International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 13 Issue: 01 | Jan 2026 www.irjet.net p-ISSN: 2395-0072

A Comprehensive Literature Survey on Block chain-Enabled Techniques for Secure Document Verification

Ch Tejaswini[1], Hemani B[2], J Harshitha[3], Dr. B Kalpana[4]

[1,2,3] Department of Computer Science and Engineering, JNN Institute of Engineering, Chennai, Tamil Nadu, India.
[4]Head of the Department Computer Science and Engineering, JNN Institute of Engineering, Chennai, Tamil Nadu, India.

Abstract - *The rapid growth of digital transformation has significantly increased the use of electronic documents in sectors such as education, healthcare, finance, and legal services. However, the centralized storage and management of digital documents make them vulnerable to forgery, unauthorized modification, and data breaches, leading to serious concerns regarding trust and authenticity. Traditional document verification system relays heavily on intermediaries and centralized authorities, which may introduce delays, inefficiencies, and security risks. Block chain technology offers a decentralized, immutable, and transparent framework that ensures document integrity and tamper resistance. This study explores blockchain-based techniques for secure document verification by utilizing cryptographic hashing, distributed ledgers, and smart contracts to authenticate documents without the need of third-party verification. The proposed approach enhances transparency, improves trust among stakeholders, and enables real-time verification of Document authenticity. Furthermore, this works analyses existing blockchain-based document verification models, highlighting their advantages, limitations, and practical challenges. The finding demonstrates that block chain technology can significantly improve the reliability, security, and efficiency of digital documents verification systems. This research provides a strong foundation for developing scalable, secure, and trustworthy document authentication solutions for future digital ecosystems.*

Key Words: **Block chain, Document Verification, Cryptographic Hashing, Smart Contract, Decentralized Systems, and Privacy Preservation.**

1. INTRODUCTION

Document verification plays a critical role in modern digital ecosystems, ensuring the authenticity and integrity of sensitive information. Documents such as educational certificates, identity proofs, legal contracts, and medical records are fundamental for decision-making processes across various domains. Any compromise in document verification may lead to serious consequences, including identity theft, fraud, and legal disputes. Therefore, establishing secure and reliable document verification mechanisms is essential to maintain trust and prevent misuse.

Traditional document verification systems are typically centralized and managed by a single authority or organization. Verification often requires manual intervention or reliance on third-party intermediaries, which can introduce delays, inefficiencies, and single points of failure. Moreover, centralized systems lack transparency and are vulnerable to data manipulation, unauthorized access, and cyber-attacks. These limitations highlight the need for more secure, transparent, and efficient verification framework.

II. METHODOLOGY

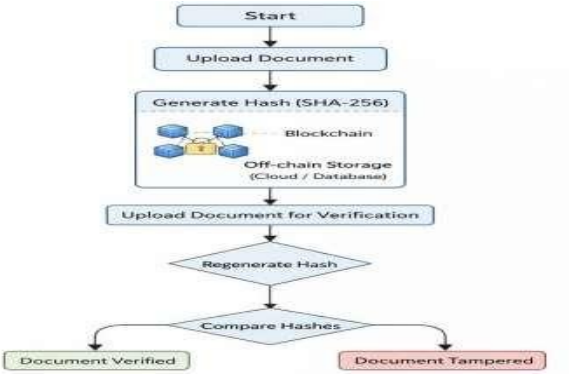

Figure 1 : Workflow of the application

The proposed system follows a secure, decentralized, and tamper-proof methodology for document verification using blockchain technology. The main objective is to ensure that once a document is issued, it cannot be modified or forged, and its authenticity can be verified instantly by any authorized party

A. System Actors

The System consists of three entities: issuer, blockchain network, and verifier. The issuer uploads documents into the system. The blockchain stores documents hashes securely. The verifier checks document authenticity. This ensures decentralized and trusted verification.

B. Document Generation and Upload

The issuing authority first generates the academic document in digital format (PDF). Each document is assigned a unique identifier such as Student ID or certificate number. The document is then uploaded into the system by the administrator. Before storing the document, a Cryptographic hash function (SHA-256) is applied to generate a fixed-length hash value. This hash acts as a digital fingerprint of the document. Even a small change in the document content results in a completely different hash, ensuring integrity verification.

C. Blockchain Registration Using Smart Contracts

A Smart contract is deployed on the Ethereum blockchain to store document hashes along with metadata such as: Document ID, Issuer ID, Time stamp. Once the hash is written into the blockchain, it becomes immutable, meaning it cannot be altered or deleted. This guarantees that document records remain tamper-proof and verifiable at any time.

D. Decentralized Storage Using IPFS

Since block chain storage is expensive and inefficient for large files, original document is stored in the interplanetary File System(IPFS). IPFS generates a unique content identifier (CID) for each file, which is linked with the block chain record. This hybrid approach ensures:

- Blockchain-Stores proof(hash)
- IPFS-stores actual document

E. Verification Process

When a user submits a document for verification, the system generates its cryptographic hash. This hash is compared with the hash stored on the blockchain through the smart contract. If both values match, the document is confirmed as authentic. If they do not match, the document is marked as invalid. This process ensures fast and tamper-proof verification.

F. Result Generation

The system displays verification results instantly. User receives either verified or not verified status. Verification logs can be maintained for auditing. This improves trust and transparency. The system is user-friendly and fast.

III. Proposed System

A. System Overview:

The proposed system consists of three major components: the user interface, blockchain network, and decentralized storage system. The user interface allows institutions to upload documents and verifier to validate them. The blockchain layer manages smart contracts that store cryptographic hashes of documents, ensuring immutability and transparency. The decentralized storage layer (IPFS) stores the actual documents securely while maintaining content integrity.

The User Interface allows user such as students, institutions, and organizations to upload documents and request verifications services. When a document is uploaded, it is forwarded to the Application Server, where a cryptographic hash is generated using secure hashing algorithms such as SHA-256. The actual document is stored securely in the off-chain storage system (cloud or database), while the generated hash and metadata are recorded on the blockchain network through smart contracts.

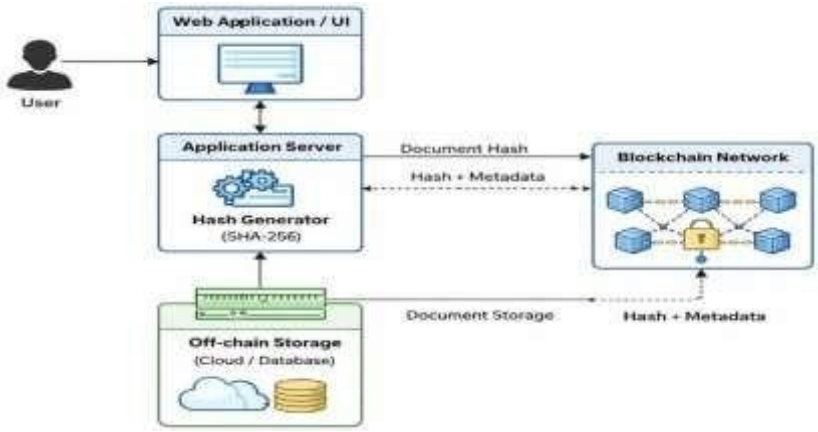

Figure 2 System Architecture

B. Data Flow Diagram

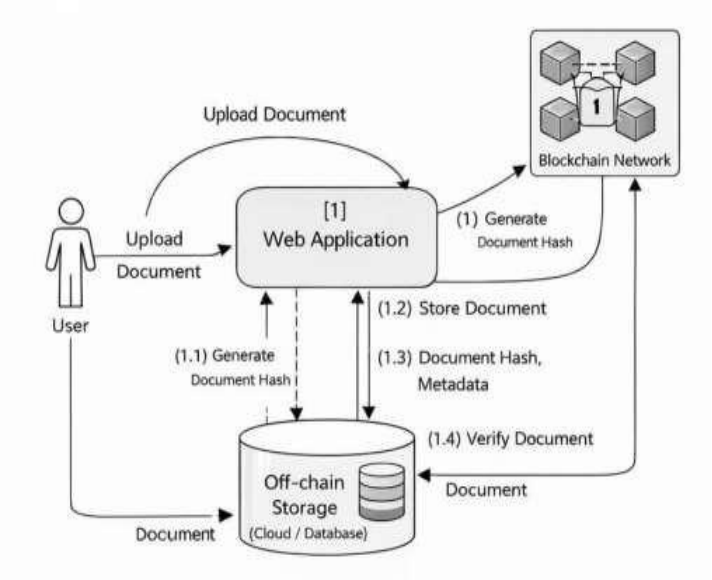

Figure 3: Data Flow Diagram

IV. CONCLUSION

This paper presented a secure and decentralized document verification system using blockchain technology. By leveraging blockchain's immutability, transparency, and decentralization, the proposed system effectively eliminates document forgery and reduces dependency on centralized authorities. The integration of IPFS ensures efficient and decentralized storage, while smart contracts automate the verification process. Experimental implementation results demonstrate that the system provides fast, reliable and tamper-proof document verification. The proposed solution is suitable for educational institutions, recruitment organizations, and government agencies. In the future, the system can be extended to support multi-institution verification networks, identity management systems, and large-scale digital credential platforms.

REFERENCES

[1] Y. Chen, S. Ding, Z. Xu, H. Zheng, and S. Yang, "Blockchain-Based Medical Records Secure Storage and Medical Service Framework," Journal of Medical Systems, vol. 43, no. 1,PP.1-9,2019.

[2] M. Crosby, P. Pattanayak, S. Verma, and V. kalyanaraman, "Blockchain Technology: Beyond Bitcoin," Applied Innovation Review,no. 2,2016

[3] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the internet of Things," IEEE Access, vol. 4,pp.2292-2303, 2016

[4] V. Buterin, "A Next-Generation Smart Contract and Decentralized Application Platform," Ethereum White Paper, 2013.

[5] M. Swan, Blockchain: Blueprint for a New Economy, O; Reily Media, 2015

[6] J. Benet, "IPFS- Content Addressed, Versioned, P2P File System," arXiv:1407.3561, 2014

[7] A. Ali, F. Khan, and M. Hussain, "Blockchain-Based Secure Document Verification System," International Journal of Computer Application, Vol. 182, no. 45, PP. 12-18, 2021

[8] P. Tapscott and A. Tapscott, Blockchain Revolution, Penguin Random House, 2016

[9] M. Sharples and J. Domigue, "The Blockchain and kudos: A Distributed System for Educational Record, Reputation and Reward," Proc. 11th European Conf. on Technology Enhanced Learning, PP. 490-496, 2016

[10] A. Grech and A. F. Camilleri, "Blockchain in Education," Joint Research Centre, European Commission, 2017.