International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 06 | June - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Designing a Blockchain-Driven Evault System for Legal Document Preservation

Ms.PUSHPALATHA M
Assistant Professor
Dept of Computer Science and Engineering
Presidency University
pushpalatha.m@presidencyuniversity.in

GANASHREE M
Dept of Information Science and Engineering Presidency University
Bangalore, India
maheshganashree@gmail.com

KARAN R
Department of Information Science and Engineering
Presidency University
Bangalore, India
rkaran2825@gmail.com

Abstract— This research is focused on constructing a blockchain-powered eVault system that is programmed to securely archive and manage legal documents. Driven by increasing demand for high-quality digital storage solutions, the system utilizes blockchain technology to facilitate the authenticity, integrity, and controlled access of information. Coupled with the use of smart contracts and cryptography methods, it automates features like verification, access control, and audit logging, thus increasing security and efficiency. Its tamper-resistant ledger and decentralized structure give a robust foundation for safe management and sharing of legal information as well as compliance standards. The native audit capabilities of blockchain also provide a transparent and traceable history of document activity, which enhances trust and regulatory compliance.

Keywords—Blockchain,eVault,LegalRecordsManagement

I. INTRODUCTION

The legal industry is experiencing a major shift as automation and electronic documents improve accessibility and efficiency. However, the protection of digital legal documents is still difficult when it comes to reliability, security, and uniform access. Typical issues faced by conventional systems are inadequate protection against unauthorized access, data loss, and tampering

To address these issues, "eVault for Legal Records using Blockchain" is the proposed project which aims to harness the potential of blockchain technology. Blockchain technology can be used more efficiently to deal with sensitive legal documents because of its unresolved single point of failure, immutability, decentralized nature, and cryptographic security. Blockchains ensure complete transparency and verifiability of all records and provide immunity against tampering.

The objective of this project is to create a blockchain-based eVault for legal documents, promoting security, transparency, and efficiency in operation. The system aims to offer a secured environment for interaction to legal professionals, clients, and regulatory custodians through adherence to established legal and regulatory standards providing protection for sensitive documents.

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

II. RELATED WORKS

The incorporation of blockchain technology in legal and record management systems has gained significant attention, leading to a variety of innovative solutions for enhancing data integrity, security, and transparency. In their paper, Verma and Ashwin introduced NyaYa, an EL management system based on blockchain that encompasses phases of stakeholder registration, inter-organizational monitoring of cases, and resolution by smart contracts. Simulations demonstrated that NyaYa performed better than conventional electronic legal (EL) storage systems in terms of mining costs, response times to queries, and trust, ultimately improving the security and efficiency of digital evidence handling.

Lemieux reviewed the wider uses of blockchain as a distributed ledger technology in areas such as finance, healthcare, and real estate. The research highlighted blockchain's ability to offer secure and transparent recording through cryptographically chained transaction blocks, with advantages including enhanced change detection and increased privacy through public-private key encryption, along with some mention of weaknesses regarding scalability and legal considerations

TTasnim and their team created a blockchain method for secure storage and management of criminal records. By integrating records into blockchain technology and using peerto-peer cloud

aimed to end data tampering and enhance security. Encryption, blockchain, and digital signatures facilitated law enforcement and authorized users to deal with and recover documents in an effective way, while ensuring their authenticity and integrity.

Jeba et al. presented a revolutionary method for handling legal documents through a blockchain-based eVault platform. They aimed at creating a safe, transparent, and accessible place for the players such as lawyers, judges, clients, and registrars. The solution had a robust blockchain platform like Ethereum, using smart contracts to

handle access, permission, and transactions in an efficient manner, thereby ensuring security and transparency in every interaction within the system.

In a companion study, researchers proposed a blockchain-based eVault for the secure storage and management of legal documents. Meeting the growing need for reliable digital record-keeping solutions, the proposed eVault used blockchain technology to guarantee data authenticity, integrity, and easy access. Through the use of smart contracts and cryptographic techniques, the system sought to automate verification, access control, and auditing processes, thereby improving the efficiency of legal document management.

Also, studies proposed a blockchain and smart contract-based framework for handling judicial cases, proposing a transition from private to public blockchain to develop an open, decentralized, and robust system. This framework aimed to incorporate technology into industries with process focus and multiple stakeholders, which need transparency, accuracy, and scalability.

These research results collectively identify the revolutionary potential of blockchain technology in legal document management. But most current systems are domain-specific or do not have complete compliance with changing legal standards. The suggested blockchain-based eVault intends to improve upon these by being specifically designed for legal document management, addressing both technical and regulatory needs to facilitate 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

The system adopted in this proposed project has a layered architectural system in place to facilitate secure, efficient, and tamper-proof management of legal documents by means of blockchain technology. Each layer is assigned roles of specific function, which helps in the overall solidity and operability of the eVault.

The Data Input and Access Layer is the initial layer, offering a clear interface through which users can register, log in, and upload lawful documents. This is supported by the use of a web application in collaboration with MetaMask, a cryptocurrency wallet that supports safe login as well as Ethereum address identification. React.js is used for developing the front-end while Web3.js is utilized to create contact 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 guarantees the integrity of the document and can be utilized to confirm that the content has not altered over time. Furthermore, metadata including the timestamp, document type, and user ID is readied for recording on the blockchain.

The Blockchain and Smart Contract Layer is fundamental to the system. This layer guarantees that every document hash and its related metadata are permanently stored on the Ethereum blockchain. Smart contracts, created in Solidity, control the operational logic of the system, encompassing the recording of document hashes, verification of access permissions, and handling of transactions. These contracts are crafted and evaluated using Truffle and Ganache prior to being deployed.

Given the limitations in both size and cost associated with directly storing files on the blockchain, the actual legal documents are kept off-chain in the Storage Layer by utilizing the InterPlanetary File System (IPFS). IPFS offers a decentralized and secure method for file storage, generating a unique content identifier (CID) for every document uploaded. This CID is subsequently recorded on the blockchain through smart contracts, enabling secure referencing and retrieval of the file as needed. Services such as Pin.

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. Each attempt to access or interact with data is recorded as an event on the blockchain, resulting in an immutable audit trail that increases accountability and trust.

Ultimately, the Presentation Layer provides an intuitive dashboard for engaging with the system. Developed with React.js and styled with Bootstrap, this dashboard showcases uploaded documents, their verification statuses, and access logs. Users can examine documents, share access through blockchain-based permissions, and track any actions related to their files. The integration with Ethers.js facilitates seamless interaction with the blockchain backend to obtain pertinent data in real time..

Combined, these layers create a reliable, distributed, and clear structure for handling legal documents.. 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 utilizes a comprehensive approach to design and implement a blockchain-based eVault system for the management of legal documents. The prime goal is to address pertinent concerns on the integrity, accessibility, security, and compliance with regulations of digital legal files through a secure decentralized approach. The methodology entails problem analysis, system design, developing a layer-based architecture, incorporating security features, and compliance with legal requirements.

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 primary goals of this research include:

- Creating a decentralized framework for the storage of legal document metadata that guarantees immutability and resistance to tampering.
- To integrate strong access control mechanisms that ensure only verified and authorized users can access or modify legal records.
- To ensure adherence to global data protection regulations like 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 is the front-end interface that allows users to engage with the system. It is developed using React.js and offers access for various user roles, including legal professionals, clients, and administrators. Integration with MetaMask guarantees secure login and the verification of digital signatures through blockchain wallet credentials.

2. Blockchain Layer

Smart contracts written in Solidity are launched on the Ethereum blockchain. These contracts handle metadata related to legal records, along with 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). Documents are encrypted prior to being uploaded to IPFS. The hash for each file is documented on the blockchain to ensure validation.

4. Access Control Layer

Role-Based Access Control (RBAC) is implemented to define and regulate user roles along with their associated 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 system's design also prioritizes adherence to legal regulations. The architecture complies with standards like the GDPR, which requires protection of user data, access rights, and the right to be forgotten. Although blockchain immutability presents a challenge in the case of data erasure, the use of offchain 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 eVault system, built on blockchain technology for legal records, aims to provide a secure, transparent, and decentralized method for the storage and management of 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

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 secured using AES (Advanced Encryption Standard) for symmetric encryption and RSA (Rivest–Shamir–Adleman) for asymmetric encryption. This ensures that only users with the appropriate private keys are able to 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) systems are used to define user permissions, whereas Attribute-Based Access Control (ABAC) guarantees precise policy implementation that considers user roles, attributes, and context.

4.ConsensusAlgorithms:

Depending on the blockchain platform, consensus is achieved and transactions are validated using either Proof-of-Work (PoW) or Proof-of-Stake (PoS). 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 walletbased 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 application of digital signatures guarantees that only the rightful sender of the document can confirm its authorship, while the blockchain's audit log captures 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

Fig.4

Fig5

The developed blockchain-based eVault system has demonstrated a high degree of effectiveness in addressing key issues associated with legal document management. One of the key results was the system's capacity to maintain data integrity and prevent alteration. 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. Merkle trees enhanced the method of confirming document integrity by allowing for efficient and scalable validation.

Regarding security and access management, the system demonstrated remarkable resilience. The integration of role-based access control (RBAC), multi-factor authentication (MFA), and public-private key encryption guaranteed that only permitted users, including lawyers, judges, and clients, were able to upload, access, or verify legal documents. 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

Implementing a blockchain-based eVault for legal records provides a revolutionary answer to the persistent issues of data integrity, security, and access in the management of legal documents. By leveraging the decentralized and tamper-resistant nature of blockchain, combined with robust encryption methods and rolebased access controls, the system guarantees that sensitive legal information stays secure and can only be accessed by authorized personnel. Utilizing tools like Ganache, MetaMask, and IPFS showcased the system's practicality and effectiveness in a realworld context, allowing for transparent audit trails and rapid document verification. This method not only improves trust and accountability within legal processes but also aligns with the shifting digital and regulatory requirements, setting the stage for a smarter and more 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

[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