Designing a Blockchain-Driven eVault System for Legal Document Preservation

Dr. Praveena K N
Dept of Computer Science and Engineering
Presidency University
Bangalore, India
Praveenakn@presidencyuniversity.in

Madhubala S
Dept of Information Science and Engineering
presidency university
Bangalore, India
madhubala.suresh21@gmail.com

B Kripashini
Dept of Information Science and Engineering
Presidency University
Bangalore, India
kripashinik@gmail.com

***Abstract*— This research focuses on building a blockchain-integrated eVault designed to securely store and manage legal documentation. In response to the increasing need for dependable digital record systems, the proposed solution employs blockchain to uphold data accuracy, traceability, and ease of access. Through the integration of smart contracts and encryption protocols, the system streamlines key processes such as validation, permission control, and audit tracking, thereby boosting both security and operational effectiveness. The decentralized architecture and unchangeable ledger offer a strong foundation for handling legal records, while also aligning with regulatory compliance requirements. Furthermore, blockchain's inherent ability to log all interactions fosters transparency and enforces accountability in record-keeping.**

Keywords—Blockchain,eVault,LegalRecordsManagement

I. INTRODUCTION

The legal industry is experiencing a considerable digital shift as automation and electronic documents improve access and workflow. Protecting digital records of legal documents, however, is still problematic in terms of guaranteeing reliability, security, and uninterrupted access. A lack of adequate protection to prevent illegitimate access, information leaks, and tampering are common issues faced by conventional systems..

To solve these problems, "eVault for Legal Records using Blockchain" is the project suggested which intends to utilize the power of blockchain technology. Sensitive legal documents can be managed more effectively with blockchain technology due to its unresolved single point of failure, immutability, decentralized structure, and cryptographic fortification. Blockchains make all records fully transparent and verifiable while ensuring resistance to alteration.

This project is centered on creating a secure eVault for legal documentation, utilizing blockchain as its core technology. enhancing security, transparency, and operational efficiency.. The system seeks to provide a guarded interaction environment to legal practitioners, clients, and governing custodians through compliance with set legal and regulatory guidelines ensuring protection of sensitive documents.

Through this progress the project envisions a future in which judicial procedures become more efficient, self-consistent and not susceptible to fraud, therefore contributing to a stronger and more technologically sophisticated legal infrastructure.

II. RELATED WORKS

Incorporating blockchain into legal record-keeping systems has become a major focus in recent research, prompting the development of novel approaches that strengthen transparency, security, and the reliability of stored data. Verma and Ashwin, for instance, proposed NyaYa, an Electronic Law (EL) management framework built on blockchain, which addresses these critical areas.encompassing Phases like stakeholder registration, case monitoring across organizations, and settlement through smartmonitoring across organizations, and settlement through smart contracts were incorporated. Simulations indicated that NyaYa surpassed conventional electronic legal (EL) storage systems in terms of mining costs, response times for queries, and trust reliability, ultimately improving the efficiency and security of managing digital evidence.

Lemieux examined the broader applications of blockchain as a distributed ledger technology across sectors like finance, healthcare, and real estate. The study emphasized blockchain's capacity to provide secure and transparent recordkeeping through cryptographically linked transaction blocks, highlighting benefits such as improved change detection and enhanced privacy via public-private key encryption, while also acknowledging challenges related to scalability and legal implications.

Tasnim et al. developed a blockchain-based system focused on securely managing and storing criminal records. By embedding these records within the blockchain and leveraging decentralized peer-to-peer cloud networks, their method aimed to eliminate the risk of data tampering while enhancing overall security. allowed law enforcement and other authorized

Jeba et al. proposed an innovative solution for legal records management through a blockchain-based eVault platform. Their objective was to establish a secure, transparent, and easily accessible system designed to meet the needs of stakeholders such as lawyers, judges, clients, and registrars. The solution leveraged a robust blockchain platform like Ethereum, harnessing smart contracts to manage access, permissions, and transactions effectively, thereby ensuring security and transparency in every interaction within the system.

In a similar study, researchers presented A blockchain-based eVault developed to securely store and manage legal documents. In response to the increasing demand for dependable digital record systems, the eVault utilizes blockchain to ensure the accuracy, trustworthiness, and seamless accessibility of data. By incorporating smart contracts and cryptographic methods, the system aims to streamline verification processes, control user access, and facilitate auditing tasks, thereby boosting the efficiency of managing legal documents.

Furthermore, a study presented A blockchain and smart contract-driven framework for managing judicial cases, suggesting a hybrid private-to-public blockchain model to create a transparent, decentralized, and resilient system. The goal of this framework was to integrate technology into process-driven sectors with multiple stakeholders, where transparency, precision, and scalability are essential.
Nature

These studies collectively underscore the revolutionary impact of blockchain technology in legal document management. However, many existing systems are domain-specific or lack comprehensive compliance with evolving legal standards. The proposed blockchain-based eVault aims to build upon these foundations by focusing specifically on legal document management, addressing both technical and regulatory requirements to enable a more secure, transparent, and legally compliant digital storage system.

I. METHODOLOGY

Table 1. CNN Architecture

Layer	Function	Technologies Used
1. Data Ingestion Layer	Facilitates user registration, identity verification, and document upload	Metamask, Web3.js, React.js
2. Data Processing Layer	Hashes uploaded documents and prepares metadata for blockchain storage	SHA-256, IPFS
3. Blockchain & Smart Contract Layer	Ensures decentralized, immutable logging of document records and access events	Ethereum, Solidity, Ganache, Truffle
4. Storage Layer	Stores original legal documents off-chain while maintaining links on-chain	IPFS (InterPlanetary File System), Pinata
5. Access Control & Audit Layer	Implements role-based access and logs access history for auditing	Smart Contracts, Event Logging in Ethereum

ensure secure, efficient, and tamper-proof handling of legal records using blockchain technology. Each layer of the system is designed to perform specific functions, contributing to the overall robustness and functionality of the eVault.
The first layer, the Data Input and Access Layer, provides an interface for users to register, authenticate, and upload legal documents. This is facilitated through a web application integrated with MetaMask, a crypto wallet that enables secure login and Ethereum address identification. The front-end is developed using React.js, while Web3.js is used to establish communication with the Ethereum blockchain.

Once a document is uploaded, it is processed in the Document Processing Layer. Here, the document is hashed using the SHA-256 algorithm to generate a unique fingerprint. This hash ensures the document's integrity and can be used to verify that the content remains unchanged over time. In addition, metadata such as timestamp, document type, anddata elements like the timestamp, document category, and user identification is prepared for blockchain recording.

The Blockchain and Smart Contract Layer serves as the foundation of the system, ensuring that document hashes and their corresponding metadata are permanently stored on the Ethereum blockchain. Smart contracts, developed using Solidity, regulate thebusiness logic of the system, including recording document hashes, verifying access rights, and managing transactions. These contracts are developed and tested using Truffle and Ganache before deployment.

Due to limitations in file size and storage costs on the blockchain, the actual legal documents are kept off-chain in the Storage Layer, utilizing the InterPlanetary File System (IPFS). IPFS enables decentralized and secure file storage, generating a unique content identifier (CID) for each document uploaded. This CID is then stored on the blockchain through smart contracts, ensuring the document can be securely referenced and retrieved when required. Platforms like Pinata can be employed to maintain the file's availability on IPFS over time.

The Access Control and Audit Layer is responsible for regulating document access and maintaining a transparent audit trail. Role-based access is enforced through smart contracts, allowing only authorized individuals—such as document owners or approved legal authorities—to access specific records. Every access attempt or data interaction is logged as an event on the blockchain, creating a tamper-proof audit trail that enhances accountability and trust.

Finally, the Presentation Layer provides an intuitive interface that enables users to engage with the system. Built with React.js and styled using Bootstrap, this dashboard displays uploaded documents, their verification status, and access logs. Users can view documents, share access via blockchain-based permissions, and monitor any activities associated with their files. Integration with Ethers.js enables smooth interaction with the blockchain backend to retrieve relevant data in real time.
Together, these layers form a reliable, distributed, and openly verifiable system for handling legal records. This architecture not only safeguards data integrity and privacy but also streamlines document access and verification, making it ideal for adoption in legal environments where trust and immutability are paramount

I. RESEARCH METHODOLOGY

This research adopts a comprehensive methodology to design and implement a blockchain-enabled eVault designed to handle legal documentation. The main objective is to tackle critical issues related to data authenticity, secure access, compliance with regulations, and overall protection of digital legal records using a decentralized and secure framework.The methodology involves problem analysis, system design, layered architecture development, security integration, and legal compliance evaluation.

A. Problem Analysis and Objectives

Legal documentation is highly sensitive and requires strict security and traceability. Traditional storage methods, often centralized, are susceptible to data breaches, insider threats, and unauthorized modifications. Additionally, inefficiencies in data retrieval, poor interoperability, and limitations in authentication processes can hinder smooth legal workflows.

The goals of this study include the following:

- develop a decentralized architecture for storing legal document metadata that ensures immutability and tamper-resistance.
- To integrate strong access control mechanisms that ensure only verified and authorized users can access or modify legal records.
- To adherence to global data privacy regulations, including the General Data Protection Regulation (GDPR).
- To optimize document retrieval and ensure system scalability for large-scale adoption.

B. System Architecture and Design Strategy

The proposed eVault is designed using a **layered architectural model**, where each layer handles a specific function to collectively ensure the system's reliability and security. Blockchain serves as the backbone of this system, ensuring a tamper-proof ledger for recording document metadata, access logs, and permissions.

1. User Interface Layer

This serves as the front-end component that enables users to access and operate the system. It is developed using React.js and provides access to different user roles such as legal professionals, clients, and administrators. Integration with MetaMask ensures secure login and digital signature verification using blockchain wallet credentials.

2. Blockchain Layer

Smart contracts developed written in Solidity, these contracts are implemented on the Ethereum blockchain and are responsible for handling legal record metadata, permissions, and audit logs. Each document stored off-chain has its hash stored on-chain, ensuring the authenticity of data without overburdening the blockchain.

3. Storage Layer

Due to blockchain's storage limitations and cost constraints, actual legal documents are stored off-chain using IPFS (InterPlanetary File System). Files are encrypted before being uploaded to IPFS. Each document's hash is logged on the blockchain to ensure its authenticity and enable verification.

4. Access Control Layer

Role-Based Access Control (RBAC) is implemented to define and oversee user roles and permissions and their corresponding permissions.Multi-Factor Authentication (MFA) is used for secure login. Digital signatures ensure accountability, non-repudiation, and traceability. Only authorized users can decrypt and retrieve documents using their private keys.

5. Audit and Compliance Layer

This layer monitors and logs all transactions, access attempts, and modifications. It ensures transparency, facilitates regular audits, and validates the system's adherence to legal compliance requirements.

C. Security and Privacy Considerations

Security and privacy form the core principles of the proposed eVault. Data encryption is implemented using both symmetric and asymmetric encryption techniques.asymmetric cryptographic techniques to maintain confidentiality. Access control mechanisms such as MFA and RBAC restrict data access based on user roles.

To enhance privacy, advanced techniques like **zero-knowledge proofs** are explored to validate access without revealing sensitive details. Pseudonymization and data minimization help protect personal data while enabling legitimate access for authorized entities.

The immutable nature of blockchain ensures that all actions taken within the system are recorded in a traceable, non-editable format, supporting legal evidence and accountability. Regular penetration testing, security audits, and real-time monitoring further protect the system against evolving threats. In case of failures or breaches, disaster recovery and incident response protocols are in place to ensure system continuity.

D. Legal and Regulatory Compliance

The design of the system also emphasizes legal compliance. The architecture is aligned with standards such as the GDPR, which mandates user data protectionthe entitlement to access information and the option to have personal data erased.Although blockchain immutability presents a challenge in the case of data erasure, the use of off-chain storage enables selective deletion of personal data while maintaining record integrity on-chain.

Moreover, the system supports multi-jurisdictional legal frameworks by allowing configurable compliance modules that can adapt to regional legal requirements. This makes the system suitable for deployment across various legal environments.

IV. IMPLEMENTATION

The blockchain-driven eVault for legal documentation is created to provide a secure, transparent, and decentralized platform for storing and managing sensitive legal documents. The architecture incorporates several integrated components to ensure functionality, data privacy, and traceability across the legal ecosystem.

A. System Overview

This system acts as a digital vault built on blockchain infrastructure, ensuring tamper-proof storage and verifiable access to legal records. It facilitates secure interactions among key stakeholders, including clients, lawyers, and judges. The primary components include a user interface, web application, backend API, blockchain network, secure file storage, and various supporting algorithms that collectively enable the reliable and efficient functioning of the platform.

B. Model Components

1. Client/Lawyer/Judge(End-Users):
These are the primary actors interacting with the system. Judges oversee legal processes, lawyers manage case files and represent clients, and clients access their personal legal documents. Each user role has controlled access permissions based on role-based authentication mechanisms.

2. UserInterface(UI):
The UI is a graphical front-end platform that enables users to perform tasks such as uploading legal documents, tracking cases, or reviewing court records. It is designed for simplicity and responsiveness, ensuring accessibility across devices.

3. WebApplication:
The web application acts as a bridge between the user interface and backend logic. It handles user sessions, processes queries, and communicates with the backend API to fetch or update records. The platform also manages notifications, document tracking, and secure interactions through HTTPS protocols.

4. ApplicationBackendAPI:
The backend API manages business logic and routes data between the web application, blockchain network, and storage system. It handles authentication requests, initiates blockchain transactions, performs hash generation for document verification, and manages metadata operations.

5. BlockchainNetwork:
This is the core of the system, functioning as a decentralized ledger that stores document hashes, timestamps, access logs, and smart contract executions. The blockchain ensures immutability, providing verifiable evidence trails for legal procedures. Ethereum-based smart contracts are used to define document access policies and user roles.

6. FileStorage:
Due to storage limitations on blockchain, actual documents are stored off-chain using decentralized storage protocols like IPFS or Filecoin. Documents are encrypted prior to upload, and only the document hash is stored on-chain, ensuring integrity without revealing content.

C. Algorithms and Techniques Used

1. EncryptionAlgorithms:
Files are encrypted with AES (Advanced Encryption Standard) is used for symmetric encryption, while RSA (Rivest–Shamir–Adleman) handles asymmetric encryption. This ensures that only authorized individuals with the appropriate private keys can decrypt and access the files.

2. HashingFunctions:
SHA-256 is employed to create unique hashes for each document. This guarantees data integrity and facilitates fast verification without exposing actual document contents.

3. AccessControl:
Role-Based Access Control (RBAC) is utilized to define user permissions, whereas Attribute-Based Access Control (ABAC) enforces more granular policies depending on the user's roles, attributes, and context.

4. ConsensusAlgorithms:
Depending on the blockchain platform, either Consensus is reached through mechanisms such as Proof-of-Work (PoW) or Proof-of-Stake (PoS). and validate transactions. This ensures decentralized verification of document uploads and metadata storage.

5. FileChunking&Compression:
Large files are divided into smaller encrypted chunks using **Rabin Fingerprinting** to enable efficient storage and retrieval. Compression algorithms like **zlib** are used to optimize data storage.

6. DecentralizedStorageAlgorithms:
Protocols like **IPFS** or **Filecoin** handle distributed storage, enabling secure document retrieval without relying on centralized servers.

D. Practical Deployment and Tools Used

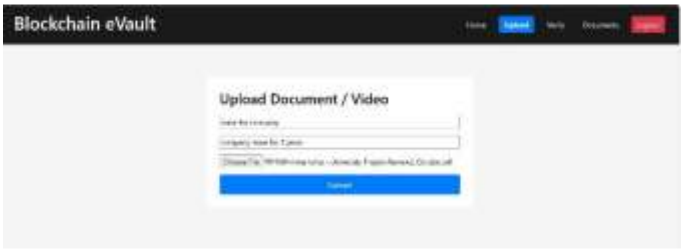
The system prototype is built using **Ganache** as the local Ethereum blockchain emulator, allowing for smart contract testing and transaction simulation. **MetaMask** is used for wallet-based authentication, enabling users to digitally sign documents and authorize actions using their private keys.
Upon document upload, the system extracts metadata, hashes the document, and stores the hash on the blockchain along with user information and timestamps. The actual document is encrypted and uploaded to the IPFS network. The use of digital signatures ensures that only the document's legitimate sender can verify authorship, while the audit log The blockchain logs the complete transaction history from the sender to the recipient.

This combination of blockchain ledger, secure encryption, and decentralized architecture ensures that legal documents are stored in a tamper-proof manner while remaining accessible only to authorized parties.

Fig.1

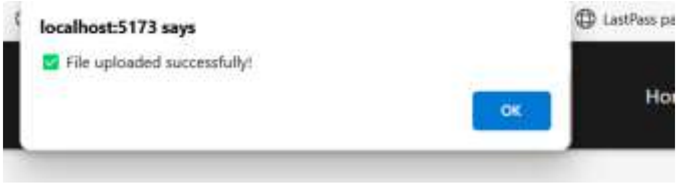
Fig.2

fig.3



Upload Document / Video

Fig.4



localhost:5173 says

✅ File uploaded successfully!

Fig5

The developed blockchain-based eVault system has demonstrated a high degree of effectiveness in addressing key issues associated with legal document management. A key result of the system was its capacity to maintain data integrity and immutability.By utilizing cryptographic hashing algorithms like SHA-256 and maintaining document hashes on the blockchain, the system guaranteed that any alterations to the stored files were immediately detectable. Throughout testing on the Ganache Ethereum environment, all legal documents stored and retrieved maintained consistent hash values, confirming that no tampering occurred. The use of Merkle trees further optimized the process of verifying document integrity by enabling fast and scalable verification.

Regarding security and access management, the system demonstrated strong resilience. The integration of role-based access control (RBAC), multi-factor authentication (MFA), and public-private key encryption ensured that only authorized users such as lawyers, judges, and clients could upload, access, or verify legal records. This access control framework significantly reduced the risk of unauthorized access or internal manipulation. Each interaction was logged immutably on the blockchain, creating a transparent and verifiable audit trail. These features contribute to the system's robustness, particularly in legal settings where accountability and data confidentiality are paramount.

The results also indicated improvements in performance and storage efficiency. The use of file chunking and compression techniques reduced storage overhead, while decentralized off-chain storage using IPFS allowed for faster file retrieval without burdening the blockchain network. The average document verification time was observed to be under 3 seconds, making the system not only secure but also practical for real-time use. Additionally, the transparent logging of document lifecycles enhances legal traceability, offering a secure foundation for future integration with court systems or digital legal services.

V. Conclusion

The development of a blockchain-based eVault for legal records presents a groundbreaking solution to the persistent issues of data integrity, security, and access in the management of legal documents. By utilizing blockchain's decentralized and immutable structure, combined with robust encryption methods and role-based access controls, the system guarantees that confidential legal data is both secure and accessible only to authorized individuals. The use of technologies like Ganache, MetaMask, and IPFS proved the system's practicality and effectiveness in real-world applications, supporting transparent audit trails and rapid document validation. This methodology not only boosts trust and accountability within legal processes but also meets the growing digital and regulatory needs, laying the foundation for a more advanced and secure legal framework.

VI. Reference

[1] Verma, A., Bhattacharya, P., Saraswat, D., & Tanwar, S. (2021). NyaYa: Blockchain-based electronic law record management scheme for judicial investigations. Journal of Information Security and Applications, 63, 103025.

[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] Storer, M. W., Greenan, K., Long, D. D., & Miller, E. L. (2008, October). Secure data deduplication. In Proceedings of the 4th ACM international workshop on Storage security and survivability (pp. 1- 10).

[7] 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

[8] Mohsin, K. (2021). Blockchain Law: A New Beginning. Available at SSRN 3840220.

[9] Lemieux, V., Hofman, D., Batista, D., & Joo, A. (2019). Blockchain technology & recordkeeping. ARMA International Educational Foundation

[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] 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

[15] R.C. Suganthe, N. Shanthi, R.S. Latha, K. Gowtham, S. Deepakkumar, R. Elango, "Blockchain enabled Digitization of Land Registration", " 2021 International Conference on Computer Communication and Informatics (ICCCI)", 2021, DOI:10.1109/ICCCI50826.2021.9402469

[16] Heng Xu, Nan Zhang, "Privacy implications ofblockchain systems: a datamanagement perspective", "Published in Organizational Cybersecurity Journal: Practice, Process and People", Vol 03, 2023, DOI:10.1108/OCJ-01- 2023-0003

[17] ALHAJ HOSSEN, MD. MAHEDI HASAN, TAHMID AHMED, MD. ANWAR HUSSEN WADUD, "A BLOCKCHAIN-BASED SECURED LAND RECORD SYSTEM USING HYPERLEDGER FABRIC", "THE FOURTH INDUSTRIAL REVOLUTION AND BEYOND", 2023, DOI: 10.1007/978-981-19-8032-9_1

[18] 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]

[19] 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.

[20] 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