Vol-08 Issue 11, November -2024 ISSN: 2456-9348
Impact Factor: 7.936

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

BLOCKCHAIN BASED E-VAULT

Authors:
Ankur Singh
Kaustubh Shivarkar
Aditya Waghade
Amit sabale

Project Guide:
Mrs. Renuka Patil
Department of Information Technology, Dr. D.Y.Patil College of Engineering,Akurdi, India.

1.ABSTRACT
Blockchain-based digital storage systems have become crucial for ensuring security and privacy, especially in protecting sensitive data from security attacks, single points of failure, and unauthorized access. The growing need for a secure and decentralized solution for storing confidential digital assets has driven interest in blockchain technology. This paper presents the concept of a "Blockchain-Based E-vault," designed to provide a trusted, immutable, and transparent platform for securely storing, sharing, and verifying digital assets and sensitive documents. Leveraging blockchain's decentralized architecture, the proposed eVault eliminates the risks associated with traditional centralized storage solutions. The system ensures data integrity, prevents unauthorized access, and provides an auditable trail of access and modifications. By integrating encryption and smart contracts, the eVault offers a robust solution to the ongoing challenges of data security, fraud prevention, and transparency in digital asset management.

Keywords:
Blockchain, eVault, decentralized storage, smart contracts, data integrity.

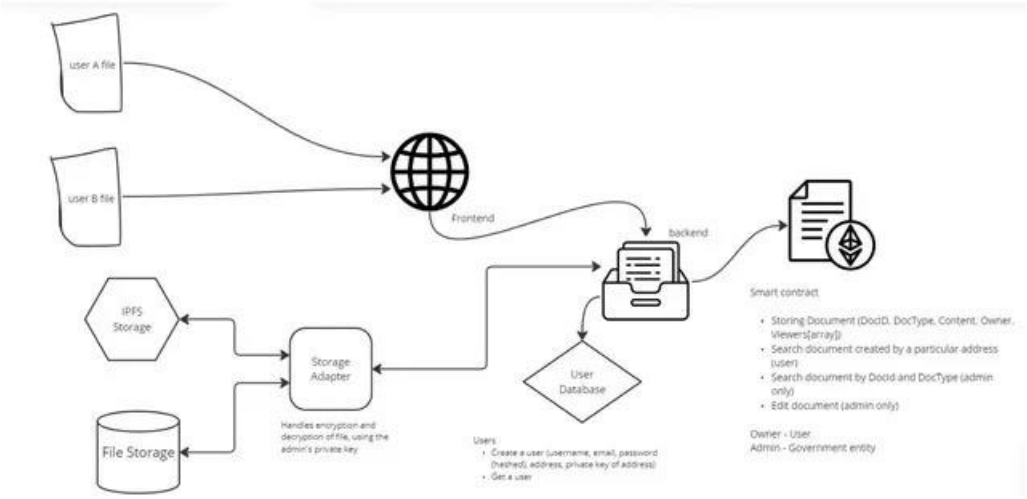
2.INTRODUCTION
The blockchain-based eVault offers a secure and transparent solution for managing legal documents by utilizing blockchain’s core features of decentralization and immutability. By integrating blockchain technology, the eVault ensures the integrity of stored legal documents, making it nearly impossible for unauthorized parties to alter or tamper with sensitive information. This system revolutionizes legal document management by enhancing security, transparency, and efficiency through decentralized access control and the use of smart contracts. These features allow users to manage document permissions, streamline collaboration, and maintain a detailed audit trail of all transactions. The eVault provides a tamper-proof environment equipped with essential features such as time-stamped auditing, cryptographic security, and an intuitive user interface, all designed to simplify the storage, sharing, and verification processes of legal documents.
The motivation to develop this blockchain-based eVault stems from the challenges inherent in traditional legal document management, such as security vulnerabilities, document tampering, and inefficiencies caused by reliance on centralized systems. Blockchain’s decentralized nature and cryptographic principles ensure that legal documents remain secure and immutable, fostering trust among legal professionals and their clients. The transparency provided by blockchain technology creates an unforgeable record of all document-related activities, while smart contracts automate routine legal processes, reducing manual intervention and increasing overall efficiency. Additionally, the system empowers users by allowing them to control access to their documents, ensuring that only authorized individuals can view or modify sensitive files, thereby enhancing privacy and user control. By addressing the limitations of traditional document management systems, the blockchain-based eVault offers a robust and efficient platform for legal professionals. The integration of smart contracts

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

and cryptographic techniques not only enhances the security and integrity of legal documents but also reduces operational costs and simplifies document management. This innovative approach to managing legal documents positions blockchain technology as a transformative tool in the legal industry, providing a more secure, transparent, and efficient system for document storage and access.

3. METHODOLOGY

The development of the eVault system for legal records is based on blockchain technology to ensure the security, transparency, and integrity of document storage, management, and sharing. The system is designed to securely handle legal documents while integrating seamlessly with existing legal databases and case management systems. The following modules are proposed for implementing the blockchain-based eVault:



1. User Management Module:
This module manages user registration, authentication, and profile handling. It defines and controls user roles and permissions within the eVault system, ensuring that only authorized individuals can access sensitive documents. Blockchain-based identity verification solutions are integrated to enhance user authentication, creating a secure environment where users' identities are cryptographically protected.

2. File Upload and Encryption Module:
This module allows users to upload legal documents securely. Before storing or transmitting any files, the system encrypts the data to ensure confidentiality. Metadata such as file name, size, and type are stored in the blockchain to provide an immutable record of the uploaded documents. The encryption process ensures that unauthorized users cannot access the file contents, preserving the integrity of sensitive legal documents.

3. Decentralized Storage Module:
To achieve high data availability and redundancy, the eVault utilizes decentralized storage solutions like InterPlanetary File System (IPFS) or Filecoin. These technologies distribute files across a network of nodes, preventing data loss and eliminating single points of failure. The decentralized architecture ensures that legal documents are always accessible, even in the event of system outages.

4. Access Control Module:
Access to the documents is governed by this module, which enforces security policies through blockchain-based smart contracts. It determines who can view, edit, or delete documents based on predefined user permissions. This system ensures that only authorized users have access to particular files, safeguarding confidential legal information.

5. File Sharing Module:
This module allows users to securely share legal documents with other parties, such as lawyers or clients. The system includes metadata indexing to help users search for specific files quickly. Smart

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

contracts further facilitate secure sharing by automating access permissions, ensuring that only designated individuals can view or modify the shared files.

6. Smart Contract Module:

The smart contract module manages the creation, execution, and enforcement of contracts within the eVault system. These contracts govern file ownership, access control, and user permissions, automating legal processes to enhance efficiency. Smart contracts also provide a transparent and auditable trail of all transactions, ensuring accountability within the system.

7. Blockchain Integration and Interaction Module:

This module handles interactions with the underlying blockchain network. It processes blockchain events and transactions, including the execution of smart contracts. All document-related transactions, such as uploads, access requests, and permission changes, are recorded on the blockchain to provide a tamper-proof log of system activity.

By integrating these modules, the proposed blockchain-based eVault offers a secure, decentralized, and transparent system for managing legal documents, ensuring data integrity and efficiency in legal document handling.

4. DEVELOPMENT STACK AND IMPLEMENTATION

The Blockchain-based eVault system will be built using a combination of blockchain technology, decentralized storage, and a modern web application framework for secure and scalable legal document management.

1. **Frontend (ReactJS)**:The ReactJS frontend will provide an intuitive user interface for managing legal documents, including uploading, sharing, and controlling access. It will offer responsive design and real-time interactions for efficient document handling and tracking.
2. **Backend (Node.js and Express)**:The backend, built with Node.js and Express, will manage API requests, user authentication, and data processing. It will also handle communication with the blockchain for document verification and enforce access control through smart contracts.
3. **Blockchain and Smart Contracts (Ethereum/Hyperledger)**:Smart contracts will be developed to manage document ownership, permissions, and audit logs. These contracts will automate access control and ensure immutability. The blockchain will record all document transactions to provide a transparent, tamper-proof system for legal document handling.
4. **Database (MongoDB)**:MongoDB will be used to store user data, document metadata, and system logs, ensuring flexibility for handling large datasets. The database will manage essential information for document storage and access control.
5. **Decentralized Storage (IPFS/Filecoin)**:Decentralized storage solutions like IPFS/Filecoin will be integrated to store documents across distributed nodes, ensuring redundancy, availability, and enhanced security for legal records.

5.RESULT AND ANALYSIS:

5.1 Dataset Acquisition

The dataset for the Blockchain-based eVault system consists of legal documents and metadata, including contracts, agreements, and legal certificates. This dataset forms the foundation for blockchain-based document storage and management.

1.Metadata Preparation:

The dataset includes essential metadata such as document types, creation timestamps, author information, and file identifiers. This metadata is crucial for proper classification, access control, and audit trails in the eVault system..

2. Preprocessing Preparation:

The dataset is being preprocessed to extract key metadata and ensure that documents are cleaned and formatted appropriately for blockchain integration. This ensures compatibility with decentralized storage systems and enhances document integrity for secure storage.

5.2 Model Training Initiation

Initial model training has started to develop the system's capabilities for document verification, access control, and smart contract management within the Blockchain-based eVault. While still in the early stages, the training has shown promising results.

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

1. Document Authentication:
Initial training has shown that the system can successfully authenticate documents using blockchain's cryptographic features. Early tests demonstrate the potential for detecting tampered or altered documents based on cryptographic hashes.

2. Access Control Insights:
Early analysis of user interaction and access control data has shown patterns of document access. This indicates that the system will be capable of automating access control decisions and generating audit logs for every document access and modification.

5.3 Data Pipeline Development
A critical component of the eVault system, the data pipeline, is under development. This pipeline will ensure that legal documents are securely processed, stored, and managed in the decentralized environment.

1. Data Cleaning and Structuring:
The pipeline will handle the removal of irrelevant data, such as unnecessary metadata or outdated versions, and structure the document content for seamless integration with blockchain storage. This step ensures that only relevant and validated data is stored on the blockchain.

2. Scalability:
The data pipeline is designed for scalability, enabling it to handle large volumes of legal documents while maintaining security and performance. This scalability ensures that the system can grow with the increasing demands of the legal industry, providing real-time access control and document management for users.

6. CONCLUSION
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.. Digital signatures and encryption enhance data authenticity and security, while a decentralized storage approach eliminates the risks of centralized data breaches. The platform provides a transparent, auditable trail of document transactions, enabling trust and accountability. This comprehensive solution significantly improves document security, access control, and traceability, positioning the eVault as a reliable tool for modern legal document management.

7. REFERNCES
1] Mihir Nevpurkar1, Chetan Bandgar2, Ranjeet Deshmukh3, Jay Thombre4, Rajashri Sadafule5,Suhasini Bhat6 . Decentralized File Storing and Sharing System using Blockchain and IPFS.
2] Lemieux, V. L. (2021). Blockchain and Recordkeeping. Computers, 10(11), 135.
3] Tasnim, M. A., Omar, A. A., Rahman, M. S., & Bhuiyan, M. Z. A. (2018). Crab: Blockchain based criminal record management system. In Security, Privacy, and Anonymity in Computation, Communication, and Storage: 11th International Conference and Satellite Workshops, SpaCCS 2018, Melbourne, NSW, Australia, December 11-13, 2018, Proceedings 11 (pp. 294-303). Springer International Publishing.
4] Ali, S., Wang, G., White, B., & Cottrell, R. L. (2018, August). A blockchain-based decentralized data storage and access framework for pinger. In 2018 17th IEEE international conference on trust, security and privacy in computing and communications/12th IEEE international conference on big data science and engineering (TrustCom/BigDataSE) (pp. 1303 1308). IEEE
5] Malomo, O., Rawat, D., & Garuba, M. (2020). Security through block vault in a blockchain enabled federated cloud framework. Applied Network Science, 5(1), 1-18.
6] Batista, D., Mangeth, A. L., Frajhof, I., Alves, P. H., Nasser, R., Robichez, G., ... & Miranda, F. P. D. (2023). Exploring Blockchain Technology for Chain of Custody Control in Physical Evidence: A Systematic Literature Review. Journal of Risk and Financial Management, 16(8), 360
7] 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.

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

8] Shovon Niverd Pereira, Noshin Tasnim, Rabius Sunny Rizon, Muhammad Nazrul Islam "Blockchain-Based Digital Record Keeping in Land Administration System", "Proceedings of International Joint Conference on Advances in Computational Intelligence", 2021, pp.431-443