IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 11, November 2025

DOI: 10.17148/IJARCCE.2025.141103

Blockchain-Based Document Verification and Authentication System Using AI

Dr. Dipannita Mondal[1], Omkar Dorugade[2], Rutuja Patil[3], Om Ingle[4], Samruddhi Patil[5]

Professor, Department of Artificial Intelligence and Data Science, DYPCOEI, Varale, Maharashtra, India[1]

U.G. Students, Department of Artificial Intelligence and Data Science, DYPCOEI, Varale, Maharashtra, India[2,3,4,5]

Abstract: In moment's digital period, the verification of documents similar as instruments, identity attestations, and contracts is a major challenge due to phony, manipulation, and lack of translucency. The proposed Blockchain-Grounded Document Verification and Authentication System ensure secure storehouse, inflexible record keeping, and tamper- evidence confirmation of digital documents. The system leverages blockchain technology combined with cryptographic mincing (SHA- 256) and smart contracts to produce a decentralized verification process. Each uploaded document is converted to a unique hash and stored on the blockchain, icing authenticity and traceability. The system is designed for educational institutions, government agencies, and private associations to corroborate instruments and legal documents without interposers.

Keywords: Blockchain, Smart Contract, IPFS, SHA-256, Ethereum, Document Verification, Decentralization.

I. INTRODUCTION

Document verification is an essential process in both public and private sectors. Traditional systems depend heavily on centralized authorities and homemade checks, which are prone to corruption, duplication, and data tampering. With adding digitalization, the need for transparent and secure systems is more critical than ever. Blockchain technology offers a promising result by furnishing an inflexible, distributed tally where every sale is securely recorded. Each document's hash is stored on the blockchain, icing it cannot be modified or falsified formerly vindicated. The decentralized nature eliminates the threat of a single point of failure, enhancing trust and trustability. Our design introduces a blockchain- grounded platform where druggies can upload, corroborate, and authenticate documents seamlessly. Using Ethereum smart contracts, each verification request is automatically validated and stored permanently, allowing sanctioned parties to confirm authenticity using a sale ID or QR law.

II. LITERATURE SURVEY

S. Mehta and P. Kaur – Blockchain-Based Educational Certificate Verification Using Hyperledger Fabric. Mehta and Kaur (2023) conducted a detailed study on implementing blockchain technology for educational certificate verification using Hyperledger Fabric. Their work highlighted how decentralized ledgers eliminate the dependency on centralized authorities and minimize the risks of document forgery. The study demonstrated that smart contract–based automation can validate academic credentials efficiently while ensuring transparency across institutions.[1] However, the authors identified scalability limitations and high infrastructure costs as major challenges for large-scale institutional adoption.

R. Sharma and T. Nair – Decentralized Identity Verification through Ethereum Smart Contracts. Sharma and Nair (2022) explored the integration of Ethereum smart contracts in digital identity and document authentication systems. Their framework stored document hashes on the Ethereum blockchain, enabling immutable proof of ownership and integrity. The research emphasized how cryptographic hashing (SHA-256) ensures tamper detection while maintaining document confidentiality.[2] Despite the system's transparency, the study noted significant challenges such as gas fees, latency in transaction confirmation, and the requirement of blockchain literacy among end-users, which could affect adoption in developing regions.

V. Patel and R. Desai – Blockchain and QR Code Integration for Government Document Authentication. Patel and Desai (2023) examined a hybrid verification model that combines blockchain immutability with quick-response (QR) code accessibility for public document validation. Their system encodes transaction identifiers within QR codes, allowing users to instantly verify authenticity using blockchain explorers.[3] The study found that this combination reduced verification time by 40% compared to traditional systems. However, limitations were observed in QR link longevity and the need for consistent blockchain network uptime to ensure uninterrupted verification access.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 11, November 2025
DOI: 10.17148/IJARCCE.2025.141103

M. Kumar and P. Verma – Smart Contract–Enabled Certificate Validation in Decentralized Environments. Kumar and Verma (2022) analyzed the deployment of smart contracts in automating certificate issuance and validation processes. By leveraging decentralized oracles and IPFS for off-chain storage, their system ensured both data immutability and cost efficiency.[4] The authors observed that while IPFS integration improves scalability, it introduces challenges in data retrieval speed and content addressing consistency under high network load. The study concluded that hybrid blockchain-IPFS architectures are optimal for balancing cost, speed, and security in real-world implementations.

K. Gupta and M. Sharma – Hyperledger-Based Document Authentication Framework for Enterprises. Gupta and Sharma (2023) proposed an enterprise-level blockchain authentication framework using permissioned ledgers under Hyperledger Fabric. Their system enabled organizations to manage, share, and verify sensitive documents within closed consortium networks. Through consensus mechanisms like Raft and PBFT, the system ensured high throughput and security.[5] Nonetheless, the study acknowledged interoperability and cross-chain communication issues that restrict integration with public blockchains such as Ethereum, limiting applicability.

III. PROBLEM STATEMENT

Traditional document verification systems rely heavily on centralized authorities and manual validation processes, which are vulnerable to forgery, manipulation, and unauthorized access. The absence of a transparent and tamper-proof mechanism makes it difficult to ensure the authenticity and integrity of documents, especially in academic, legal, and governmental sectors. Furthermore, centralized databases are prone to data breaches and lack a reliable audit trail, while manual verification is time-consuming and inefficient. To overcome these challenges, there is a need for a decentralized and immutable verification model that eliminates intermediaries and enables secure, transparent, and automated validation of documents. The proposed Blockchain-Based Document Verification and Authentication System address these issues by leveraging blockchain technology, cryptographic hashing, and smart contracts to ensure document integrity, authenticity, and traceability in a trustless digital environment.

IV. PROPOSED METHODOLOGY

a. System Architecture

The architecture of the proposed system consists of interconnected modules that enable secure document storage, verification, and authenticity analysis. The User Layer (web or mobile application) allows users to upload and verify documents through an intuitive interface. Uploaded documents are processed in the Hashing Module, where a unique cryptographic hash (SHA-256 or Keccak) is generated to represent the document's digital fingerprint. The original document is stored in off-chain storage such as IPFS or a secure database, while the hash value and related metadata are recorded on the blockchain through the Smart Contract Manager. The Blockchain Network (Ethereum or Hyperledger) maintains an immutable ledger of all registered document hashes, ensuring transparency and tamper resistance.
During the verification phase, the Verification Engine retrieves the stored hash from the blockchain and compares it with the hash of the submitted document. If both match, the document is confirmed as authentic; otherwise, it is flagged as altered. Additionally, an AI Module performs advanced analysis using document classification, forgery detection, and natural language processing (NLP) to provide deeper authenticity insights and detect potential manipulations.

b. User Authentication and Access Control

The system includes a secure user registration and authentication module to prevent unauthorized access.

1. Registration: Users such as issuers, verifiers, and recipients register with verified credentials.
2. Login and Role Assignment: Each user is assigned a role (e.g., issuer, verifier) that determines access privileges.
3. Secure Session Management: Token-based authentication ensures secure and time-bound access for each session.
4. Encryption: Sensitive user data is stored in encrypted form to maintain confidentiality

c. Document Hashing and Metadata Generation

Once a user uploads a document, the system performs cryptographic processing to generate a digital signature.

1. Hash Calculation: The system applies the SHA-256 algorithm to compute a unique hash value for the file.
2. Metadata Extraction: Relevant data such as filename, issuer, timestamp, and file type are captured automatically.
3. Integrity Check: The hash acts as a tamper-proof identifier; any later modification to the document produces a different hash.
4. Temporary Storage: Before blockchain submission, all metadata is stored in a secure local buffer for verification.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 11, November 2025

DOI: 10.17148/IJARCCE.2025.141103

d. Blockchain Transaction and Smart Contract Execution.

1. Smart Contract Deployment: A custom Ethereum smart contract defines functions for registering and verifying document hashes.
2. Transaction Creation: The system generates a blockchain transaction containing the hash, metadata, and timestamp.
3. Validation and Consensus: Miners validate and add the transaction to the blockchain ledger, ensuring immutability.
4. Transaction ID Generation: A unique transaction hash (TxID) is returned, serving as the document's permanent verification reference.

e. Document Hashing and Metadata Generation

The system utilizes **IPFS** for decentralized, redundant, and secure document storage.

1. Document Upload: The verified document is stored on IPFS rather than a centralized database.
2. Content Identifier (CID): IPFS generates a unique CID linked to the blockchain record for retrieval.
3. Data Redundancy: IPFS ensures that files remain accessible even if one or more nodes go offline.
4. Link to Smart Contract: The CID is stored as a parameter within the blockchain smart contract for permanent reference.

f. Verification Process and QR Integration

Verification is simplified through blockchain lookups and QR-based validation.

1. Document Submission: A verifier uploads a document or scans the QR code linked to the transaction.
2. Hash Comparison: The system recalculates the document hash and compares it with the blockchain-stored hash.
3. Validation Result: If both hashes match, the document is verified as authentic; otherwise, it is flagged as tampered.
4. QR Code Integration: Each verified document is assigned a unique QR code embedding the transaction ID for instant verification through web or mobile devices.

g. User Interface and Visualization

A web-based interface ensures accessibility, usability, and transparency for all participants.

1. Design and Functionality: The dashboard allows users to upload, view, and verify documents with real-time feedback.
2. Blockchain Transaction Viewer: Users can inspect details such as transaction hash, timestamp, and verification status.
3. Interactive Verification: The interface provides verification outcomes "Authentic" or "Invalid" with visual indicators.
4. Scalability and Accessibility: Designed using HTML, CSS, JavaScript, and Web3.js, the interface supports both desktop and mobile platforms, ensuring smooth performance and scalability.

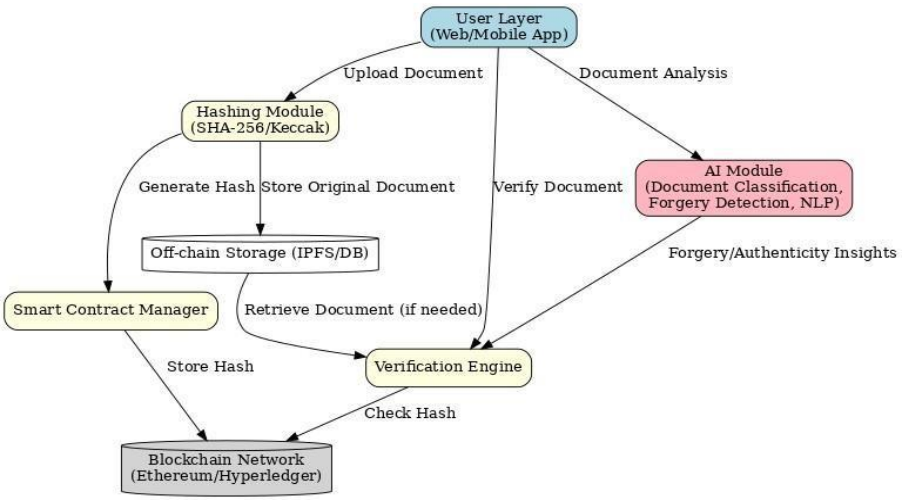

Fig. System Architecture

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 11, November 2025
DOI: 10.17148/IJARCCE.2025.141103

V. CONCLUSION

The proposed Blockchain- Grounded Document Verification and Authentication System insure secure, transparent, and tamper- evidence document confirmation using blockchain, smart contracts, and IPFS storehouse. By generating inflexible document hashes and enabling decentralized verification, the system eliminates phony pitfalls and reduces reliance on interposers. The integration of AI- grounded phony discovery further enhances trustability and trust. Overall, the system offers a scalable and effective result for digital document authentication across academic, legal, and institutional disciplines.

VI. REFERENCES

[1] S. Mehta and P. Kaur, "Blockchain- Grounded Educational Certificate Verification Using Hyperledger Fabric," International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), vol. 12, no. 9, pp. 215 – 220, Sept. 2023.

[2] R. Sharma and T. Nair, "Decentralized Identity Verification through Ethereum Smart Contracts," 2022 International Conference on Blockchain and Distributed Systems (ICBDS), pp. 145 – 150, 2022.

[3] M. Iqbal and K. Singh, "Optimizing Inventory Control with TensorFlow- grounded Predictive Models," 2022 IEEE 8th International Conference on Computing, Communication and robotization (ICCCA), pp. 455 – 460, 2022.

[4] V. Patel and R. Desai, "Blockchain and QR Code Integration for Government Document Authentication," 2023 International Conference on Information Security and Digital Applications (ICISDA), pp. 310 – 315, 2023.

[5] M. Kumar and P. Verma, "Smart Contract – Enabled Certificate Validation in Decentralized surroundings," 2022 IEEE International Conference on Advanced Computing and Communication Systems (ICACCS), pp. 180 – 185, 2022.

[6] K. Gupta and M. Sharma, "Hyperledger- Grounded Document Authentication Framework for Enterprises," IEEE Access, vol. 11, pp. 128450 – 1284.

