A REPORT

ON

DEVELOPING A BLOCKCHAIN-BASED EVAULT FOR LEGAL RECORDS

Submitted by,

Mr. GOVIND CHAUDHARY	- 20211CBC0006
Mr. YASH SINGH	- 20211CBC0029
Mr. AMITH GOWDA M	- 20211CBC0048
Mr. SHOAIB ABDULLA KHAJI	- 20221LBC0003

Under the guidance of,

Mr. RAMAMURTHY KETHA

in partial fulfillment for the award of the degree of

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE AND ENGINEERING (BLOCK CHAIN)

At

GAIN MORE KNOWLEDGE
REACH GREATER HEIGHTS

PRESIDENCY UNIVERSITY

BENGALURU

MAY 2025

PRESIDENCY UNIVERSITY

PRESIDENCY SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

CERTIFICATE

This is to certify that the Project report **"DEVELOPING A BLOCKCHAIN-BASED EVAULT FOR LEGAL RECORDS"** being submitted by "**GOVIND CHAUDHARY, YASH SINGH, AMITH GOWDA M, SHOAIB ABDULLA KHAJI**" bearing roll number(s) "**20211CBC0006, 20211CBC0029, 20211CBC0048, 20221LBC0003**" in partial fulfillment of the requirement for the award of the degree of Bachelor of Technology in Computer Science and Engineering (Block Chain) is a bonafide work carried out under my supervision.

Mr. RAMAMURTHY KETHA
Assistant Professor
PSCS
Presidency University

Dr. S. PRAVINTH RAJA
Professor & HoD
PSCS
Presidency University

Dr. MYDHILI NAIR
Associate Dean
PSCS
Presidency University

Dr. SAMEERUDDIN KHAN
Pro-Vice Chancellor - Engineering
Dean –PSCS / PSIS
Presidency University

PRESIDENCY UNIVERSITY

PRESIDENCY SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

DECLARATION

We hereby declare that the work, which is being presented in the project report entitled **PSCS218 – " DEVELOPING A BLOCKCHAIN- BASED EVAULT FOR LEGAL RECORDS"** in partial fulfillment for the award of Degree of **Bachelor of Technology in Computer Science and Engineering (Block Chain)**, is a record of our own investigations carried under the guidance of **Mr. RAMAMURTHY KETHA, ASSISTANT PROFESSOR, School of Computer Science and Engineering, Presidency University, Bengaluru.**

We have not submitted the matter presented in this report anywhere for the award of any other Degree.

NAME	ROLL NO	SIGNATURE
GOVIND CHAUDHARY	20211CBC0006	
YASH SINGH	20211 CBC0029	Yash
AMITH GOWDA M	20211CBC0048	
SHOAIB ABDULLA KHAJI	20221LBC0003	

ABSTRACT

Blockchain technology is transforming digital security and data integrity across industries. This project, **Legal eVault**, leverages blockchain to revolutionize the storage and management of legal records, ensuring immutability, transparency, and secure access control. The system integrates **smart contracts and decentralized storage (IPFS)** to eliminate unauthorized alterations while enhancing record verification. Key features include **tamper-proof document storage, role-based access management, cryptographic security, and audit trails**, ensuring compliance with legal standards.

Optimized for efficiency and designed for user accessibility, **Legal eVault** bridges the gap between traditional legal record-keeping and modern digital solutions. By automating verification processes and reducing dependency on intermediaries, the project underscores the transformative potential of blockchain in **creating a secure, transparent, and efficient ecosystem for legal documentation management**.

By enhancing **data integrity, reducing legal paperwork, and expediting judicial processes**, **Legal eVault** aims to improve access to justice and increase trust in the legal system.

A REPORT
ON

DEVELOPING A BLOCKCHAIN-BASED EVAULT FOR LEGAL RECORDS

Submitted by,

Mr. GOVIND CHAUDHARY	- 20211CBC0006
Mr. YASH SINGH	- 20211CBC0029
Mr. AMITH GOWDA M	- 20211CBC0048
Mr. SHOAIB ABDULLA KHAJI	- 20221LBC0003

Under the guidance of,

Mr. RAMAMURTHY KETHA

in partial fulfillment for the award of the degree of

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE AND ENGINEERING (BLOCK CHAIN)

At

GAIN MORE KNOWLEDGE
REACH GREATER HEIGHTS

PRESIDENCY UNIVERSITY

BENGALURU

MAY 2025

PRESIDENCY UNIVERSITY

PRESIDENCY SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

CERTIFICATE

This is to certify that the Project report **“DEVELOPING A BLOCKCHAIN-BASED EVAULT FOR LEGAL RECORDS”** being submitted by “**GOVIND CHAUDHARY, YASH SINGH, AMITH GOWDA M, SHOAIB ABDULLA KHAJI**” bearing roll number(s) “**20211CBC0006, 20211CBC0029, 20211CBC0048, 20221LBC0003**” in partial fulfillment of the requirement for the award of the degree of Bachelor of Technology in Computer Science and Engineering (Block Chain) is a bonafide work carried out under my supervision.

Mr. RAMAMURTHY KETHA
Assistant Professor
PSCS
Presidency University

Dr. S. PRAVINTH RAJA
Professor & HoD
PSCS
Presidency University

Dr. MYDHILI NAIR
Associate Dean
PSCS
Presidency University

Dr. SAMEERUDDIN KHAN
Pro-Vice Chancellor - Engineering
Dean –PSCS / PSIS
Presidency University

PRESIDENCY UNIVERSITY

PRESIDENCY SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

DECLARATION

We hereby declare that the work, which is being presented in the project report entitled **PSCS218 – " DEVELOPING A BLOCKCHAIN- BASED EVAULT FOR LEGAL RECORDS"** in partial fulfillment for the award of Degree of **Bachelor of Technology in Computer Science and Engineering (Block Chain)**, is a record of our own investigations carried under the guidance of **Mr. RAMAMURTHY KETHA, ASSISTANT PROFESSOR, School of Computer Science and Engineering, Presidency University, Bengaluru.**

We have not submitted the matter presented in this report anywhere for the award of any other Degree.

NAME	ROLL NO	SIGNATURE
GOVIND CHAUDHARY	**20211CBC0006**	
YASH SINGH	**20211 CBC0029**	
AMITH GOWDA M	**20211CBC0048**	
SHOAIB ABDULLA KHAJI	**20221LBC0003**	

ABSTRACT

Blockchain technology is transforming digital security and data integrity across industries. This project, **Legal eVault**, leverages blockchain to revolutionize the storage and management of legal records, ensuring immutability, transparency, and secure access control. The system integrates **smart contracts and decentralized storage (IPFS)** to eliminate unauthorized alterations while enhancing record verification. Key features include **tamper-proof document storage, role-based access management, cryptographic security, and audit trails**, ensuring compliance with legal standards.

Optimized for efficiency and designed for user accessibility, **Legal eVault** bridges the gap between traditional legal record-keeping and modern digital solutions. By automating verification processes and reducing dependency on intermediaries, the project underscores the transformative potential of blockchain in **creating a secure, transparent, and efficient ecosystem for legal documentation management**.

By enhancing **data integrity, reducing legal paperwork, and expediting judicial processes**, **Legal eVault** aims to improve access to justice and increase trust in the legal system.

ACKNOWLEDGEMENTS

First of all, we indebted to the **GOD ALMIGHTY** for giving me an opportunity to excel in our efforts to complete this project on time.

We express our sincere thanks to our respected dean **Dr. Md. Sameeruddin Khan**, Pro-VC - Engineering and Dean, Presidency School of Computer Science and Engineering & Presidency School of Information Science, Presidency University for getting us permission to undergo the project.

We express our heartfelt gratitude to our beloved Associate Dean **Dr. Mydhili Nair,** Presidency School of Computer Science and Engineering, Presidency University, and **Dr. S. Pravinth Raja,** Head of the Department, Presidency School of Computer Science and Engineering, Presidency University, for rendering timely help in completing this project successfully.

We are greatly indebted to our guide **Mr. Ramamurthy Ketha, Assistant Professor** and Reviewer **Ms. Suma N G, Assistant Professo**r, Presidency School of Computer Science and Engineering, Presidency University for her inspirational guidance, and valuable suggestions and for providing us a chance to express our technical capabilities in every respect for the completion of the internship work.

We would like to convey our gratitude and heartfelt thanks to the CSE7301 University Project Coordinators **Mr. Md Ziaur Rahman and Dr. Sampath A K,** department Project Coordinator **Ms. Suma N G** and Git hub coordinator **Mr. Muthuraj.**

We thank our family and friends for the strong support and inspiration they have provided us in bringing out this project.

Govind Chaudhary (20211CBC0006)
Yash Singh (20211CBC0029)
Amith Gowda M (20211CBC0048)
Shoaib Abdulla Khaji (20221LBC0003)

LIST OF TABLES

LIST OF FIGURES

TABLE OF CONTENTS

CHAPTER-1

INTRODUCTION

1.1 Background

Legal records are crucial to the functioning of the justice system, serving as the backbone for legal proceedings and ensuring that relevant information is available when needed. These records include a wide range of documents, such as case files, contracts, evidence, court rulings, and legal notices. They are essential for maintaining the integrity and transparency of the judicial process, enabling lawyers, judges, and clients to access pertinent information for decision-making. Traditionally, legal records have been stored and managed in centralized databases or physical storage systems. Centralized systems are typically maintained by government agencies, law firms, or courts, but they often present challenges in terms of security, transparency, and accessibility. Physical storage, while providing tangible access to documents, is vulnerable to damage, loss, or theft and lacks the flexibility required for modern legal processes. Similarly, centralized digital storage systems are susceptible to hacking, data breaches, and unauthorized access, creating a need for a more secure, transparent, and efficient solution for managing legal records.

1.1.1 Challenges in Traditional Legal Record System

- **Vulnerability to Cyberattacks**: Centralized systems are prime targets for cyberattacks, as they store all data in one location, making them a single point of failure.
- **Unauthorized Access**: A centralized structure increases the risk of unauthorized access by both internal and external actors, leading to potential data theft, manipulation, or loss.
- **Data Breaches**: A successful cyberattack on centralized systems could result in large-scale data breaches, compromising sensitive personal, financial, or legal information.
- **Tampering of Records**: With a centralized database, the risk of tampering with or altering records is higher, undermining the integrity and trustworthiness of the information.

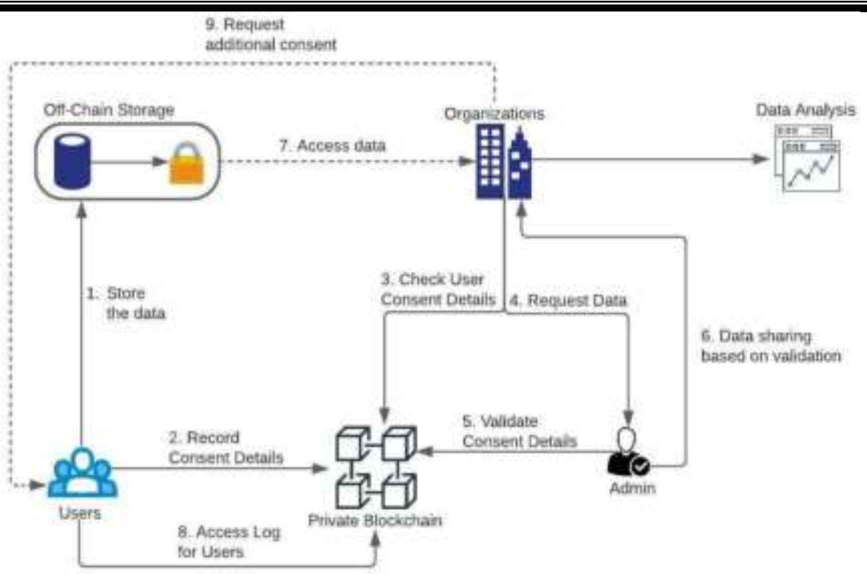

9. Request additional consent
Off-Chain Storage
Organizations
Data Analysis
7. Access data
1. Store the data
3. Check User Consent Details
4. Request Data
6. Data sharing based on validation
5. Validate Consent Details
2. Record Consent Details
Users
Private Blockchain
Admin
8. Access Log for Users

Figure 1.1 Block diagram of blockchain-based eVault

1.1.2 Need for Innovation in Legal Records Management

- With the rise of digital records, there is a growing need to ensure data integrity, accessibility and security
- There is a demand for solutions that can streamline document management while maintaining privacy and confidentiality.

1.2 Blockchain in Legal Records Management

Blockchain provides a decentralized, immutable ledger, allowing for secure, transparent, and tamper-proof data storage. It offers several advantages, such as increased transparency, reduced reliance on intermediaries, and enhanced data integrity. By ensuring that all participants have access to the same version of data, blockchain prevents unauthorized modifications and discrepancies, enhancing trust across the network. Additionally, its decentralized nature makes it resistant to single points of failure, increasing the overall security of the system. Furthermore, blockchain enables faster transactions by eliminating the need for intermediaries, streamlining processes, and reducing transaction delays.

Blockchain also facilitates greater accountability in transactions. Each action on the blockchain is recorded with a timestamp and linked to previous actions, making it easier to trace the history of data or transactions. This audit trail promotes responsible behavior, as participants know their actions are permanently recorded and can be reviewed. Additionally, blockchain has the potential to enable innovative applications in various industries, such as supply chain management, healthcare, and finance, by offering secure, transparent, and efficient methods of tracking and verifying information.

1.2.1 Blockchain Features for Legal Records

- **Immutability**: Once a document is recorded on the blockchain, it cannot be altered or deleted, ensuring a permanent, tamper-proof record.
- **Decentralization**: Data is not stored in a single location, reducing the risk of single-point failures or security breaches.

1.2.2 Smart Contracts for Access Control and Permissions

- **Smart Contracts** enable automated processes, where predefined conditions are executed without intermediaries.
- They can be used to **manage access permissions** for legal records based on roles, such as lawyers, judges, and clients..

1.2.3 Decentralized Storage Solutions (IPFS)

- **IPFS (InterPlanetary File System)** offers decentralized storage, making it ideal for storing large legal documents securely and efficiently.
- By storing records on IPFS, documents are accessible across multiple nodes, ensuring redundancy and fault tolerance.

1.3 The Need for a Blockchain-Based eVault System

Existing legal records management systems face significant challenges, including inefficiencies, security risks, and a lack of interoperability. Many of these systems depend on outdated methods, such as paper records or legacy software, which can lead to slow document retrieval, human errors, and difficulties in keeping track of important records. Security is a major concern, with centralized systems often vulnerable to unauthorized access, data breaches, or tampering. Additionally, these systems struggle to integrate effectively with other legal or governmental databases, further complicating processes. To overcome these issues, the legal sector needs a modern solution that ensures privacy, maintains data integrity, and offers seamless access to records. This system must also comply with legal standards and allow smooth data exchange across different entities, ensuring a more efficient and secure legal workflow.

1.3.1 Current Systems' Drawbacks

- The Centralized storage systems can be easily targeted, leading to potential data loss or tampering.
- Paper-based processes or legacy systems slow down legal proceedings, requiring manual intervention for document sharing and updates.

1.3.2 Lack of Interoperability

- Existing systems often fail to integrate with **modern digital platforms**, making it difficult to share documents across various stakeholders, including courts, lawyers, and clients.
- A **blockchain-based solution** can provide seamless integration with **existing databases** and case management systems.

1.3.3 Privacy and Confidentiality Concerns

- The Traditional systems struggle to provide robust **privacy controls** for sensitive legal documents.
- A **blockchain solution** can employ cryptographic techniques and **smart contracts** to ensure that access is limited to authorized individuals only, guaranteeing **confidentiality**.

CHAPTER-2

LITERATURE SURVEY

2.1 Overview of Blockchain Technology in Legal Systems

Existing legal records management systems are often burdened by inefficiencies that hinder their effectiveness in handling the vast amount of data generated in the legal sector. Many of these systems still rely on outdated technologies or manual, paper-based workflows, which can result in significant delays, human errors, and difficulty in organizing or retrieving documents. As a result, legal professionals waste valuable time searching for records, and the overall speed of legal proceedings is slowed down. Additionally, when physical files are lost, damaged, or misplaced, it compromises the integrity and availability of critical information. These inefficiencies not only affect the speed of legal work but also increase the likelihood of errors and inconsistencies, making it difficult to maintain a reliable record-keeping system.

In addition to inefficiency, security risks are a major concern for legal records management systems. Sensitive legal documents are often stored in centralized databases or physical records, making them prime targets for cyberattacks, unauthorized access, and tampering. Without proper security measures in place, confidential client information, case details, or evidence could be compromised, leading to legal and financial repercussions. Furthermore, many existing systems lack the necessary interoperability to seamlessly exchange data across various legal stakeholders, such as courts, law firms, and governmental bodies. To address these issues, the legal sector needs a modern, secure system that guarantees privacy, data integrity, and ease of access, while also enabling smooth data sharing and ensuring compliance with legal standards.

2.1.1 Key Findings:

- Blockchain can enhance the security and transparency of legal records by making data tamper-proof and auditable.
- It provides an immutable record of legal documents and transactions, ensuring data integrity and reducing fraud.
- Blockchain-based systems can automate legal workflows, reduce administrative burdens, and improve overall efficiency.

2.2 Blockchain-Based eVault Systems

The eVault systems are digital vaults designed to securely store and manage sensitive information. When integrated with blockchain technology, eVault systems offer enhanced security, ensuring that only authorized parties have access to legal documents. These systems leverage blockchain's distributed ledger to store legal records and manage permissions, ensuring that data is accessible only by authorized individuals while maintaining a transparent record of document access and modifications. Blockchain-based eVaults are designed to meet legal compliance standards and enhance trust in the handling of sensitive legal information.

2.2.1 Key Findings:

- Blockchain-based eVaults provide secure, decentralized storage of legal records, ensuring that documents cannot be altered without detection..
- These systems can automatically verify the authenticity of legal documents and transactions, reducing the potential for fraud.
- Blockchain's immutability ensures that documents stored in the eVault remain permanently unaltered, improving the reliability of legal records.

2.3 Smart Contracts in Blockchain for Legal Record Management

Smart contracts are self-executing contracts with the terms of the agreement directly written into code. In the context of legal records, smart contracts can automate processes such as document signing, storage, and sharing. Once predefined conditions are met, smart contracts execute actions automatically, eliminating the need for manual intervention. This ensures that all actions are timely, transparent, and legally binding.

2.3.1 Key Findings:

- Smart contracts can automate the creation, storage, and management of legal records.
- They provide a secure, transparent, and tamper-proof method of managing legal agreements.
- By eliminating intermediaries, smart contracts reduce costs and the potential for fraud or human error.

2.4 Decentralized Storage Systems for Legal Documents

Traditional legal document management systems rely heavily on centralized databases or physical storage, making them vulnerable to security breaches, data loss, and unauthorized access. Decentralized storage systems, such as IPFS (InterPlanetary File System), offer a solution by distributing data across a network of nodes. This ensures that documents are not reliant on a single point of failure. By decentralizing legal records, blockchain technology ensures better availability, redundancy, and protection against data loss. Decentralized storage also improves the transparency and security of legal records.

2.4.1 Key Findings:

- IPFS and other decentralized storage platforms provide secure, tamper-proof storage.
- These platforms distribute data across multiple nodes, eliminating the risk of data loss or single points of failure.
- Decentralized storage systems offer better scalability and can handle large volumes of legal data without compromising security.

2.5 Security and Privacy Considerations in Blockchain-based Legal Systems

The adoption of blockchain in legal record management introduces several concerns, particularly regarding data security and privacy. Blockchain's core feature of transparency, where all records are visible to network participants, presents a challenge when dealing with sensitive legal information, such as personal data, confidential contracts, or case details. Public visibility of this data could lead to unauthorized access or exposure of private information, compromising client confidentiality and violating privacy laws. This issue raises significant concerns for the legal sector, where protecting the privacy and integrity of information is paramount. Therefore, finding ways to leverage blockchain’s benefits without jeopardizing sensitive data has become a critical focus for adopting blockchain in legal contexts.

To address these concerns, advanced encryption techniques and privacy-preserving technologies are employed to secure data while still maintaining the advantages of blockchain. Methods like attribute-based encryption and zero-knowledge proofs ensure that sensitive information remains encrypted and accessible only to authorized parties. Attribute-based encryption allows access control based on predefined attributes, ensuring that only users with the appropriate permissions can view certain details. Zero-knowledge proofs enable verification of data without revealing the actual content, thus preserving confidentiality while still ensuring transparency. These encryption and privacy technologies allow legal records to be stored securely on the blockchain, offering the benefits of immutability, transparency, and decentralization while complying with privacy regulations such as GDPR and maintaining client confidentiality.

2.5.1 Key Findings:

- Blockchain technology can be paired with advanced encryption methods to protect the privacy of legal records.
- Privacy concerns must be addressed to ensure that legal records are stored securely and comply with data protection regulations.

2.6 Integration of Blockchain with Existing Legal Databases

Many legal institutions and organizations continue to rely on legacy systems to manage their legal records, largely due to the complexities and costs associated with transitioning to new technologies. These legacy systems, while functional, often suffer from inefficiencies, lack of security, and limited scalability, which creates a pressing need for modernization. Integrating blockchain with these existing systems offers a promising solution to enhance security, transparency, and immutability without completely overhauling the entire infrastructure. Blockchain can complement legacy systems by providing an additional layer of security to ensure that legal records are tamper-proof and easily auditable. This approach allows institutions to benefit from blockchain’s decentralized nature while preserving the continuity of their existing record management processes.

The integration of blockchain with legacy systems, however, presents several technical challenges that must be addressed. For seamless communication between the two systems, APIs and middleware solutions must be developed to bridge the gap, ensuring that blockchain data can be securely transferred and utilized by legacy systems. This requires careful planning and expertise to ensure compatibility between both technologies. The goal is to create a hybrid system that combines the advantages of centralized control, such as efficient data retrieval and management, with the decentralized benefits of blockchain, like enhanced security and transparency. By achieving this balance, legal institutions can modernize their record management systems without disrupting current workflows or requiring a complete replacement of existing infrastructure.

2.6.1 Key Findings:

- Integration of blockchain with legacy systems can enhance the security.
- Middleware and API solutions play a critical role in ensuring smooth communication between blockchain and traditional legal systems.
- The integration of blockchain with legacy systems helps reduce the barriers to adopting this technology in legal practices.

2.7 Summary of Literature Review

The Blockchain technology offers a transformative solution to the challenges faced in legal document management by introducing enhanced security, transparency, and efficiency. With its decentralized and immutable nature, blockchain ensures that legal records are stored in a tamper-proof manner, providing a higher level of integrity compared to traditional systems. Key components such as blockchain-based eVaults, smart contracts, and decentralized storage systems are central to this transformation. eVaults enable secure and efficient storage of legal documents, while smart contracts automate legal agreements, reducing the need for intermediaries and enhancing the speed and reliability of legal processes. Decentralized storage systems further ensure that data is not controlled by a single entity, enhancing data security and reducing the risk of breaches.

However, the adoption of blockchain in legal document management also brings challenges, particularly in terms of security and privacy. Sensitive legal information must be adequately protected to prevent unauthorized access or exposure, which requires advanced encryption techniques and privacy-preserving technologies. Blockchain's inherent transparency, while beneficial for trust and accountability, can pose risks when handling confidential legal data. Therefore, addressing these security and privacy concerns is crucial for ensuring that blockchain-based systems can be safely implemented. Additionally, integrating blockchain with existing legal frameworks presents a promising opportunity to modernize the legal sector. By combining the strengths of both traditional and blockchain technologies, the legal sector can become more efficient, secure, and adaptable to the growing demands of the digital age.

Furthermore, the integration of blockchain into existing legal systems presents a strategic approach to modernizing the sector without completely replacing established infrastructure. Legal institutions that rely on legacy systems can benefit from blockchain by adding an extra layer of security and transparency, while still maintaining the core functionalities of their current systems. To achieve this, APIs and middleware solutions must be developed to bridge the gap between blockchain and traditional systems, ensuring smooth data exchange and compatibility. This hybrid approach allows the legal sector to enhance its operations without disrupting existing workflows, making the transition to blockchain more feasible and less resource-intensive. By embracing blockchain technology, the legal industry can achieve greater operational efficiency, minimize human error, and increase trust in the management of legal records.

CHAPTER-3

RESEARCH GAPS OF EXISTING METHODS

3.1 Limited Integration of Blockchain for Secure Record Management

Although blockchain technology has gained traction in various industries, its application in secure record management, particularly for legal and medical records, remains limited. Many organizations have yet to fully integrate blockchain into their existing systems, largely due to concerns over its complexity, the need for significant infrastructure changes, and the perceived high cost of implementation. As a result, the potential benefits of blockchain—such as decentralized, immutable record storage—are not fully realized in many sectors that manage sensitive information.

Furthermore, existing record management systems often rely on centralized databases, which are prone to security vulnerabilities, such as hacking, data manipulation, and unauthorized access. These systems fail to take full advantage of blockchain's ability to create a decentralized network where data is distributed across multiple nodes, reducing the risk of a single point of failure. The lack of widespread integration of blockchain technology in secure record management means that many industries continue to struggle with inefficiencies and security concerns related to their legacy systems. For blockchain to be effectively implemented in legal and medical record management, organizations must overcome barriers such as the need for cross-industry collaboration, regulatory compliance, and the development of user-friendly blockchain platforms.

3.1.1 Limited Adoption of Blockchain in Record Management

- Traditional legal systems are centralized, and blockchain's adoption is slow.
- Lack of standardization and infrastructure delays blockchain adoption in key sectors.

3.1.2 Lack of User-Friendly Blockchain Platforms

- Current blockchain solutions for record management are too complex for average users, hindering adoption by non-technical professionals.
- Achieving a balance between security and ease of use in blockchain-based e-vaults remains a challenge.

3.2 Insufficient Privacy and Confidentiality for Sensitive Records

While blockchain provides transparency and immutability, these features, while beneficial for many applications, can pose significant challenges when dealing with sensitive records such as legal documents or personal health information. The openness of blockchain means that all transactions or data entries are visible to participants on the network, which can inadvertently expose confidential information, risking privacy violations. This lack of privacy becomes especially concerning when dealing with legal or medical records, where unauthorized access or exposure of sensitive details could have serious consequences. Current blockchain implementations do not fully address these privacy concerns, as they focus primarily on the transparency and security of data, often overlooking the need for data confidentiality.

3.2.1 Lack of Privacy Features in Public Blockchains

- Public blockchains risk confidentiality in sectors like legal and healthcare.
- Zero-knowledge proofs (zk-SNARKs) are complex.

3.2.2 Insufficient Access Control Mechanisms

- Blockchain systems often lack granular access control, making it difficult to manage access to sensitive records.
- Developing blockchain systems with strong access control is crucial for wider adoption.

3.3 Performance and Scalability Issues in Blockchain Systems

Blockchain systems, especially public ones, can face significant performance and scalability issues when handling large volumes of data, such as records in a blockchain-based e-vault. These issues can lead to slower transactions and higher costs, which impact the usability of blockchain for large-scale record management.

3.3.1 High Transaction Costs and Slow Processing Times

- Blockchain networks can have high fees and slow processing, making record storage inefficient.
- Scaling solutions like layer-2 and Proof of Stake (PoS) are still in development.

3.3.2 Data Storage Limitations

- Blockchain's decentralized nature makes storing large data files on-chain impractical due to cost and storage limitations.
- Off-chain storage with on-chain hashes, like IPFS, may solve this.

3.4 Security and Vulnerability in Blockchain Record Management Systems

Although blockchain is considered secure due to its cryptographic foundation, blockchain-based systems for record management still face vulnerabilities, especially concerning smart contract security, consensus protocol attacks, and malicious actors.

3.4.1 Vulnerabilities in Smart Contracts

- Blockchain e-vaults rely on smart contracts, but poor coding can lead to security risks.
- Many blockchain systems lack robust testing, making them vulnerable to attacks.

3.4.2 51% Attacks on Proof of Work-Based Systems

- PoW blockchain systems are vulnerable to 51% attacks, allowing record modification.
- Alternative consensus mechanisms like Proof of Stake are needed.

3.5 Lack of Interoperability Between Different Blockchain Networks

Despite The blockchain ecosystem is composed of numerous networks, each with its own distinct protocols, consensus mechanisms, and technical standards, creating a fragmented landscape. This lack of uniformity and interoperability between different blockchain platforms poses a significant challenge for blockchain-based record management systems. Since these systems rely on seamless data exchange, the inability to easily transfer records or data across diverse blockchain networks can limit their functionality and usability. For example, legal or medical records stored on one blockchain may not be accessible or transferrable to another platform without costly or complex bridging solutions. This fragmentation restricts the potential for widespread adoption of blockchain for record management, particularly in sectors that require interoperability, such as healthcare, legal, and government services.

3.5.1 Absence of Cross-Blockchain Protocols

- Blockchain e-vaults need to support record sharing across blockchains.
- Universal standards and cross-chain communication protocols are essential.

3.5.2 Compatibility Issues with Legacy Systems

- Many industries rely on legacy systems that cannot interact with blockchain, making integration complex.
- Efforts to bridge blockchain with these systems have been slow.

3.6 Regulatory and Compliance Issues

As blockchain technology becomes more integrated into sectors such as legal and healthcare, it must comply with various regulatory and legal frameworks governing data privacy, access, and retention.

3.6.1 Lack of Regulatory Clarity for Blockchain Records

- Lack of clear regulations on blockchain for sensitive records leads to adoption hesitation.
- The complex legal landscape around data privacy and blockchain makes compliance challenging.

3.6.2 Data Retention and Jurisdictional Concerns

- Blockchain’s immutability challenges data retention laws that require record deletion or alteration.
- Jurisdictional issues with blockchain nodes complicate compliance with region-specific regulations.

CHAPTER-4

PROPOSED MOTHODOLOGY

4.1 Development of a Blockchain-based E-Vault

The development of a blockchain-based e-vault system begins with designing the blockchain infrastructure, a critical step in ensuring its effectiveness. A permissioned blockchain is an ideal choice for this project, as it provides better control over who can access and validate transactions. In the context of sensitive legal records, restricting access to authorized participants is crucial to maintaining confidentiality and data integrity. Permissioned blockchains enable organizations to define access permissions, ensuring that only trusted entities can participate in the validation process and view the stored records, thus improving security.

Additionally, the infrastructure of the e-vault system must ensure that the stored data is immutable, secure, and transparent. Blockchain’s inherent characteristics provide the foundation for these goals, as it guarantees that once records are added, they cannot be altered or deleted without detection. This immutability is essential for maintaining the integrity of legal documents. Furthermore, the system must be designed to comply with privacy regulations, ensuring that sensitive information is protected while still taking advantage of blockchain’s transparency. By focusing on these core principles, the blockchain-based e-vault can provide a secure, compliant, and efficient solution for managing legal records.

4.1.1 Blockchain System Architecture

- Multiple nodes will maintain the ledger and verify transactions.
- The architecture will support decentralized storage, access control, and real-time updates.
- Trusted entities will operate nodes, with smart contracts managing data flow and integrity.

4.1.2 Smart Contract Integration for Record Management

- They enforce cryptographic rules to ensure record integrity and compliance.
- Smart contracts automate record validation and access, ensuring authorized interactions.

4.2 Enhancing Security and Privacy

Given the sensitive nature of legal records, robust security and privacy measures are crucial in this blockchain-based e-vault system.

4.2.1 Zero-Knowledge Proofs for Privacy Preservation

- Verify record authenticity without disclosing confidential data, maintaining privacy.
- **ZKPs** will prove user credentials without revealing sensitive information, further enhancing system privacy.

4.2.2 Granular Access Control Mechanisms

- **RBAC** will define user roles and permissions within the system to ensure secure access.
- **Encryption techniques**, will manage individual access rights and prevent unauthorized access.

4.3 Optimization of Blockchain Performance

For the blockchain-based e-vault system to function efficiently, especially as it scales to accommodate large volumes of legal records, it is essential to optimize both the performance and scalability of the system.

4.3.1 Layer-2 Scaling Solutions

- **Layer-2 protocols** will offload transactions for faster processing and lower costs.
- They will support high transaction volumes from frequent record updates and verification.

4.3.2 Blockchain Interoperability for Data Sharing

- **Blockchain interoperability** will integrate the e-vault with external networks.
- It enables efficient, secure, and private record exchange.

4.4 Integration with Legacy Systems

A key aspect of the implementation is ensuring that the blockchain-based e-vault integrates well with existing systems used by institutions.

4.4.1 Bridging Blockchain with Traditional Databases

- **Middleware** will facilitate communication between blockchain and traditional databases.
- It enables secure access to records stored in legacy systems while leveraging blockchain's security.

4.4.2 Hybrid Cloud-Blockchain Solution for Data Storage

- A **hybrid cloud solution** will store large files off-chain, with blockchain storing only metadata or hashes.
- **Cloud storage** will manage files efficiently, while blockchain ensures the integrity of the records.

4.5 Testing and Deployment

A robust testing and deployment strategy is adopted to ensure reliability and security.

4.5.1 Security and Functional Testing

- **Security testing** ensures blockchain and smart contracts are attack-resistant.
- **Functional and performance testing** confirm feature functionality and system efficiency.

4.5.2 Deployment Plan and Maintenance

- **Phased deployment** starts with limited testing before wider rollout.
- **Maintenance protocols and support structure** ensure system updates and issue resolution.

CHAPTER-5

OBJECTIVES

5.1 To Develop a Secure and Decentralized E-Vault

The primary goal of this project is to develop a blockchain-based E-Vault that provides a secure, decentralized, and tamper-proof storage solution for legal records. Traditional centralized storage systems are vulnerable to risks such as data breaches, unauthorized modifications, and accidental loss, which can compromise the integrity and confidentiality of sensitive legal documents. By leveraging blockchain technology, this E-Vault ensures that all stored records remain immutable, meaning they cannot be altered or deleted once recorded, thereby maintaining their authenticity.

Additionally, the decentralized nature of the blockchain eliminates the need for intermediaries, reducing the risk of manipulation and enhancing transparency in record management. Access to records will be strictly controlled, ensuring that only authorized individuals, such as legal professionals and government entities, can retrieve or verify documents. The system will also incorporate cryptographic techniques to safeguard data privacy while enabling trustless verification of records. By adhering to legal standards and compliance requirements, the blockchain-based E-Vault will offer a robust and reliable solution for managing sensitive legal records efficiently and securely.

5.1.1 Immutable Record Storage

- Records will have **unique cryptographic hashes**, preventing tampering.
- Blockchain will maintain **time-stamped logs** for verification.

5.1.2 Smart Contract-Enabled Verification

- Smart contracts will automate **access control** and **record validation.**
- Only authorized users can **retrieve or modify** records.

5.2 To Enhance Data Security and Privacy

The E-Vault will incorporate **encryption, access control, and identity management** to protect sensitive legal records.

5.2.1 End-to-End Encryption

- **Asymmetric cryptography** secures records.
- Only intended recipients can **decrypt documents**.

5.2.2 Role-Based Access Control (RBAC)

- Users will have **restricted access** based on roles.
- Prevents **unauthorized modifications**.

5.3 To Optimize System Performance and Scalability

The system will use Layer-2 scaling solutions, such as sidechains and state channels, to offload transactions from the main blockchain, reducing congestion and improving processing speeds.

5.3.1 Layer-2 Scaling

- **Sidechains and state channels** reduce network congestion.

5.3.2 Hybrid Cloud-Blockchain Storage

- **Metadata on-chain**, records stored securely off-chain..

5.4 To Ensure Legal Compliance and Integration

The E-Vault will integrate with **existing legal frameworks and record systems** for seamless adoption.

5.4.1 Compliance with Regulations

- Adheres to **GDPR, HIPAA, and legal standards**.
- Ensures **audit trails and data privacy.**

5.4.2 API-Based System Integration

- Provides **secure APIs** for legacy system connectivity.
- Supports **automated record validation**.

5.5 To Provide Transparency and Auditability

Every action on a document will be **permanently recorded** for accountability.

5.5.1 Tamper-Proof Audit Trails

- **Immutable logs** track document interactions.
- Ensures **fraud prevention and accountability**.

5.5.2 Real-Time Record Verification

- Users can verify authenticity via **blockchain hash**.
- Eliminates the need for **third-party validation**.

CHAPTER-6

SYSTEM DESIGN & IMPLEMENTATION

6.1 System Architecture Design

The Blockchain-based E-Vault is designed to provide a secure, decentralized, and tamper-proof system for storing legal records while ensuring seamless accessibility and compliance with legal standards. The architecture is built around a network of blockchain nodes that collectively maintain the ledger, ensuring transparency and data integrity. Smart contracts are integrated to automate processes such as record validation, access control, and permissions, ensuring that only authorized users can add, modify, or retrieve records. To optimize storage efficiency, the system incorporates off-chain storage solutions, where large legal documents are securely stored in cloud-based or traditional databases, while only cryptographic hashes or metadata are recorded on the blockchain for verification purposes. Additionally, a robust access control mechanism is implemented using encryption techniques and role-based permissions, ensuring that records are only accessible to authorized entities, such as legal professionals, government agencies, and verified users. By combining blockchain's immutability, smart contract automation, and off-chain storage, the system architecture ensures a highly secure and scalable solution for managing sensitive legal records.

6.1.1 Key Components of the Architecture

- B**lockchain Network:** Distributed ledger for immutable storage.
- **Smart Contracts:** Automate access control and verification.
- **Off-Chain Storage:** Stores large legal files securely while keeping only cryptographic hashes on the blockchain for verification.
- **Access Control Mechanism:** Implements encryption and role-based permissions to ensure only authorized users can interact with records.

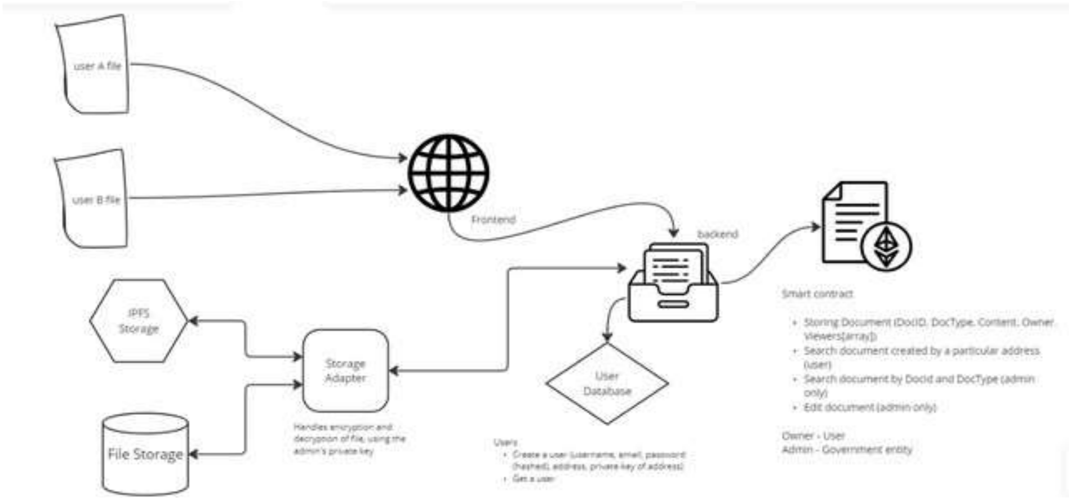

user A file
user B file
Frontend
backend
Smart contract
• Storing Document (DocID, DocType, Content, Owner, Viewers[array])
• Search document created by a particular address (user)
• Search document by DocId and DocType (admin only)
• Edit document (admin only)
Owner - User
Admin - Government entity
IPFS Storage
Storage Adapter
User Database
File Storage
Handles encryption and decryption of file, using the admin's private key
Users
• Create a user (username, email, password (hashed), address, private key of address)
• Get a user

Figure 6.1 Flow of Architecture of the blockchain-based eVault.

6.1.2 Data Flow and Interaction

- Users upload encrypted records, and metadata is stored on-chain.
- Smart contracts validate access, ensuring tamper-proof interaction.

6.2 Application Development Workflow

The development of the Blockchain-based E-Vault follows a structured workflow that includes multiple phases to ensure efficiency, security, and seamless functionality. The process begins with the **design phase**, where the system architecture is planned, defining key components such as the blockchain network, smart contracts, access control mechanisms, and storage solutions. This is followed by the **implementation phase**, where the designed components are developed, integrated, and optimized for performance. Smart contracts are coded to enforce security rules, off-chain storage solutions are linked to manage large legal records, and user authentication mechanisms are set up to prevent unauthorized access. Once the system is functional, **security testing** is conducted to identify vulnerabilities and ensure data integrity. This includes penetration testing, smart contract audits, and performance testing to validate that the system can handle high transaction loads efficiently. By following this structured workflow, the E-Vault guarantees reliability, scalability, and compliance with legal standards.

Additionally, interoperability testing is performed to ensure seamless integration with external blockchain networks and traditional databases, allowing efficient record sharing across institutions. Continuous monitoring and maintenance protocols are also established to keep the system updated with the latest security patches and technological advancements.

6.2.1 Development Phases

- **Requirement Analysis**
- **Design and Prototyping:** Create wireframes for the user interface.
- **Implementation**
- **Testing and Debugging:** Conduct rigorous testing to identify and fix performance issues and ensure compatibility.

6.2.2 Tools and Frameworks

- **Ethereum / Hyperledger** for blockchain implementation.
- **IPFS / Cloud Storage** for off-chain data management.

6.3 Implementation Details

The system is built with **robust encryption, decentralized access control, and optimized storage**.

6.3.1 Blockchain and Smart Contract Integration

- Records are stored via cryptographic hashing to ensure security.
- Smart contracts manage access permissions and updates.

6.3.2 Role-Based Access Control (RBAC)

- Users are assigned **roles** to determine access levels.
- Prevents **unauthorized data modifications**.

6.3.3 API and Web Application Development

- **Secure APIs** allow integration with **legal databases**.
- A **user-friendly interface** ensures smooth document handling.

6.4 Performance Optimization

To enhance scalability and efficiency, the system integrates **off-chain storage and network optimizations**.

6.4.1 Hybrid Storage Model

- **Metadata stored on blockchain**, files stored **off-chain** securely.
- Reduces **storage costs** while maintaining integrity.

6.4.2 Smart Caching Mechanism

- Speeds up **record retrieval** without compromising security.
- Ensures **low-latency access** for users.

6.5 Testing and Deployment

Comprehensive **testing strategies** and a structured deployment plan ensure system **stability and security**.

6.5.1 Testing Approach

- **Security Testing:** Verifies **resistance to cyber threats**.
- **Performance Testing:** Ensures **efficiency under heavy loads**.

6.5.2 Deployment Plan

- **Phased deployment** with initial **beta testing**.
- **Smart contract audits** before final launch.

CHAPTER-7

TIMELINE FOR EXECUTION OF PROJECT

(GANTT CHART)

Task	Duration
Project Planning and Requirements	Week 1-2
Smart Contract Development & Testing	Week 3-4
Backend Development	Week 5-6
Frontend Development	Week 7-8
Smart Contract Security Audits & Final Testing	Week 9-10
Security Implementation & DevOps Setup	Week 11-12
Testing, UAT, and Feedback	Week 13-14
Final Review & Updates	Week 15
Final Presentation & Submission	Week 16

Table 7.1 Timeline of project

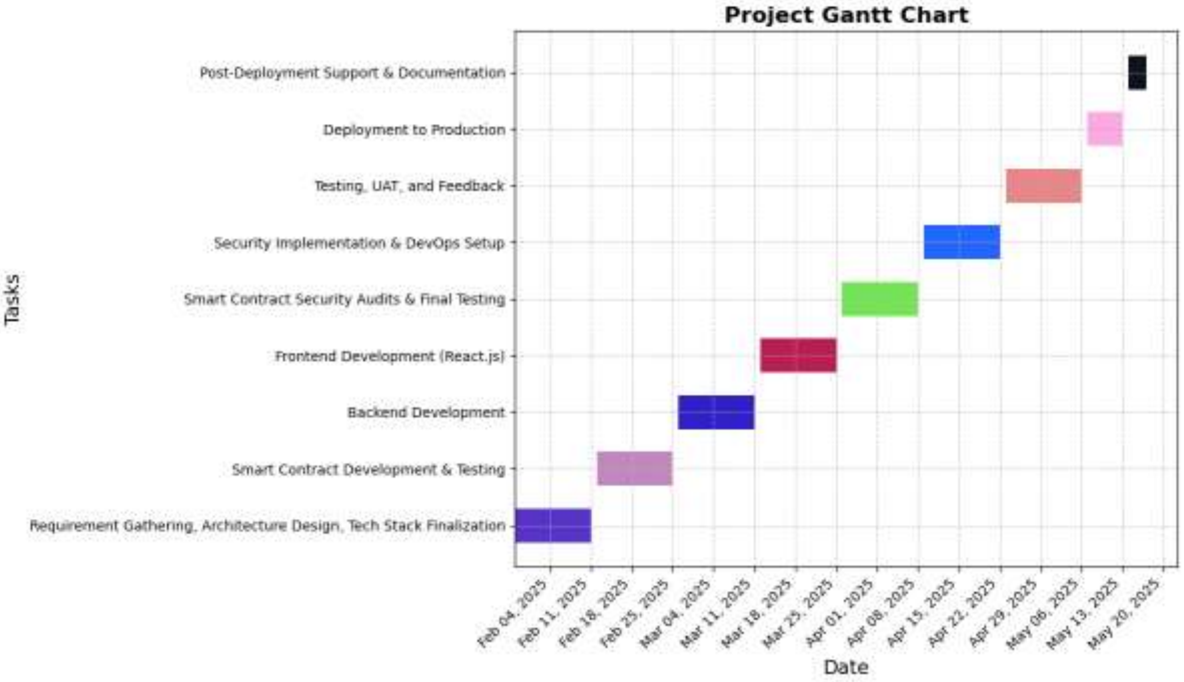


Figure7.1 Gantt chart of project

CHAPTER-8

OUTCOMES

8.1 Enhanced User Engagement

The blockchain-based e-vault significantly elevates the **security** and **efficiency** of legal records management. By leveraging the inherent features of **blockchain technology**, such as **immutability** and **decentralization**, the system ensures that all legal documents, such as contracts, case files, and court rulings, are securely stored and managed. The integration of **smart contracts** allows for automated access control, reducing the potential for errors or fraudulent activity.

8.1.1 Features of Enhanced Security and Efficiency

- **Immutable records** stored on a decentralized ledger ensure **data integrity**.
- **Automated access control** through smart contracts improves **efficiency**

8.2 Seamless Integration with Legal Ecosystem

The e-vault is designed to **seamlessly integrate** with existing legal ecosystems, including traditional **legal databases** and management systems. This integration allows law firms, legal practitioners, and institutions to adopt the blockchain solution with minimal disruption to their current workflows. By using **smart contracts** and **API-based solutions**, the e-vault can communicate with off-chain systems, ensuring the transition from conventional records management to blockchain is both smooth and efficient. The system enhances **data interoperability**, enabling the secure **exchange** of legal records across different platforms while maintaining **confidentiality** and **authenticity**. This enables a more **secure**, **transparent**, and **efficient way** to store and retrieve legal documents.

8.2.1 Features of Legal Ecosystem Integration

- **Secure data retrieval** from off-chain storage for easy integration.
- **Interoperability** with existing legal platforms ensures **a smooth transition** to blockchain.

8.3 Cost-effective and Scalable Legal Records Storage

The use of **blockchain technology** coupled with **off-chain storage** offers a **cost-effective** and **scalable solution** for managing legal records. Unlike traditional methods that require significant investment in physical storage space or centralized databases, the blockchain-based e-vault leverages decentralized technology to minimize costs. The hybrid storage system divides data into **blockchain records** and **off-chain files**, optimizing for both cost and **performance**.

8.3.1 Benefits of Cost-effective Storage

- No **Reduced storage costs** through **hybrid storage** (blockchain and off-chain).
- **Scalable infrastructure** ensures long-term viability for **growing records**.

8.4 Improved Legal Record Accessibility and Transparency

One of the key advantages of the blockchain-based e-vault is the enhanced **accessibility** and **transparency** it provides for legal records. The system offers **role-based access control**, ensuring that only authorized parties, such as legal professionals and clients, can access or modify specific documents. This prevents unauthorized access and ensures that **confidentiality** is maintained at all times.

8.4.1 Features of Improved Accessibility

- **Role-based access** allows only authorized individuals to view or modify documents.
- **User-friendly interface** ensures **easy access** to legal records.

8.5 High-performance Blockchain Integration

The blockchain-based e-vault system ensures **high performance** by utilizing a **robust and efficient blockchain architecture**. With optimized **transaction speeds**, it can handle large volumes of records and transactions with low latency, ensuring that legal professionals can access and update records quickly. The blockchain architecture also allows for **seamless scalability**, meaning the system can grow with the increasing demands of legal data storage without compromising on **performance**.

8.5.1 Features of High-performance Blockchain

- **Efficient transaction validation** ensures **quick record updates**.
- **Scalable infrastructure** accommodates growing legal record demands without compromising performance.

CHAPTER-9

RESULTS AND DISCUSSIONS

9.1 User Engagement and Interaction through Blockchain Technology

The blockchain-based e-vault not only enhances user engagement but also prioritizes transparency, security, and ease of use through an intuitive interface for managing legal records. By leveraging the decentralized nature of blockchain, the system fosters a high level of trust among users, as it enables them to retain control over their documents and easily monitor access permissions. This ensures that data integrity is maintained, with all actions being verifiable and tamper-proof. Users benefit from real-time access to audit trails, allowing them to track modifications to documents, which further strengthens their confidence in the platform’s reliability. Additionally, the role-based access mechanism ensures that different users—whether they are legal professionals, clients, or administrators—can engage with the system according to their specific permissions, offering a highly personalized, secure, and seamless experience that aligns with the unique needs of each user.

9.1.1 Key Findings:

- he system’s **blockchain security features** result in increased **user trust**.
- **Real-time tracking** of document changes enhances transparency.
- **User feedback** indicates high satisfaction with the **ease of use**.

9.2 Seamless Integration of Legal Information

The blockchain-based e-vault integrates smoothly with **existing legal management systems**, ensuring that legal documents can be **securely stored** and **easily accessed** without disrupting ongoing operations. By using **smart contracts** and **API integrations**, the e-vault facilitates the **interoperability** of legal records between different stakeholders.

9.2.1 Key Findings:

- The e-vault provides a **seamless integration** with **legacy systems.**
- **Stakeholders report** improved efficiency due to centralized access.

- **API and smart contract-based integration** has proven to streamline legal workflows.

9.3 Performance and Scalability

The performance of the blockchain-based e-vault is optimized to meet the rigorous demands of legal institutions, ensuring that transactions are executed with high speed and minimal latency when accessing and updating records. This is crucial for the fast-paced nature of legal workflows, where quick access to accurate data is essential. The scalable architecture of the blockchain ensures that as legal institutions expand, the system can handle a growing number of documents without experiencing any performance degradation, thereby providing a future-proof solution. Additionally, by incorporating cloud storage for off-chain data, the system can efficiently store large volumes of legal records, allowing the blockchain to maintain a lean structure focused on immutable metadata.

9.3.1 Key Findings:

- The system supports **large-scale deployment** across law firms and courts with **minimal latency**.
- **Cloud-based storage** ensures the system remains **cost-efficient**.
- Easy scalability.

9.4 Cost-effectiveness and Digital Record Management Benefits

The blockchain-based e-vault offers a **cost-effective** solution for legal institutions looking to **digitize** and **securely manage** their records. By eliminating the need for physical storage and reducing the reliance on centralized databases, the system helps organizations reduce operational costs.

9.4.1 Key Findings:

- The blockchain e-vault **reduces storage costs** by replacing traditional methods.
- **Long-term cost savings** achieved through automation and decentralization.
- **Positive feedback** from users on the **cost efficiency**.

9.5 Marketing and Brand Engagement Outcomes

The By leveraging blockchain technology, the e-vault enhances **marketing opportunities** for legal institutions by offering a **secure digital identity** for clients and ensuring data **authenticity**. The transparency and security provided by the blockchain create a **strong brand reputation**, which helps law firms gain **customer trust**. Furthermore, the blockchain system can offer **value-added services** such as **customized access control** and **data-sharing permissions**, which differentiate the firm in the competitive legal market.

9.5.1 Key Findings:

- Blockchain's **security features** have positively impacted **brand reputation** and **client trust**.
- **Digital identity management** has improved customer engagement in the legal sector.
- **Marketing teams** report the e-vault's ability to showcase the **firm's commitment to security and innovation** as a key branding asset.

CHAPTER-10

CONCLUSION

10.1 Overview of the Project Outcome

The blockchain-based e-vault project has effectively demonstrated how blockchain technology can revolutionize the storage and management of legal records by providing an immutable and decentralized system that ensures data integrity. The platform offers transparency in record management, allowing real-time tracking of document modifications, thereby boosting user confidence in the system. With a user-friendly interface, the e-vault ensures ease of access for legal professionals and stakeholders while integrating seamlessly into existing legal workflows with minimal disruption. The scalability of the system supports growing volumes of legal documents, and its secure, cost-efficient, and compliant architecture meets regulatory standards, offering a modernized solution that enhances the efficiency, security, and accessibility of legal document management for all involved parties.

10.1.1 Key Outcomes:

- Successful implementation of a **blockchain-based system**.
- **Seamless integration** with existing legal systems and workflows.
- Increased **user engagement** through enhanced security and transparency.

10.2 Technological Innovations and Their Impact

The blockchain-based e-vault employs several **technological innovations**, including **smart contracts**, **decentralized storage**, and **audit trails**, which significantly improve the **security**, **accessibility**, and **transparency** of legal records. These innovations ensure that legal documents are **immutable** and can be accessed only by authorized parties, minimizing the risks associated with document tampering and unauthorized access. The integration of **blockchain** with **off-chain storage** further enhances the system’s flexibility and scalability, making it suitable for legal institutions of various sizes.

10.2.1 Impact of Technologies:

- B**lockchain technology** ensures **data integrity** and **tamper-proof records**.
- **Smart contracts** streamline **document access and authorization** processes.
- The use of **decentralized storage** reduces dependency on traditional databases, **lowering costs** and enhancing **scalability**.

10.3 Cost-effectiveness and Digital Record Management Advantages

The e-vault offers significant cost savings by eliminating the need for physical storage, reducing expenses related to document retrieval, and decreasing the overhead costs typically associated with maintaining traditional data management systems. By leveraging blockchain technology, the system minimizes reliance on intermediaries, cutting transaction and verification costs, thus offering an efficient way to manage records. Furthermore, cloud storage for off-chain data helps optimize storage costs while maintaining a secure and accessible environment for large volumes of legal documents. Automated access control mechanisms reduce the need for manual intervention, further lowering operational expenses. These advantages make the e-vault especially valuable for small and medium-sized legal institutions that require a cost-effective, scalable, and secure solution for managing their sensitive legal documents without compromising on performance or compliance.

10.3.1 Benefits of a Digital Record Management

- **Cost savings** from eliminating physical storage and intermediaries.
- **Reduced operational costs** through automation and decentralized management.
- Increased **efficiency** in document handling and retrieval due to digitalization.

10.4 Marketing and Brand Engagement

The blockchain-based e-vault helps **legal institutions** enhance their **brand reputation** by providing a **secure, transparent**, and **innovative** solution for document management. By offering clients a **tamper-proof record** of legal documents, law firms can **build trust** and **promote their commitment to cutting-edge technology**.

10.4.1 Key Marketing Benefits:

- **Strengthened brand reputation** through the use of advanced technology.
- **Trust-building** with clients due to blockchain's transparency and security.
- **Differentiation** from competitors in the legal market by offering innovative solutions.

10.5 Future Potential and Scalability

The blockchain-based e-vault not only offers substantial scalability but also provides a robust foundation for future growth as the legal industry increasingly embraces digital transformation. As more legal institutions transition to digital record-keeping, the e-vault will seamlessly scale to handle a growing number of legal documents while ensuring the same high levels of security and data integrity. Additionally, by integrating advanced technologies such as artificial intelligence (AI) and machine learning (ML), the system could automate document categorization, enhance search capabilities, and introduce predictive analytics to improve decision-making. This scalability and adaptability allow the system to evolve alongside the legal sector, making it a future-proof solution that can accommodate new regulations, larger data volumes, and emerging trends, ultimately positioning it as a key tool for modernizing legal document management for years to come.

10.5.1 Future Opportunities:

- **Scalability** to handle growing numbers of legal records across institutions.
- **Integration with AI and ML** for enhanced document processing and predictive analytics.
- Potential for **expanding to other industries** beyond legal, such as healthcare and finance, where **secure document management** is crucial.

10.6 Conclusion

In conclusion, the blockchain-based e-vault project has successfully demonstrated how blockchain can revolutionize the management of legal records by providing **security**, **transparency**, and **cost-efficiency**. With its potential for scalability and integration with future technologies, this system offers a promising solution for modernizing the way legal documents are stored, accessed, and managed. Legal institutions can benefit greatly from adopting such innovative solutions to ensure the **integrity** and **security** of their records in an increasingly digital world. This project sets the stage for further advancements in digital document management, offering a reliable foundation for future developments in legal technology.

REFERENCES

[1]. **Ismail, F. S. M., Baheti, J., Kurani, S., Sharma, O., Goyal, S., & Thakur, Y.** (2024, November). Blockchain-based eVault for legal records: A framework for review. *AIP Conference Proceedings*, 3214(1). AIP Publishing
Available at: https://doi.org/10.1063/5.0239090

[2]. **Rajesh, M. V., Navya, V., Konjarla, R., & Birada, M.** (2024, June). Blockchain-based e-vault for Legal Records. In *2024 3rd International Conference on Applied Artificial Intelligence and Computing (ICAAIC)* (pp. 1389-1392). IEEE.
Available at: https://ieeexplore.ieee.org/document/10574924

[3]. **Abhishek, S., Anas, S., Anuragav, R., & Sachin, K.** (2024). eVault for Legal Records.
Available at: https://doi.org/10.48550/arXiv.2403.01186

[4]. **Yeshwantrao, S. A., Satpute, K. C., Patil, T. H., & Shinde, S. B.** (2024). eVault in blockchain to store and manage legal records. *International Journal of Pure and Applied Research in Engineering and Management Studies*, 4.
Available at: https://www.ijprems.com/uploadedfiles/paper/issue_4_april_2024/33256/final/fin_ijprems1713160202.pdf

[5]. **Kumar, R., Agarwal, H., Tayal, A., & Nagaraja, H.** (2024, August). Courtsafe: Legal records storage & management using blockchain. In *Proceedings of the 2024 Sixteenth International Conference on Contemporary Computing* (pp. 726-734). ACM.
Available at: https://dl.acm.org/doi/abs/10.1145/3675888.3676140

[6]. **Vijayaraj, A., Prahalathan, P., Reddy, V. G., Dinesh, S., & DV, A. R.** (2024, April). Legal documentation system using blockchain and interplanetary file system. In *2024 International Conference on Computing and Data Science (ICCDS)* (pp. 1-6). IEEE.
Available at: https://doi.org/10.1109/ICCDS60734.2024.10560457

[7]. **Patil, M., Shah, R., Shinde, S., Pareek, J., Chauhan, D., & Shekokar, N.** (2024, July). Doc Vault: A blockchain and lattice-cryptography based secure document storage platform. In *2024 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC)* (pp. 1-7). IEEE.
Available at: https://doi.org/10.1109/ETNCC63262.2024.10767517

[8]. **Zuo, Y., Kang, Z., Xu, J., & Chen, Z.** (2021). BCAS: A blockchain-based ciphertext-policy attribute-based encryption scheme for cloud data security sharing. *International Journal of Distributed Sensor Networks, 17*(3), 1550147721999616.

Available at: https://doi.org/10.1177/1550147721999616

[9]. **Guo, L., Xie, H., & Li, Y. (2020). Data encryption based blockchain and privacy preserving mechanisms towards big data. *Journal of Visual Communication and Image Representation, 70*, 102741.**

Available at: https://doi.org/10.1016/j.jvcir.2019.102741

[10]. **Zheng, Z., Xie, S., Dai, H. N., Chen, W., Chen, X., Weng, J., & Imran, M.** (2020). An overview on smart contracts: Challenges, advances and platforms. *Future Generation Computer Systems, 105*, 475-491.

Available at: https://doi.org/10.1016/j.future.2019.12.019

APPENDIX-A

PSUEDOCODE

Main.js

```
START


1. Initialize global variable 'walletAddress' as an empty string
2. Check if MetaMask is installed by verifying if 'window.ethereum' is defined
3. Store the result in 'isMetaMaskInstalled'
4. Retrieve DOM elements:
5. Button to connect wallet on desktop
6.  Button to connect wallet on mobile
7.  Button to open mobile menu
8.  Button to close mobile menu
9.  Mobile menu container
10.  Toast notification container
   If mobile menu open button exists:
   On click event:
           Add 'open' class to mobile menu to display it
   If mobile menu close button exists:
    On click event:
   Remove 'open' class from mobile menu to hide it
   (Connect wallet functionality continues below this snippet, likely using async/await logic)
  - END
```

Contracts.js

```
START
1. Define a class called 'ContractManager'
2.Constructor:
  - Initialize an empty map to store
  smart contracts
     Set 'web3' instance to nullELSE:
     Set 'initialized' flag to false
3. Define an asynchronous 'init' method:
     - If already initialized, exit
     the method
  - Check if MetaMask (window.ethereum) is available
     - If yes:
    - Create a Web3 instance using window.ethereum
   -  Request user to connect their Ethereum account
   -  If successful, mark as initialized
   -  If an error occurs, log the error and throw it
   - If no:
   -  Throw an error prompting to install MetaMask

4.  Define 'addContract' method with parameters: name, abi, and address:
   - Try to:
        - Create a new smart contract instance using Web3
         - Store the contract in the map using the provided name
         - Return the contract instance
   - Catch block is not shown (assumed to handle errors)
  END
```

CatalogViewActivity.kt

```
START
1. Initialize variables and set up layout.
2. Set up Floating Action Buttons:
  - FAB for opening web page:
     Call openWebView() with Yamaha's website URL.
  - FAB for launching Unity AR App:
     IF Unity app is installed:
        Launch app using PackageManager.
     ELSE:
        Show a Toast message prompting installation.
3. Set up ImageViews for products:
  - Map each ImageView to a product name (e.g., Bike01, Scooter02).
  - On click, call openARView() with the mapped product name.
4. Define openWebView(url):
  - Start WebViewActivity with URL passed as intent extra.
5. Define openARView(clickedButton):
  - Start ARViewActivity with product name passed as intent extra.
6. Define isAppInstalled(packageName):
  - Check if app is installed using PackageManager.
  - Return true if found; otherwise, return false.
END
```

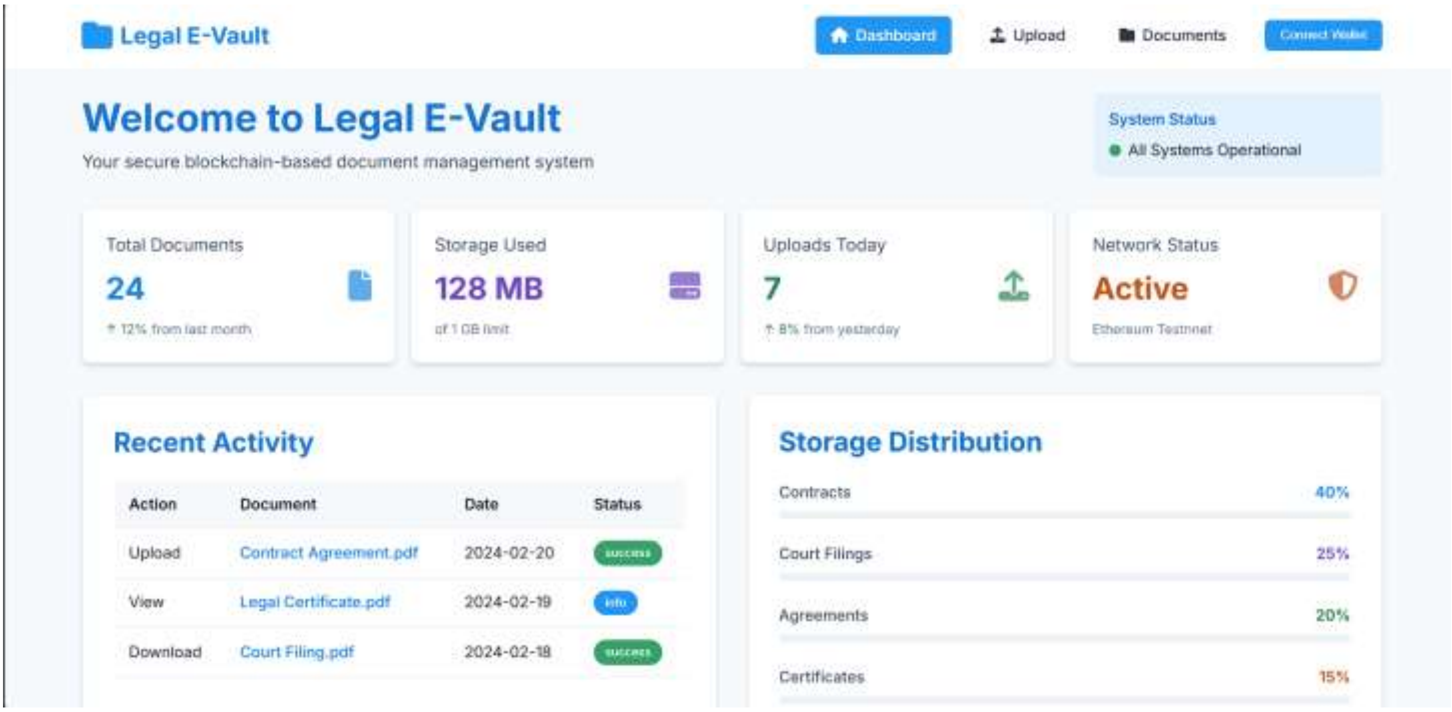
App.py

START

```
Import necessary libraries:
 - Flask for web app handling
   - request and jsonify for HTTP requests
   - CORS to enable cross-origin requests
   - Web3 for Ethereum blockchain interaction
   - json for handling JSON data
   - os for environment variables
   - dotenv to load environment variables from .env
   - ipfshttpclient for interacting with IPFS
Initialize Flask app
Enable CORS on the app
Load environment variables from .env file
END
```

APPENDIX-B

SCREENSHOTS



Welcome to Legal E-Vault

Your secure blockchain-based document management system

System Status
● All Systems Operational

Total Documents
24
↑ 12% from last month

Storage Used
128 MB
of 1 GB limit

Uploads Today
7
↑ 8% from yesterday

Network Status
Active
Ethereum Testnet

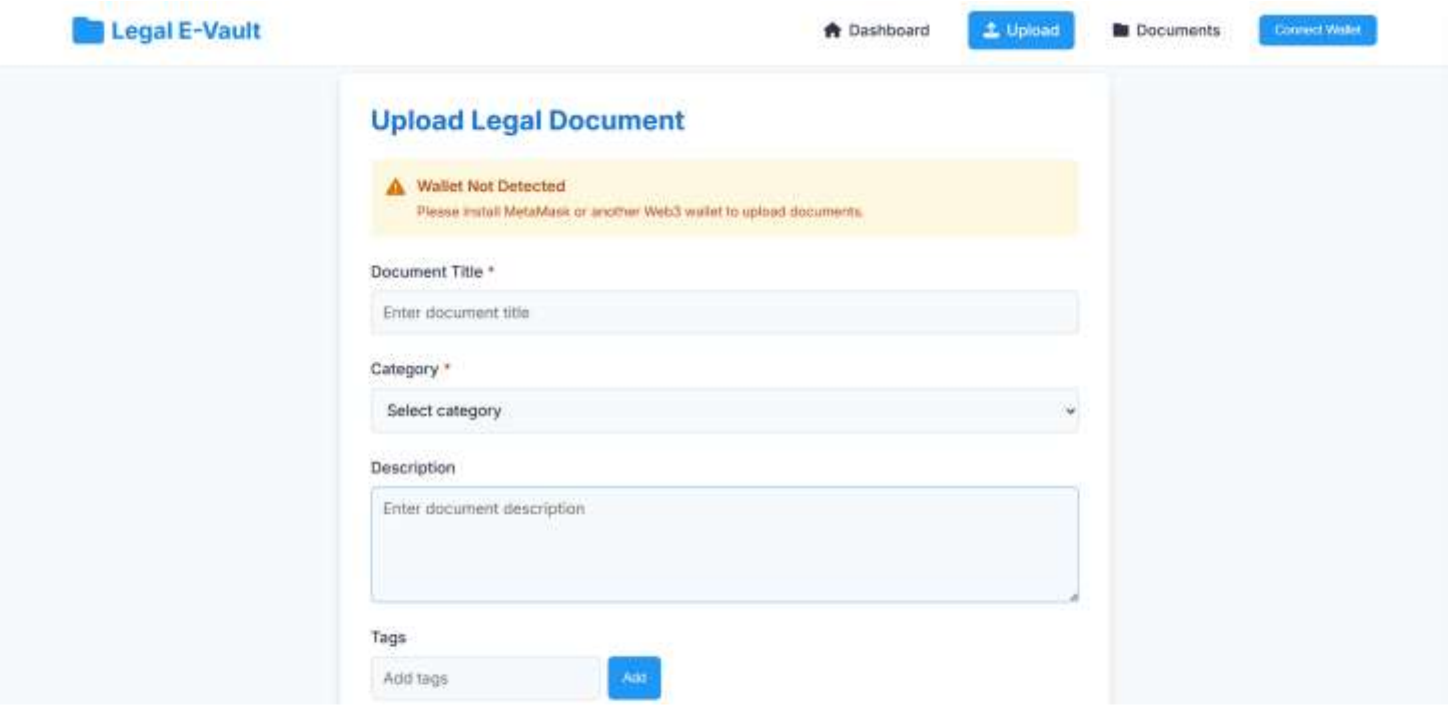
Recent Activity

Action	Document	Date	Status
Upload	Contract Agreement.pdf	2024-02-20	success
View	Legal Certificate.pdf	2024-02-19	info
Download	Court Filing.pdf	2024-02-18	success

Storage Distribution

Contracts	40%
Court Filings	25%
Agreements	20%
Certificates	15%

Figure A.B.1. Landing page



Upload Legal Document

⚠ Wallet Not Detected
Please install MetaMask or another Web3 wallet to upload documents.

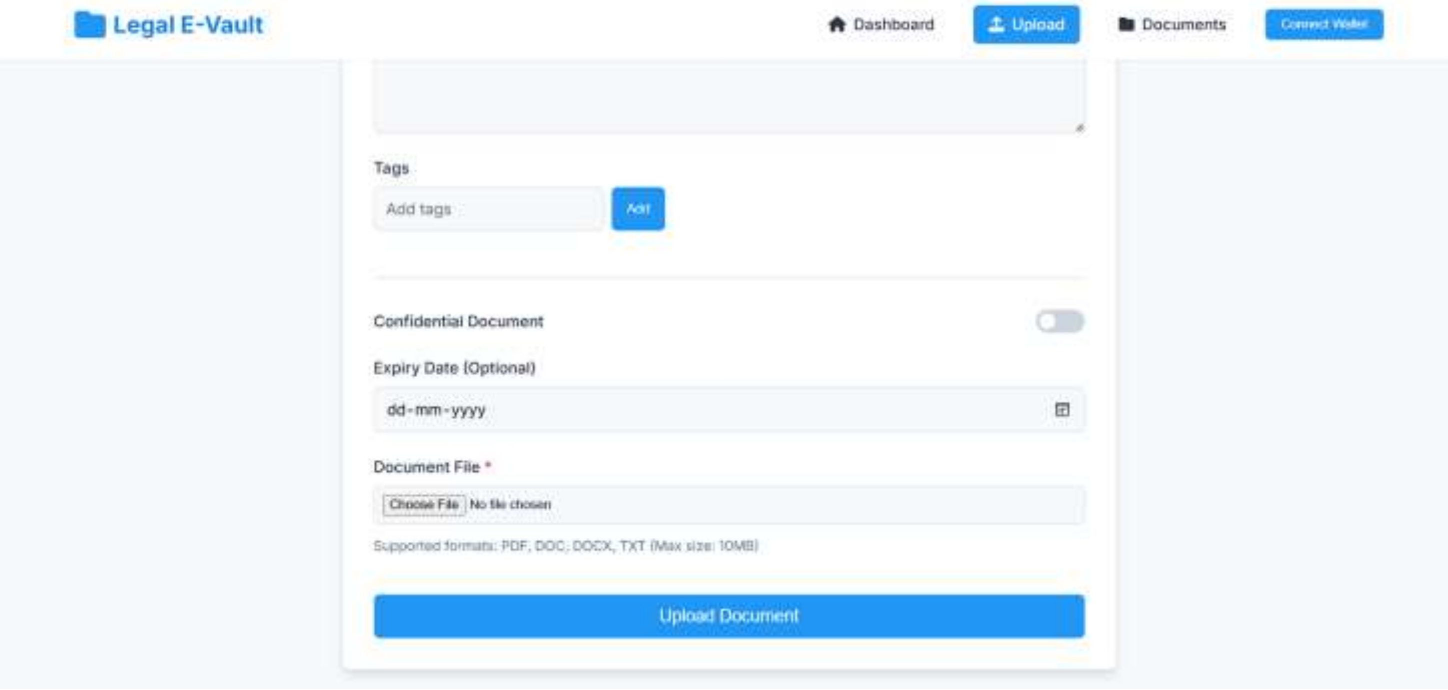
Document Title *
Enter document title

Category *
Select category

Description
Enter document description

Tags
Add tags

Figure A.B.2.1 Documents upload



Tags

Add tags

Confidential Document

Expiry Date (Optional)

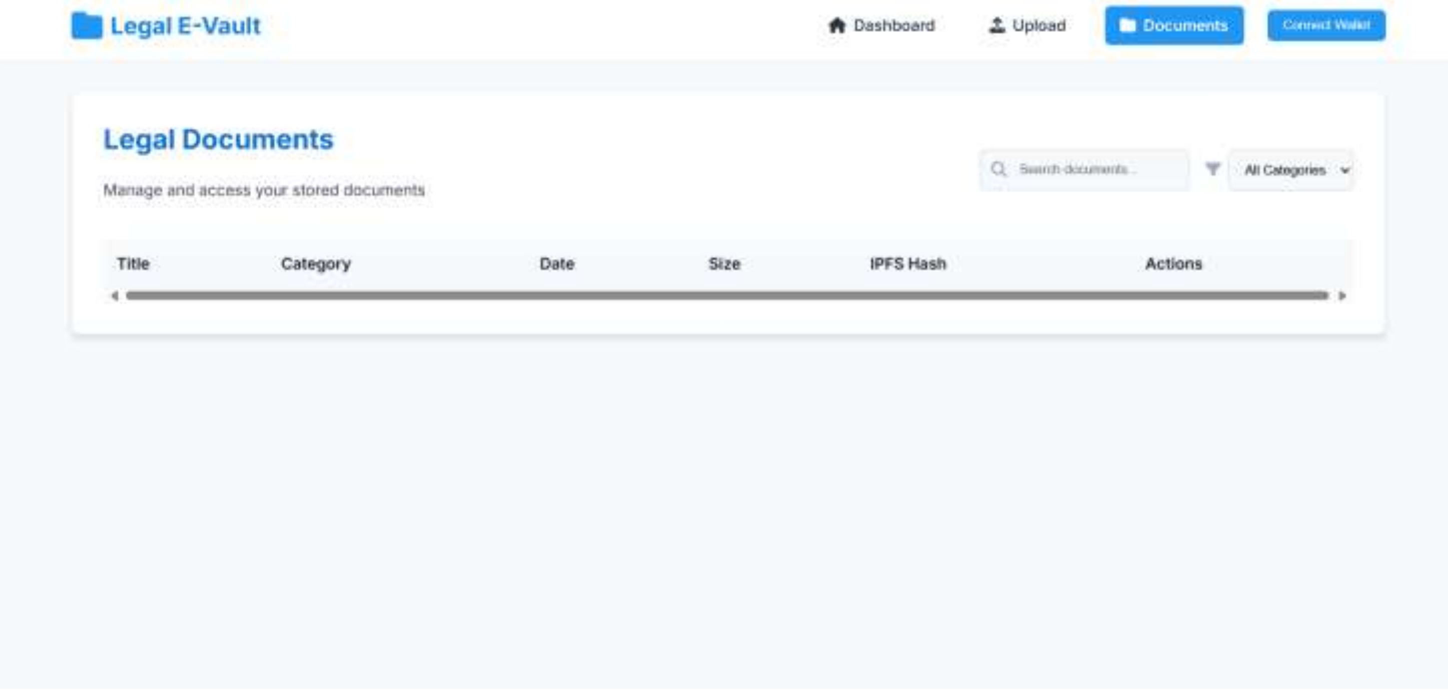
dd-mm-yyyy

Document File *

Choose File No file chosen

Supported formats: PDF, DOC, DOCX, TXT (Max size: 10MB)

Figure A.B.2.2 Documents upload

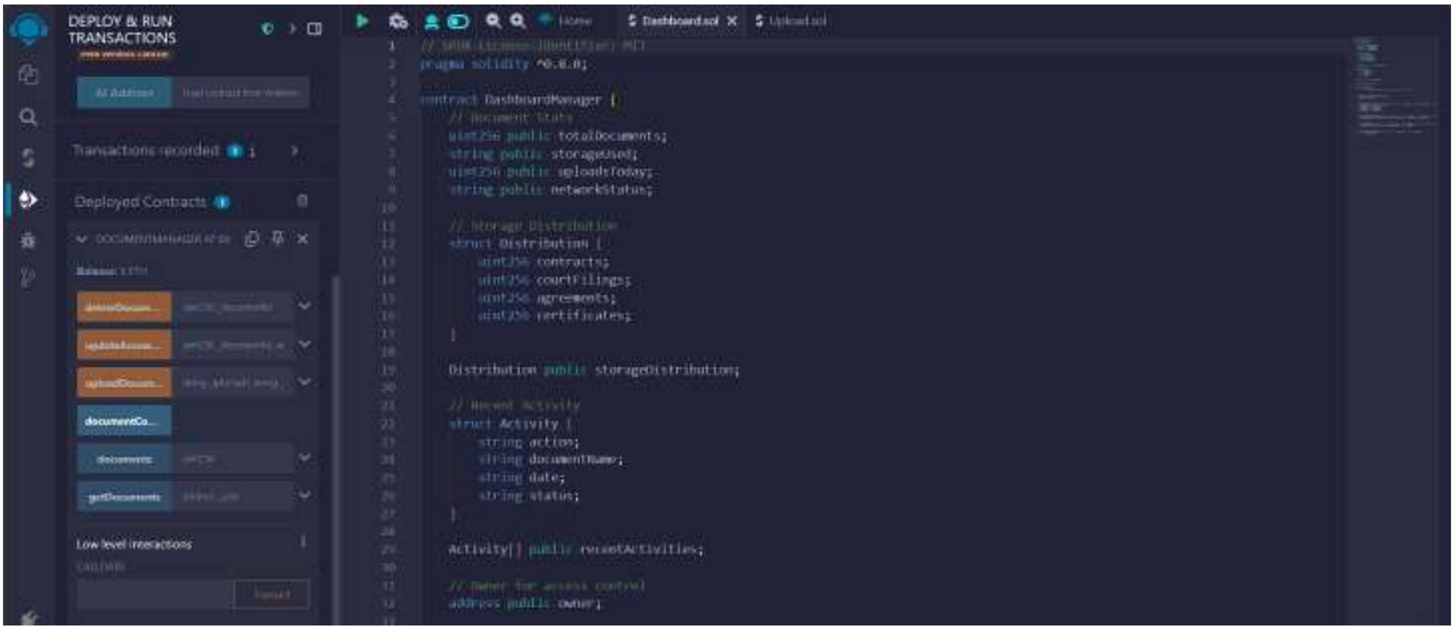


Legal Documents

Manage and access your stored documents

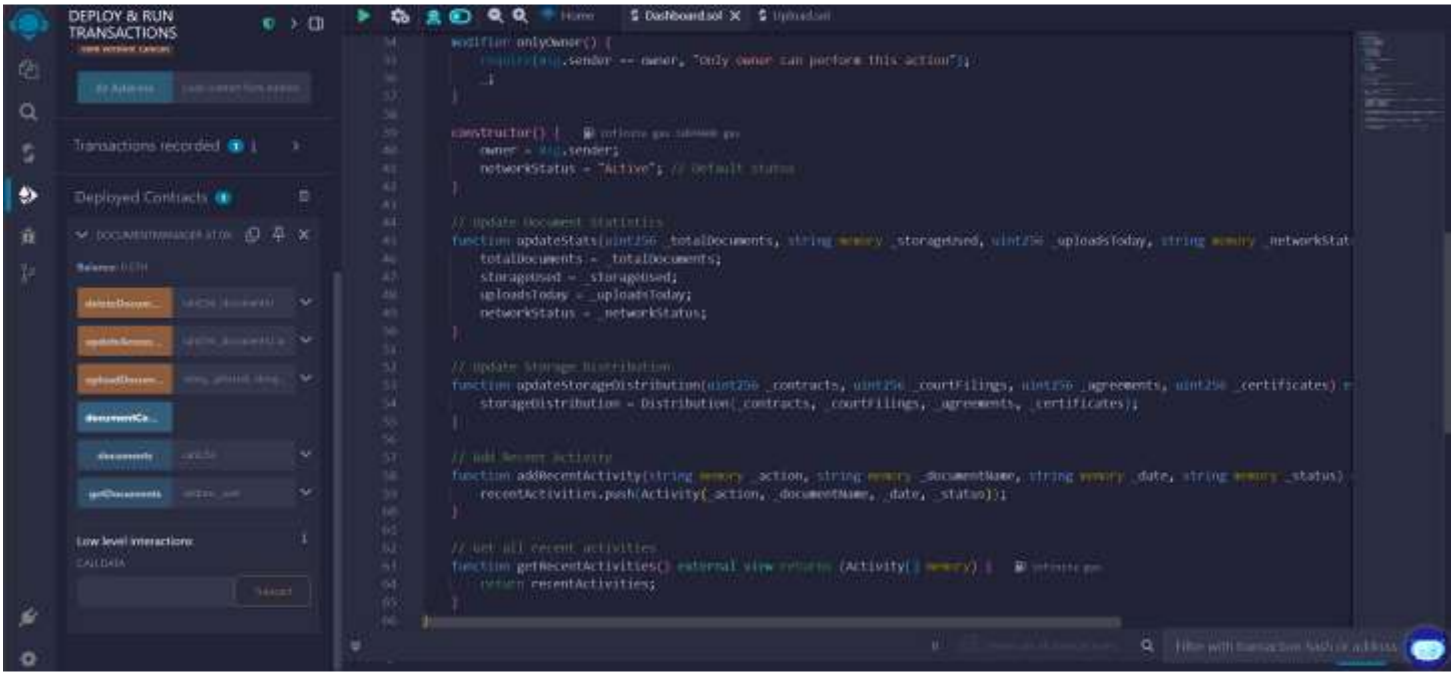
Title	Category	Date	Size	IPFS Hash	Actions

Figure A.B.3 View Documents



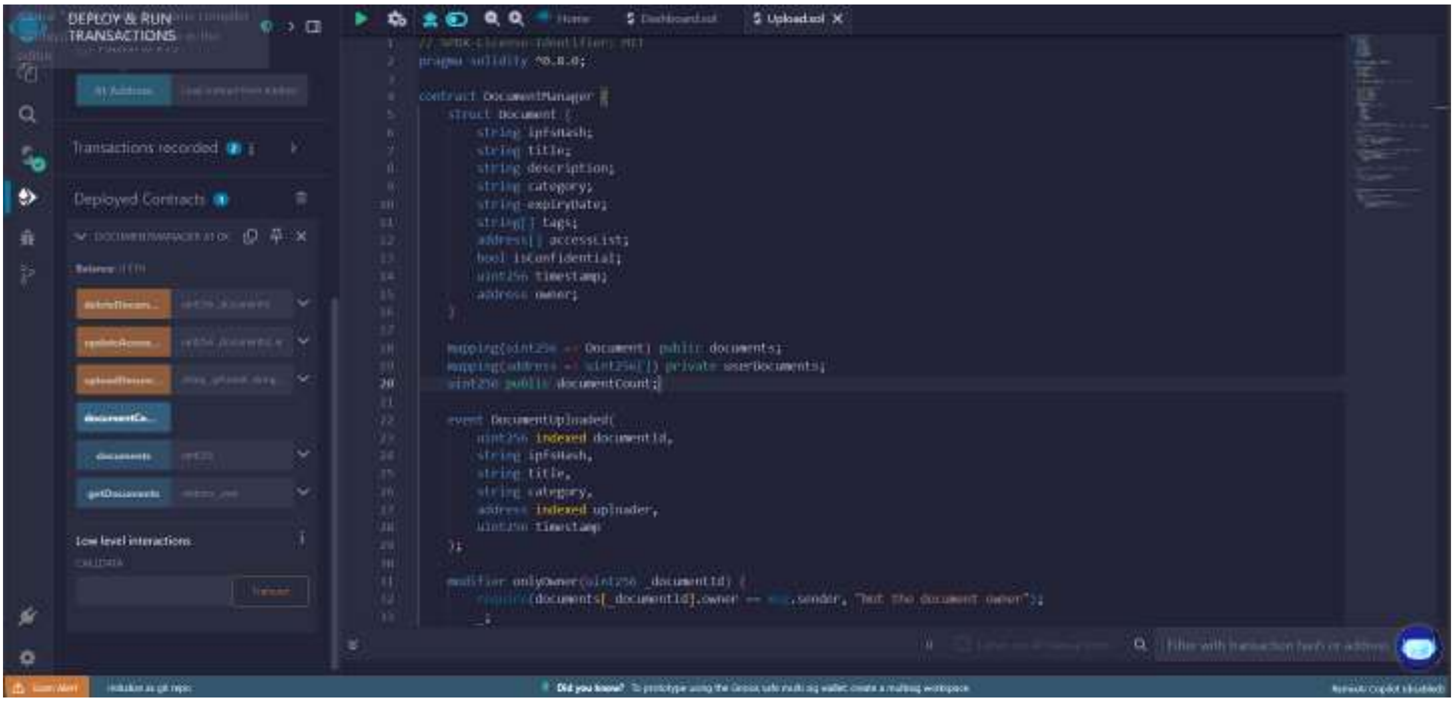
```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

contract DashboardManager {
    // Document Stats
    uint256 public totalDocuments;
    string public storageUsed;
    uint256 public uploadsToday;
    string public networkStatus;

    // Storage Distribution
    struct Distribution {
        uint256 contracts;
        uint256 courtFilings;
        uint256 agreements;
        uint256 certificates;
    }

    Distribution public storageDistribution;

    // Recent Activity
    struct Activity {
        string action;
        string documentName;
        string date;
        string status;
    }

    Activity[] public recentActivities;

    // Owner for access control
    address public owner;
```

Figure A.B.4.1 Dashboard solidity code



```
    modifier onlyOwner() {
        require(msg.sender == owner, "Only owner can perform this action");
        _;
    }

    constructor() {
        owner = msg.sender;
        networkStatus = "Active"; // Default status
    }

    // Update Document Statistics
    function updateStats(uint256 _totalDocuments, string memory _storageUsed, uint256 _uploadsToday, string memory _networkStat
        totalDocuments = _totalDocuments;
        storageUsed = _storageUsed;
        uploadsToday = _uploadsToday;
        networkStatus = _networkStatus;
    }

    // Update Storage Distribution
    function updateStorageDistribution(uint256 _contracts, uint256 _courtFilings, uint256 _agreements, uint256 _certificates) e
        storageDistribution = Distribution(_contracts, _courtFilings, _agreements, _certificates);
    }

    // Add Recent Activity
    function addRecentActivity(string memory _action, string memory _documentName, string memory _date, string memory _status)
        recentActivities.push(Activity(_action, _documentName, _date, _status));
    }

    // Get all recent activities
    function getRecentActivities() external view returns (Activity[] memory) {
        return recentActivities;
    }
```

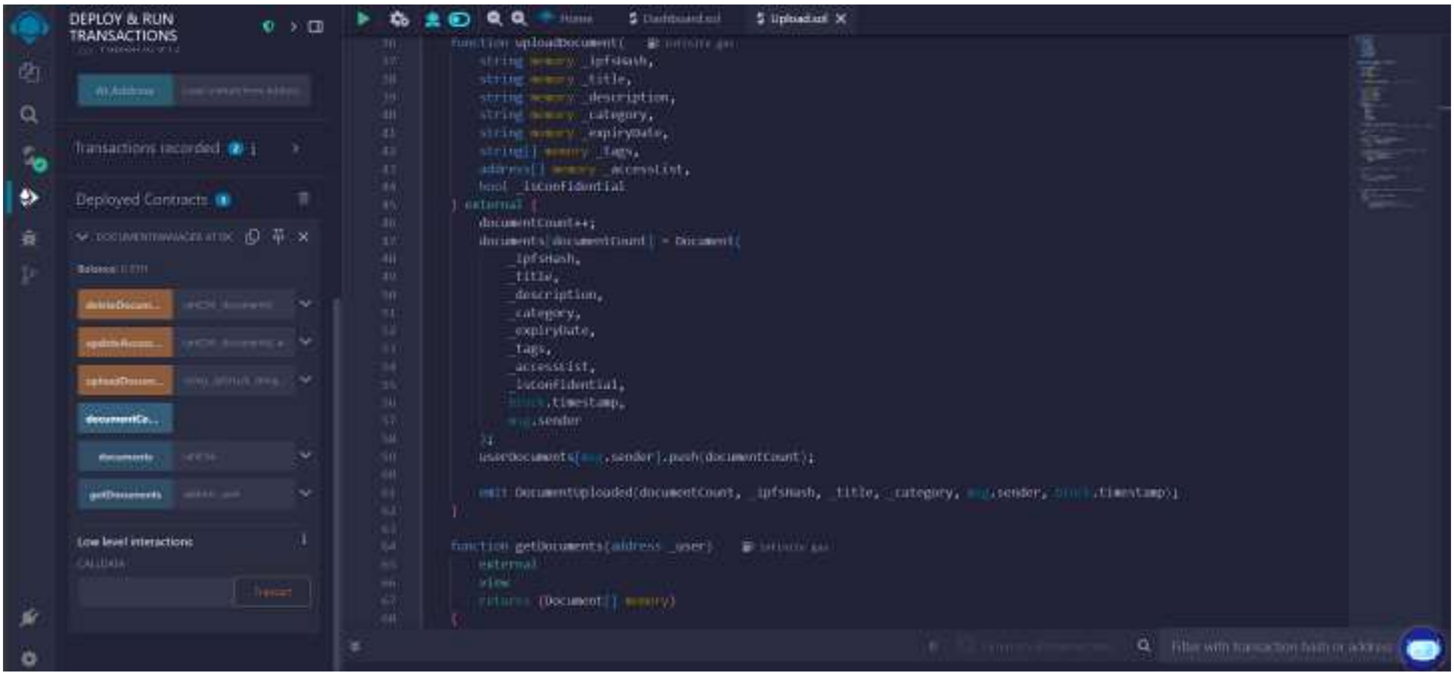
Figure A.B.4.2 Dashboard solidity code



```solidity
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

contract DocumentManager {
    struct Document {
        string ipfsHash;
        string title;
        string description;
        string category;
        string expiryDate;
        string[] tags;
        address[] accessList;
        bool isConfidential;
        uint256 timestamp;
        address owner;
    }

    mapping(uint256 => Document) public documents;
    mapping(address => uint256[]) private userDocuments;
    uint256 public documentCount;

    event DocumentUploaded(
        uint256 indexed documentId,
        string ipfsHash,
        string title,
        string category,
        address indexed uploader,
        uint256 timestamp
    );

    modifier onlyOwner(uint256 _documentId) {
        require(documents[_documentId].owner == msg.sender, "Not the document owner");
        _;
```

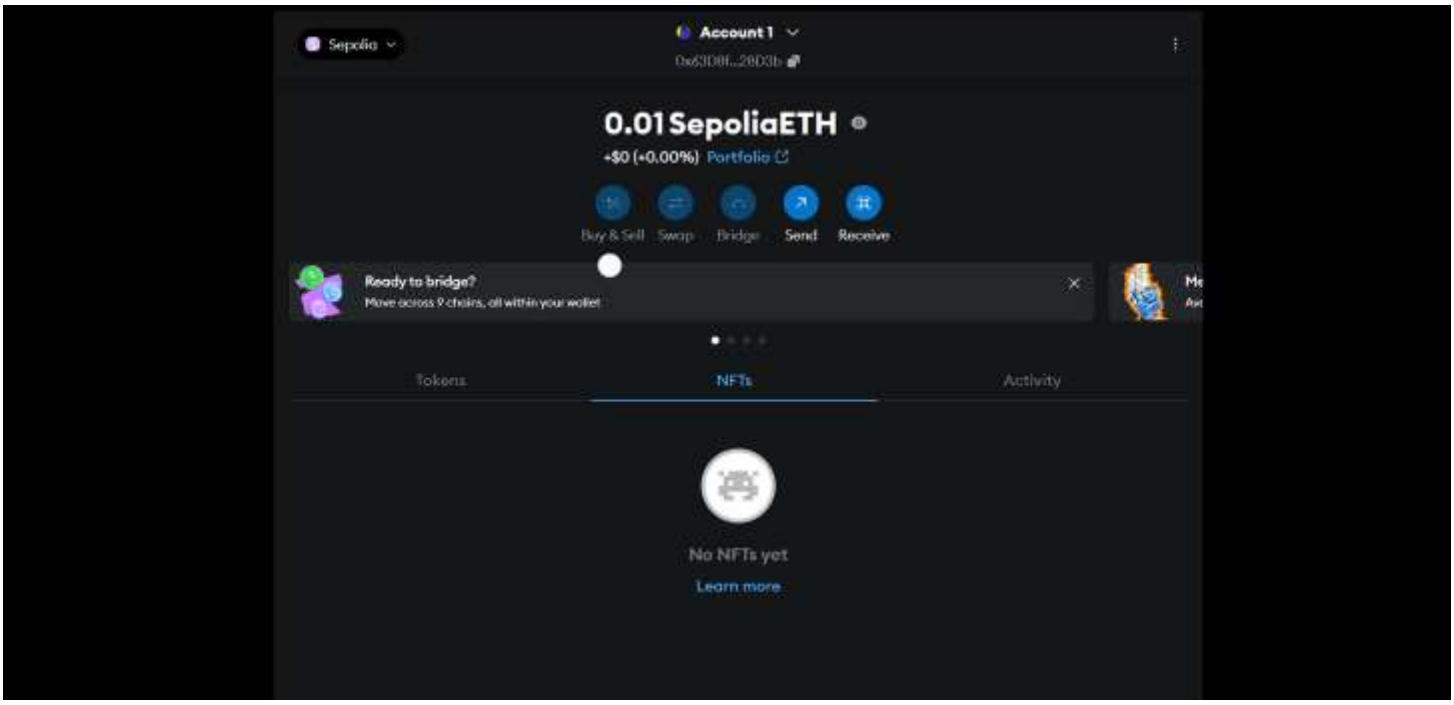
Figure A.B.5.1 Uploading documents solidity code

0



```solidity
    function uploadDocument(
        string memory _ipfsHash,
        string memory _title,
        string memory _description,
        string memory _category,
        string memory _expiryDate,
        string[] memory _tags,
        address[] memory _accessList,
        bool _isConfidential
    ) external {
        documentCount++;
        documents[documentCount] = Document(
            _ipfsHash,
            _title,
            _description,
            _category,
            _expiryDate,
            _tags,
            _accessList,
            _isConfidential,
            block.timestamp,
            msg.sender
        );
        userDocuments[msg.sender].push(documentCount);

        emit DocumentUploaded(documentCount, _ipfsHash, _title, _category, msg.sender, block.timestamp);
    }

    function getDocuments(address _user)
        external
        view
        returns (Document[] memory)
    {
```

Figure A.B.5.2 Uploading documents solidity code



0.01 SepoliaETH

+$0 (+0.00%) Portfolio

Ready to bridge?

Move across 9 chains, all within your wallet

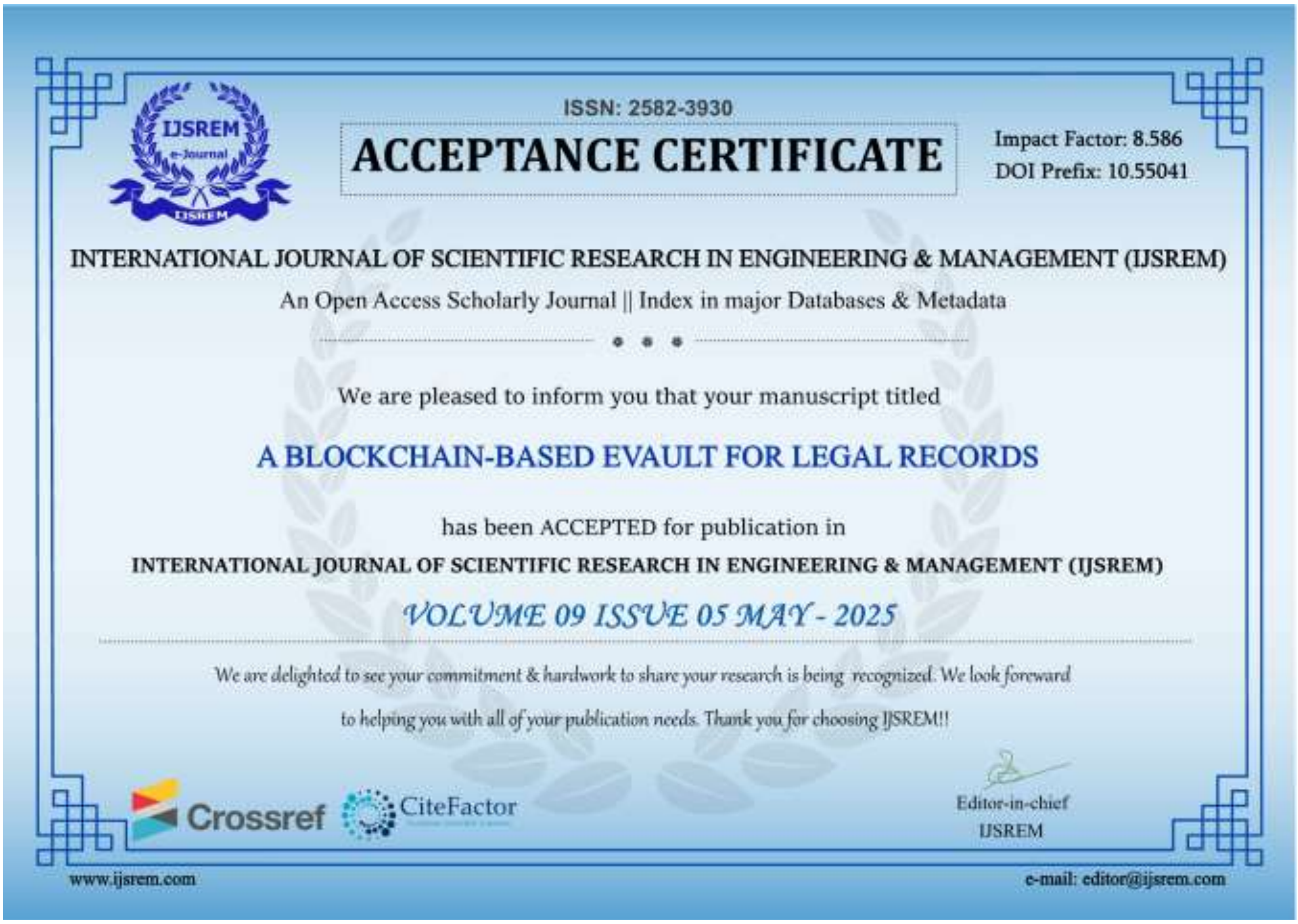
No NFTs yet

Figure A.B.6 Metamask wallet

APPENDIX-C

ENCLOSURES

1. Journal publication certificates of all students.



ISSN: 2582-3930

ACCEPTANCE CERTIFICATE

Impact Factor: 8.586
DOI Prefix: 10.55041

INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING & MANAGEMENT (IJSREM)

An Open Access Scholarly Journal || Index in major Databases & Metadata

We are pleased to inform you that your manuscript titled

A BLOCKCHAIN-BASED EVAULT FOR LEGAL RECORDS

has been ACCEPTED for publication in

INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING & MANAGEMENT (IJSREM)

VOLUME 09 ISSUE 05 MAY - 2025

We are delighted to see your commitment & hardwork to share your research is being recognized. We look foreward to helping you with all of your publication needs. Thank you for choosing IJSREM!!

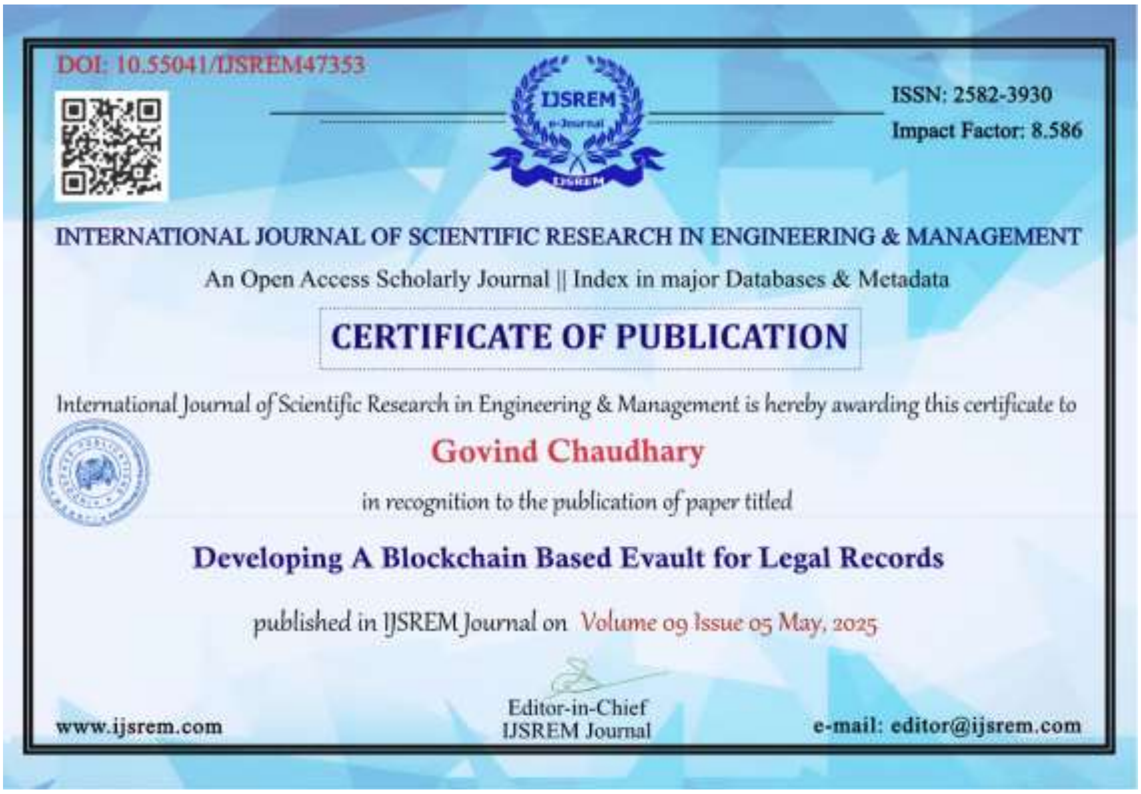
Crossref CiteFactor

Editor-in-chief
IJSREM

www.ijsrem.com

e-mail: editor@ijsrem.com

Figure A.C.1 Publication certificate



DOI: 10.55041/IJSREM47353

ISSN: 2582-3930

Impact Factor: 8.586

INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING & MANAGEMENT

An Open Access Scholarly Journal || Index in major Databases & Metadata

CERTIFICATE OF PUBLICATION

International Journal of Scientific Research in Engineering & Management is hereby awarding this certificate to

Govind Chaudhary

in recognition to the publication of paper titled

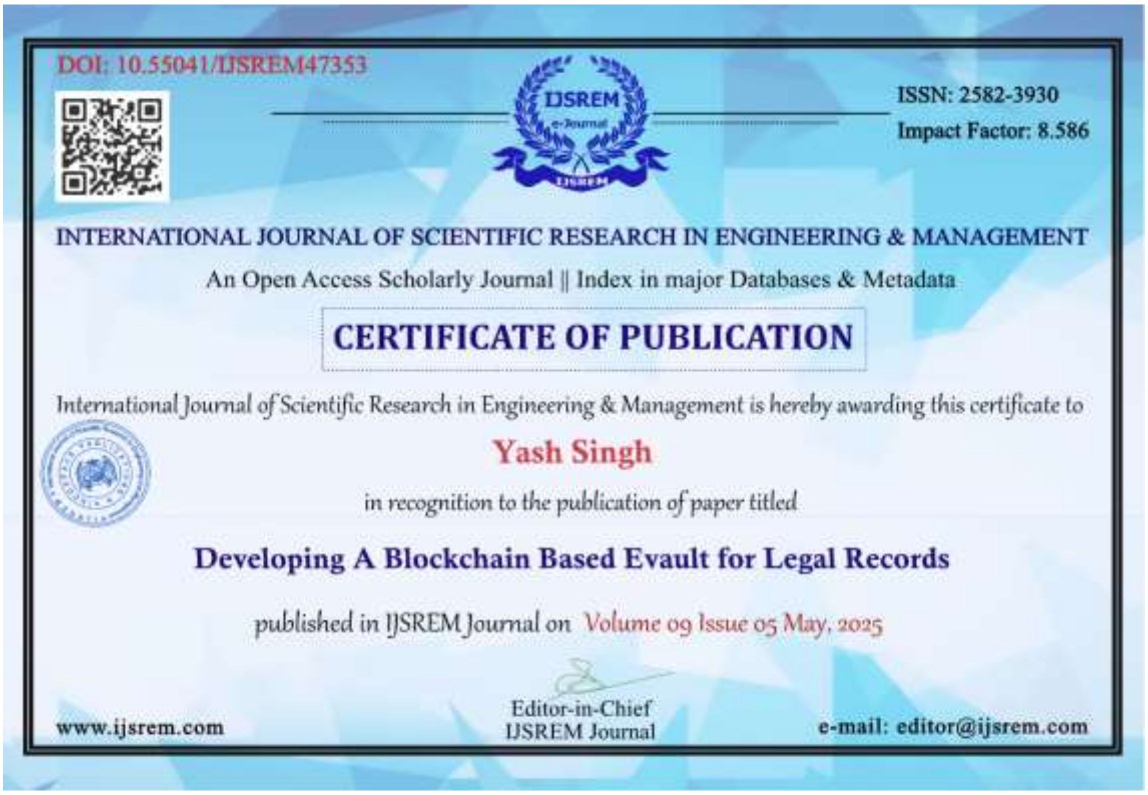
Developing A Blockchain Based Evault for Legal Records

published in IJSREM Journal on Volume 09 Issue 05 May, 2025

www.ijsrem.com

Editor-in-Chief
IJSREM Journal

e-mail: editor@ijsrem.com



DOI: 10.55041/IJSREM47353

ISSN: 2582-3930

Impact Factor: 8.586

INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING & MANAGEMENT

An Open Access Scholarly Journal || Index in major Databases & Metadata

CERTIFICATE OF PUBLICATION

International Journal of Scientific Research in Engineering & Management is hereby awarding this certificate to

Yash Singh

in recognition to the publication of paper titled

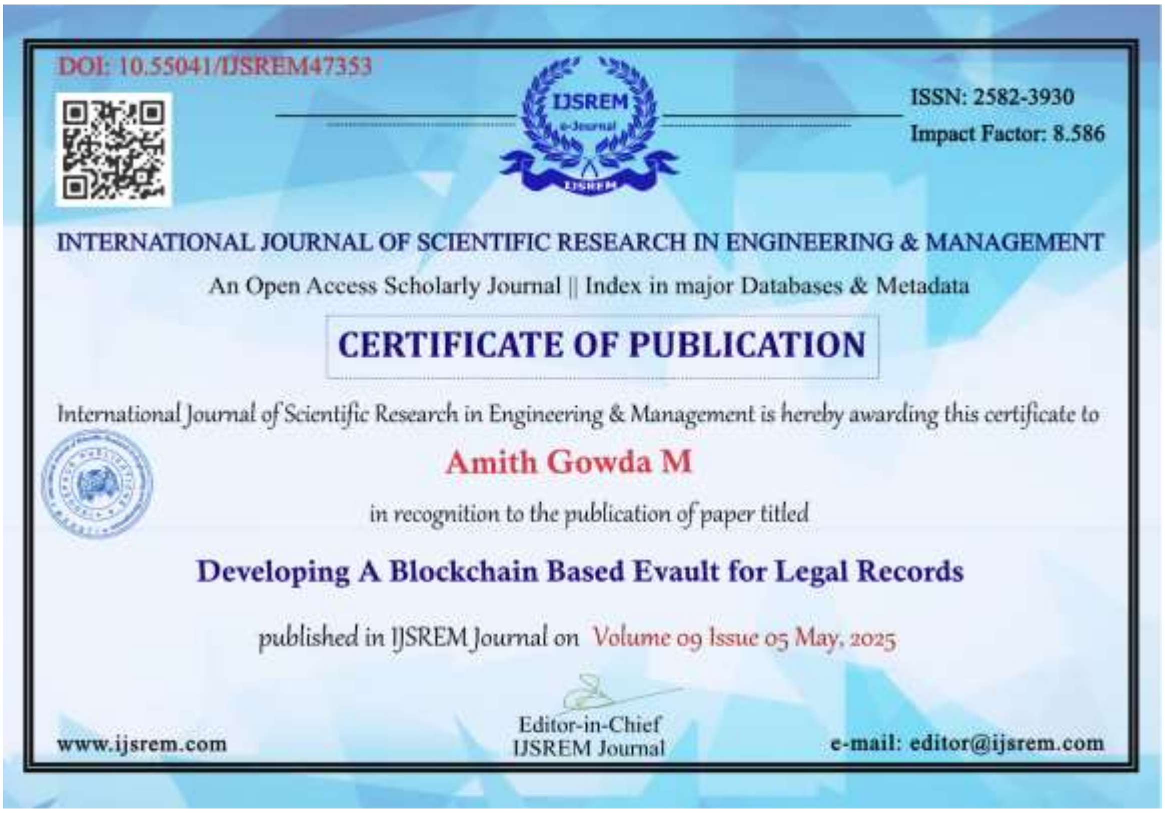
Developing A Blockchain Based Evault for Legal Records

published in IJSREM Journal on Volume 09 Issue 05 May, 2025

www.ijsrem.com

Editor-in-Chief
IJSREM Journal

e-mail: editor@ijsrem.com



DOI: 10.55041/IJSREM47353

ISSN: 2582-3930
Impact Factor: 8.586

INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING & MANAGEMENT

An Open Access Scholarly Journal || Index in major Databases & Metadata

CERTIFICATE OF PUBLICATION

International Journal of Scientific Research in Engineering & Management is hereby awarding this certificate to

Amith Gowda M

in recognition to the publication of paper titled

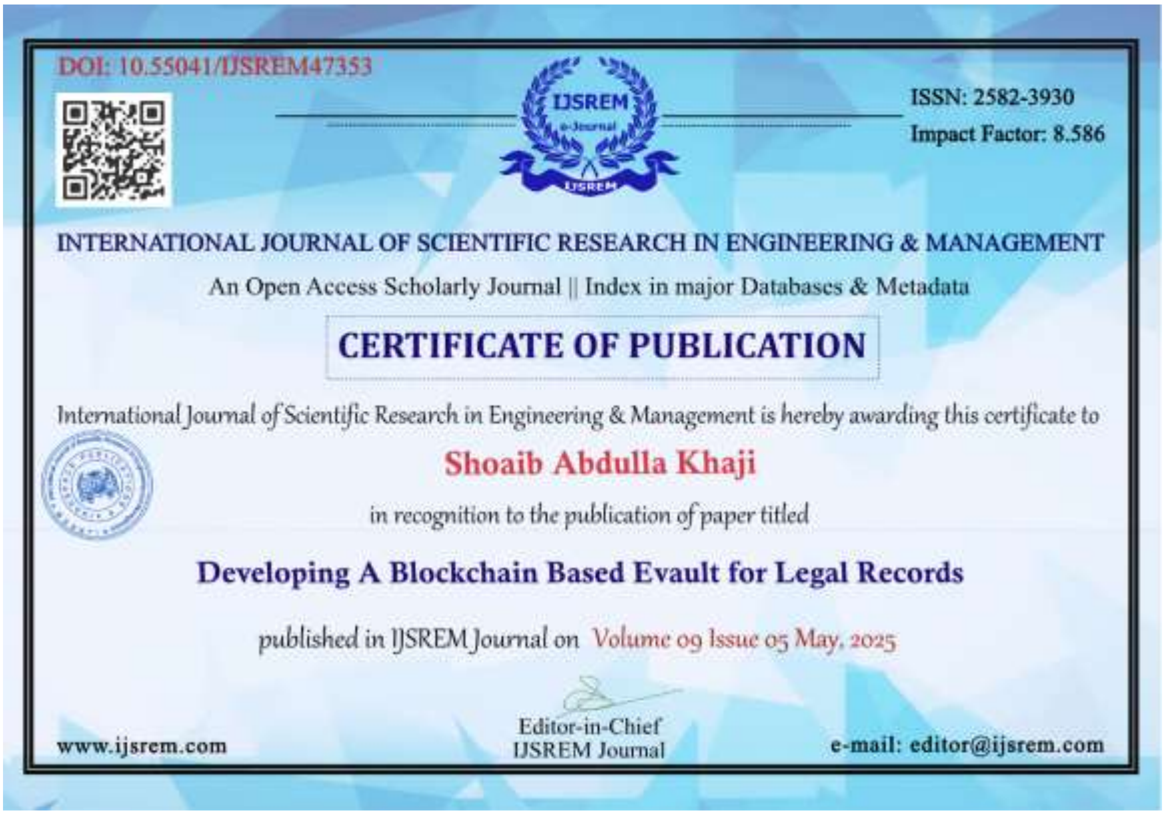
Developing A Blockchain Based Evault for Legal Records

published in IJSREM Journal on Volume 09 Issue 05 May, 2025

www.ijsrem.com

Editor-in-Chief
IJSREM Journal

e-mail: editor@ijsrem.com



DOI: 10.55041/IJSREM47353

ISSN: 2582-3930
Impact Factor: 8.586

INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING & MANAGEMENT

An Open Access Scholarly Journal || Index in major Databases & Metadata

CERTIFICATE OF PUBLICATION

International Journal of Scientific Research in Engineering & Management is hereby awarding this certificate to

Shoaib Abdulla Khaji

in recognition to the publication of paper titled

Developing A Blockchain Based Evault for Legal Records

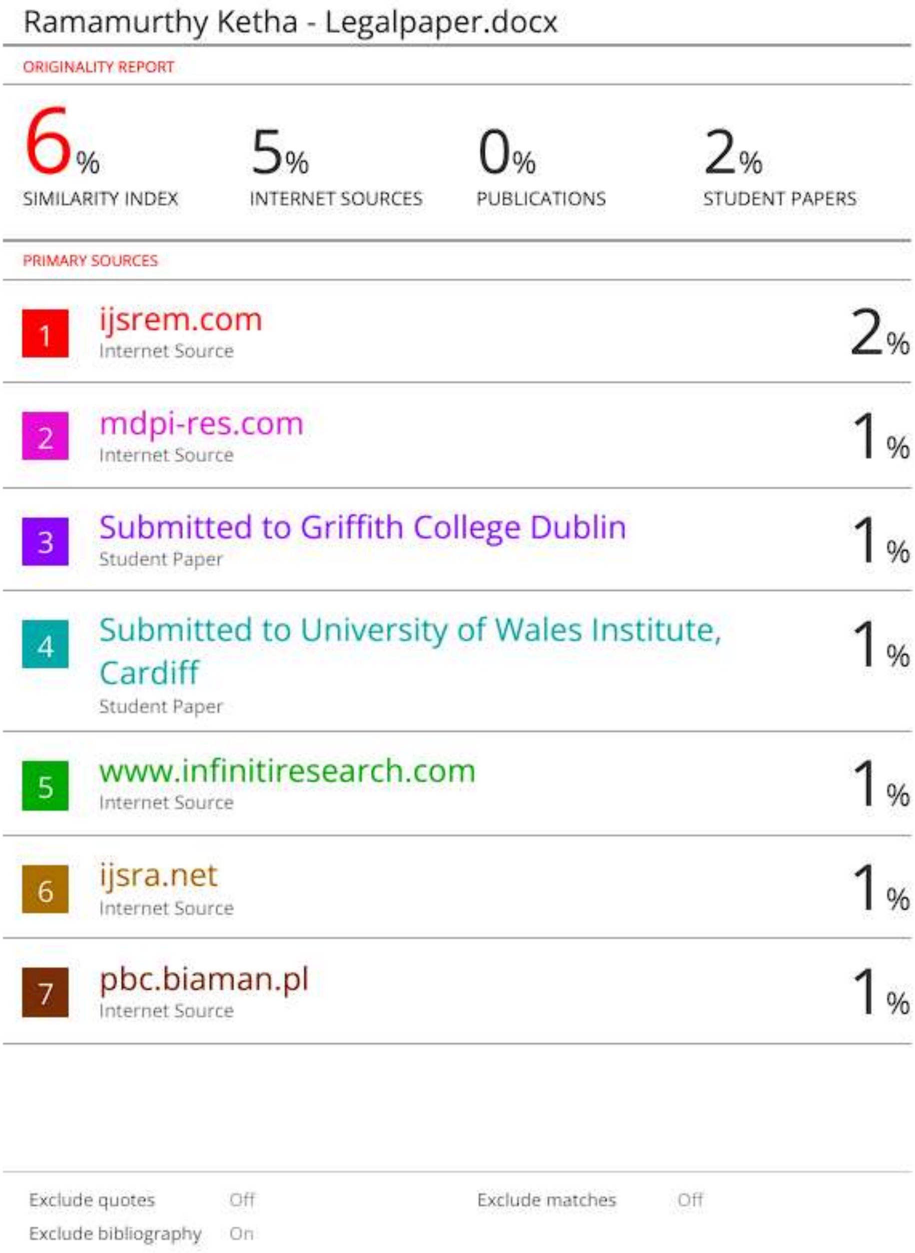
published in IJSREM Journal on Volume 09 Issue 05 May, 2025

www.ijsrem.com

Editor-in-Chief
IJSREM Journal

e-mail: editor@ijsrem.com

2. Similarity Index / Plagiarism Check report clearly showing the Percentage (%).



Ramamurthy Ketha - Legalpaper.docx

ORIGINALITY REPORT

6%	5%	0%	2%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	ijsrem.com Internet Source	2%
2	mdpi-res.com Internet Source	1%
3	Submitted to Griffith College Dublin Student Paper	1%
4	Submitted to University of Wales Institute, Cardiff Student Paper	1%
5	www.infinitiresearch.com Internet Source	1%
6	ijsra.net Internet Source	1%
7	pbc.biaman.pl Internet Source	1%

Exclude quotes Off
Exclude bibliography On
Exclude matches Off

Figure A.C.2 Plagiarism Report

3. Details of mapping the project with the Sustainable Development Goals (SDGs).

SUSTAINABLE DEVELOPMENT GOALS
17 GOALS TO TRANSFORM OUR WORLD
1 NO POVERTY
2 ZERO HUNGER
3 GOOD HEALTH AND WELL-BEING
4 QUALITY EDUCATION
5 GENDER EQUALITY
6 CLEAN WATER AND SANITATION
7 AFFORDABLE AND CLEAN ENERGY
8 DECENT WORK AND ECONOMIC GROWTH
9 INDUSTRY, INNOVATION AND INFRASTRUCTURE
10 REDUCED INEQUALITIES
11 SUSTAINABLE CITIES AND COMMUNITIES
12 RESPONSIBLE CONSUMPTION AND PRODUCTION
13 CLIMATE ACTION
14 LIFE BELOW WATER
15 LIFE ON LAND
16 PEACE, JUSTICE AND STRONG INSTITUTIONS
17 PARTNERSHIPS FOR THE GOALS
SUSTAINABLE DEVELOPMENT GOALS

Figure A.C.3 SDG mapping

- The project is mapped to:
- SDG 16 (Peace, Justice, and Strong Institutions): Ensures secure, transparent, and tamper-proof legal records to enhance trust in the judicial system.
- SDG 9 (Industry, Innovation, and Infrastructure): Leverages blockchain technology to improve digital infrastructure for legal record management.
- SDG 10 (Reduced Inequalities): Provides equitable access to legal records, reducing barriers to justice for marginalized communities.
- SDG 17 (Partnerships for the Goals): Encourages collaboration between legal institutions, technology providers, and governments for digital transformation.