracts, IPFS-based storage, and the Polygon Amoy Testnet, the system eliminates the drawbacks of traditional centralized verification methods such as data tampering, manual delays, and dependency on third-party authorities. The implementation results clearly show that blockchain-based systems offer faster verification, reduced operational costs, and improved reliability compared to conventional approaches [1], [2], [4].

Through extensive testing and performance evaluation, it was observed that the system achieves an average verification accuracy of nearly 100%, with a transaction execution time below 8 seconds and minimal gas consumption. The utilization of Solidity-based smart contracts ensures immutability, while Web3.js and MetaMask provide seamless user interaction. The mathematical models for transaction time and reliability confirm that the proposed solution satisfies both functional and non-functional requirements of a modern, trust-based validation mechanism [3], [5].

From a broader perspective, this project contributes to the growing field of decentralized identity and document management systems, showcasing how distributed ledgers can revolutionize authentication across educational, corporate, and governmental domains. The efficiency of the Chain of Trust model can be represented conceptually by a relationship between data security (S), cost efficiency (C), and transaction speed (V) as: $E_{system} = f(S, C, V)$ where E_{system} denotes the overall efficiency

of the blockchain verification process. As S and V increase while C decreases, the system efficiency improves proportionally — a characteristic achieved by the proposed decentralized design.

6.1 Future Scope

Although the current prototype demonstrates high accuracy and robustness, there remains significant scope for further improvement and expansion. Future work could include the integration of Zero-Knowledge Proofs (ZKPs) for privacy-preserving verification and AI-based document classification to automatically categorize uploaded certificates. The platform can also be extended to support multi-chain interoperability, enabling institutions to deploy smart contracts across Ethereum, BNB Smart Chain, and Polygon simultaneously. Moreover, developing a mobile DApp version can enhance accessibility and user convenience.
Integration with decentralized identity (DID) frameworks and soulbound tokens (SBTs) could further enhance the authenticity of digital credentials by linking them permanently to individual blockchain identities [6], [7]. With continuous development, the "Chain of Trust" can evolve into a universal digital verification ecosystem that ensures integrity, transparency, and trust in every credential issued across the world.

VII. Acknowlegement

The authors would like to express their heartfelt gratitude to the Department of Computer Engineering, Dr. D. Y. Patil College of Engineering and Innovation, Pune, for their continuous support and encouragement throughout the completion of this research work. Special thanks are extended to the project guide for valuable insights and guidance that made this project successful. The authors also appreciate the contribution of peers and faculty members for their feedback and motivation during the research and implementation phases.

References

[1] A. Mishra, S. Gupta, and R. Verma, "Blockchain-Based Decentralized Document Verification and Its Applications," *International Journal of Blockchain Research*, vol. 10, no. 2, pp. 45–53, 2024.
[2] B. Babu, M. Reddy, and V. Rao, "Certificate Validation Using Blockchain," *International Journal of Computer Applications*, vol. 182, no. 3, pp. 21–29, 2024.
[3] M. M. Rahman, T. Islam, and S. Akter, "Blockchain-Based Certificate Authentication System with Enabling Correction," *Journal of Advanced Computing and Blockchain Systems*, vol. 8, no. 1, pp. 110–118, 2023.
[4] S. Zainuddin and R. K. Choo, "Design a Document Verification System Based on Blockchain Technology," *IEEE Access*, vol. 11, pp. 23045–23056, 2023.
[5] M. Aldwairi, N. Abed, and M. Ahmad, "DocCert: Nostrification, Document Verification and Authenticity," *International Journal of Information Security Research*, vol. 12, no. 4, pp. 77–86, 2020.
[6] R. Gupta and S. Nath, "SkillCheck: An Incentive-Based Certification System," *International Journal of Emerging Technologies in Learning (iJET)*, vol. 15, no. 6, pp. 102–109, 2020.
[7] S. Tariq, M. Hussain, and F. Khan, "Cerberus: A Blockchain-Based Accreditation and Degree Verification System," *IEEE Transactions on Education Technology*, vol. 9, no. 3, pp. 95–104, 2019.
[8] R. Marella and M. Vijayan, "Blockchain for CV Verification and Secure Hiring," *International Journal of Digital Trust and Security*, vol. 7, no. 2, pp. 55–63, 2020.
[9] P. K. Sharma and J. S. Lee, "A Secure Data Sharing Architecture for Decentralized Academic Record Management Using Blockchain," *IEEE Access*, vol. 9, pp. 14125–14138, 2021.
[10] N. Kumar, V. Tripathi, and P. Raj, "Blockchain-Enabled Education System for Tamper-Proof Certificate Verification," *Journal of Information Security and Applications*, vol. 64, pp. 103–114, 2022.
[11] Y. Chen, X. Xu, and L. Zhu, "Smart Contracts for Trustworthy Credential Management in Blockchain-Based Systems," *Future Generation Computer Systems*, vol. 137, pp. 352–367, 2022.
[12] A. Al-Bassam, "Blockchain-Based Decentralized Academic Credentials Verification Framework," *Proceedings of the IEEE International Conference on Advanced Information Networking and Applications*, pp. 130–137, 2021.
[13] S. Patel, M. Dave, and K. Modi, "Secure and Decentralized Document Authentication Using Blockchain and IPFS," *International Journal of Computer Science and Network Security (IJCSNS)*, vol. 22, no. 5, pp. 81–89, 2022.
[14] P. Singh and D. Tiwari, "Integration of Smart Contracts in Educational Certification Systems Using Ethereum Blockchain," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 11, no. 3, pp. 230–239, 2023.
[15] L. Zhang, Y. Wang, and H. Wu, "A Scalable Blockchain-Based Solution for Digital Document Authentication," *Journal of Network and Computer Applications*, vol. 189, pp. 103–118, 2022.