Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

Legal eVault: Decentralized Legal Document Storage and Access Framework using Blockchain

Shital Dinde[1], Suresh Shirgave[2]

[1]Department of Technology, Shivaji University, Kolhapur, India,
[2]DKTE's College of Engineering and Textile, Ichalkaranji, India
Email: shitalhdinde@gmail.com

The legal sector is notorious for its vast paperwork, posing significant challenges in storage, organisation, accessibility, and management of sensitive documents. Legal firms face immense pressure to efficiently maintain and secure confidential documents over time. Blockchain technology presents a promising solution to these issues. By utilizing a decentralised ledger, it removes the necessity for a central authority, ensuring that documents stay accessible even if conventional servers go offline. Blockchain secures information through encryption and hashing, safeguarding data integrity and confidentiality. The Legal eVault utilizes a permissioned blockchain to securely manage document metadata while storing actual documents off-chain, enhancing storage efficiency and privacy. Role-Based Access and Security model (RBAS) mechanism is implemented to allow document access to only authorized personnel, ensuring confidentiality and compliance. This framework addresses critical concerns in legal document management by providing a transparent, auditable, and tamper-resistant system. By reducing reliance on intermediaries, blockchain enhances trust in legal transactions and improves overall efficiency in document handling.

Keywords: Blockchain, Distributed System, Transparency, Smart Contract, Document Management System (DMS), Role-Based Access (RBA).

1. Introduction

The legal industry is experiencing a profound transformation in the digital era, with electronic documents and records becoming increasingly central to its operations. This shift has brought about significant improvements in efficiency and accessibility of vital legal information. However, it has also introduced new challenges in maintaining the integrity and security of these digital records.

Current storage solutions for legal documents often struggle to meet the stringent security requirements necessary for protecting sensitive information. Many existing systems lack the robust safeguards needed to prevent unauthorized access, tampering, or loss of critical legal data. This vulnerability poses significant risks to law firms, courts, and their clients.

Moreover, as the volume of digital legal documents continues to grow, traditional storage methods are proving inadequate in terms of organization, retrieval, and long-term preservation. The legal sector requires a system that not only secures data but also allows for quick and efficient access to specific documents when needed.

These shortcomings in current document management practices underscore the pressing need for an innovative approach to legal record-keeping. The ideal solution would combine cutting-edge security measures with user-friendly accessibility, ensuring that legal professionals can confidently store and retrieve sensitive information without compromising its integrity.

As the legal field continues to digitize, addressing these challenges becomes increasingly urgent. The development of a secure, efficient, and reliable system for managing electronic legal documents is crucial for the continued evolution and effectiveness of the legal profession in the digital age.

Legal documents, such as power of attorney, agreements, case papers, and case studies, often contain sensitive and highly confidential information. Losing an in-process document could result in a significant setback. Moreover, these documents need to be securely maintained for extended periods, such as 10, 20 years, or even a lifetime. This responsibility falls not only on law firms but also on the legal departments of various organizations, which act as custodians of critical paperwork essential for the firm's operations. Ensuring the longevity and security of these documents is crucial. While physical copies with signatures may be the valid versions, they are inherently challenging to preserve over time.

Document Management Systems (DMS) were built to enhance and speed up the digitization of paper-based information. This software helps businesses store, manage, access, share, collaborate and track information on their systems. This helps create a single source of information and reduces the time and energy spent on managing, storing, or finding paper-based documentation. But these solutions are not without their limitations. Their biggest drawback is that such solutions offer centralized data storage to businesses, making it infinitely easier for malicious attackers to steal or forge sensitive and confidential information. A centralized system also makes it difficult to access information if there's some issue with the central server.

To ensure the longevity of documents, creating electronic copies is the most viable solution, as they have a longer lifespan. Properly stored electronic documents are also easier to retrieve, significantly reducing the time spent searching for a specific document or section. Additionally, digitization enhances security through advanced encryption tools and layers of protection that comply with regulatory standards.

The management of legal documentation has long been plagued by significant challenges in security and operational efficiency. Traditional document storage systems frequently expose critical legal records to risks of unauthorized access, manipulation, and potential data breaches. To address these fundamental issues, an innovative approach emerges: utilizing blockchain technology as a transformative solution for legal document management.

Blockchain technology, originally pioneered through cryptocurrencies like Bitcoin, presents a compelling architectural framework for secure information storage. Its decentralized nature offers multiple advantages for legal document preservation. By distributing document

verification across a network of authenticated nodes, blockchain creates an environment where tampering becomes exponentially difficult, and document integrity remains paramount.

This initiative seeks to redefine the management of legal records by enhancing their security, transparency, and efficiency while ensuring compliance with stringent legal and regulatory standards. By establishing a digital eVault for legal records on a blockchain, the project aims to establish a future where legal professionals, clients, and authorities can rely on an advanced system to safeguard the integrity of legal documents and streamline legal processes.

A pioneering digital infrastructure aims to revolutionize legal record management through cutting-edge technological solutions. By leveraging advanced distributed ledger technologies, this innovative platform establishes a comprehensive system that prioritizes document security, accessibility, and verifiability.

The core design centers on creating an unalterable digital repository where legal documents can be stored and managed with unprecedented levels of protection. Key features include robust encryption, decentralized storage, and granular access controls that prevent unauthorized modifications or breaches. This approach ensures that every legal document maintains its original integrity while providing authorized stakeholders with efficient, secure access.

Legal professionals and clients will benefit from a streamlined system that transforms traditional record-keeping practices. The platform's architecture allows for precise document tracking, instant verification, and seamless information sharing—all while maintaining strict compliance with contemporary data protection frameworks and industry regulatory standards.

A. Blockchain Technology

Blockchain technology is decentralized digital ledger technology that represents a groundbreaking approach to managing and verifying information across interconnected computer networks. This system creates a sequential, tamper-resistant record where digital transactions are grouped into interconnected segments. Each segment is cryptographically authenticated and permanently linked to the previous ones, ensuring an immutable and transparent historical trail of data exchanges.

The key innovations of this technology include its distributed nature, which eliminates the need for a central authority, and its robust security mechanisms that make unauthorized modifications extremely difficult. By design, the system maintains a comprehensive and verifiable log of interactions, with each new data entry building upon the cryptographic foundations of its predecessors.

The key features of blockchain include:

- Decentralization: No single authority controls the entire network.
- Transparency: All participants can view the transaction history.
- Security: Cryptographic techniques protect data integrity.
- Immutability: Once recorded, data is extremely difficult to change.

Decentralized ledger technologies like blockchain have the potential to revolutionize traditional transaction and record-keeping systems by removing centralized intermediaries. This innovative approach can significantly reduce operational costs and enhance process efficiency across multiple sectors.

The technology's versatility extends far beyond digital currencies, finding practical applications in diverse fields such as automated contract execution, transparent supply chain tracking, and robust digital identity management. By distributing data across a network of computers, blockchain creates a transparent, tamper-resistant system of record-keeping.

The blockchain's expansion occurs through a dynamic process of block validation and addition[6][15] as given figure 1, where network participants collaborate to authenticate and integrate new transaction records. Complex consensus mechanisms and distributed peer-to-peer networking architectures work in tandem to maintain the system's integrity, security, and continuous operational reliability.

Here is the detail breakdown of its key components and concepts:

1. Decentralization: The decentralized structure of blockchain technology is one of its defining characteristics. In this system, control and information are distributed across multiple computers or nodes in a network, rather than being managed by a single central entity. This approach offers several advantages such as shared responsibility, increased reliability, reduced vulnerability, Enhanced data integrity. This decentralized architecture contributes significantly to the blockchain's robustness and security, making it resistant to many traditional forms of data manipulation or system failure

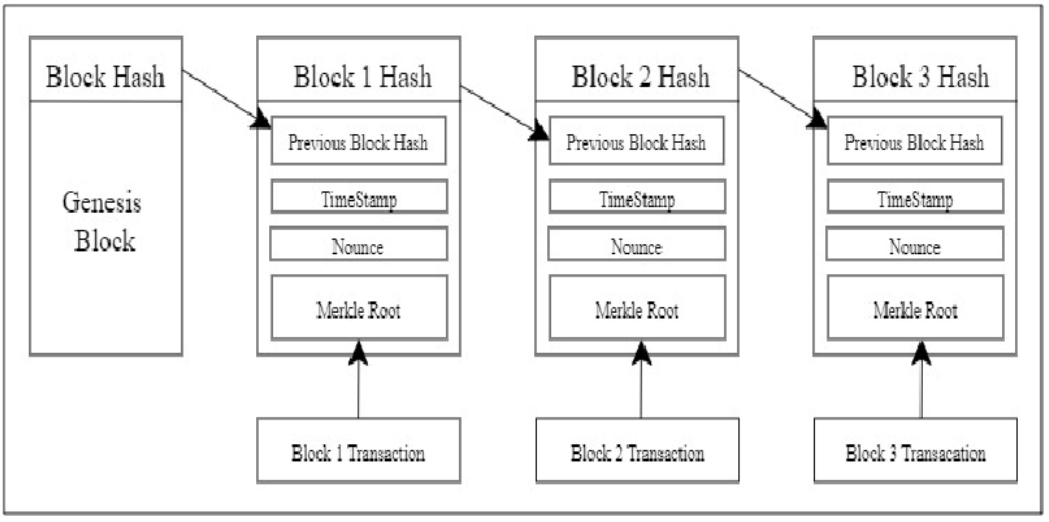

Figure 1. Block Structure

2. Distributed Ledger: Blockchain technology introduces a revolutionary approach to data management through distributed ledger systems. Unlike traditional centralized databases controlled from a single point of authority, these digital ledgers function across a decentralized

network of interconnected computer nodes. Each participating node independently maintains a complete and synchronized record of all transactions and data entries.

The architecture of distributed ledgers provides numerous critical advantages. By eliminating a single point of failure, these systems enhance resilience and reliability. The decentralized nature ensures that no single entity has complete control, promoting transparency and reducing the risk of manipulation. Additionally, the cryptographic mechanisms underlying blockchain technology create an environment of robust security and data integrity. The unique block-based structure of blockchain ledgers adds an extra layer of protection against unauthorized modifications.

3. Consensus Mechanisms: Blockchain networks rely on innovative consensus protocols to achieve synchronized and trustworthy operation across distributed systems. These algorithmic frameworks enable multiple independent participants to collectively verify and agree upon the blockchain's current state without requiring centralized authority.

Core Functions of Consensus Mechanisms includes Synchronize network participants' understanding of transaction history, Prevent malicious actors from manipulating blockchain records, Create a secure, tamper-resistant mechanism for transaction validation, Enable decentralized governance and decision-making processes

Key Consensus Approaches:

- Proof of Work (PoW): In this computational-intensive approach, network nodes compete to solve complex cryptographic challenges. The first node successfully solving the mathematical puzzle earns the right to validate transactions and add a new block to the blockchain. Bitcoin's pioneering implementation exemplifies this method.

- Proof of Stake (PoS): Unlike PoW's energy-demanding model, PoS selects transaction validators based on their economic stake in the network. Participants who lock up larger cryptocurrency amounts have higher probabilities of being chosen to verify transactions, creating a financial incentive for network integrity.

- Delegated Proof of Stake (DPoS): This democratic variant allows token holders to vote for a limited group of trusted delegates. These elected representatives are responsible for transaction validation and network maintenance, introducing a more efficient and representative governance model.

Each consensus mechanism represents a unique approach to addressing blockchain's fundamental challenges of security, efficiency, and decentralization. The selected protocol profoundly influences a blockchain network's overall performance, scalability, and reliability.

4. Cryptographic Security: Cryptographic techniques are essential to blockchain's security and functionality. They contribute to data protection, user authentication, and maintaining the blockchain's integrity.

Key cryptographic elements in blockchain include:

1. Public Key Cryptography: Users have a public key (similar to a bank account number) for receiving funds, Private keys (like a secret PIN) are used to authorize transactions, This system enables secure, verifiable transactions without revealing sensitive information

2. Hash Functions: These algorithms convert data of any size into a fixed-length string of characters. In blockchain, hashing is used to: a) Create unique identifiers for blocks and transactions b) Link blocks together in the chain c) Ensure data integrity

5. Smart Contracts: The concept of smart contracts was introduced by computer scientist and legal scholar Nick Szabo in the 1990s [17]. In the context of blockchain, smart contracts are self-executing programs that automatically enforce the terms of an agreement when specific conditions are met. Smart contracts facilitate peer-to-peer transactions of digital assets or data without requiring trusted third parties[18]. This can potentially reduce costs, increase efficiency, and minimize the risk of fraud or manipulation.

Different blockchain platforms implement smart contracts in various ways:

1. Ethereum: One of the first platforms to widely implement smart contracts, using its own programming language called Solidity.

2. Hyperledger Fabric: Refers to smart contracts as "chaincode," which can be written in general-purpose programming languages like Go or Java.

Beyond its original use case in crypto currency, blockchain technology holds significant potential for revolutionizing various industries, including data storage and management.

2. Literature Review

Nakamoto, S. (2008) [16], in this seminal paper, Satoshi Nakamoto introduced the concept of blockchain technology as the underlying framework for Bitcoin. It laid the foundation for decentralized data storage and transaction validation. Swan, M. (2015) [17], this book provides an overview of blockchain technology and its potential applications beyond cryptocurrencies. It discusses the principles of decentralized data storage and its implications for various industries.

Buterin, V., and Griffith, V. (2017) [18], introduce a novel consensus protocol specifically designed to enhance security and reliability in distributed storage networks. The research focused on developing robust mechanisms to ensure transaction finality and data integrity across decentralized platforms. Kosba, A., Miller, A., Shi, E., Wen, Z., and Papamanthou, C. (2016) [19], have made significant strides in creating advanced frameworks for privacy-protected smart contract implementations. These frameworks offer sophisticated approaches to managing sensitive information, with potential applications spanning multiple domains that require secure, transparent transaction processing. Cheng, C. (2018) [20], have highlighted blockchain's transformative potential in specialized industries. Notably, researchers have examined how blockchain technologies could revolutionize complex administrative processes, particularly in sectors requiring meticulous documentation and transparent record-keeping. Key research contributions have demonstrated blockchain's capacity to address critical challenges in data management, security, and institutional efficiency. By developing sophisticated consensus mechanisms and privacy-preserving technologies, scholars are expanding the practical applications of distributed ledger systems across various professional and technological domains.

Michal Munk, Petr Hajek, and Farhana Akter Sunny [1] (2022), conducted an extensive review of blockchain technology. Their work delved into the comprehensive landscape of blockchain applications, providing valuable insights into the technology's broader potential and transformative capabilities across different sectors. Daniel Diaz-Fuentes, Judith Clifton, and Diego Cagigas [2] (2021), this research specifically investigates blockchain's applications in public service contexts. Their methodological approach involved creating an extensive database and performing in-depth analyses to uncover the potential benefits and inherent challenges of blockchain implementation in governmental and public sector environments.

Li, M., Kshetri, N., & Vo, H. D. (2023) [23], This paper provides a comprehensive review of blockchain-based decentralized storage solutions, discussing their architecture, features, and applications in various domains, including legal document management. Zhang, Y., Hu, S., & Liu, Y. (2022) [24]. This systematic review examines the use of blockchain technology in legal document management, focusing on its potential benefits, challenges, and emerging trends.

Ashwin and Aditya Vijaykumar Singh Ompraksha Tiwari, Vivian Brian Lobo, and Shreyash Sanjay Singh [3] (2018), explored innovative applications of blockchain technology in critical administrative domains, particularly in criminal justice record management. Recent scholarly investigations have highlighted the potential of distributed ledger technologies to transform traditional record-keeping systems by enhancing data security, transparency, and verifiability. This examines how blockchain can revolutionize criminal record management. By implementing decentralized digital systems, researchers propose solutions that could significantly improve the integrity and accessibility of sensitive legal documentation. The approach aims to create a more secure and tamper-resistant method of storing and managing critical law enforcement information.In accordance with Fran Casino, Constantinos Patsakis, and Thomas K. Dasaklis [4] (2018), extensively analyzed blockchain's transformative potential across multiple sectors. Systematic reviews of technological applications demonstrate how distributed ledger technologies can address fundamental challenges in data management, offering more robust and transparent solutions compared to conventional centralized systems.

Wang, Q., Chen, W., & Li, X. (2022) [21], this study presents case studies of blockchain-based legal document management systems, highlighting their implementation challenges, user experiences, and lessons learned. Clark, S., & Smith, P. (2023) [22], this paper discusses regulatory and ethical considerations associated with blockchain-based legal document management systems, addressing issues such as data privacy, ownership, and liability.

Verma and Ashwin introduced NyaYa [7] (2021), a blockchain-based Electronic Law (EL) management system for digitized judicial investigations. NyaYa has four phases: stakeholder registration, case registration on a public blockchain with meta-hash keys, updates among law enforcement agencies, and case settlement via smart contracts. Simulation shows NyaYa outperforms traditional EL storage in various aspects like mining cost, query time, and trust probability, making it an effective solution for secure and efficient digital evidence management in the legal system.

Victoria L. [8] (2021) Lemieux paper is about Blockchain, a distributed ledger technology, aims to create immutable records of transactions. It's rapidly transforming various sectors like healthcare, real estate, and finance, promising trustworthy and secure recordkeeping. The

technology involves blocks of transaction records cryptographically chained together, ensuring transparency and detectability of alterations. Transactions involve transferring blockchain representations (tokens) of assets between addresses using public-private key pairs. Blockchains can be decentralized or centralized, and they can be public or permissioned. In recordkeeping, blockchain proves advantageous by detecting alterations and enhancing privacy through individual data control. However, challenges like scalability and legal concerns persist

Maisha Afrida Tasnim, Abdullah Al Omar, Mohammad Shahriar Rahman and Md Zakirul Alam Bhuiyan[9] (2018) introduces a groundbreaking approach to criminal record management that leverages blockchain technology to address critical challenges in data security and integrity. The proposed system introduces a comprehensive solution for storing and managing sensitive legal documentation through a decentralized and tamper-resistant framework. The proposed system allows authorized users like law enforcement and general users to efficiently manage and access criminal records. The decentralized data management process involves pre-registered users, digital signatures, encryption, and blockchain technology to ensure data authenticity and prevent tampering.

Ali, Saqib, Wang Guojun, White Bebo, and Roger Leslie (2018) [10] proposed a novel blockchain-based framework designed specifically for PingER, a global initiative focused on Internet performance measurement. This framework integrates a permissioned blockchain with Distributed Hash Tables (DHT) to manage metadata on the blockchain, while storing actual files off-chain in a decentralized manner via DHT. By decentralizing storage and leveraging distributed processing, the framework reduces reliance on centralized repositories and enhances file retrieval efficiency. The use of permissioned blockchains enhances security by allowing only authenticated and authorized participants to access the system, ensuring data integrity and confidentiality. This design is not limited to cryptocurrency applications but also extends to peer-to-peer cloud storage and other decentralized applications. The framework aims to significantly improve data management and accessibility within the PingER initiative, highlighting its potential for broader applications in distributed systems and decentralized networks.

Olumide Malomo, Danda Rawat and Moses Garuba [11] (2020) address 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.

Mark W. Storer, Kevin Greenan, Darrell D. E. Long, and Ethan L. Miller (2008) [13] tackle the issue of balancing data security with storage efficiency in archival systems. Traditional deduplication aims to optimize storage by removing redundant data, but it conflicts with encryption, which obscures data patterns. The paper proposes generating encryption keys consistently from data chunks to allow deduplication while maintaining encryption. This

ensures that identical chunks produce the same ciphertext, with keys kept confidential. Their approach supports both single-server and distributed storage systems, enhancing data security and storage efficiency. The paper details the security mechanisms and evaluates the system's effectiveness in achieving secure deduplication.

A recent systematic literature review (SLR) by a Danielle Batista[12] and his team of researchers in 2023 investigated the potential of blockchain technology in forensic evidence management, particularly focusing on the chain of custody for physical evidence. The study, which analyzed 26 relevant resources, highlighted a significant research gap in this area.

The review revealed a lack of in-depth studies exploring blockchain-based solutions specifically designed to address challenges in maintaining the chain of custody for physical evidence in forensic investigations. This finding points to an important area for future research and development in the field of digital forensics and blockchain applications.

The scarcity of research in this particular domain suggests that there are untapped opportunities for innovative blockchain solutions to enhance the integrity and traceability of physical evidence handling in forensic processes. As blockchain technology continues to evolve, its potential applications in ensuring the security and reliability of forensic evidence management remain largely unexplored.

This research gap identified by the SLR underscores the need for further investigation into how blockchain can be effectively implemented to improve current practices in forensic evidence custody. Future studies in this area could potentially lead to the development of more robust and transparent systems for managing physical evidence throughout the forensic investigation process.

Kamshad Mohsin [14] (2021) discusses blockchain technology and its interaction with legal frameworks, particularly focusing on its implications for contracts, intellectual property, personal data protection, and global legalities. It highlights the dichotomy between enabling and prohibitive legislation concerning blockchain and explores its potential benefits and challenges. The emerging field of Blockchain Law is acknowledged, emphasizing the need to align technology with evolving legal requirements globally. The document also mentions the impact of blockchain on distributed ledger technology, urging compliance with diverse data regulations worldwide. Additionally, regulatory sandboxes and their role in fostering blockchain innovation are discussed.

Victoria Lemieux [15] (2018) introduces a novel framework for assessing the potential of blockchain and distributed ledger technology in delivering trustworthy and immutable recordkeeping, focusing on archival science principles. Blockchain's ability to create trusted, unalterable records without reliance on a central authority is drawing global interest, especially in applications like land transfers and healthcare records. The paper emphasizes the need to evaluate blockchain's capabilities through an archival science lens, which is crucial for use cases heavily reliant on secure and authentic recordkeeping, highlighting its relevance in assessing blockchain-based recordkeeping systems.

3. System Architecture

To create a blockchain-based eVault system for legal records, the focus is on ensuring security, transparency, and accessibility for all stakeholders. This system will securely store, manage, and share legal records, leveraging blockchain technology to enhance efficiency and trust. It will have the capability to integrate seamlessly with existing legal databases and case management systems, facilitating seamless data exchange and enhancing overall operational effectiveness in the legal domain.

The Legal eVault framework consists of several interconnected components that work together to create a comprehensive digital legal ecosystem. At its core, this system allows users to interact with judicial processes through a variety of digital interfaces and applications.

These user-facing tools provide functionality for managing cases, submitting evidence, and engaging in dispute resolution processes. By digitizing these interactions, the system aims to streamline legal procedures and improve accessibility for all parties involved.

A key feature of this framework is the integration of automated protocols that execute predefined legal procedures. These digital agreements operate based on established rules and conditions, reducing the need for intermediaries and potentially speeding up certain legal processes.

These nodes play multiple crucial roles:

1. They verify the validity of transactions within the system.
2. They execute the automated legal protocols.
3. They record all activities in a shared, decentralized database.

This distributed approach to data management and processing helps ensure that the system remains transparent, secure, and resistant to unauthorized alterations. By spreading these responsibilities across multiple nodes, the framework aims to create a more robust and trustworthy platform for legal operations.

The components of the proposed system are given below:

a. Legal Entities: Serve as users and providers of legal documents to the eVault system. Law firms, courts, and other legal institutions interact with the eVault to upload, retrieve, and verify documents.

b. User Interfaces and Applications (API Layer): Provides an interface for legal entities to interact with the eVault. Allows users to view documents stored in the eVault. Provide mechanisms to verify the authenticity and integrity of documents. Additional tools for managing, sharing, and collaborating on legal documents. User-friendly interfaces and applications for interacting with the judicial system, including case management, document submission, evidence presentation, dispute resolution, and legal analytics.

c. Access Control and Authentication: Ensures secure access to the eVault by authenticated and authorized users. Provides a secure token-based authentication mechanism, ensuring that only authorized users can access and modify documents.

d. eVault Gateway: Acts as an intermediary between the API layer and the blockchain network by functioning as a node within the blockchain. This node handles transactions and interacts with smart contracts. Network participants validate transactions, execute smart contracts, and uphold the distributed ledger. These nodes work in concert to maintain security, promote transparency, and preserve the integrity of the entire framework. Their coordinated efforts create a robust and reliable infrastructure, crucial for handling sensitive legal information.

e. Blockchain Network: Legal document management systems utilize metadata and access logs to ensure both immutability and transparency. Self-executing digital agreements, commonly known as smart contracts, play a key role in streamlining legal procedures. These programmable protocols contain predefined conditions and rules that automatically trigger specific actions when met. By encoding legal logic into blockchain-based software, smart contracts can automate numerous aspects of legal workflows, such as including contract execution, dispute resolution, evidence management, court proceedings, identity verification, and legal document management. The Consensus Layer is responsible for validating and confirming transactions through its mechanisms, while the Storage Layer maintains the metadata of documents (but not the documents themselves), safeguarding their integrity and immutability.

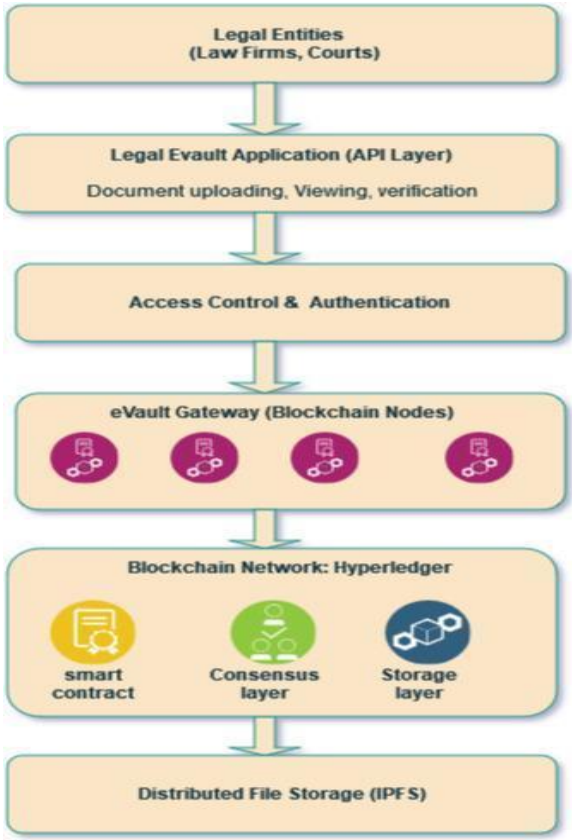

Figure 2. Legal eVault framework

f. Distributed File Storage (IPFS): Legal documents are stored in a decentralized manner using the IPFS (InterPlanetary File System) protocol, which is designed for distributed file storage and sharing [5]. IPFS employs content-addressed storage, where files are identified and accessed based on their content rather than traditional location-based addressing (e.g., URLs). This approach enhances retrieval speed and efficiency, as the protocol utilizes techniques similar to BitTorrent for caching and distributing files. Furthermore,

The system contains the following Functionalities:

I. Uploading and retrieving documents

In a legal e-vault system using blockchain technology, uploading and retrieving documents involves storing documents securely on the blockchain and providing mechanisms for users to access and retrieve them.

Before uploading, the document undergoes hashing to generate a unique cryptographic hash. This hash serves as the document's digital fingerprint and ensures its integrity. Depending on the system's security requirements, the document may be encrypted to protect its contents.

Encryption keys are securely managed to ensure that only authorized users can decrypt the documents.

Users interact with a smart contract deployed on the blockchain to upload documents. The smart contract receives the document's hash and stores it along with relevant metadata (e.g., document ID, uploader's address, timestamp) on the blockchain. Only authorized users can initiate document uploads, ensuring data integrity and security. Figure 3 gives the code snippet for uploading documents.

Users provide the necessary information to identify the document they wish to retrieve (e.g., document ID, unique identifier, metadata). Before providing access to the document, the smart contract verifies the user's permissions to ensure they are authorized to retrieve it.

If the user meets the access criteria, the smart contract returns the document's hash and metadata. If the document was encrypted during uploading, authorized users can decrypt it using their encryption keys. Decryption occurs locally on the user's device to maintain privacy and security. Based on the returned document hash, users can retrieve the corresponding document from a secure storage location (e.g., off-chain storage, decentralized file system).

Figure 4 gives the code snippet for downloading the document with permissions.

```go
func (s *SmartContract) UploadDocument(ctx contractapi.TransactionContextInterface, id string, name string, content []byte) error {
    // Upload to IPFS
    ipfsHash, err := uploadToIPFS(content)
    if err != nil {
        return err
    }

    // Create document struct
    doc := Document{
        ID:          id,
        Name:        name,
        IPFSHash:    ipfsHash,
        Owner:       ctx.GetClientIdentity().GetID(),
        Permissions: []string{ctx.GetClientIdentity().GetID()},
        CreatedAt:   time.Now(),
        UpdatedAt:   time.Now(),
    }

    // Store document metadata in the ledger
    docJSON, err := json.Marshal(doc)
    if err != nil {
        return err
    }

    return ctx.GetStub().PutState(id, docJSON)
}

func uploadToIPFS(content []byte) (string, error) {
    sh := shell.NewShell("localhost:5001")
    hash, err := sh.Add(bytes.NewReader(content))
    if err != nil {
        return "", err
    }
    return hash, nil
}
```

Figure 3. Code Snippet for document uploading

All document uploads and retrievals are recorded on the blockchain, providing an immutable record keeping of transactions for transparency and accountability. Along with document hashes, relevant metadata such as timestamps, uploader information, and access permissions are stored on the blockchain to facilitate document management and retrieval.

```go
func (s *SmartContract) DownloadDocument(ctx contractapi.TransactionContextInterface, id string) ([]byte, error) {
    // Retrieve document metadata from the ledger
    docJSON, err := ctx.GetStub().GetState(id)
    if err != nil {
        return nil, err
    }

    var doc Document
    err = json.Unmarshal(docJSON, &doc)
    if err != nil {
        return nil, err
    }

    // Check permissions
    if !s.hasPermission(ctx, doc.Permissions) {
        return nil, fmt.Errorf("permission denied")
    }

    // Download from IPFS
    return downloadFromIPFS(doc.IPFSHash)
}

func downloadFromIPFS(hash string) ([]byte, error) {
    sh := shell.NewShell("localhost:5001")
    reader, err := sh.Cat(hash)
    if err != nil {
        return nil, err
    }
    defer reader.Close()

    return ioutil.ReadAll(reader)
}
```

Figure 4. Code Snippet for document downloading

II. Authentication and Access Control Mechanism

To join the legal e-vault system, users must complete a registration process that includes providing essential personal information. This typically involves entering their name, email address, and creating a secure password.

To bolster security, the system implements additional verification measures. A common approach is the use of two-factor authentication (2FA), which adds an extra layer of protection to user accounts.

Upon registration, each user is assigned a unique digital identity based on cryptographic principles. This identity consists of a pair of keys: a public key and a private key. The public key is recorded on the blockchain, making it visible to other network participants. In contrast, the private key is kept securely on the user's personal device.

For authentication purposes, users can utilize their blockchain wallet addresses. These addresses serve as unique identifiers within the system. The e-vault links access rights and permitted actions to these wallet addresses, creating a secure and transparent authentication mechanism.

User authentication is managed through smart contracts deployed on the blockchain. These contracts contain logic to verify user identities by checking their public keys or wallet addresses against the recorded information.

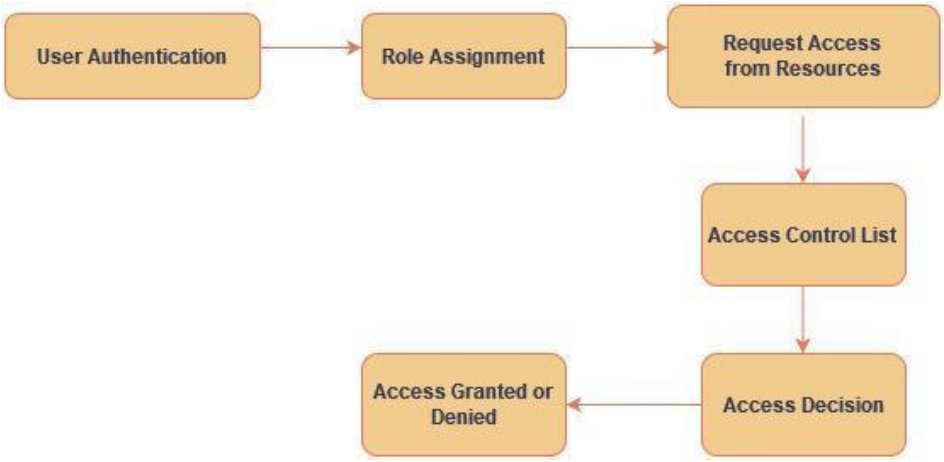

Figure 5. Role-Based Access and Security Model

Role-Based Access and Security Model (RBAS) is implemented which assigns roles and permissions to users based on their responsibilities and privileges within the legal e-vault system. Roles such as admin, uploader, reviewer, and viewer can be defined, each with specific access rights. Access control logic is enforced within smart contracts deployed on the blockchain. Smart contracts verify users' permissions before allowing them to perform actions such as uploading, modifying, or accessing documents. Figure 3 depicts the Role-Based Access and Security mechanism. Figure 6 gives the code snippet to assign the roles to the users and Figure 7 checks the permissions for accessing the documents.

Access Control Lists (ACLs) are maintained within smart contracts to specify granular access control settings for individual documents or document categories. ACLs define which users or roles have permission to perform specific actions on each document. All authentication attempts and access control actions are recorded on the blockchain. Mechanisms to revoke access permissions in case of user termination, role changes, or security breaches are

implemented. Access permissions are updated in real-time on the blockchain, ensuring immediate enforcement of changes.

```go
func (s *SmartContract) AssignRole(ctx contractapi.TransactionContextInterface, userID string, role string) error {
    userJSON, err := ctx.GetStub().GetState(userID)
    if err != nil {
        return err
    }

    var user User
    if userJSON != nil {
        err = json.Unmarshal(userJSON, &user)
        if err != nil {
            return err
        }
    } else {
        user = User{ID: userID, Roles: []string{}}
    }

    user.Roles = append(user.Roles, role)
    userJSON, err = json.Marshal(user)
    if err != nil {
        return err
    }

    return ctx.GetStub().PutState(userID, userJSON)
}
```

Figure 6. Code Snippet for Role Assignment to users

III. Verification of Documents:

Figure 4 depicts the document verification process. The user (e.g., a lawyer, court official) requests verification of a document by providing its unique Document ID. The request includes the Document ID and is sent to the API layer of the eVault system.

```go
func (s *SmartContract) hasPermission(ctx contractapi.TransactionContextInterface, allowedRoles []string) bool {
    userID := ctx.GetClientIdentity().GetID()
    userJSON, err := ctx.GetStub().GetState(userID)
    if err != nil {
        return false
    }

    var user User
    err = json.Unmarshal(userJSON, &user)
    if err != nil {
        return false
    }

    for _, role := range user.Roles {
        for _, allowedRole := range allowedRoles {
            if role == allowedRole {
                return true
            }
        }
    }

    return false
}
```

Figure 7. Code Snippet for Checking access permissions of user

The API layer receives the verification request and coordinates with the blockchain node, distributed file storage, and verification service. The blockchain node retrieves the document's metadata (e.g., hash, timestamp, and other relevant data) stored on the blockchain using smart contract. The document is retrieved from the distributed file storage using the hash or other identifier stored on the blockchain.

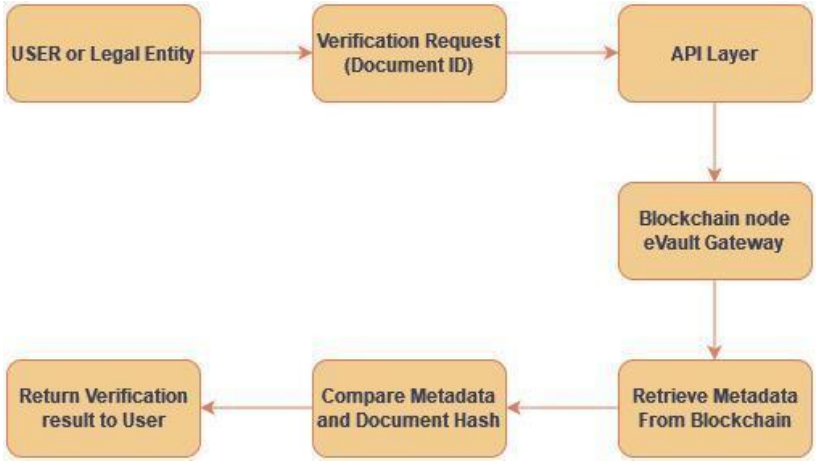

Figure 8. Document Verification Process

The verification service compares the hash of the retrieved document with the hash stored in the blockchain metadata to ensure integrity and authenticity. Other verification checks (e.g., digital signatures, timestamps) can also be performed. The retrieved document hash is compared with the blockchain-stored hash to confirm that the document is unaltered and authentic. The verification result, which indicates whether the document is authentic and unchanged, is returned to the user. If the verification fails, the user is informed that the document could not be verified. Figure 9 shows the code snippet for verifying the documents.

This verification process ensures that legal documents in the eVault are authentic, unaltered, and valid, leveraging blockchain technology and distributed storage systems to provide a secure and transparent verification mechanism.

A. Implementation Requirement

To create a decentralized system for storing and accessing legal documents, can leverage the open-source blockchain technology offered by the Hyperledger Project. Specifically, Hyperledger Fabric provides a robust foundation for building a secure and efficient Legal eVault. Here's an outline of the essential components and steps for implementing such a system:

- Setup Hyperledger Fabric Network: Install and set up Hyperledger Fabric on the designated servers or cloud infrastructure. Defined the network topology including peers, orderers, and channels. Set up the Certificate Authority (CA) for managing identities and permissions.

```go
func (s *SmartContract) VerifyDocument(ctx contractapi.TransactionContextInterface, id string, contentHash string) (bool, error) {
    docJSON, err := ctx.GetStub().GetState(id)
    if err != nil {
        return false, fmt.Errorf("failed to read document metadata: %v", err)
    }
    if docJSON == nil {
        return false, fmt.Errorf("document does not exist")
    }

    var doc Document
    err = json.Unmarshal(docJSON, &doc)
    if err != nil {
        return false, fmt.Errorf("failed to unmarshal document metadata: %v", err)
    }

    // Check permissions
    if !s.hasPermission(ctx, doc.Permissions) {
        return false, fmt.Errorf("permission denied")
    }

    // Download document from IPFS
    content, err := downloadFromIPFS(doc.IPFSHash)
    if err != nil {
        return false, fmt.Errorf("failed to download document from IPFS: %v", err)
    }

    // Calculate hash of the downloaded content
    calculatedHash := calculateSHA256(content)

    // Compare the calculated hash with the provided hash
    return calculatedHash == contentHash, nil
}

// Helper function to calculate SHA256 hash
func calculateSHA256(data []byte) string {
    hash := sha256.Sum256(data)
    return hex.EncodeToString(hash[:])
}
```

Figure 9. Code Snippet for Document Verification

- Smart Contract Development: Developed the smart contracts (chaincode) to manage document storage, access control, and transactions. Used the supported languages like Go (Golang) or Node.js for developing chaincode. Implemented the logic for document encryption, decryption, access control rules (RBAC), and audit trail recording.

- Document Storage and Metadata Management: Defined the structure for storing legal documents and associated metadata on the blockchain or off-chain with references on the blockchain. Stored the document metadata (e.g., timestamps, hashes) on the blockchain for transparency and auditability.

- Access Control and Privacy: Implemented RBAC to enforce access permissions based on user roles and document ownership. Ensuring that sensitive information is securely handled and accessible only to authorized parties.

B. Significance

Besides decentralized data storage, the framework has the potential to provide the following capabilities:

This framework provides a tamper-resistant and transparent ledger where legal documents are stored. Each transaction (document upload, access, etc.) is cryptographically secured and recorded, enhancing document integrity. Documents can be encrypted and stored securely on off-chain with references on the blockchain, assures that only authorized parties can decrypt and access them.

This framework removes the requirement for a central authority or intermediary, which decreases dependency on conventional methods of storing legal documents. This can

streamline processes and reduce costs associated with intermediaries. Documents can be accessed globally at any time, facilitating faster transactions and document verification processes.

Every interaction with the documents (viewing, editing, sharing) is stored as a log on the blockchain, providing transaction logging that can be verified by all parties involved. Automation through smart contracts can enforce predefined rules and conditions, such as access permissions and document validation, further enhancing transparency and reducing disputes.

Blockchain technology's distributed structure eliminates the reliance on a central authority in legal transactions, fostering an environment of increased confidence among participants. This decentralized approach spreads data storage and decision-making across multiple nodes, creating a robust system that is less vulnerable to isolated failures or targeted attacks.

4. Performance Evaluation

A. Evaluation of the Smart Contract Deployment Cost

The Ethereum blockchain relies on miners to verify and record transactions. To ensure that transactions are processed, users must compensate miners. This compensation is measured in units called gas, which reflects the computational work required for each operation. When starting a transaction on the Ethereum network, the sender must define two key elements: the gas limit and the gas price. These parameters are crucial for determining the transaction's cost and execution.

The gas limit is the maximum amount of computational power, measured in units of gas, that the sender is willing to allocate for the transaction. This cap ensures that transactions don't consume excessive resources or run indefinitely.

On the other hand, the gas price represents the cost for each unit of gas, denominated in ETH (Ethereum's native cryptocurrency). This price fluctuates based on network demand and congestion.

By setting these two values, users can control their transaction costs and prioritize their operations within the Ethereum ecosystem. Understanding and properly configuring these parameters is essential for efficient and cost-effective use of the network.

The platform features three primary types of contracts written in Solidity: the User Identity Key contract, the Uploading, Downloading Documents Contract, and the verifying Documents Contract.

- User Identity Key Contract: This contract facilitates the registration of new users into the sharing system.
- Uploading, Downloading Documents Contract: Used by data owners to outsource data uploads, this contract manages anonymous and auditable access controls and records data locations on the IPFS network.

- Verifying Documents Contract: The verification process ensures that legal documents in the eVault are authentic, unaltered, and valid, leveraging blockchain technology and distributed storage systems to provide a secure and transparent verification mechanism.

The costs associated with deploying these contracts are detailed in Table I.

Contracts	Transaction Cost	Execution Cost	Total Cost
Uploading, Downloading Documents Contract	1318303	951831	2270134
User Identification Contract	641176	446080	1087256
verifying Documents Contract	442294	802498	1244792

Table I: Deployment Cost measurement of smart contracts

B. Comparing Legal eVault with traditional methods

Table II gives the comparative between Blockchain-Based Storage, Traditional Centralized Database Storage , Cloud Storage . Blockchain-Based Storage excels in immutability and decentralization but faces challenges with scalability, cost, and energy consumption. Traditional Centralized Database Storage offers flexibility and scalability with relatively low energy consumption and cost but has vulnerabilities related to centralization and potential data manipulation. Cloud Storage provides excellent scalability, flexibility, and cost-effectiveness but relies on centralization and the security practices of cloud providers.

	Blockchain-Based Storage	Traditional Centralized Database Storage	Cloud Storage
Immutable	Yes	No	No
Transparency	Yes	No	No
Decentralization	Yes	No	No
Security	Most Secure	Secure	More Secure
Flexibility	Less flexible	More flexible	Highly flexible
Scalability	Less Scalable	More scalable	Highly scalable
Energy Consumption	High	Low	Depends
Cost	High	Low	Moderate

Table II: Comparing Legal eVault with traditional methods

5. Conclusion

This study presents a decentralized framework for storing and accessing legal documents using blockchain technology. The framework eliminates the need for centralized repositories by

replacing traditional data paths with write-only access entries on the blockchain. This decentralization shifts the legal eVault system away from reliance on centralized computing resources for storage, processing, and uptime. Blockchain's cryptographic security ensures the integrity and authenticity of document metadata, safeguarding legal records from unauthorized alterations.

The framework supports efficient verification of document authenticity and integrity, reducing fraud risks and fostering trust in the legal system. Role-Based Access and Security Model (RBAS) is implemented to restrict document access and modifications to authorized users, thereby meeting rigorous privacy and security standards.

Implementing a blockchain-based eVault system for legal records can significantly enhance access to justice in India. It promises faster court proceedings, reduced costs, improved data integrity, and heightened trust in the justice system. Future developments may integrate AI for advanced document analysis, ensure interoperability across blockchain networks, and enhance security measures. Improvements in user interfaces, regulatory compliance, and scalability are also pivotal for creating an efficient, secure, and globally accessible legal document management system.

References

[1] Farhana Akter Sunny,Petr Hajek, Michal Munk, Mohammad Zoynul Abedin, Md. Shahriare Satu, Md. Iftekharul Alam Efat, Md. Jahidul Islam "A Systematic Review of Blockchain Applications", "Blockchain, applications, business and industry, internet of things, privacy and security", Vol 10, 2022, DOI: 10.1109/ACCESS.2022.3179690

[2] Diego Cagigas, Judith Clifton, Daniel Diaz-Fuentes,Marcos Fernández-Gutiérrez "Blockchain for Public Services: A Systematic Literature Review", "Blockchain, public services, government, civil servants, eGovernment, public sector innovation, systematic literature review.", Vol 09, 2021, DOI:10.1109/ACCESS.2021.3052019

[3] Aditya Vijaykumar Singh, Ashwin Omprakash Tiwari, Shreyash Sanjay Singh, Vivian Brian Lobo, "A Criminal Record Keeper System using Blockchain", 2018 Ivannikov Ispras Open Conference (ISPRAS), DOI:10.1109/ICOEI53556.2022.9776725

[4] Fran Casino, Thomas K. Dasaklis, Constantinos Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues", Vol 36, 2018, DOI: 10.1016/j.tele.2018.11.006

[5] J. Benet, “Ipfs-content addressed, versioned, p2p file system,” arXiv preprint arXiv:1407.3561, 2014.

[6] “Filecoin: A decentralized storage network.

[7] 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.

[8] Lemieux, V. L. (2021). Blockchain and Recordkeeping. Computers, 10(11), 135.

[9] 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.

[10] 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.
[11] 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.
[12] 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).
[13] 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.
[14] Mohsin, K. (2021). Blockchain Law: A New Beginning. Available at SSRN 3840220.
[15] Lemieux, V., Hofman, D., Batista, D., & Joo, A. (2019). Blockchain technology & recordkeeping. ARMA International Educational Foundation.
[16] Nakamoto, S.. Bitcoin: A Peer-to-Peer Electronic Cash System. (2008)
[17] Swan, M. Blockchain: Blueprint for a New Economy. (2015).
[18] Buterin, V., & Griffith, V. Casper the Friendly Finality Gadget, Cryptography and Security (2017).
[19] Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016). Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts. 2016 IEEE Symposium on Security and Privacy (SP).
[20] Cheng, C. (2018). Blockchain and Smart Contracts for Insurance: Is the Technology Mature Enough? February 2018, Future Internet 10(2):20
[21] Wang, Q., Chen, W., & Li, X. (2022). Case Studies of Blockchain-Based Legal Document Management Systems. January 2022Automation in Construction 133(4):104001
[22] Clark, S., & Smith, P. (2023). Regulatory and Ethical Considerations in Blockchain-Based Legal Document Management
[23] Li, M., Kshetri, N., & Vo, H. D. (2023). Decentralized Storage Solutions: A Review of Blockchain-Based Systems.
[24] Zhang, Y., Hu, S., & Liu, Y. (2022). Blockchain Technology in Legal Document Management: A Systematic Review
[25] N. Szabo, (1997), Formalizing and securing relationships on public networks, First Monday, vol. 2, no. 9. [Online]. Available: http: //ojphi.org/ojs/index.php/fm/article/view/548
[26] K. Christidis and M. Devetsikiotis (2016), "Blockchains and smart contracts for the internet of things," IEEE Access, vol. 4, pp. 2292–2303.