IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

DOC-BLOCK: A Blockchain Based Authentication System for Digital Documents

[1]Dhanalakshmi M,[2]Abdulkarim S,[3]Malavika E,[4]Koyafateena s, [5]Catherine pushpa riya r

[1]Student,[2]Assistant Professor,[3,4,5]Student

[1]Department of Computer Science and Engineering,

[1]Aalim Muhammed Salegh College of Engineering, Chennai, India

Abstract:With the proliferation of information technology, document forgery has become a growing concern across various sectors. Traditional document verification processes are time-consuming, error-prone, and unreliable. This paper introduces DOC-BLOCK, a decentralized web application based on the Ethereum blockchain to securely verify digital documents. By leveraging cryptographic hashing, peer-to-peer storage, and smart contracts, the system ensures data integrity, transparency, and authenticity. Our model minimizes human error, reduces verification time, and offers a tamper-proof alternative to conventional methods, ensuring a future-ready approach to document verification

Index Terms - **Blockchain, Hashing, Ethereum, Document Verification, Digital Signature, Cryptography**

I.INTRODUCTION

The advancement of information technology has transformed the way individuals and organizations manage documents. With the shift towards digitalization, digital documents have become widespread across industries such as banking, education, healthcare, and governance. However, the authenticity and security of these documents have emerged as significant concerns due to the increasing ease of document forgery facilitated by readily available editing tools and affordable technology.Traditional methods of document verification often involve labor-intensive processes and reliance on human judgment, which are not only slow but also susceptible to errors and manipulations. The involvement of multiple intermediaries further adds to the inefficiency and vulnerability of the verification process. In a globalized economy, where transactions and verifications happen across borders in real time, the shortcomings of conventional document authentication systems have become increasingly evident.

In Blockchain technology presents an innovative solution tothese challenges. A blockchain is a decentralized, immutable
ledger that records transactions securely and transparently. Its distributed nature ensures that no single entity can alter or tamper with the recorded data, making it ideal for applications requiring trust and integrity. In particular, Ethereum's smart contract functionality allows for automated, self-executing contracts that enhance the functionality of blockchain networks.DOC-BLOCK harnesses the power of blockchain to offer a decentralized platform for the storage, verification, and retrieval of digital documents. The system uses the SHA-256 hashing algorithm to generate unique fingerprints for each document, ensuring that even the slightest modification is detectable. The documents and their respective hashes are stored on a blockchain, while the files themselves are distributed across a peer-to-peer network using the InterPlanetary File System (IPFS).

The DOC-BLOCK platform is designed with user-friendliness in mind. Through an intuitive web interface, users can upload documents, verify the authenticity of submitted documents, and download verified files. Smart contracts on the Ethereum blockchain manage the validation logic, ensuring that document verification is performed accurately and without the need for centralized oversight.

Furthermore, the use of blockchain minimizes the risk of document tampering, significantly reduces verification times, and enhances operational transparency. Organizations, educational institutions, and individuals can benefit from this robust and efficient system. By addressing the gaps in traditional verification methods and leveraging cutting-edge blockchain technologies, DOC-BLOCK proposes a future-proof solution to the pervasive problem of document forgery.In addition to addressing authenticity concerns, DOC-BLOCK also empowers organizations by minimizing reliance on third-party verifiers and reducing operational costs associated with traditional document management. With the growing prevalence of remote interactions, such as virtual admissions, cross-border trade, and telemedicine, the need for a reliable and independent document verification platform has never been more critical.

II. BACKGROUND

The prevalence of counterfeit documents poses a major threat to trust, security, and operational efficiency across numerous sectors. As more businesses and governments transition to digital operations, the need for reliable document verification mechanisms has intensified. Traditional verification approaches, often reliant on centralized authorities and manual inspection, are becoming increasingly inadequate in an era of rapid digital transactions.

Blockchain technology, introduced with the inception of Bitcoin, revolutionized the concept of decentralized, tamper-proof records. Unlike conventional databases controlled by a single entity, blockchain distributes data across a network of nodes, each maintaining a complete copy of the ledger. This decentralized architecture ensures data immutability, transparency, and resilience against attacks. Any attempt to alter information on the blockchain would require simultaneous changes across a majority of nodes, making unauthorized tampering virtually impossible.

Ethereum, as an evolution of blockchain technology, introduced the concept of smart contracts—self-executing agreements coded directly onto the blockchain. Smart contracts eliminate the need for intermediaries by automatically enforcing contract terms based on predefined rules. This feature is particularly beneficial for document verification, where conditions for authenticity can be codified and enforced without human intervention.

In the context of document management, cryptographic hashing serves as a cornerstone for ensuring data integrity. A hash function generates a unique, fixed-size output for any given input. Even a minor alteration in the input results in a dramatically different hash output, making hashes ideal for detecting tampering. DOC-BLOCK utilizes the SHA-256 hashing algorithm, widely regarded for its collision resistance and computational security, to create fingerprints for each document.

The InterPlanetary File System (IPFS) complements blockchain by offering decentralized file storage. IPFS divides files into small blocks, stores them across various nodes, and retrieves them using content-based addressing rather than location-based addressing. This decentralized approach not only enhances data redundancy and availability but also aligns with the principles of blockchain in promoting distributed trust.

Several existing studies and projects have explored the potential of blockchain for document verification. Systems like IDStack and various academic initiatives have demonstrated blockchain's efficacy in securing identities and validating certificates. However, many of these solutions involve complex integrations, reliance on centralized components, or lack scalability.

DOC-BLOCK addresses these limitations by offering a user-centric, scalable, and fully decentralized platform. By combining Ethereum’s smart contracts, IPFS decentralized storage, and cryptographic security, the system ensures end-to-end authenticity without compromising user experience. The platform’s design abstracts blockchain complexities, providing users with a seamless interface to manage, verify, and retrieve digital documents securely and efficiently.This background establishes the technicalfoundations and practical

motivations behind the development of DOC-BLOCK, setting the stage for an in-depth exploration of its system architecture and operational workflow

III.ARCHITECTURE

The architecture of the proposed DOC-BLOCK system is meticulously designed to ensure secure, transparent, and efficient authentication of digital documents in an increasingly digital world. This system strategically integrates a combination of decentralized technologies, including blockchain, smart contracts, cryptographic hashing, and peer-to-peer storage networks, to create a robust and tamper-resistant verification framework. Each component in the system serves a critical role: blockchain provides an immutable ledger that records all document hashes securely, ensuring that once a document's authenticity is recorded, it cannot be altered or tampered with. Ethereum's blockchain is specifically leveraged for its smart contract functionality, enabling automated, self-executing verification processes without the need for human oversight. Smart contracts enforce business logic and validation workflows transparently, reducing the chances of human error and fraud. Cryptographic hashing, using the SHA-256 algorithm, ensures that every digital document is assigned a unique fingerprint, making even the smallest alteration detectable and providing a solid guarantee of integrity.

Furthermore, decentralized file storage through the InterPlanetary File System (IPFS) allows documents to be distributed across multiple nodes, ensuring redundancy, faster retrieval times, and protection against data loss. By utilizing content-based addressing in IPFS rather than traditional location-based methods, the system ensures that documents are retrieved based on their cryptographic hash, enhancing security and reliability. The DOC-BLOCK system architecture is also built with user accessibility in mind, abstracting the complexity of blockchain and peer-to-peer technologies behind an intuitive web interface that allows users to upload, verify, and retrieve documents with ease. This user-centric design ensures that even individuals with minimal technical knowledge can confidently participate in document verification processes. Overall, by combining decentralization, cryptographic security, and automation, the DOC-BLOCK architecture represents a future-ready solution capable of addressing the evolving challenges associated with digital document management and verification across diverse industries.

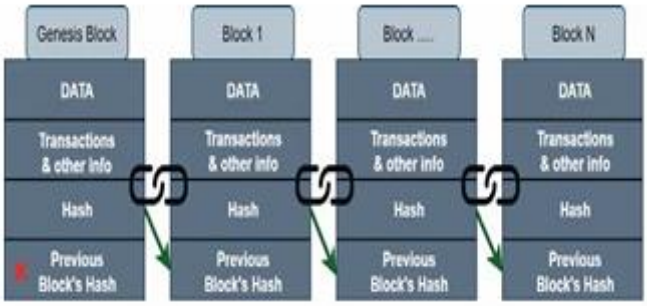


Fig. 1. Blockchain Structure.

A. Blockchain

Blockchain is an advanced technology that offers greater convenience and security compared to traditional centralized data storage systems. It is a transaction-based data storage network where information is stored in a decentralized manner through a distributed network. In this network, personal computers, known as nodes, connect through a Peer-to-Peer (P2P) communication protocol. No single node can independently manipulate data, as all nodes maintain access to the actual records. Each block is securely encrypted with a hash algorithm and stores the hash code of the preceding block, linking all blocks together like a chain. Any alteration in a block results in changes to its hash code, thereby invalidating the chain, which ensures transparency and reliability. A typical block contains its own hash, the hash of the previous block, and transaction data. The first block in the network isknown as the Genesis Block, which does not reference any prior block.

B. Ethereum

Ethereum is a global, public, distributed blockchain-based network created to manage the computational infrastructure of blockchain applications. It is an open-source platform providing functionalities such as smart contracts and the native cryptocurrency, Ether. Smart contracts are programming codes deployed on the Ethereum network that execute automatically when predefined conditions are met. They operate in a self-executing, distributed, and immutable manner across the blockchain. Ether serves as the transaction fee within the Ethereum network and facilitates the execution of smart contracts and decentralized application functionalities.

C. Solidity

Solidity is a high-level, object-oriented programming language specifically designed for writing smart contracts on blockchain networks like Ethereum. It draws inspiration from popular programming languages such as C++, Python, and JavaScript. Solidity is used to define business logic and computational workflows embedded in smart contracts, which are then executed within the Ethereum Virtual Machine (EVM). It provides developers with a structured, efficient environment for building decentralized applications with robust functionality.

D. Infura

Infura is utilized in the proposed system to facilitate interaction with the Ethereum blockchain without the need to host a local Ethereum node. Generally, interacting with the Ethereum network requires users to create and maintain their own Ethereum wallet and node infrastructure. Infura simplifies this process by offering a hosted node cluster, allowing seamless communication with the Ethereum blockchain through an API. This service maintains the principles of decentralization while eliminating the complexities of node management for users and developers.

E. InterPlanetary File System (IPFS)

The InterPlanetary File System (IPFS) is a peer-to-peer data storage, distribution, and transfer protocol that uses a content-based addressing system. Unlike traditional location-basedstorage, IPFS identifies and accesses files based on their cryptographic content hash. When a document is uploaded,it isdivided into smaller chunks, each assigned a unique hash, and distributed across multiple nodes in the network. This method ensures enhanced redundancy, availability, and security. Users can retrieve or host files from any node in the network using the content address, supporting efficient and decentralized data management.

F. Hashing Function SHA-256

The SHA-256 hashing algorithm is employed in the proposed system to ensure document integrity and security. SHA-256 generates a unique, fixed-size 256-bit hash output for any given input, regardless of the input's size. Even minor alterations to the input data produce entirely different hash outputs, making the algorithm highly effective in detecting tampering. Hashing functions are one-way operations, meaning it is computationally infeasible to reconstruct the original input from the output hash. This property makes SHA-256 a reliable mechanism for securing digital documents without requiring the storage of the original files on the blockchain.

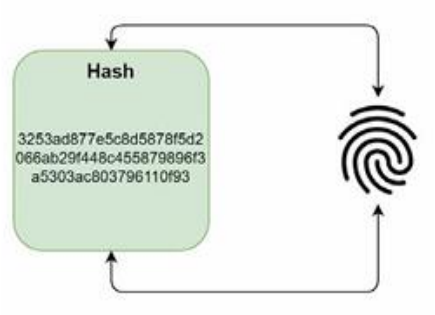


Fig. 2. Hash.

G. Admin Section Workflow

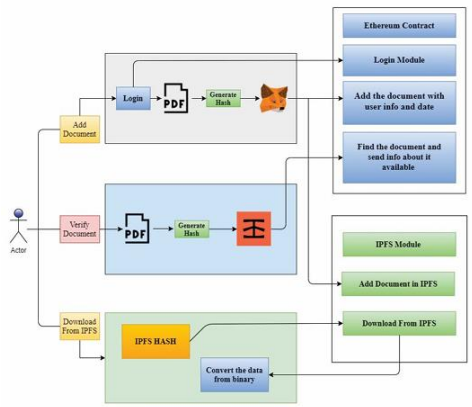
The admin section in the DOC-BLOCK system is tailored for organizations or institutions that need to manage and authenticate documents. Administrators can upload verified documents onto the blockchain by generating the document's SHA-256 hash, which is then recorded along with the admin's public Ethereum address and a timestamp. The system provides an IPFS hash corresponding to the stored document, enabling administrators to retrieve or share the document securely when needed. This workflow ensures that organizations can maintain full control over the authenticity of their uploaded documents, minimizing the risk of forgery and unauthorized alterations.

H. User Section Workflow

The user section enables general users to verify the authenticity of submitted documents and retrieve documents using an IPFS hash. During verification, users upload a document, and the system computes its SHA-256 hash. This computed hash is then compared with the hashes recorded on the blockchain. A successful matchconfirms that the document is authentic, while any mismatch indicates tampering or corruption. Users can also input an IPFShash to download original documents directly from the decentralized network. This process ensures that document verification and retrieval are straightforward, secure, and reliable for all users.

I. Proposed System

The proposed DOC-BLOCK system ensures secure document authentication by integrating blockchain technology with decentralized storage. Documents are hashed using SHA-256 and the hash values are recorded on the Ethereum blockchain, while the original files are stored in IPFS. Smart contracts automate the verification process, enabling fast, reliable, and tamper-proof validation. The overall system architecture focuses on enhancing security, transparency, and user accessibility. The process flow of the proposed system is illustrated in the following figure.



IV. CONCLUSION

Document forgery and authenticity issues have long challenged organizations, institutions, and individuals around the world. As digitalization accelerates, traditional document verification methods have proven increasingly inadequate in ensuring the integrity, confidentiality, and reliability of critical records. The DOC-BLOCK system, through its innovative integration of Ethereum blockchain technology, smart contracts, cryptographic hashing mechanisms, and decentralized storage via IPFS, effectively addresses these longstanding gaps. By leveraging blockchain's immutability and transparency, DOC-BLOCK ensures that document authenticity can be validated with a high degree of accuracy and trustworthiness. Smart contracts automate the verification process, reducing reliance on manual inspection and minimizing the possibility of human errors or fraudulent activities. Furthermore, the use of IPFS for document storage enhances system resilience, improves redundancy, and protectsuser privacy by ensuring distributed file management across a global network.The proposed architecture demonstratessignificantimprovements in operational efficiency, security, and ease of use when compared to conventional centralized verification methods. By abstracting complex blockchainoperations behind a user-friendly interface, DOC-BLOCK enables seamless access even for users with limited technical expertise, thereby promoting broader adoption of decentralized authentication technologies.

Looking toward the future, DOC-BLOCK offers several promising avenues for enhancement and scalability. Future developments could include the integration of Layer-2 scaling solutions such as Optimistic Rollups or zk-Rollups to improve transaction throughput and reduce gas costs on the Ethereum network. Additionally, expanding support for multiple file uploads, integrating advanced identity management systems, and building terminal-based or mobile interfaces could further enhance the platform's flexibility and usability in professional and enterprise settings. Enhancing interoperability with other blockchain networks, such as Polygon or Binance Smart Chain, could also enable cross-chain document verification, increasing the platform's versatility. Despite these potential upgrades, the current version of DOC-BLOCK already marks a significant advancement in digital document management, providing a secure, transparent, and efficient verification framework. By embracing decentralized solutions like DOC-BLOCK, organizations can dramatically reduce instances of fraud, enhance public trust, and ensure that document authenticity and integrity are no longer barriers to operational excellence in the evolving digital landscape.

V.REFERENCES

[1] S. Leible, S. Schlager, M. Schubotz, and B. Gipp, "A Reviewon Blockchain Technology and Blockchain Projects Fostering
Open Science," Frontiers in Blockchain, 2019.
[2] A. Prashanth Joshi, M. Han, Y. Wang, "A Survey on Securityand Privacy Issues of Blockchain Technology," Mathematical
Foundations of Computing, 2018.
[3] W. Chen, Z. Xu, S. Shi, Y. Zhao, and J. Zhao, "A Survey of Blockchain Applications in Different Domains," ACM Digital
Library, 2018.
[4] K. Gilani, E. Bertin, J. Hatin, and N. Crespi, "Blockchain-Based Identity Management," BRAINS Conference, 2020.
[5] J. Wang, S. Wang, G. Junqi, Y. Du, S. Cheng, and X. Li,"Blockchain in Intellectual Property," Procedia Computer Science,
2019.
[6] S. Rouhani and R. Deters, "Security, Performance, andApplications of Smart Contracts," IEEE Access, 2019.
[7] D. Yue, R. Li, Y. Zhang, W. Tian, and C. Peng, "Blockchain-Based Data Integrity Verification in P2P Cloud Storage," IEEE
ICPADS, 2018.
[8] H. Teymourlouei and L. Jackson, "Blockchain for IdentityAuthentication and Data Protection," 2019.
[9] X. Zhu, "Blockchain-Based Identity Authentication andIntelligent Credit Reporting," Journal of Physics: Conference Series, 2020.

[10] L. Arjomandi, G. Khadka, Z. Xiong, and N. Karmakar,"Document Verification Using Chipless RFID," IEEE Access,2018.