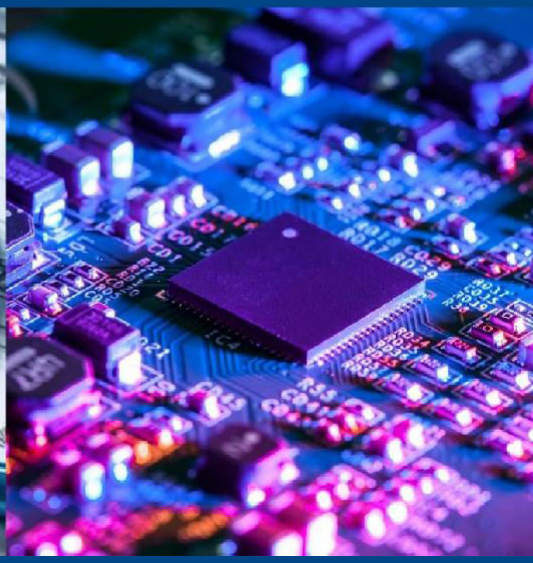
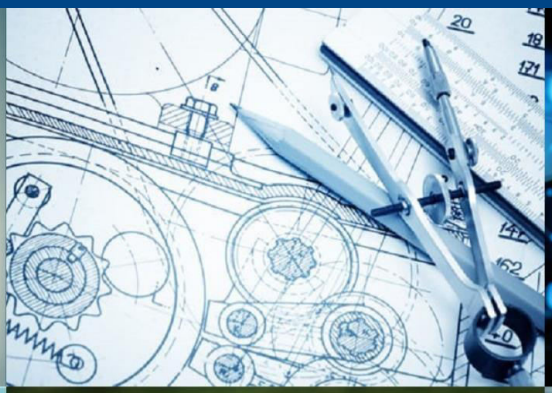
ISSN: 2582-7219

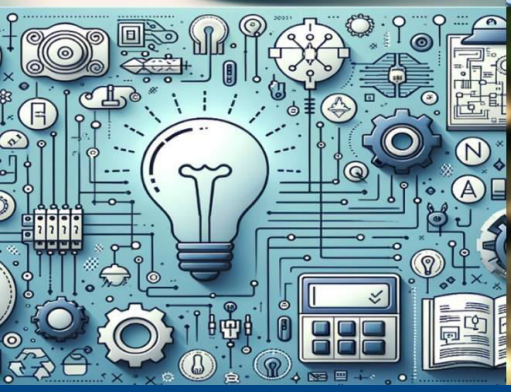




International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206

Volume 8, Issue 8, August 2025

© 2025 IJMRSET | Volume 8, Issue 8, August 2025| DOI:10.15680/IJMRSET.2025.0808031

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Blockchain-Based Document Authentication System

Lalith Kumar D, Prof. Swetha C S

P.G Student, Master of Computer Application, Bangalore Institute of Technology, VV Puram, Bangalore, India

Assistant Professor, Master of Computer Application, Bangalore Institute of Technology, VV Puram, Bangalore, India

ABSTRACT: Authentication of documents in the digital age is a very significant aspect of schools, government organizations, and businesses. The traditional verification systems tend to be prone to data loss, tampering and unauthorized access due to the centralization of such systems which increases the risks. The following paper will present a new Blockchain-Based Document Authentication System that would rely on the combination of immutable and decentralized nature of the blockchain and cryptographic security to provide trustful and tamper-resistant document verification. The system employs IPFS (Inter Planetary File System) as a distributed storage solution, SHA-256 hashing to provide integrity to data and Ethereum smart contracts as immutable record keeping.

The verified institutions can then upload documents which are stored along with their hashes on blockchain and end users or verifiers are given a platform to check integrity within a short time. This system tackles security, scalability, and timely verification issue in the current systems by eliminating the centralized nature of systems and providing clear accessibility.

KEYWORDS: Blockchain, Document Authentication, IPFS, SHA-256, Smart Contracts, Ethereum, Decentralized Verification.

I. INTRODUCTION

False documents and fraudulent claims are also an issue of concern that spread all over the world, especially in education, hiring, and in the government. The traditional document verification processes may require manual document checks, third parties, and the use of central databases- aspects that serve to prolong the verification process, make it expensive and susceptible to fraud. The offered paradigm is the blockchain technology that provides immutable, transparent, distributed ledgers and provides measures to prevent unauthorized changes.

The following paper introduces a Blockchain-based Document Authentication System in which the documents are stored on IPFS to be accessed in a decentralized way, and the digest of their unique hash in SHA-256 is stored on an Ethereum blockchain. A document can be authenticated at any time by any verifier by comparing the hash that the file was recalculated to against the on-chain record. The proposed solution has the role-based access control where only verified institutions can post documents and the general population can approve them.

We look at the architecture, workflow, and secure considerations as well as the benefits of using blockchain over legacy verification systems.

II. LITERATURE SURVEY

A. BLOCKCHAIN IN DOCUMENT VERIFICATION

Multiple studies have pointed out that blockchain is a suitable method of data integrity and authenticity. The inviolability of the blockchain assures that in case the hash value of a document is stored in the blockchain, it is impossible to change it without being identified.

B. IPFS FOR DECENTRALIZED STORAGE

IPFS is a distributed file system of which files are hashed into content identifiers (CID). Boxes Unknown In contrast to centralized servers, IPFS makes documents accessible around the world and independent of any specific server.

© 2025 IJMRSET | Volume 8, Issue 8, August 2025| DOI:10.15680/IJMRSET.2025.0808031

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

C. HASHING ALGORITHMS IN SECURITY

SHA-256 hashing gives a fixed, non-repeatable-length identifier to any particular file. Such a minor modification to the document has a totally different hash, which can effectively be used to detect tampering.

D. SMART CONTRACT APPLICATIONS

Through smart contracts, the verification logic can be carried out without a third party. This eliminates human error, enables faster verification and makes it transparent.

III. PROPOSED METHODOLOGY

Our proposed system has the following stages:

1. Institution Registration and approval by Admin:

The institution registers themselves to the system and wait for the approval by admin of the system. After the admin approves the institution, then it can upload the documents.

2. Document uploading and hashing that document:

Approved Institutions will upload the document and a SHA 256 hash of this document will be generated. The actual file that the institution uploads will be stored in IPFS and a CID will be returned.

3. Logging the hash on Blockchain

The generated hash will be store in the Ethereum blockchain via smart contract and other metadata like student name, email, date of issuing, etc., will be store in any database (ex. MongoDB).

4. Verifying the uploaded documents

The people who view verifications insert or post the document to be verified. The system does the computation of its hash in SHA-256 and checks it against the blockchain record. If this recalculated hash is present in the blockchain, then it will return as valid document else it will return as fake document.

5. Role based access to the system

Only Approved Institutions have the ability to upload the documents. The students or learners are able to view their documents uploaded by institutions and Document verification is open to anybody who sign up with the system.

System Architecture:

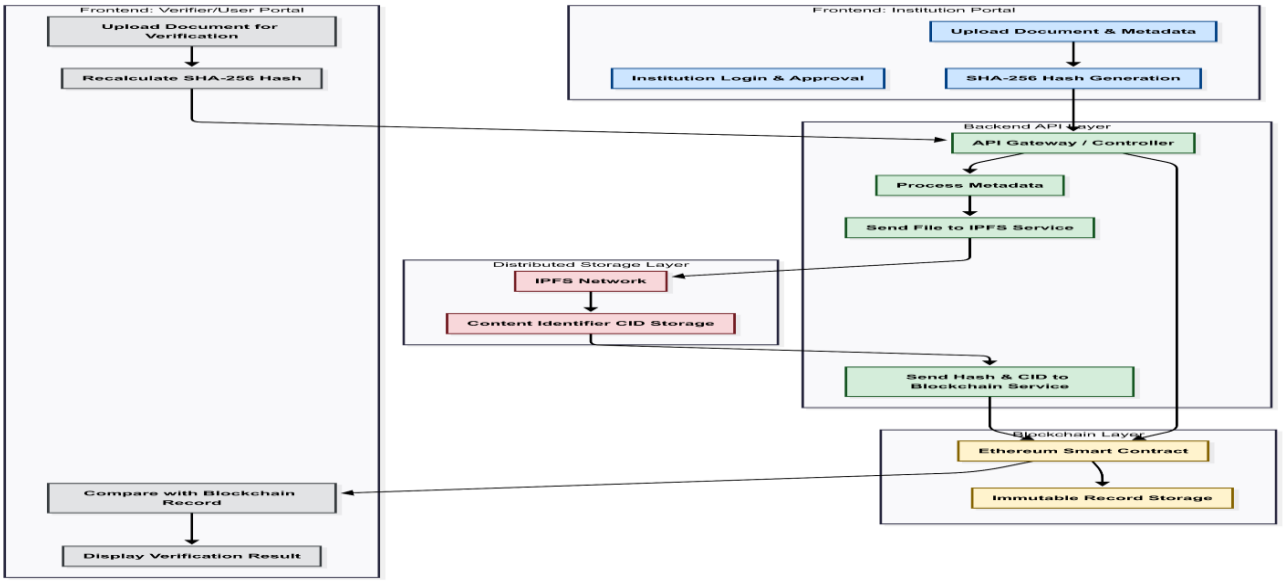


Fig1: End to end architecture of this system

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Security Considerations

1. Data Integrity - personnel can ensure that any correction to the document will produce a different hash and, thus, permit the detection of document tampering by using SHA-256.
2. Decentralization Once maintained by a single or a few machines, documents are now always available due to lack of a single point of failure.
3. Immutability- once written in blockchain the records cannot be modified again and thus maintaining historical integrity.
4. Role Based Permissions -Institutions need to be approved to upload and thus minimize the possibility of fraud entries.
5. In-transit encryption: documents pass between the location with the help of safe protocols (HTTPS, TLS).
6. Smart Contract Auditing - An auditing of the contract is made with the objective of identifying the weaknesses of the contract prior to its introduction.

Besides the above security, the fact that the suggested system relies on the decentralized character of the blockchain technology itself provides enhanced levels of security. The verification itself is based on the unalterable transaction records and on the distributed file storage so, there is no unified point of failure which is vulnerable to the attacker. Even when the IPFS network encounters the failure of the nodes, the content can still be retrieved in the IPFS network through other nodes sharing the same data. The series of hashing and immutability combination of blockchain guarantees that any unauthorized hack of a document becomes immediately noticeable. Moreover, under strict role-based control, audited organizations are allowed to insert records in blockchain and as a result, the occurrence of the fraudulent inserts is also avoided. Such multifactor security, which envelops encryption, decentralizing, immutability, and control on access offers a solid security to threats both immediate and distant, hence resulting in the permanence of the system.

Experimental tests of the suggested system proved that it can improve the effectiveness of document verification, enhance its integrity, and be capable of defending against tampering greatly. Verification with multiple file types affirmed that when a single bit in the document was altered, the hash changed giving a totally different output thus enabling immediate detection of changes. IPFS integration has made the platform less storage dependent on central servers and increased the speed in retrieving the documents based on content addresses and distributed caching provisions. Smart contracts on Ethereum allowed having a permanent and non-hacked record of verification, which could be checked by any third party without the involvement of intermediary parties. In comparison with the traditional verification process, which required hours and days to conduct, the use of the blockchain-based one took only several seconds, at a specific administrative minimum. Such findings confirm that the system is capable of offering a scalable, secure and low cost method of document authentication across the various application areas of education, recruitment and government services.

IV. CONCLUSION

The Blockchain-Based Document Authentication System does well to eliminate the challenge of traditional centralized document verification according to the benefit of the blockchain immutability, decentralized storage through IPFS, and cryptographic hashing. The use of hash-type algorithm SHA-256 guarantees the integrity of data because even the slightest change to a document is immediately identified. The system provides the following benefits over the traditional verification methods: it eliminates the delay in the verification process driven by dependence on one authority, minimizes the probability of verification alteration by an unknown party, and provides levels of transparency to the entire stakeholders involved in the verification system. Role-based access control also enhances trust in the fact that only authoritative institutions will be able to upload and register documents onto the block chain. This is not only a security enhancing method but also it dramatically increases the efficiency in the process of document verification.

Performance-wise, the given system is shown to be fast in verification, retrieval speeds and it is also tolerant to faults. By decentralizing the storage to the IPFS protocol, the documents are accessed when segments of the network fail, and the blockchain records can feature a log of historical transactions of all the verifications. Its flexible nature has seen the system implemented in various areas such as educational institutions, corporate hiring practice, legal records, and the system of record management at the government level. In the future, one can develop intersecting the concept of advanced cryptography and cryptographic privacy-Preserving verification, utilizing a multi-chain redundancy mechanism and Machine learning-based identification of fraud to enhance the platform in any possible way. It seems

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

that using the potential advantages of blockchain, this system will pave the way to an easily scalable, globally available, safe structure of verification of documents via digital means.

REFERENCES

[1] Nakamoto, S. (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System."
[2] Benet, J. (2014). "IPFS - Content Addressed, Versioned, P2P File System."
[3] Crosby, M. et al. (2016). "Blockchain technology: Beyond Bitcoin." Applied Innovation Review.
[4] Wood, G. (2014). "Ethereum: A Secure Decentralised Generalised Transaction Ledger." Ethereum Project Yellow Paper.
[5] Zhang, P., White, J., Schmidt, D. C., Lenz, G., & Rosenbloom, S. T. (2018). “FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data.” arXiv.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com