

International Journal of Engineering Research and Science & Technology



www.ijerst.org

ISSN : 2319-5991

Vol. 22 No. 2(3) (2026)



ijerst.editor@gmail.com
editor@ijerst.com

Research Paper

Leveraging Smart Contracts for Automated and Secure Legal Document Management

P. Anupama¹, Akhilandeshwari¹, Shama Priyanka¹, Putta Srihari¹, Moturi Sai Ram¹

¹Department of Computer Science and Engineering, ¹Sree Dattha Institute of Engineering and Science, Nagarjuna Sagar Road, Sheriguda, Ibrahimpatnam, Rangareddy Dist, 501510, Telangana, India.

ABSTRACT

The increasing digitization of administrative and personal records has created a strong demand for systems that guarantee secure storage, data integrity, and reliable verification of sensitive documents. Conventional document management solutions typically depend on centralized servers, where files are vulnerable to unauthorized modification, loss, or deletion without clear traceability. This centralized model reduces trust, increases exposure to cyber threats, and often requires time-consuming manual verification to confirm document ownership and authenticity. Consequently, individuals and organizations encounter challenges such as document forgery, inconsistent records, unauthorized access, and delays in retrieval, emphasizing the necessity for a more secure and tamper-resistant solution. In traditional vault systems, documents are usually stored as basic files with minimal metadata, lacking cryptographic protection and comprehensive audit mechanisms. Due to the absence of immutability, detecting alterations in stored documents becomes difficult. Additionally, reliance on manual validation processes introduces inefficiencies and a higher likelihood of errors. These drawbacks make centralized systems unsuitable for handling critical records such as legal documents, identity credentials, certificates, and criminal records, which require strict integrity and security measures. To overcome these limitations, the proposed solution combines blockchain technology with a Django-based web platform to establish a decentralized and tamper-proof digital vault. Key document metadata, including ownership information, descriptions, timestamps, and file references, is recorded on the blockchain using smart contracts, ensuring permanent and unalterable entries. The actual files are securely stored on the server, while Web3 enables seamless communication between the application and the blockchain network. Functionalities such as document upload, search, verification, and secure access support complete transparency and data integrity. This framework significantly strengthens trust by preventing unauthorized modifications and maintaining a permanent, verifiable history of all stored documents. By integrating blockchain immutability with an intuitive web interface, the system delivers a secure, scalable, and future-oriented solution suitable for government agencies, legal bodies, and organizations managing sensitive records.

Keywords: Blockchain, Digital Vault, Document Management System, Decentralized Storage, Smart Contracts, Cryptographic Security.

1. INTRODUCTION

Records act as documented proof of business operations, activities, and transactions, making them valuable information assets. For records to fulfill this role effectively, they must be authoritative, meaning they should be authentic, dependable, complete, unchanged, and accessible when needed. A records system can be defined as an information system that captures, organizes, manages, and enables access to records over time. An effective records system supports the creation, proper utilization, and long-term preservation of reliable records.

Every organization typically maintains at least one records system, and often multiple systems to handle different types of information. These systems include not only technical components such as software

applications but also non-technical aspects like organizational policies, established procedures, and the involvement of stakeholders.



Fig. 1: Secure legal document management.

Distributed ledger technologies (DLT), including blockchains defined by the International Standards Organization with the input of over 300 international experts from 50 countries as a ‘distributed ledger with confirmed blocks organized in an append-only sequential chain using cryptographic links’, with a distributed ledger being a ‘ledger that is shared across a set of DLT nodes and synchronized between the DLT nodes using a consensus mechanism’ combine the use of cryptography and distributed networks to achieve a novel form of records system designed for tamper-resistance and immutability. Over the past several years, these capabilities have made DLT increasingly popular as a general-purpose technology used for recordkeeping in a variety of sectors and industry domains. Indeed, developers were already experimenting with this possibility in the early days of DLT, as evidenced by a number of what a former lead maintainer of Bitcoin’s codebase is reported to have referred to as ‘bizarre hacks’ to embed content into the Bitcoin blockchain. Observers of these early developments took note, however, recognizing the potential of the underlying ledger to meet the need for ‘a trustworthy record, something vital for transactions of every sort’.

2. LITERATURE SURVEY

Ranjith, et al. [1] Reviewed the decentralized management of legal documents using blockchain technology, offering a transformative solution to enhance security, integrity, and transparency. Unlike traditional centralized systems that are susceptible to data breaches, unauthorized modifications, and loss due to corruption or mismanagement, the proposed framework eliminates reliance on intermediaries and prevents inefficiencies, tampering, and disputes. While digital documentation was historically an advancement, it still lacked the robustness needed to address escalating challenges in data integrity and security gaps that the proposed blockchain-driven approach effectively overcomes. Cristina Regueiro et, al. [2] presented a risk assessment of evidence in the certification domain to identify the main security risks. To mitigate these risks, it also proposes an adaptation of an existing Blockchain-based audit trail system to create an evidence trustworthiness system enhancing security and usability. This system covers specific additional requirements from auditors: evidence confidentiality and integrity verification automation. The system has been validated with cloud service providers to increase the security of evidence for a cybersecurity certification process. However, it can be also extended to other certification domains.

Androulaki, et al. [3] Introduced Hyperledger Fabric, a blockchain framework designed for enterprise environments. Hyperledger Fabric is a permissioned blockchain that offers modularity, scalability, and flexibility for developing distributed ledger applications. It provides a detailed explanation of its architecture, consensus mechanisms, and how it enhances privacy and security for enterprise applications. This is particularly relevant to the proposed project as it can be adapted for securing legal

documents within a private and permissioned environment. Essaid, et al. [4] Examined the application of blockchain technology to address these challenges, with a focus on data integrity, access control, and traceability. This paper proposed a blockchain-based framework that leverages decentralized security, smart contracts, and edge computing to mitigate vulnerabilities, including unauthorized access and data manipulation. Malomo, et al. [5] Addressed the critical issue of offsite data recovery and security in the face of cyber-attacks and disasters. Cyber threats, especially related to data storage, have become highly sophisticated and challenging to defend against. Ransomware attacks targeting sensitive data have shown a significant rise, highlighting the need for secure offsite storage solutions. The paper proposes a Blockchain enabled federated cloud computing framework that offers efficient, private, and secure offsite storage for digital assets. By leveraging blockchain technology and implementing strict access controls, the framework aims to enhance data security, prevent breaches, and outperform traditional approaches in terms of efficiency and effectiveness. Macrinici, et al. [6] Conducted a systematic study of smart contracts and their applications in blockchain technology. They explore the use of smart contracts for automating processes across different sectors, such as law, finance, and healthcare. This is highly relevant for the project, as smart contracts can automate the validation, approval, and access control of legal documents, ensuring that their integrity is maintained without human intervention.

Li, et al. [7] Provided a comprehensive review of blockchain-based decentralized storage solutions, discussing their architecture, features, and applications in various domains, including legal document management.

Obadah Hammoud, et al. [8] proposed system solves the main challenges of distributed data storage by grouping data into clusters and managing them with a load balancer, while preventing data tempering using a blockchain network. The considered DApps storage methodology easily scales horizontally in terms of distributed file storage and can be deployed on cloud computing technologies, while minimizing the required storage space. Jongbeen Han, et al. [9] proposed DDMS encrypts digital documents using a symmetric key and then the key is divided and distributed among multiple users through Shamir's secret sharing scheme. The encrypted documents are stored using the Inter Planetary file system (IPFS), ensuring integrity through content-based addressing. And blockchain-based smart contracts manage access permissions and document retrieval, ensuring access is only granted when a predefined number of participants agree. Nabeel Khan, et al. [10] attempted to review the security of cloud systems when using the blockchain Ethereum, and cloud computing was briefly discussed with its advantages and disadvantages. The idea of a decentralized cloud was briefly demonstrated with blockchain technology. Leonardo Juan Ramirez Lopez, et al. [11] provided a comprehensive and insightful examination of the modern landscape concerning the integration of blockchain and cloud advances, highlighting the current challenges and building a solid foundation for future development. Furthermore, it is very important to increase the integration of blockchain security with the dynamic potential of cloud computing while guaranteeing information integrity and security remain uncompromised

Sheikh Mohammad Idrees, et al. [12] provided insights into the current developments within blockchain technology and explores its ability to revolutionize the multiple industrial application areas such as supply chain industry, Internet of Things (IoT), healthcare, governance, finance and manufacturing. It investigated and provided insights into the security issues and threats related to the blockchain implementations, and also, they proposed possible solutions in detail for enhancing the security of the blockchain for industrial applications along with significant directions for future explorations. Diana Laura Silaghi et al. [13] assessed blockchain-based proposals for academic certificates management, aiming to highlight globally recognized best practices, explore the latest applications, and identified key challenges hindering the widespread adoption of blockchain technology in education. Ozan Zorlu, et al. [14] presented a comprehensive approach and offers a new viewpoint to the field of blockchain

while establishing a fundamental baseline for future improvements in data management systems and addressing the shortcomings of previously proposed existing frameworks to fulfil the complex needs of secure data management. Prudvikrishna, et al. [15] leveraged blockchain's decentralized architecture, enabling stakeholders to securely store, access, and validate documents without reliance on intermediaries. Smart contracts can automate processes such as approvals, access permissions, and notarization, reducing manual errors and delays.

3. PROPOSED SYSTEM

This system establishes a secure, transparent, and tamper-resistant framework for document management by integrating user interaction through Django, blockchain-based immutability, smart contract automation, and structured file storage. The architecture demonstrates the practicality of blockchain for safeguarding sensitive records and ensuring trusted access in digital vault environments.

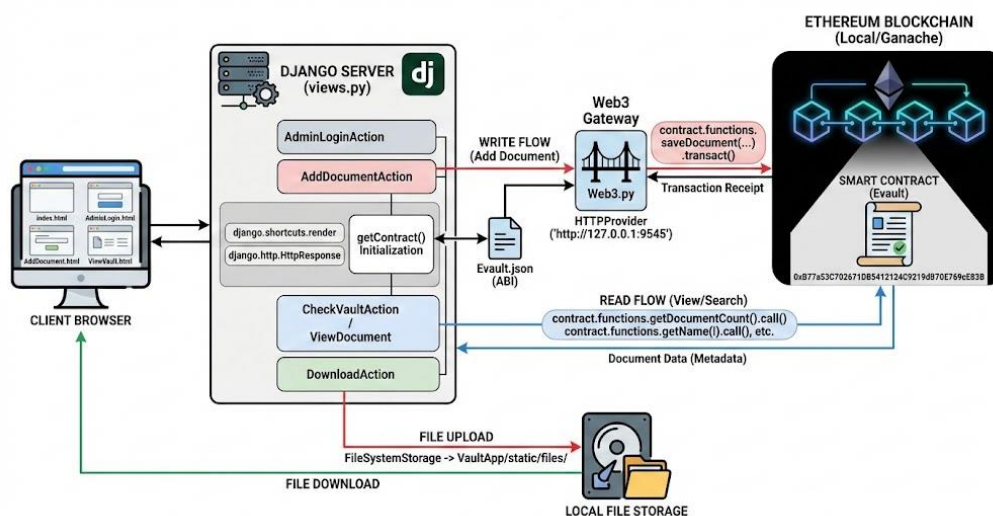


Fig. 2: Proposed system architecture of blockchain-enabled decentralized document vault for secure information management.

Here is the description of the proposed methodology:

- The system tackles major challenges in conventional document management, such as unauthorized modification, centralized storage vulnerabilities, and lack of verifiable audit trails, by utilizing smart contracts and the immutable nature of the blockchain ledger.
- A Django-based web application handles administrator authentication, document submission, vault search operations, and secure file downloads, forming the primary interface between users and the blockchain-backed vault.
- When a document is uploaded, only its metadata such as name, type, description, owner details, address, UID, phone number, criminal record, and timestamp is stored on the blockchain, ensuring integrity and preventing tampering, while the actual file is maintained in local storage to optimize performance.
- The blockchain maintains permanent, traceable records of all uploaded documents, allowing every metadata entry to be verified through its corresponding transaction receipt, providing transparency and enabling reliable auditing.
- During vault access or document viewing, the Django application retrieves the metadata stored on chain using smart contract calls, ensuring that all displayed information originates from the immutable ledger.
- An integrated keyword-based search mechanism enables users to locate documents by comparing input terms with on-chain metadata fields, supporting efficient retrieval without compromising data authenticity.

- Smart contract enforcement ensures that stored metadata cannot be altered or removed, strengthening the security model and protecting sensitive records from internal or external attempts.
- The separation of on-chain metadata and off-chain file storage enhances scalability and reduces overhead while maintaining high security, making the design adaptable to applications requiring reliable document verification.
- The architecture is suitable for secure digital vaults used in identity verification, legal documentation, police records, and administrative archives, offering a robust, traceable, and tamper-proof record management system.

Benefits and Innovation

- Eliminates reliance on centralized storage systems, reducing the risk of unauthorized data manipulation or single-point failures.
- Ensures high integrity and transparency of document metadata by leveraging blockchain verification and immutable smart contract records.
- Streamlines administrative processes through automated contract-based registration and retrieval of document details.
- Builds trust among administrators, users, and organizations by ensuring that all stored records are verifiable, traceable, and securely linked to corresponding file data.

Secure File Handling and Storage

Although metadata resides on the blockchain, actual legal documents are stored securely in the local file system. This algorithm ensures proper handling, naming, writing, and retrieval of uploaded files. The technique ensures safe storage without data corruption, conflicts, or overwriting issues.

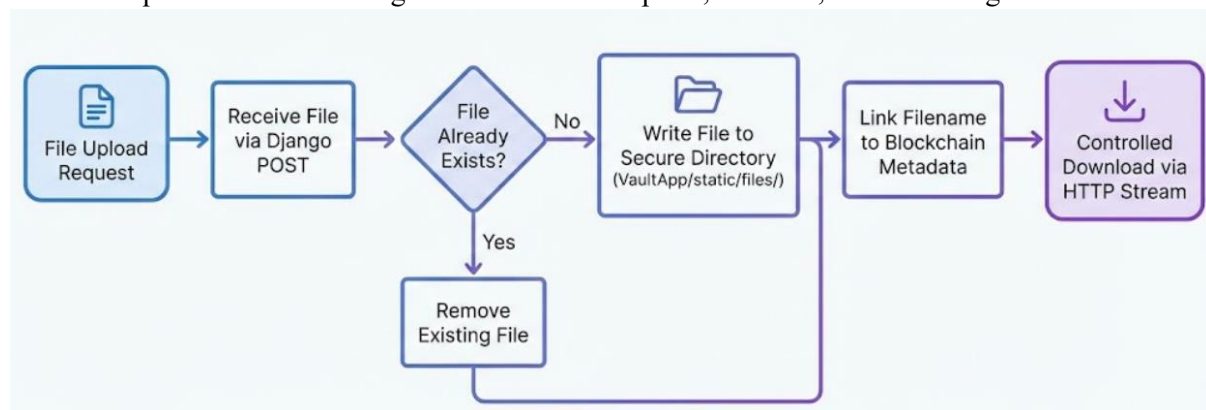


Fig. 3: Secure File Handling and Storage Flow

Internal Workflow

1. The uploaded file is received from the Django POST request.
2. The system checks if the file already exists and removes it if necessary.
3. The file is written to the secure directory VaultApp/static/files/.
4. The filename is linked to the metadata stored on the blockchain.
5. Downloads are handled using a controlled HTTP response stream.

4. RESULTS DESCRIPTION

Fig. 4 depicts the document upload module where the administrator enters legal document details and submits them for secure storage. This interface captures structured metadata such as document identity, ownership details, UID, and verification attributes before processing. Upon submission, the backend validates inputs, stores the document file in the server repository, and invokes the smart contract to record metadata on the blockchain. The workflow ensures synchronized file storage and immutable blockchain logging. This step forms the core data ingestion pipeline of the Evault system, enabling secure and auditable document registration.



Add Legal Document Screen

Document Name

Document Type

Description

Person Name

Address

Phone No

Criminal Record No

UID No

Upload Document

Fig. 4: Add legal document interface of the blockchain-based document vault



Add Legal Document Screen

Document Details Added to Blockchain with below Transaction Details

Fig. 5: Blockchain transaction confirmation after document upload

Fig. 5 illustrates the confirmation stage that occurs after a legal document is successfully submitted to the system. Once the administrator uploads the document, the backend triggers a smart contract call to store the associated metadata on the blockchain. The system then retrieves and displays the blockchain transaction details, confirming immutable record creation. This step verifies successful synchronization between server-side file storage and blockchain ledger entry. The confirmation ensures transparency, traceability, and audit assurance for each uploaded legal document.



Anyone using this device can see downloaded files

unnamed (1).jpg
146 KB • Done

Document Name	Document Type	Description	Document Belongs To	Address	Phone No	Criminal Record	UID No	Upload Date	Download Document Data
house documents	images	these are the legal documents of my house	prasad	sak informatics	100	0	23	2026-01-28 10:58:31.719832	Click Here

Fig. 6: View documents list and secure download interface of the blockchain-based document vault

Fig. 6 presents the document listing module that displays all stored legal documents retrieved from the blockchain-backed vault. Each record shown in the table is populated using metadata fetched from the smart contract, ensuring consistency with the immutable ledger. The interface allows administrators to verify document details such as ownership, UID, and upload timestamp before initiating retrieval. The download action triggers a controlled backend process that securely streams the corresponding file from server storage. This module completes the document lifecycle by enabling transparent verification and authorized access to store legal records.

Fig. 7 illustrates the document search module that enables users to query the blockchain-backed vault using keyword-based input. The entered search string is processed by the backend to match against stored document metadata such as document name, description, owner details, UID, and related attributes. Upon submission, the system validates the input and triggers the vault matching logic to filter relevant records. Matching results are dynamically generated and prepared for structured display. This interface facilitates efficient discovery and verification of stored legal documents without direct access to the underlying blockchain or file system.

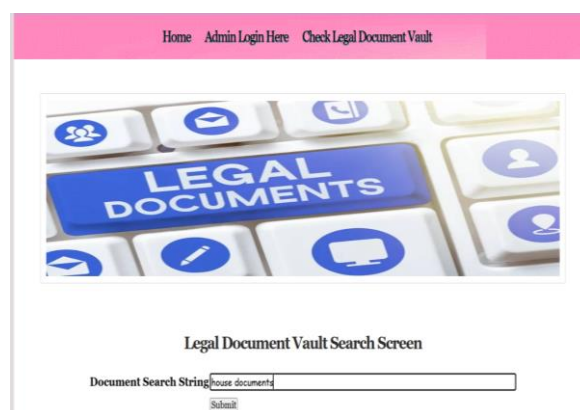


Fig. 7: Legal document vault search interface



Document Name	Document Type	Description	Document Belongs To	Address	Phone No	Criminal Record	UID No	Upload Date
house documents	images	these are the legal documents of my house	prasad	sak informatics	100	0	23	2026-01-28 10:38:31.719832

Fig. 8: Vault search result display of the blockchain-based document management system

Fig. 8 illustrates the result presentation module that displays documents matching the user's search criteria. The table is populated using metadata retrieved from the blockchain, ensuring that all displayed records reflect immutable ledger entries. Each row represents a verified document with ownership, UID, and upload timestamp details. The backend filtering logic ensures only relevant records are shown based on keyword matching. This stage completes the search workflow by providing transparent and verifiable access to stored legal document information.

5. CONCLUSION

This study effectively demonstrates how the integration of blockchain technology with a web-based document management system can provide a secure, tamper-proof, and auditable solution for handling legal records. By utilizing smart contracts, the system ensures that document metadata is permanently recorded and cannot be altered, thereby enhancing trust and maintaining data integrity when compared to traditional centralized approaches. System performance is optimized by combining lightweight server-side storage for files with blockchain-based metadata management, minimizing blockchain load while still ensuring reliable verification. Efficient document access is achieved through keyword-based vault search and organized retrieval methods, eliminating the need for complex indexing techniques. Security is further reinforced through role-based access control and well-defined operational workflows, ensuring both protection and ease of use. Additionally, transaction receipt validation

increases transparency and accountability during the process of document registration. The system's modular design simplifies maintenance and supports scalability, allowing it to handle growing volumes of documents effectively.

REFERENCES

- [1] Dr. Ranjith, K. Tejaswi, K. Sreeja, K. Sneha Reddy. (2024). Decentralizing Legal Documents Management Enhancing Security and Integrity Through Blockchain Technology. International Journal of Communication Networks and Information Security (IJCNIS), 16(5), 660–668. Retrieved from <https://ijcnis.org/index.php/ijcnis/article/view/7871>
- [2] Regueiro, Cristina & Seco Aguirre, Iñaki & Gutierrez-Aguero, Ivan & Urkizu, Borja & Mansell, Jason. (2021). A Blockchain-Based Audit Trail Mechanism: Design and Implementation. Algorithms. <https://doi.org/14.341.10.3390/a14120341>.
- [3] Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., ... & Muralidharan, S. (2018). Hyperledger fabric: a distributed operating system for permissioned blockchains. Proceedings of the Thirteenth EuroSys Conference.
- [4] Essaid, M.; Ju, H. Blockchain Solutions for Enhancing Security and Privacy in Industrial IoT. Appl. Sci. 2025, 15, 6835. <https://doi.org/10.3390/app15126835>
- [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] Macrinici, D., Cartoceanu, C., and Gao, S. (2018). Smart contract applications within blockchain technology: A systematic mapping study. Telematics and Informatics, 35(8), 2337-2354.
- [7] Li, M., Kshetri, N., & Vo, H. D. (2023). Decentralized Storage Solutions: A Review of BlockchainBased Systems.
- [8] Hammoud, O.; Tarkhanov, I.; Kosmarski, A. An Architecture for Distributed Electronic Documents Storage in Decentralized Blockchain B2B Applications. Computers 2021, 10, 142. <https://doi.org/10.3390/computers10110142>
- [9] Jongbeen Han, Yongseok Son, Design and implementation of a decentralized document management system, Expert Systems with Applications, Volume 262, 2025, 125516, ISSN 0957-4174, <https://doi.org/10.1016/j.eswa.2024.125516>.
- [10] Khan, N.; Aljoaey, H.; Tabassum, M.; Farzamnina, A.; Sharma, T.; Tung, Y.H. Proposed Model for Secured Data Storage in Decentralized Cloud by Blockchain Ethereum. Electronics 2022, 11, 3686. <https://doi.org/10.3390/electronics11223686>
- [11] Lopez, L.J.R.; Millan Mayorga, D.; Martinez Poveda, L.H.; Amaya, A.F.C.; Rojas Reales, W. Hybrid Architectures Used in the Protection of Large Healthcare Records Based on Cloud and Blockchain Integration: A Review. Computers 2024, 13, 152. <https://doi.org/10.3390/computers13060152>
- [12] Idrees, S.M.; Nowostawski, M.; Jameel, R.; Mourya, A.K. Security Aspects of Blockchain Technology Intended for Industrial Applications. Electronics 2021, 10, 951. <https://doi.org/10.3390/electronics10080951>
- [13] Silaghi, D.L.; Popescu, D.E. A Systematic Review of Blockchain-Based Initiatives in Comparison to Best Practices Used in Higher Education Institutions. Computers 2025, 14, 141. <https://doi.org/10.3390/computers14040141>
- [14] Zorlu, O., Ozsoy, A.: A blockchain-based secure framework for data management. IET Commun. 18, 628–653 (2024). <https://doi.org/10.1049/cmu2.12781>
- [15] P. Prudvikrishna, Tejavath Divya, Erroju Rajesh, Eluri Shravani, Mohammed Faeeludin, (2025). blockchain-powered legal document management for enhanced integrity and trust. International Journal of Communication Networks and Information Security (IJCNIS), 17(3), 714–720. Retrieved from DOI: <https://doi.org/10.48047/IJCNIS.17.3.714-720>