INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

IJARIIT

ISSN: 2454-132X
Impact Factor: 6.078
(Volume 10, Issue 1 - V10I1-1289)
Available online at: https://www.ijariit.com

Blockchain-Based eVault for Legal Documents

Gauri Yogeshwar Wankhade
gauriywankhade6@gmail.com
JSPM's Bhivarabai Sawant Institute of Technology and Research, Pune, Maharashtra

Shantanu Rawade
rawadeshantanu@gmail.com
JSPM's Bhivarabai Sawant Institute of Technology and Research, Pune, Maharashtra

Harshal Lokhande
harshallokhande2222@gmail.com
JSPM's Bhivarabai Sawant Institute of Technology and Research, Pune, Maharashtra

Anish Bhalerao
anishbhalerao7070@gmail.com
JSPM's Bhivarabai Sawant Institute of Technology and Research, Pune, Maharashtra

Prof. Shrishail Patil
shri.patil11@gmail.com
JSPM's Bhivarabai Sawant Institute of Technology and Research, Pune, Maharashtra

ABSTRACT

Blockchain-based centralized file-sharing platforms are not capable of providing security and privacy to data which leads to an increase in security attacks, single points of failure, and censorship. As we know the digitization of legal documents has taken a rapid growth which results in the transformation of the legal industry and provided efficiency, accessibility, and security to a multitude of stakeholders. However, there is a need for a trusted and immutable system for storing, sharing, and verifying these documents remains is a challenge. The paper is based on this concept of "Blockchain-Based eVault for Legal Documents," It leverages blockchain technology to address the issues of document authenticity, data security, and legal document managing. The proposed eVault is designed to act as a secure repository for legal documents, offering a robust solution to the persistent challenges of document tampering, fraud, and unauthorized access. By utilizing blockchain technology, which provide decentralized, transparent, this eVault ensures integrity or authenticity of legal documents.

Keywords: Blockchain, Smart contracts, decentralized file sharing,

I. INTRODUCTION

Blockchain-based eVault serves as a secure and transparent repository for legal documents, ensuring their integrity through blockchain's immutability. The Blockchain-Based eVault for Sharing and Accessing Legal Documents aims to revolutionize legal document management by leveraging blockchain technology for enhanced security, transparency, and efficiency. By decentralizing access and employing smart contracts, it grants users control over document permissions, simplifies collaboration, and maintains a detailed audit trail. It will provide a decentralized, tamper-proof environment with features such as smart contracts, time-stamped auditing, and user-friendly interfaces to streamline the storage, sharing, and verification of legal documents.

The motivation to develop a Blockchain Based eVault for Legal Documents stem from the inherent challenges and opportunities within the legal industry. Blockchain's cryptographic principles ensure the immutability and security of legal documents, making it nearly impossible for unauthorized parties to alter or manipulate sensitive information. The transparent nature of blockchain provides an unforgeable and publicly accessible record of all transactions, fostering trust among legal professionals, clients. Smart contracts on the blockchain automate routine legal processes and enhancing overall efficiency in document management. Blockchain-based eVaults enable users to control the permissions, which ensures that only authorized individuals can view and modify

© 2024, www.IJARIIT.com All Rights Reserved

specific document, thereby enhancing privacy and user control. Automation through smart contracts and the elimination of intermediaries contribute to cost savings in the long run, making legal processes more efficient and cost-effective. In conclusion, the motivation for a Blockchain-Based eVault for Legal Documents lies in addressing the limitations of traditional document management systems, providing enhanced security, transparency, and efficiency for legal professionals. By leveraging blockchain technology, this solution not only meets the immediate needs of the legal industry but also positions it for a more technologically advanced and resilient future.

The scope for a Blockchain-Based eVault for Legal Documents encompasses a comprehensive set of functionalities and considerations to ensure the successful development, deployment, and adoption of the solution. The scope is defined across various dimensions, covering technical, functional, legal, and user experience aspects. Evaluate and select a suitable blockchain platforms such as Ethereum, Hyperledger which are based on factors such as scalability, security, and features.

The blockchain-based eVault for legal documents is designed to revolutionize the storage, management, and security of legal documents. It leverages blockchain technology to create an immutable and tamper-resistant repository for legal professionals, clients, and administrators. The primary objectives of this system are Secure Document Storage: To securely store legal documents in the distributed blockchain network. Immutability: To ensure the immutability of stored documents, preventing unauthorized alterations or deletions. Auditable Transactions: To maintain an auditable record of all document-related activities and changes. Access Control: To implement robust access control mechanisms to safeguard confidential legal documents. User Friendly Interface: It offers an intuitive and user friendly interface in easy document upload, retrieval, and management.

Design a decentralized network architecture to ensure data redundancy, eliminate single points of failure, and enhance system resilience. Implement advanced cryptographic techniques to secure the storage and transmission of legal documents, ensuring confidentiality and integrity. Design a robust user authentication system with multi-factor authentication to control access to the eVault. Enable users to securely upload and store legal documents on the blockchain. Conducting security assessments, which includes penetration testing, which identifies and addresses potential vulnerabilities. Outline a roadmap for future development, including planned updates, additional features, and ongoing support to meet evolving industry needs. Design and deploy a decentralized system for storing legal documents securely. Enable efficient and transparent document management through the use of smart contracts. Enhance data integrity, reduce the risk of unauthorized access, and establish a comprehensive audit trail. Design and deploy a decentralized system for storing legal documents securely. Enable efficient and transparent document management through the use of smart contracts. Enhance data integrity, reduce the risk of unauthorized access, and establish a comprehensive audit trai

II. LITERATURE REVIEW

Sr.No	Research Paper Title	Outcomes	Limitation
1	'Blockchain Based Criminal Record Management System'	It removes all problems such as being tampered with by utilizing decentralized data storage.	Implementation needed in city, state, or country.
2	'Blockchain based Resource Management System'	Set of operations and systems to manage and control access to such digital resources using blockchain technology.	Need more User Friendly. It affect the network speed of blockchain in reading and writing data.
3	'Design and Development of a Blockchain Based System for Private Data Management'	The capacity to store data in conjunction with other parties such as cloud.	Enables users to upload data to database without validating its accuracy.

4	'Blockchain-based Decentralized Data Storage and Access Framework for PingER'	The proposed framework eliminates the need for centralized repository.	The cost of production ready application will require some costing as compared to traditional systems.

"CRAB: Blockchain Based Criminal Record Management System," highlights the advantages of decentralized data storage in mitigating tampering issues within criminal records. However, the limitation lies in the necessity for broader implementation at various scales, ranging from city tocountry levels. "Blockchain-based Resource Management System" aimed at controlling access todigital resources. While it offers a robust set of operations, the need for enhanced user-friendliness is identified as a limitation. Additionally, concerns are raised about potential impacts on blockchain network speed during data read and write operations. "Design and Development of a Blockchain-BasedSystem for Private Data Management," emphasizing the capability for storing the data in collaboration with other parties. However, a drawback is identified in the system's allowance for uploading data without ensuring it's accuracy, raising concerns about data integrity. "Blockchain-based Decentralized Data Storage and Access Framework for PingER," eliminating the need for centralized repositories.The limitation here is the expected production cost, which is noted to be higher compared to traditional systems.

III. PROBLEM STATEMENT BLOCKCHAIN-BASED EVAULT FOR LEGAL DOCUMENTS

To develop eVault system for legal records which will be based on blockchain which ensure security, transparency. The system will store, manage, and sharing of legal documents and records securely andwith the efficiency to integrate with existing legal databases and case management systems.

PROPOSED METHODOLOGY

Project Modules:

User Management Module: Handles user registration, authentication, and profile management. Manages user identity, roles, and permissions within the system. Integrates with blockchain-based identity verification solutions.
File Upload and Encryption Module: Allows users to upload files securely. Encrypts files before transmission and storage. Manages file metadata, such as name, size, and type.
Decentralized Storage Module: Utilizes a decentralized storage solution (e.g., IPFS, Filecoin) to store and retrieve files. Ensures redundancy and data availability across distributed nodes.

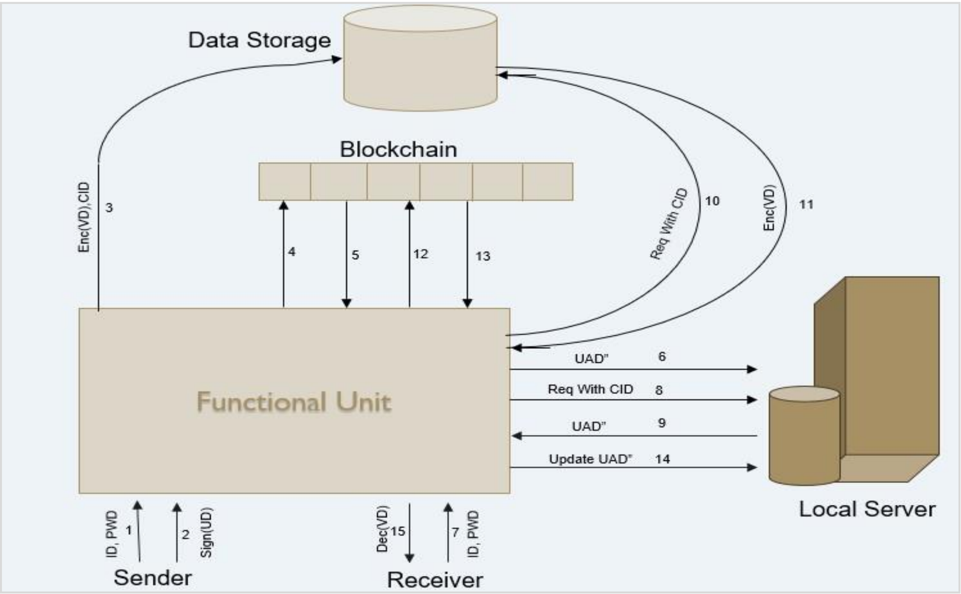

Figure No.1 Proposed System

Access Control Module: Enforces access control policies based on smart contracts. Determines who can access, view, edit, or delete files. Handles user permissions and access requests.
File Sharing Module: Allows users to share files with others. It may include metadata indexing and search algorithms.
Smart Contract Module: Contains smart contracts for managing file ownership, access control, and user permissions. Executes and enforces the rules governing the system's operation.
Blockchain Integration and Interaction Module: Facilitates interactions with the underlying blockchain network. Handles the execution of smart contracts, blockchain events, and transaction processing.

IV. ALGORITHMS

When building an eVault for a legal document of the decentralized file-sharing system using blockchain, you'll need to implement various algorithms and data structures to handle critical tasks, such as encryption, access control, consensus, and data management. Following are some key algorithms and techniques that can be used in different components of the system:

File Encryption Algorithm: Symmetric and asymmetric encryption algorithms (e.g., AES, RSA) for securing file content. Hash functions (e.g., SHA-256) for generating file checksums.

Access Control Algorithm: Role-based access control (RBAC) algorithms for managing user permissions. Attribute based access control algorithms for fine-grained access control.

Consensus Algorithm: This algorithm includes: Proof-of-Work or Proof-of-Stake for blockchain consensus, depending on the chosen blockchain platform.

Blockchain Data Management Algorithm: Merkle trees for efficiently representing and validating the integrity of data present on the blockchain. Data compression algorithms (e.g., zlib) for optimizing storage efficiency.

File Chunking Algorithm: Chunking files into smaller pieces before encryption to support efficient storage and retrieval. Algorithms like Rabin's fingerprinting for identifying chunk boundaries.

Decentralized Storage Algorithms: Interplanetary File System (IPFS) or Filecoin's distributed storage protocols for decentralized file storage.

Data Replication Algorithm: Algorithms for replicating files across multiple nodes to ensure fault tolerance and availability.

Blockchain Smart Contract Algorithms: Algorithms for coding and deploying smart contracts on the blockchain. Typically, Solidity or other blockchain-specific languages are used. Files efficiently in a decentralized environment, e.g., distributed hash tables (DHTs).

V. CONCLUSION

Our software offers a promising solution to the persistent hurdles encountered by the legal sector in managing documents through decentralized peer to peer data storage. Digital signatures are employed to validate the authenticity of uploaded data, with each sender assuming full accountability for the content they upload. Utilizing encryption enhances the security measures of our system. The use of randomly generated encryption keys guarantees that each file possesses a unique key, significantly diminishing the vulnerability to attacks. The cloud components contents data storage and blockchain, remain inaccessible to individual users. This comprehensive approach ensures data security and meticulous tracking of provenance, while also addressing potential software/hardware failures. By decentralizing control and leveraging the immutability of blockchain technology, our platform guarantees that documents housed within the eVault are impervious to tampering, instilling a high level
of trust and dependability. This not only upholds the integrity of legal documents but also mitigates the risks associated with fraud and unauthorized access.

VI. REFRENCES

1] Mihir Nevpurkar1, Chetan Bandgar2, Ranjeet Deshmukh3, Jay Thombre4, Rajashri Sadafule5,Suhasini Bhat6 . Decentralized File Storing and Sharing System using Blockchain and IPFS.

https://www.irjet.net
2] Mr. Gaurav Jadhav Ms. Sucharya Deshmukh Ms. Bhumika Mhatre Mr. Nachiket More Mrs. Rizwana Shaikh. Decentralized File Sharing using Blockchain Empowering Peer-to-Peer Collaboration:The Rise of Decentralized File Sharing. https://www.irjet.org
3] Mathis Steichen, Beltran Fiz, Robert Norvill, Wazen Shbair and Radu State. Blockchain-Based Decentralized Access Control for IPFS. https://ieeexplore.ieee.org/document/8726493 .
4] Shalom, G. R., & Nirogi, G. R. (2022, September 30). Decentralized Cloud Storage Using Blockchain. International Journal for Research in Applied Science and Engineering Technology, 10(9), 1294–1300. https://doi.org/10.22214/ijraset.2022.46810
5] Wilkinson, S., Boshevski, T., Brandoff, J., & Prestwich, J. (2014). Storj a peer-topeer cloud storage network. https://storj.io/storj.pdf
6] Durr, F., Mileo, A., & Bach, S. (2019). Towards secure IPFS-based networks: the influence of peer identities on content integrity. Journal of Reliable Intelligent Environments, 5(2), 105-124.
7] Pinata: IPFS Pinning Service. https://www.pinata.cloud
8] Buterin, V. (2013). "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform." Ethereum Whitepaper. [Link to Ethereum Whitepaper]
9] Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends." Proceedings of IEEE International Congress on Big Data.
10] G. Li and H. Sato, "A privacy-preserving and fully decentralized storage and sharing system on the blockchain," in Proceedings of the 2019 IEEE 43rd Annual Computer Software and Applications Conference, pp. 694–699, IEEE, Milwaukee, WI, USA, July 2019.
11] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf
12] Wood, G. (2014). Ethereum: A secure decentralized generalized transaction ledger. Ethereum Project Yellow Paper, 151, 1-32.
13] Benet, J. (2014). Ipfs-content addressed, versioned, p2p file system. arXiv preprint arXiv:1407.3561.
14] Wilkinson, S., Boshevski, T., Brandoff, J., & Prestwich, J. (2014). Storj a peer-to-peer cloud storage network. https://storj.io/storj.pdf
15] Protocol Labs. (2016). Filecoin: A decentralized storage network. https://filecoin.io/filecoin.pdf