BLOCK CHAIN BASED E-VAULT FOR LEGAL RECORDS

A Major Project report submitted

in partial fulfillment of requirement for the award of degree

BACHELOR OF TECHNOLOGY

in

SCHOOL OF COMPUTER SCIENCE AND ARTIFICIAL INTELLIGENCE

by

Goli Chandana	**(2103A52135)**
Mohammed Mudassir Hussain	**(2103A52058)**
Syed Khaja Mukarram Ajaz	**(2103A52069)**
Mohammed Naveed Sharief	**(2103A52159)**
Thangallapally Nihal	**(2103A52171)**
Vuppula Vashista	**(2103A52162)**

Under the guidance of

Dr. Balajee Maram

Professor, School of CS&AI.

SR UNIVERSITY

SR University, Ananthsagar,Warangal,Telagnana-506371

SR University

Ananthasagar, Warangal.

SR UNIVERSITY

CERTIFICATE

This is to certify that this project entitled **"E-vault using blockchain to store and transfer legal records**" is the Bonafide work carried out by **Goli Chandana**, **Mohammed Mudassir Hussain, Syed Khaja Mukarram Ajaz, Mohammed Naveed Sharief, Thangallapally Nihal, Vuppula Vashista** as a Major Project for the partial fulfillment to award the degree **BACHELOR OF TECHNOLOGY** in **School of Computer Science and Artificial Intelligence** during the academic year 2024-2025 under our guidance and Supervision.

Dr. Balajee Maram
Professor,
School of CS&AI
SR University
Anathasagar, Warangal

Dr. M. Sheshikala
Professor & Head,
School of CS&AI,
SR University,
Anathasagar, Warangal

Reviewer-1
Name:
Designation:
Signature:

Reviewer-2
Name:
Designation:
Signature:

ACKNOWLEDGEMENT

We owe an enormous debt of gratitude to our Capstone project guide **Dr. Balajee Maram, Professor** as well as Head of the School of CS&AI, **Dr. M. Sheshikala, Professor** and Dean of the School of CS&AI, **Dr. Indrajeet Gupta Professor** for guiding us from the beginning through the end of the Capstone Project with their intellectual advices and insightful suggestions. We truly value their consistent feedback on our progress, which was always constructive and encouraging and ultimately drove us to the right direction.

We express our thanks to project coordinator's **Mr. Sallauddin Md, Asst. Prof., and Dr.D.Ramesh Asst. Prof.** for their encouragement and support.

Finally, we express our thanks to all the teaching and non-teaching staff of the department for their suggestions and timely support.

Abstract

The legal profession is being hindered by the secure storage, transfer, and verification of legal documents using conventional systems. The E-vault Based on Blockchain to Store and Transfer Legal Records our project envisions a blockchain-based solution to provide security, integrity, and transparency in dealing with legal documents.

The E-vault system provides a secure, immutable environment for legal document management by combining blockchain technology. This means that documents are tamper-proof, with an unchallengeable history of ownership and transfer. The project utilizes a lightweight implementation of blockchain in Python, emphasizing cryptographic hashing and proof-of-work consensus algorithms.

To ensure safe storage of documents, the project has utilized AES encryption and SHA-256 hashing. Document metadata as document hash, name, type, owner ID, and timestamp of creation is stored in the blockchain in an open, immutable record of all document interactions.

An easy-to-use interface is built with Streamlit, providing straightforward interaction with the blockchain system. The functionalities involve user registration and authentication, upload and storage of documentsDocument display and verification, and document secure transfer. Blockchain explorer capabilities are offered for the display of a transaction history and verification of blockchain integrity.

Core Components of Development, Integration and Testing, and Final Touches form the project plan. Lightweight blockchain solution development for document verification, design of a safe documents storage mechanism, open mechanism development for document transfer, and a user-friendly interface are the core goals.

The E-vault blockchain initiative showcases the capabilities of blockchain technology in strengthening the security, transparency, and efficiency of legal document management. With its tamper-proof, self-verifying, and immutable platform, the E-vault system meets key challenges for conventional systems, providing a scalable and viable solution for the legal sector. Potential future improvements would involve smart contracts for rule-based document transfer, biometric verification, and a mobile interface for on-the-move access.

CONTENTS

S. No.	Chapter	Page No.
Abstract		**ii**
1	Introduction	01
	1.1 Problem Statement	01
2	Literature Survey	03
	2.1 Literature Survey table	03
	2.2 Literature Survey Summary	04
3	Existing methods vs Proposed methods	06
	3.1 Existing methods	06
	3.2 Proposed methods	08
4	System architecture/Technical Specifications	10
	4.1 System architecture	10
	4.2 Technical Specifications	12
5	Methodology	14
6	Feature and Functionalities	17
	6.1 User Registration and Authentication	17
	6.2 Secure Document Management	17
	6.3 Blockchain Explorer	17
	6.4 User Interface (Streamlit)	18
	6.5 Security Features	18
	6.6 Audit Trail	18
7	Implementation details	19
	7.1 Setup Instructions	19
	7.2 Usage Guide	19

	7.3 Document Storage and Blockchain Transaction Authentication	20
8	Results	22
9	Challenges and Solutions	29
	9.1 Challenge: Ensuring Document Integrity and Security	29
	9.2 Challenge: Managing Document Ownership and Transfer	29
	9.3 Challenge: Handling Document Ownership and Transfer	29
	9.4 Challenge: Scalability and Performance	30
10	Conclusion and Future Scope	31
	10.1 Conclusion	31
	10.2 Future Scope	31
	References	33

LIST OF TABLES

S. No.	Tables	Page No.
2.1.1	Tabular representation of Literature Survey	03
3.2.1	Existing vs Proposed Methods	09

LIST OF FIGURES

S. No.	Figures	Page No.
4.1.1	System Architecture Flowchart	11
8.1:	Landing Page	22
8.2:	Registration Page: Harry registered	22
8.3:	Initial Dashboard: Harry	23
8.4:	Uploading Document\Contract: Harry	23
8.5:	My Documents Page: Harry	24
8.6:	Transfer Document: Harry transferring to Matilda	24
8.7:	My Documents Page: Matilda –User 2. File Transferred	25
8.8:	Viewing the Document: Matilda –User 2.	25
8.9:	Document History is shown below while viewing the document: Matilda –User 2.	26
8.10:	Blockchain Explorer Page	26
8.11:	Blockchain explorer: Tracks all transactions	27
8.12:	Users Info: Harry and Matild	27

8.13: Blockchain: All Transactions are tracked 28
8.14: Documents Stored as Encrypted 28

Chapter 1

Introduction

The legal profession is facing greater needs for secure, reliable, and tamper-evident management of legal documents. Traditional document management systems inherently focus on databases, creating single points of failure and potential vulnerabilities in document integrity and security. Such systems are not providing verifiable proof of ownership of documents, open transfer histories, and document integrity over time.

Blockchain technology, which is marked by its decentralization and immutability, offers a solution to these issues. With the application of cryptography methods and distributed ledger technology, blockchain can ensure the integrity, transparency, and security of legal documents without the need of trusted third parties. This project, "E-vault using Blockchain to Store and Transfer Legal Records," seeks to create a blockchain system for securely safeguarding storing and transferring legal records while maintaining documents integrity and offering open and unalterable history of document transactions.

The E-vault system employs a lightweight implementation of a blockchain along with sophisticated and encryption algorithms to provide an efficient and secure storage system for legal documents. Python is utilized by our project to deploy blockchain, focusing on cryptographic hash functions and proof-of-work consensus algorithms to validate transactions and secure the blockchain. AES encryption and SHA-256 hash functions are also utilized by the system to ensure stored documents' confidentiality and integrity.

Among the prominent features of the E-vault system is the user interface, which is provided through Streamlit. The user interface supports intuitive interaction with the blockchain system and supports functions like user authentication and registration, document upload and storage, verification and display of documents, and secure document transfer. The user interface also incorporates a blockchain explorer that allows users to monitor transaction history and ensure blockchain integrity.

1.1 Problem Statement

The legal profession is under immense pressure to securely store legal documents because traditional document management systems have inherent limitations. The issues include:

Tamper-Proof Integrity: The ability to ascertain that the documents have not been tampered with without any indication.

Verifiable Ownership: Offering clear and verifiable proof of document ownership.

Transparent Transfer Histories: Allowing transparent and tamper-proof histories of document transfers.

Security Vulnerabilities: Bypassing likely security vulnerabilities of centralized systems, including a single point of failure.

Efficiency and Scalability: Effective processing and handling of large quantities of documents.

Traditional document management systems, which are normally centralized database and access control-based, are not suitable to meet these challenges. They require trusted third parties for verification, which can be a potential security threat and transaction cost. Moreover, these systems cannot provide tamper-proof histories and verifiable ownership transfers.

The objective of this project is to develop a blockchain-based E-vault system that addresses these problems with the security, transparency, and immutability of blockchain technology. The E-vault system will:

Ensure Document Integrity: Apply a lightweight blockchain solution for document authentication through cryptographic hashing and proof-of-work.

Secure Document Storage: Design a secure document storage system with AES encryption and SHA-256 hashing.

Transparent Document Transfer: Establish an open and permanent document transfer mechanism.

User-Friendly Interface: Design an easy-to-use interface based on Streamlit to enable the use of blockchain technology by legal practitioners.

Audit Trail: Provide a comprehensive audit trail of all document transactions.

By applying blockchain technology and stronger encryption algorithms combined with a user-friendly interface, the E-vault system offers an open, secure, and extensible system for the safekeeping of legal documents.

Chapter 2

Literature Survey

2.1 Literature Survey Table

Table 2.1.1: Tabular representation of Literature Survey

S No.	Author(s) & Year	Model Used	Parameters	Merits	Limitations & Drawbacks
1	Gamage, H.T.M. et al. (2020)	Blockchain Technology Concepts	Security, Transparency	Comprehensive overview of blockchain applications	Limited focus on specific use cases
2	Kaur, J. et al. (2022)	Smart Contracts Using Blockchain	Contract Automation	Detailed analysis of smart contract mechanisms	Implementation complexity and legal challenges
3	Ali, O. et al. (2021)	Blockchain Utilization Benefits	Efficiency, Security	Comparative study of blockchain functionalities	Generalized findings, lacking specific examples
4	Firdous Sadaf M. Ismail, & Dattatraya S Adane. (2022)	Blockchain Use Cases	Various Industries	Examination of growing blockchain applications	Identifies emerging issues but lacks deep technical insights
5	Ismail, F.S.M., Mushtaque, S.G.M. (2022)	Blockchain with 6G Networks	Connectivity, Integration	Exploration of blockchain integration with 6G	Theoretical approach, limited practical validation
6	Ismail, F. S., Mushtaque, S. G., & Adane, D. (2023)	Blockchain and 6G Networks	Network Security	Addresses potential and challenges of blockchain in 6G	Limited empirical data
7	Sarwar, M.I. et al. (2021)	Blockchain-empowered Accounting Systems	Data Integrity	Proposes secure data vaults for accounting systems	Implementation challenges in real-world scenarios
8	Paul, A. et al. (2004)	Secure Distributed Storage	Fault Tolerance	Early design of secure storage systems	Outdated technology, lacks blockchain integration
9	Hasan, R. et al. (2007)	Secure Storage for	Data Privacy	Requirements for secure healthcare data storage	Focused on healthcare, not generalizable

		Healthcare Records			
10	Li, H. and Han, D. et al. (2019)	Blockchain-based Educational Records	Data Sharing	Secure storage and sharing of educational records	Limited to educational sector
11	Verma, A. et al. (2021)	Blockchain-based Law Record Management	Judicial Records	Secure and transparent law record management	System complexity and scalability issues
12	Gururaj, H.L. et al. (2020)	Blockchain Technology	General Applications	Broad overview of blockchain technology	General, lacks specific implementation details
13	Rupa, C. et al. (2021)	Blockchain for Medical Certificates	Knowledge Management	Distributed application for managing medical certificates	Limited to medical certificates, not broadly applicable
14	Mahamure, S.S. et al. (2020)	Blockchain for Real Estate	Document Protection	Protection of real estate documents using Ethereum	Focused on real estate, lacks generalizability

2.2 Literature Survey Summary

Literature review provides an overall analysis of blockchain technology innovations and uses in various sectors. Gamage et al. (2020) gave a comprehensive description of blockchain concepts, such as its security and transparency benefits [1]. Kaur et al. (2022) analyzed the utilization of smart contracts through blockchain, with emphasis on contract automation and its implications in law [2].Ali et al. (2021) compared the advantages and functions of blockchain technology and identified its efficiency and security benefits [3].

Within particular applications, Ismail and associates discussed the convergence of blockchain with 6G networks for possible advantages and issues [5][6]. Sarwar et al. (2021) suggested secure data vaults for accounting systems with blockchain-backed empowerment, highlighting the technology's potential in increasing data integrity [7]. Verma et al. (2021) presented a blockchain-based electronic law record management system, illustrating its use in judicial investigations [11].

The survey also encompassed initial developments of secure distributed storage systems, including the paper by Paul et al. (2004) which provided fundamental information regarding secure

storage processes [8]. Hasan et al. (2007) discussed healthcare records storage needs especially in terms of security and emphasized the importance of data privacy [9].

Based on the results of these researches, our project aims to develop a blockchain-based E-vault system capable of holding and transferring legal documents. Through the use of enhanced encryption methods, a lightweight implementation of blockchain tailored to our needs, and an easy-to-use interface, the E-vault system tackles essential challenges like document integrity, security, and scalability. The use of a Streamlit-based interface also adds to accessibility, where legal practitioners can easily interact with the blockchain system without needing special technical knowledge.

Chapter 3

Existing Methods Vs. Proposed Method

3.1 Existing Methods

Legacy Document Management Systems (DMS) use centralized databases and access controls for document management. They have limited functionalities of storing, retrieving, and access control but have great limitations:

- **Centralized Trust Model:** These systems depend on a trusted central authority to authenticate and manage documents to create single points of failure and require trusting system administrators.
- **Document Tampering Detection:** Restricted detection ability for document tampering. Any alteration in a document is not always traceable and therefore may cause integrity violations.
- **Ownership Transfer:** Time consuming and frequently time taking document ownership transfer procedures, resulting in delays and potential errors.
- **Audit Trail:** Audit trails exist but can be edited by administrators and thereby compromise the document history's integrity.
- **Verification**: Third-party verification to verify document authenticity and thus incur extra costs and potential delays.
- **Security:** Prone to security attacks because of centralized storage, hence vulnerable to hacking and data loss.
- **User Experience:** Normally complex and not user-focused, requiring extensive education to utilize.Blockchain-Based Document Management

Blockchain-Based Document Management

Blockchain technology is a decentralized document management system founded on cryptographic protocols that provide data integrity. Some of the most notable characteristics of blockchain systems are:

- **Decentralized Trust Model:** The trust is distributed across the network, preventing any point of failure and reducing the risk of a single point of failure.

- **Tampering Detection:** Cryptographic hashing provides easy detection of document tampering with high integrity assurances.
- **Ownership Transfer:** Safe and automatic transfer of ownership through blockchain transactions to ensure accuracy and efficiency.
- **Audit Trail:** Unalterable audit trails that are tamper-proof, providing an unambiguous and auditable record of all document transactions.
- **Confirmation:** Self-verifying documents supported by cryptographic evidence, without needing third-party verification.
- **Security:** Improved security via distributed storage and cryptographic methods, rendering it immune to hacking and data loss.
- **User Experience:** Possibly more user-friendly with newer interfaces, but still to be in the early phase of adoption by legal management.

3.2 Proposed Methods

The E-vault system takes advantage of the application of blockchain technology to surpass the inadequacies of traditional document management systems. Our proposed solutions are:

Light Blockchain Deployment

Custom Blockchain: Python light blockchain implementation with emphasis on cryptographic hashing and proof-of-work consensus algorithms for transaction validation and blockchain security.

Document Hashing: Documents are SHA-256 hashed to offer integrity, and the hash is recorded on the blockchain to create an immutable record.

Secure Document Storage

Encryption: Files are encrypted with AES (Advanced Encryption Standard) for confidentiality. Encrypted files are stored locally, but hashes of the encrypted files are stored on the blockchain for integrity validation.

Metadata Storage: Document metadata like document hash, document name, document type, owner ID, and creation timestamp are stored on the blockchain, thereby creating an open and immutable audit history of document activity.

Streamlit Interface

- **User Registration and Authentication**: Streamlit user registration and authentication gateway to ensure secure access to the system.
- **Document Management:** Easy document upload, storage, reading, and verification, enabling users to engage with the blockchain platform at will.
- **Document Transfer**: Safe document transfer system through blockchain transactions to enable secure and efficient ownership transfer.
- **Blockchain Explorer:** Features to allow users to retrieve transaction history and confirm the integrity of the blockchain.

Comprehensive Audit Trail

- **Immutable Records**: All transactions are written to the blockchain, generating an immutable audit trail that can't be altered.
- **Transparency:** The users can view the complete document activity history, and the system is transparent and reliable.

Enhanced Security

- **Distributed Trust:** Because the blockchain is distributed, it has no single points of failure and is more secure.
- **Cryptography Techniques:** Using advanced cryptography techniques for preserving confidentiality and integrity of data.

Table 3.2.1: Existing vs Proposed Methods

Feature	Traditional DMS	E-vault Blockchain Solution
Trust Model	Centralized	Distributed
Tampering Detection	Limited	Cryptographically Ensured
Ownership Transfer	Manual Processing	Automated & Secure
Audit Trail	Can be Modified	Immutable
Verification	Requires Third Party	Self-Verifying
Cost	High Maintenance	Low Operational Costs
Security	Single Point of Failure	Distributed Security
User Experience	Complex	Streamlined

By combining blockchain technology with advanced encryption techniques and a user-friendly interface, the E-vault system offers a secure, transparent, and scalable solution for managing legal records, addressing the critical challenges faced by traditional document management systems.

Chapter 4

System Architecture / Technical Specifications

4.1 System Architecture

The system architecture of the E-vault has been designed modular to support scalability, security, and maintenance. The architecture is comprised of numerous layers which support particular functionalities. The key components of the system architecture are:

1. **User Interface Layer (Streamlit):** The layer provides a friendly and interactive interface to deal with the E-vault system.It encompasses user registration and authentication functionality, file upload and storage, document verification and viewing, and secure file sharing. The interface also has a blockchain explorer to display transaction history.
2. **Application Logic Layer (Controller):** This layer provides the fundamental application logics, such as user authentication, document handling, and transaction processing. It serves as a center between the user interface and the blockchain layer to facilitate easy interaction and data transfer.
3. **Blockchain Layer:** The deployment of the blockchain technology is done through this layer. It includes a proprietary light blockchain, with emphasis on proof-of-work consensus algorithms and cryptographic hashing for authenticating transactions and securing the blockchain. It maintains document integrity and offers a transparent and immutable history of document transactions.
4. **Document Storage Layer (Encrypted Storage):** This layer is responsible for the safe storage of documents. Documents are encrypted with AES (Advanced Encryption Standard) and hashed with SHA-256 for integrity checking. Encrypted files are maintained locally, and their hashes are added to the blockchain.
5. **Authentication Layer (User Management):** This layer verifies and controls users. It offers secure access to the system through user registration, login, and session management. User information is stored securely through salted password hash storage.

6. **Database Layer:** The layer holds non-blockchain data such as user information and document metadata. The layer facilitates fast retrieval and management of data required by the application logic layer.

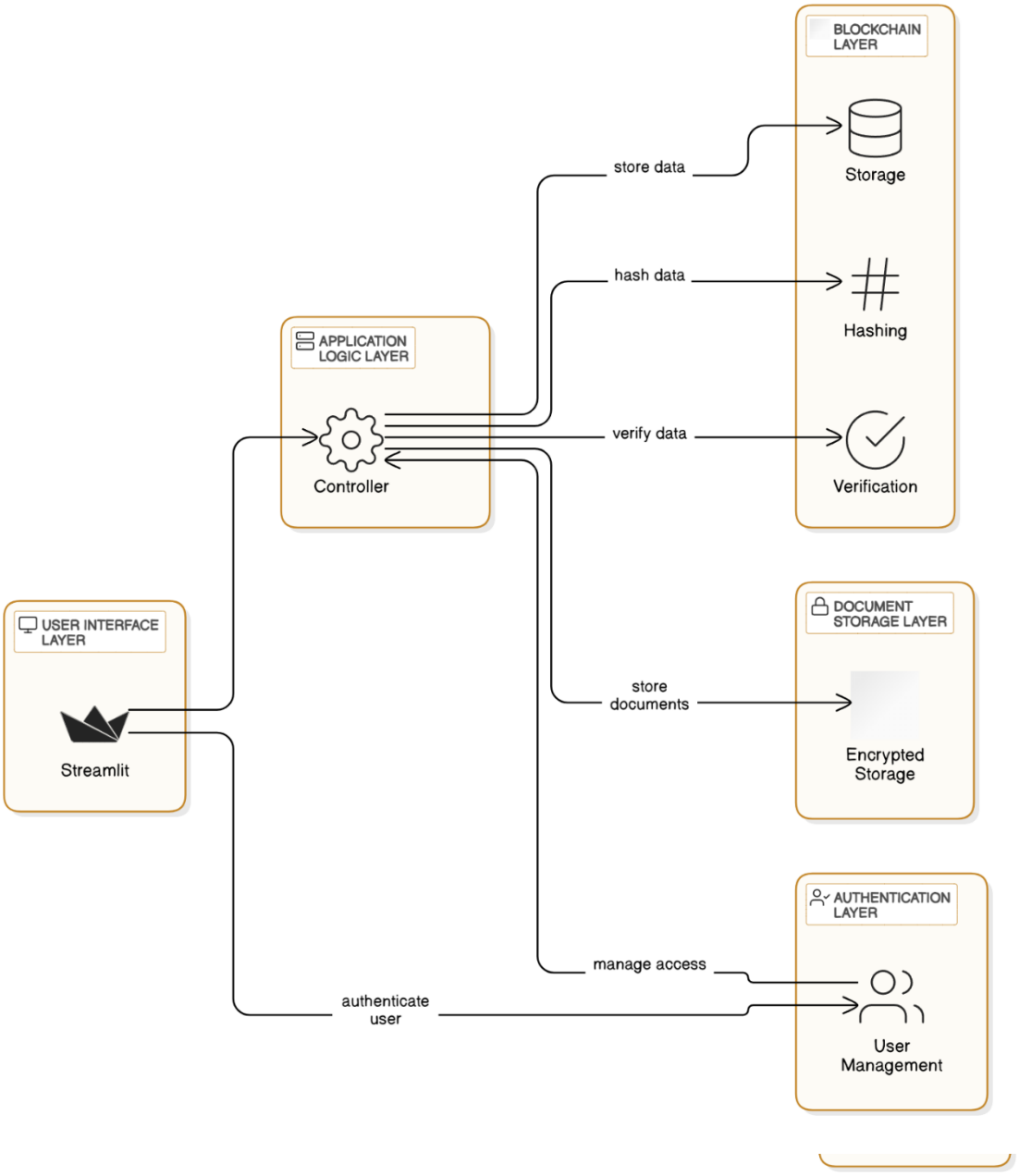

Figure 4.1.1: System Architecture Flowchart

4.2 Technical Specifications

Technical details of the E-vault system are as follows:

Backend: Python

Python is utilized in the backend with the benefit of supporting a large number of libraries and frameworks to achieve blockchain, encryption, and web development.

Blockchain: Custom Implementation

Custom light-weight blockchain implementation with Python that involves cryptographic hashing (SHA-256) and proof-of-work consensus algorithms.

Encryption: AES (Advanced Encryption Standard)

The files are encrypted with AES for confidentiality and security. The encryption key management is stored within the system securely.

Hashing: SHA-256

SHA-256 hashing is applied to enhance the integrity of documents.

The record is hashed and the hash maintaines on the blockchain establishing an irreversible, non-revisable account that can neither be changed or updates.

User Interface: Stream lit

The Stream lit is utilized to create the user interface, with a minimalistic and easy-to-use platform for interaction with the E-vault system. Stream lit supports fast web application development and deployment.

Database: SQLite (or any other lightweight database)

The database layer employs SQLite to store non-blockchain data, including user data and document metadata.SQLite is used due to its simplicity and ease of use.

Authentication: Salted Password Hashing

User authentication is managed through salted password hashing systems for storing user credentials securely.

Development Environment:

Operating System: Windows 11

IDE: Visual Studio Code

Python Version: 3.9 or higher

Dependencies:

streamlit: Used for creating the user interface

pycryptodome: Used for encryption and hashing

python-dotenv: Used for environment variable handling

Installation:

The setup and installation of the development environment include creating a virtual environment, installing dependencies necessary for installation, and installing the project structure according to the first setup guide of the project. After these technical specifications, the E-vault system offers a user-friendly, secure, and scalable environment for legal document management using blockchain technology.

Chapter 5

Methodology

The E-vault system aims to utilize blockchain technology for transparent and secure legal record management. The process for creating the E-vault system consists of several important steps: blockchain implementation, document management, user authentication, and interface design. Each of these steps is explained in the following detail.

Step 1: Blockchain Implementation

Goal: Create a light blockchain that is capable of recording securely transactions on document storage and transfer.

- **Blockchain Structure**: The blockchain is done in Python. Every block has an index, timestamp, array of transactions, previous block hash, current block hash, and a nonce value.
- **Hashing:** SHA-256 hashing is employed to hash every block's data so that even if there are some changes to the block data, it would become quite noticeable to do so.
- **Proof-of-Work:** A light-proof-of-work protocol is employed in order to attach blocks to the blockchain. Here, the process involves determining the nonce value that when combined with the data from the block together with prefixed count of leading zeros, would be produced by them.
- **Block Validation**: Validation of a new block is ensured by checking the hash of the previous block in order to keep the blockchain in its proper shape.

Step 2: Safe Document Storage

Objective: Keep documents safely via encryption and hashing.

- **Encryption:** The papers are encrypted with AES (Advanced Encryption Standard) before storage. This secures document content.
- **Hashing:** A paper is hashed with SHA-256 in order to acquire a fingerprint.The hash is kept on the blockchain for validation of the document's integrity.
- **Storage:** Local storage within the system stores data encrypted, and metadata (like hash) stored on the blockchain.

Step 3: User Authentication

Objective: Put in place a secure authentication mechanism for users to manage the access to the E-vault system.

- **User Registration:** User registration is possible by entering the password, email, and username.PASSWORDs are salted, followed by hashing and storage.
- **Login:** The user can log in using the username and password. The credentials are validated by comparing the stored hash with the hashed password.
- **Session Management:** Once the user is authenticated, they are given a session token to allow them to access the system securely.

Step 4: Document Management

- **Purpose**: Provide functionality for uploading, displaying, authenticating, and transferring files.
- **File Upload**: Uploading of files from the Streamlit interface is possible. The file is encrypted, hashed, and the encrypted file and information are stored.
- **File View:** Users can view their own uploaded files. The file is decrypted for viewing purposes and checks document integrity with stored hash.
- **Document Verification:** The authenticity of the documents can be verified by the users by comparing the present hash of the document with the hashed and saved document on the blockchain.
- **Document Transfer:** The documents can be transferred securely to other registered users.The transfer is documented as a transaction in the blockchain, resulting in a clear and irreversibly connected record.

Step 5: Interface Development

Objective: Create an accessible interface with Stream lit for use in interacting with the E-vault system.

- **Stream lit Interface:** The interface provides user registration capability, login, upload of documents, viewing documents, verification of documents, and transferring documents.
- **Blockchain Explorer:** It has an integrated blockchain explorer through which the user can see the transaction history on the blockchain and check the integrity of the blockchain.
- **User Interaction:** The system is designed intuitive and user-friendly such that the users can work with the system without needing huge technical knowledge.

Testing and Integration

Objective: Get everything to get along with one another and the system to act as intended.

1. **Unit Testing:** Every module (blockchain, encryption, authentication, document management) is tested separately in order to ensure proper functioning.
2. **Integration Testing:** The components are put together and end-to-end tests are performed to confirm all the pieces are working together as a system in harmony with each other.
3. **User Testing:** Users test the system in order to identify any usability issues and ensure that the interface is user-friendly and intuitive.

With this strategy, the E-vault system is developed to provide a secure, transparent, and user-friendly platform for storing legal documents through blockchain technology.

Chapter 6

Features and Functionalities

The E-vault system is designed to provide an entire suite of functionalities and features for facilitation of the secure, transparent, and efficient management of legal documents. The major functionalities and features of the E-vault system are enumerated as follows:

6.1 User Registration and Authentication

- **User Registration:** Makes it easy for new users with the ability to register by filling in a username, email address, and password. User accounts are also stored securely within the system with the use of salted password hashing methods to ensure safety procedures.
- **User Authentication:** Provides user logon by authenticating credentials. Session tokens are issued to users after successful authentication to allow secure communication to the system.
- **ROM-Based Access Control:** Offers access control to enable authenticated users to read or update some documents.

6.2 Secure Document Management

- **Document Upload:** Offers uploading of court documents. The application encrypts a document with AES, hashes it with SHA-256, and stores the encrypted document locally. Document metadata like the hash are stored on the blockchain to provide integrity.
- **Document Viewing:** Supports viewing of uploaded user documents. The system decrypts a document for viewing and checks its integrity against the hash stored.
- **Document Verification:** Offers functionality to make users capable of checking the integrity of their documents by comparing the document's hash in the blockchain with the document's current hash.
- **Document Transfer:** Enables secure transfer of ownership of documents to other registered users. Transfer is recorded as a transaction on the blockchain, and this has an open and immutable record.

6.3 Blockchain Explorer

- **Transaction History:** Enables users to see the entire history of transactions stored on the blockchain, such as document upload, transfers, and verification operations.

- **Block Details:** Supplies detailed information about every block of the blockchain, i.e., block index, timestamp, previous hash, current hash, nonce value, and list of transactions.
- **Blockchain Integrity:** Specifies blockchain integrity as valid and tamper-free or otherwise.

6.4 User Interface (Streamlit)

- **Dashboard:** Basic dashboard to display the user summary, i.e., recent document upload and document transfer.
- **Upload Document:** Simple upload document interface via which users can enter document information and upload documents.
- **My Documents:** A user page where users can see, authenticate, and transfer their uploaded documents.
- **Blockchain Explorer:** A built-in explorer of the blockchain where users can see transaction history and authenticate blockchain integrity.

6.5 Security Features

- **Encryption:** Performs AES encryption to secure stored documents from unauthorised access. Encryption keys applied are handled securely within the system.
- **Hashing:** Employs SHA-256 hashing to ensure integrity of documents. Each document's hash is kept on the blockchain, and any attempt at modification becomes traceable.
- **Session Management:** Ensures secure management of sessions to keep user interactions with the system secure.
- **Access Control:** Employing role-based access control to limit access to sensitive documents and functionality by roles.

6.6 Audit Trail

- **Immutable Records:** Offers an immutable audit record of all document-related activity, such as uploads, transfers, and verifications. This renders all action transparently logged and immutable.
- **Activity Logs:** Records complete histories of user activity such that administrators are able to monitor and audit system use.

Chapter 7

Implementation Details

The E-vault system is programmed using Python and Streamlit, driven by blockchain technology to store legal documents securely and transparently. The chapter provides an overview of how the application is to be installed, run, and executed, and instructions on how documents are to be stored and blockchain transactions conducted.

7.1 Setup Instructions

To get started with the E-vault system, follow these steps:

1. **Clone the Repository:**

   Clone the project repository from GitHub using the following command:sh

   - git clone https://github.com/Naveed-4/Block-Chain-Based-E-vault-for-Legal-Records.git
   - cd Block-Chain-Based-E-vault-for-Legal-Records

2. **Create a Virtual Environment:**

   - Create and activate a virtual environment for manage dependencies.

     python -m venv venv

   - Activate the virtual environment:
     - On Windows:sh

       venv\Scripts\activate

     - On macOS/Linux:sh

       source venv/bin/activate

3. **Install Dependencies:**

   Install dependencies listed in the requirements.txt file.sh

   - pip install -r requirements.txt

4. **Run the Application:**

   Run the Streamlit application using the following command:sh

   - streamlit run app.py

7.2 Usage Guide

Registration/Login:

- Go to the application in your web browser.
- Sign up for a new account by entering a username, email, and password, or sign in using current credentials.

Upload Documents:

- Click on the "Upload Document" page.
- Fill in the document details and choose the file you'd like to upload.
- Click on the "Save" button to save the document safely on the blockchain.

View Documents:

- Choose the "My Documents" page to view all your uploaded documents.
- Click the "View" button next to a document to view what it holds and the transaction history.

Transfer Documents:

- Click the "Transfer Document" page.
- Select the document to transfer and enter the recipient's username.
- Transfer the ownership of the document securely with blockchain.

Explore Blockchain:

- Utilize the application of the "Blockchain Explorer" feature to illustrate the blockchain structure and ensure its integrity.
- Present transaction and block information to provide transparency.

7.3 Checking Document Storage and Blockchain Transactions

Document Storage:

- AES-encrypted documents are locally stored in the storage directory.
- The document_storage.py application controls the document storage system such that documents are adequately encrypted before storage.

Blockchain Transactions:

- Blockchain transactions such as document uploads and transfers are regulated by the blockchain directory.
- The foundation blockchain classes exist in blockchain.py, and storage of blockchain data is in persistence.py.

- User authentication and transaction processing are handled by auth.py and evault_controller.py.

Files and Directories:

- **Main Application:** app.py
- **Blockchain Implementation:** blockchain/
    - blockchain.py: Core blockchain classes
    - persistence.py: Blockchain storage
    - auth.py: User authentication
    - evault_controller.py: Main controller
- **Document Storage:** storage/
    - document_storage.py: Document storage system
- **Dependencies:** requirements.txt

By following these steps, you can install and use the E-vault system, use the application through its user interface, and enjoy the secure storage and transfer of legal documents through the help of blockchain technology.

Chapter 8

Results

Figures 8.1 to 8.11 are the screenshots of project in run using stream lit in localhost with description of the figure.

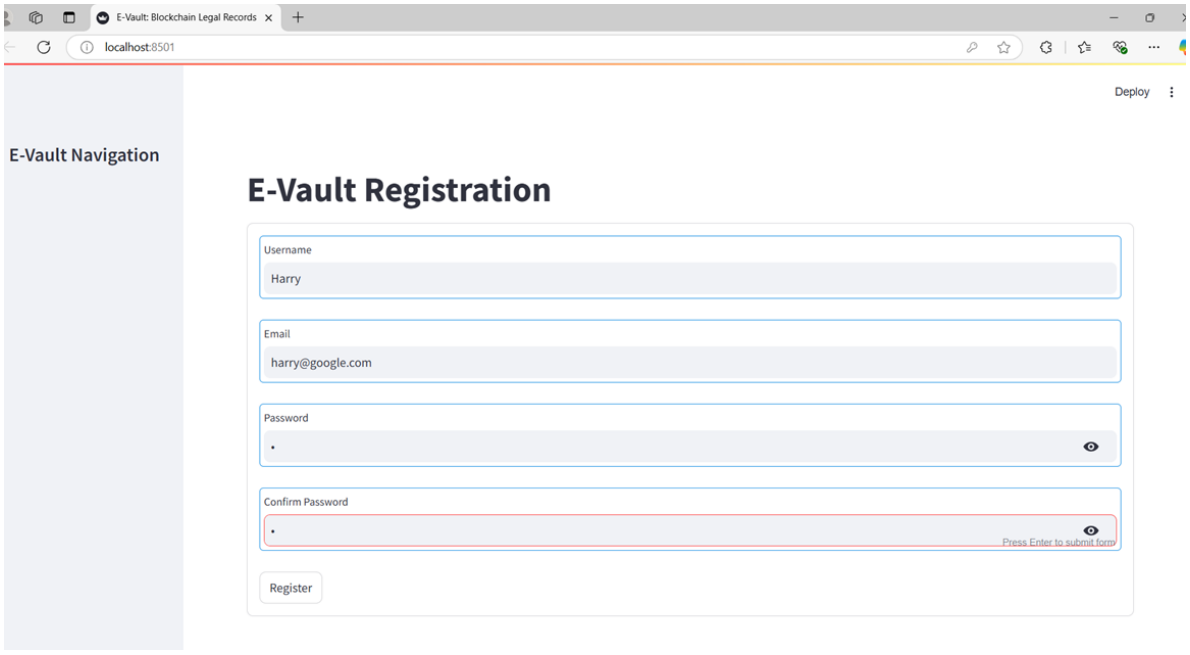

Figure 8.1: Landing Page

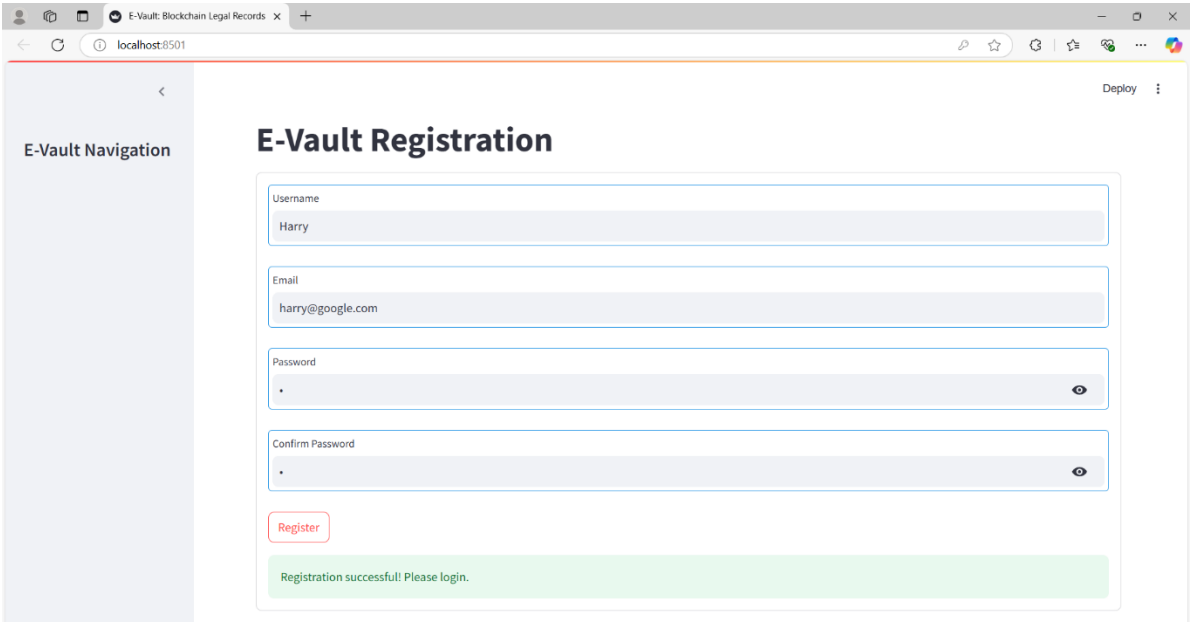

Figure 8.2: Registration Page: Harry registered

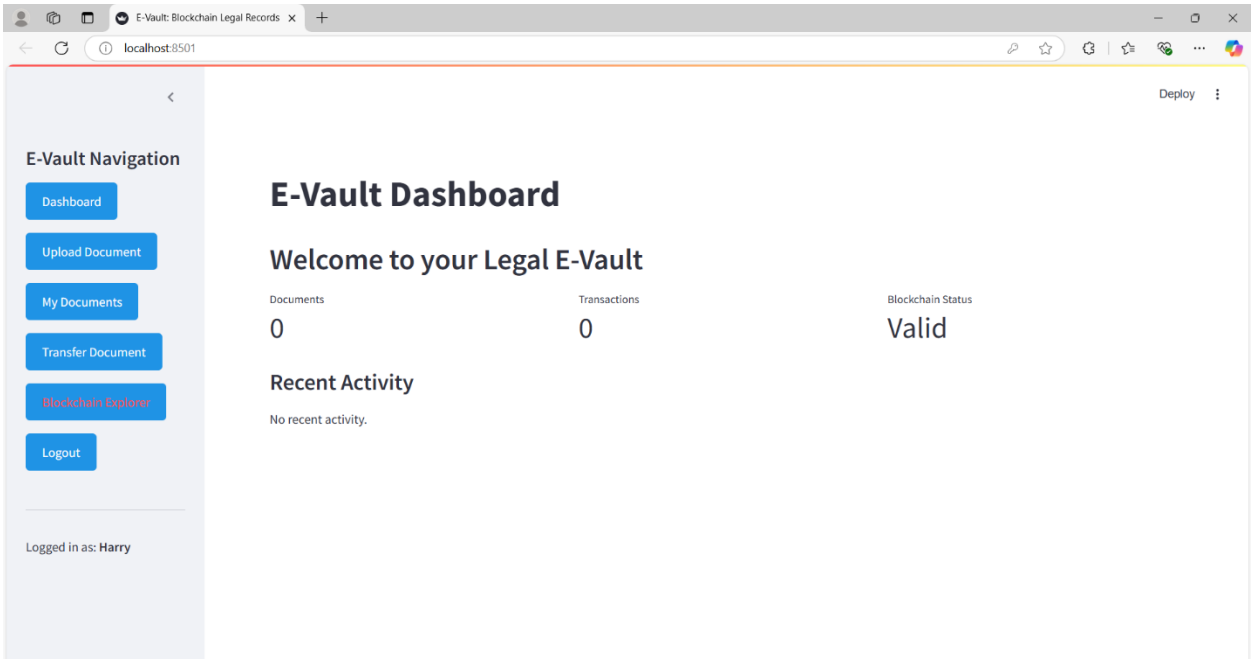

Figure 8.3: Initial Dashboard: Harry

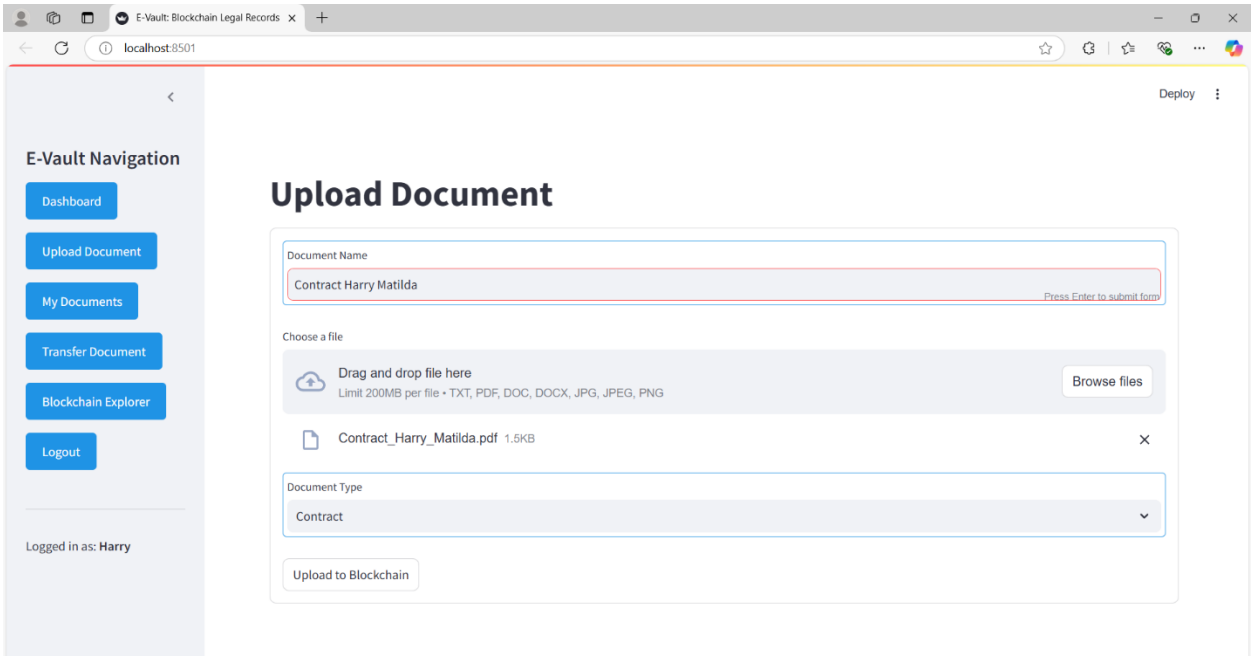

Figure 8.4: Uploading Document\Contract: Harry

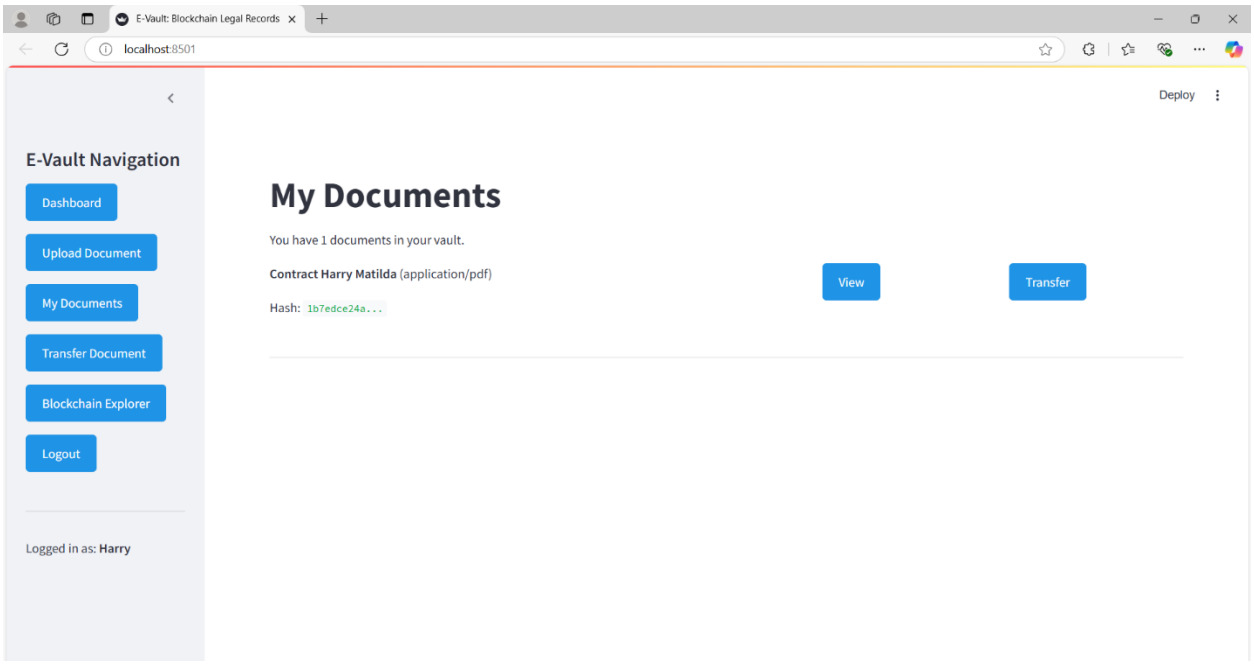

Figure 8.5: My Documents Page: Harry

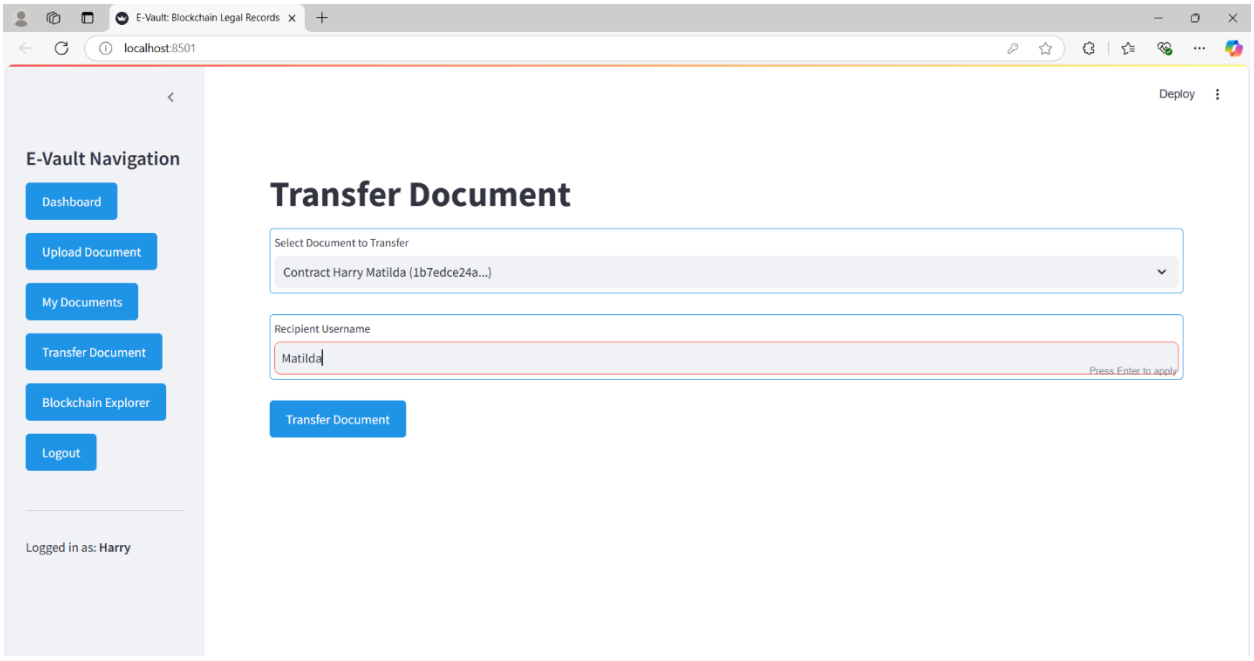

Figure 8.6: Transfer Document: Harry transferring to Matilda

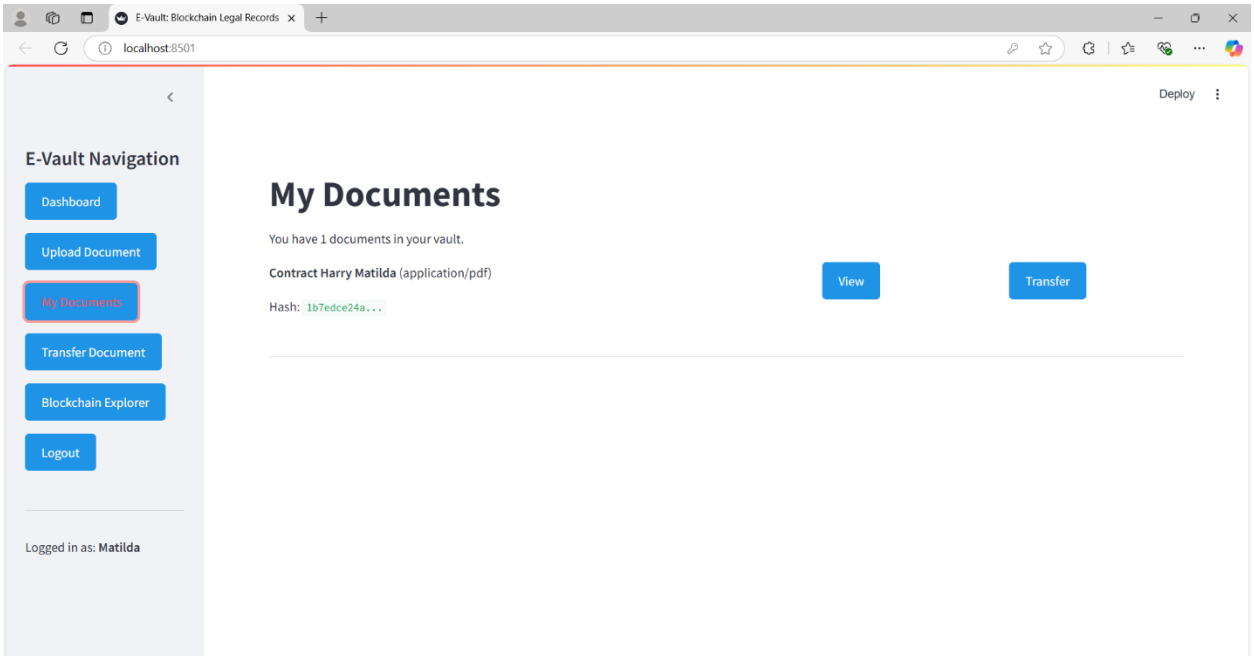

Figure 8.7: My Documents Page: Matilda –User 2. File Transferred

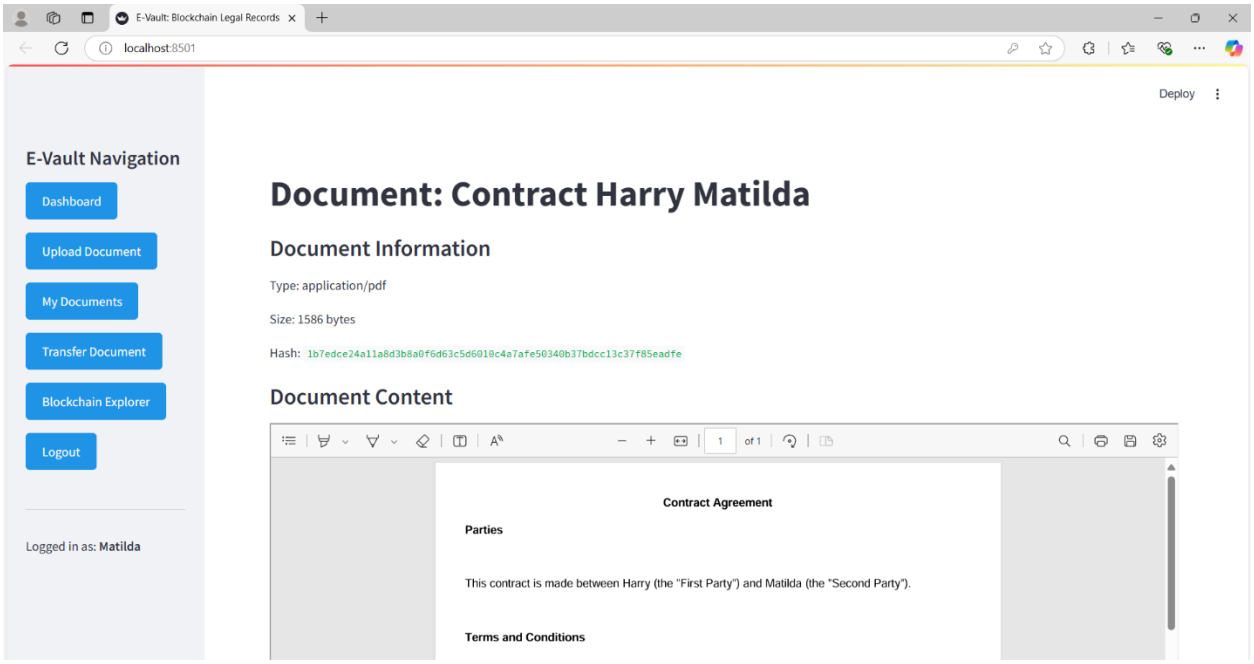

Figure 8.8: Viewing the Document: Matilda –User 2.

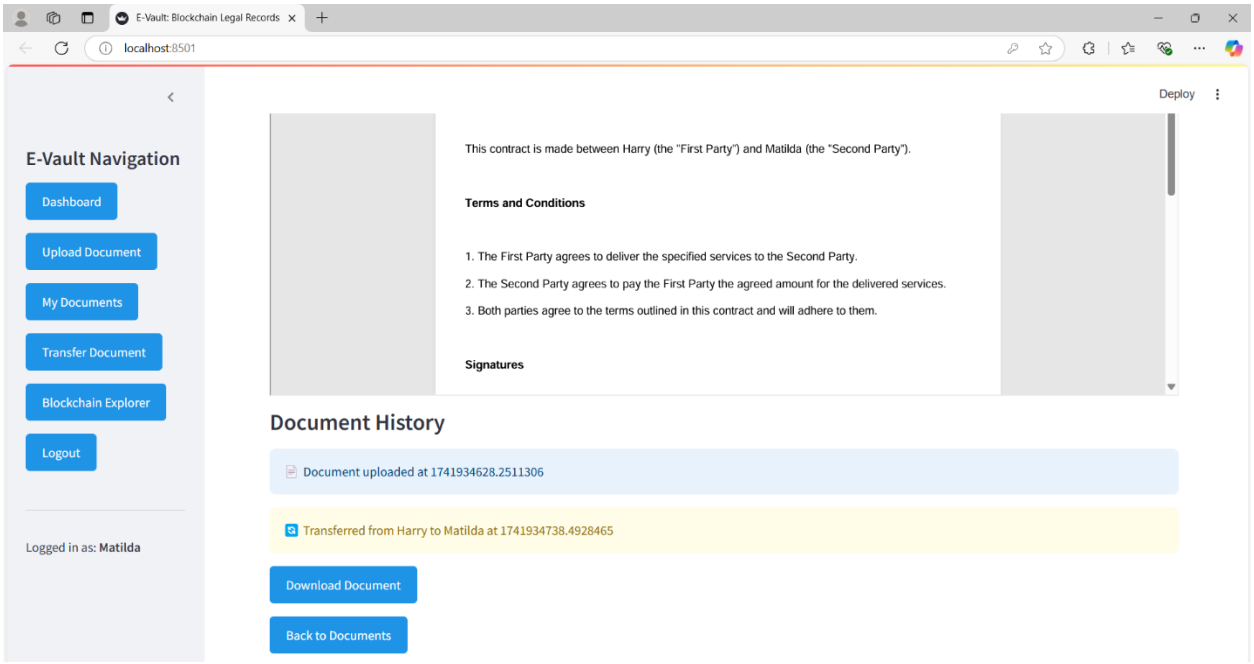

Figure 8.9: Document History is shown below while viewing the document: Matilda –User 2.

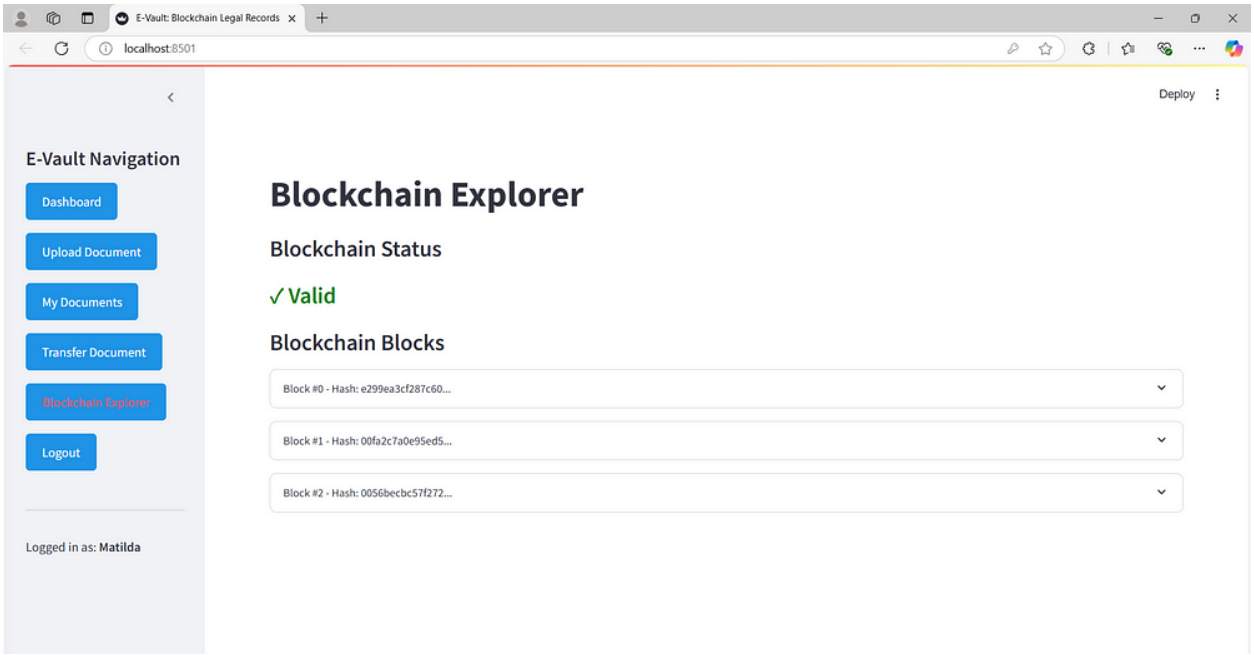

Figure 8.10: Blockchain Explorer Page

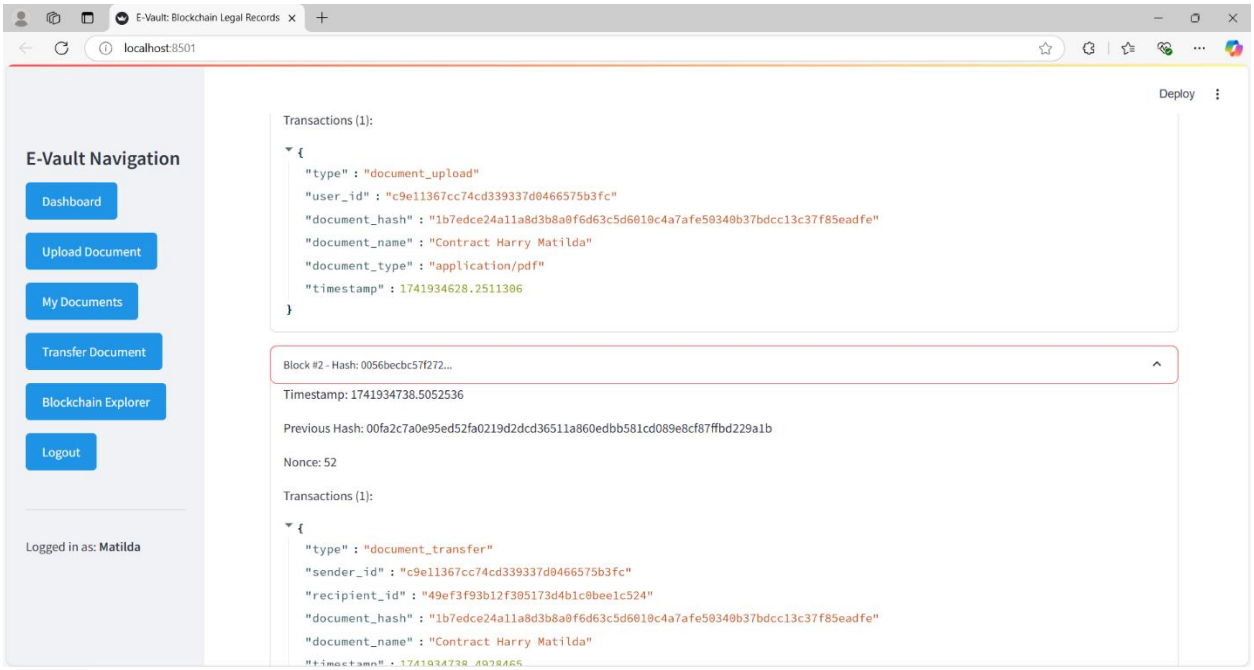

Figure 8.11: Blockchain explorer: Tracks all transactions

Figures 8.12 to 8.14 are the screenshots of document storage structure generated after running the application with Description of the figure.

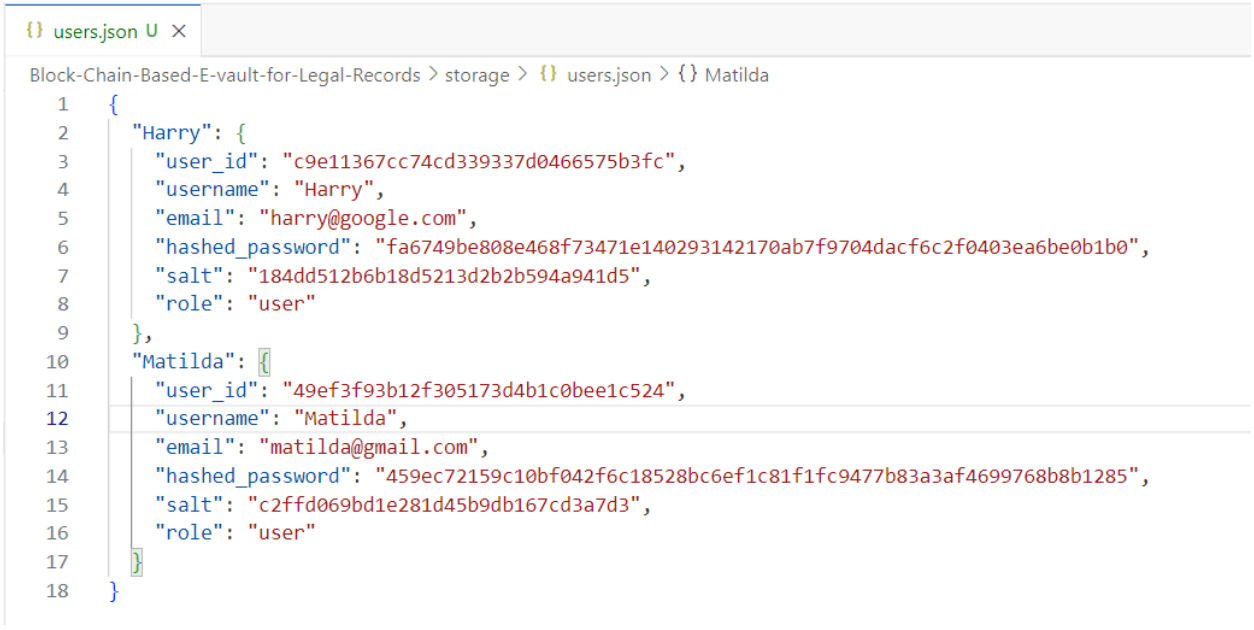

Figure 8.12: Users Info: Harry and Matilda

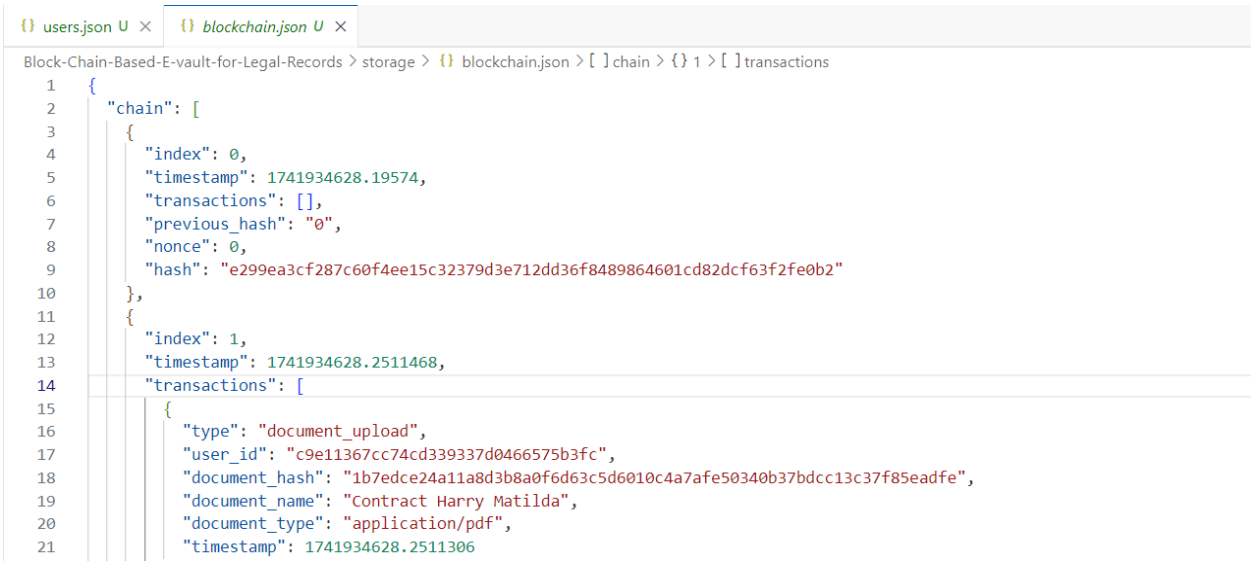

Figure 8.13: Blockchain: All Transactions are tracked

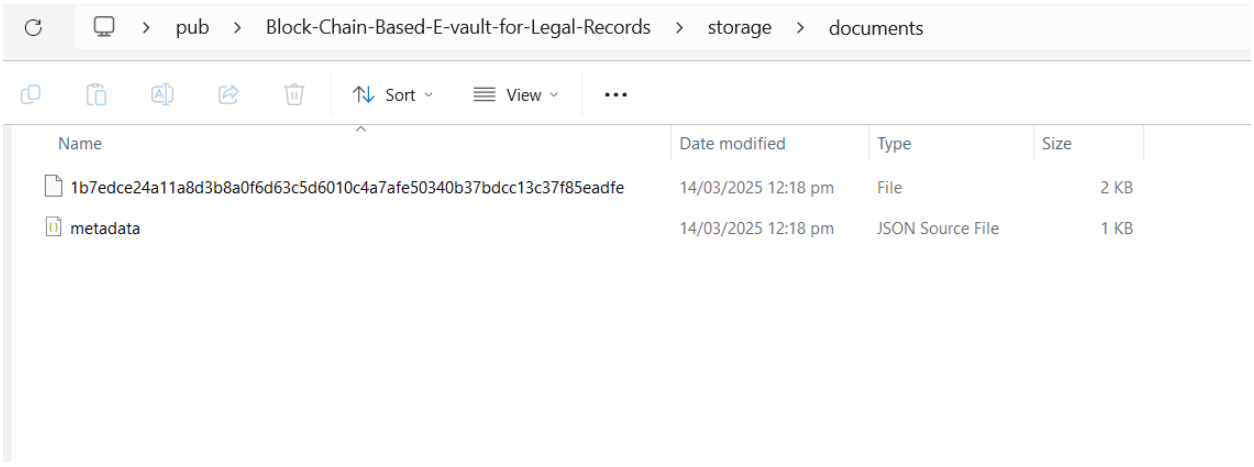

Figure 8.14: Documents Stored as Encrypted

Chapter 9

Challenges and Solutions

9.1 Challenge: Ensuring Document Integrity and Security

Problem: Integrity and security of legal documents are of the utmost importance. Traditional systems are vulnerable to tampering and unauthorized access, which can render the authenticity and confidentiality of legal documents useless.

Solution:

- **Blockchain Technology:** By leveraging blockchain's immutable ledger, we ensure that any tampering with documents is easily detectable. Each document's hash is stored on the blockchain, providing a verifiable proof of integrity.
- **AES Encryption:** Documents are encrypted using AES before storage, ensuring that only authorized users can access the document contents.
- **SHA-256 Hashing:** Each document is hashed using SHA-256 to produce a unique fingerprint. This hash is stored on the blockchain, creating a tamper-proof record of the document.

9.2 Challenge: Managing Document Ownership and Transfer

Problem: Traditional systems primarily utilize manual document transfer methods, which are time-consuming and prone to errors.

Solution:

- **Automated Transfers of Ownership:** Secure and automatic transfers of ownership of documents are enabled by E-vault system through blockchain transactions. It is performed to bring about accuracy and efficiency, minimizing room for mistakes.
- **Transparent Transfer Record:** Each transfer record is stored on the blockchain, developing an open and unmodifiable record of the ownership of documents. Users are now able to review the transfer history and verify ownership records.

9.3 Challenge: Ensuring System Usability and Accessibility

Issue: It is complicated and intimidating for lay users to use and understand blockchain technology.

Solution:

- **Streamlit Interface:** Streamlit is utilized by the E-vault system to create a user interface. This offers access with the blockchain system and facilitates easy access for legal professionals without requiring high-level technical expertise.
- **Intuitive Design:** The interface is easy to understand and utilize workflows for uploading documents, viewing, verification, and transfer. It is convenient for the user and enables users to accomplish tasks on time required.

9.4 Challenge: Scalability and Performance

Problem: The greater the number of documents and transactions, the greater the system load with the more complex work without the degradation of performance.

Solution:

- **Lightweight Blockchain Implementation:** The lightweight blockchain implementation is efficiency- and performance-oriented, enabling the system to support a large volume of transactions without redundant delays.
- **Efficient Storage:** Blockchain information and encrypted files are stored with efficient storage mechanisms, allowing rapid retrieval and processing of information.
- **Modular Structure:** Modularity within the E-vault system enables simple maintenance and scalability. One module can be added or modified separately without affecting the remainder of the system, and thus the system expands and develops but doesn't change the entire system.

With such specially tailored solutions to such problems, the E-vault system provides a secure, efficient, and easy-to-use platform for the management of legal documents through the use of blockchain technology.

Chapter 10

Conclusion and Future Scope

10.1 Conclusion

The "E-vault Using Blockchain for Secure Storage and Transfer of Legal Documents" project makes evident blockchain technology's capability to revolutionize the management of legal documents. Using blockchain, advanced encryption techniques, and user-friendly interface, the E-vault system addresses pressing challenges common in conventional document management systems, including document integrity, security, transparency, and efficiency.The most significant achievements of the project are:

- **Secure Document Storage:** AES encryption provides confidentiality of the documents, and SHA-256 hashing provides their integrity.
- **Immutable Audit Trail:** The blockchain gives an open and immutable audit trail of all document activity, such as upload, transfer, and verification.
- **Automated Ownership Transfer:** The system enables secure and automated transfer of ownership of the documents, minimizing errors and increasing efficiency.
- **Simple User Interface:** The user interface based on Streamlit is simple for legal professionals to work with, and they can leverage the blockchain without needing to know the behind-the-scenes details.
- **Improved Security:** Because it is decentralized, the blockchain reduces the number of points of failure and makes the system overall more secure.

In general, the E-vault system is a cost-efficient and economic legal record retention solution that has access security and auditable, tamper-evident records.

10.2 Future Scope

The E-vault system is a solid ground where documents can be placed, but there are numerous areas where development and expansion could be incorporated:

- **Smart Contracts:** Smart contracts can be incorporated into the system in a bid to computerize legal sophistications like rule-based document exchange and condition-based access control. This would add even more functionality and efficiency in the system.

- **Biometric Authentication:** Biometric authentication systems like fingerprint recognition or face recognition can also make user authentication and security more convenient.
- **Mobile Interface:** It would be possible for the users of the E-vault system to be online in real time with the development of a mobile app, and the system would be more user-friendly and convenient.
- **Interoperability with Other Systems:** The system can also be interfaced with other legal and document management systems in a standardized manner through APIs so that data can be merged or shared seamlessly.
- **Scalability Upgrades:** Upgrading the blockchain deployment to accommodate even larger volumes of documents and transactions as the system expands in size.
- **Forward-looking Reporting:** Incorporating forward-looking reporting and analytics functionality to provide insights into document usage, transferal trends, and system performance.
- **Compliance with the Law:** Assuring compliance with future legal and regulatory requirements for data protection, privacy, and electronic signatures.

Through such prospects for future growth, the E-vault system can further expand and evolve to accommodate the developments that are needed in the practice of law, providing an extensive and secure legal document management solution.

References

[1] Gamage, H.T.M. et al. (2020) A survey on blockchain technology concepts, applications, and issues. SN Computer Science, 1, pp. 1–15. Google Scholar

[2] Kaur, J. et al. (2022) July. Literature Review of Smart Contracts Using Blockchain Technology. In International Workshop on New Approaches for Multidimensional Signal Processing (pp. 171–187). Singapore: Springer Nature Singapore.Google Scholar

[3] Ali, O. et al. (2021) A comparative study: Blockchain technology utilization benefits, challenges and functionalities. IEEE Access, 9, pp. 12730–12749. Google Scholar

[4] Firdous Sadaf M. Ismail, & Dattatraya S Adane. (2022). Blockchain Technology: Growing Usecases and Issues to Tackle. International Journal of Next-Generation Computing, 13(5).Google Scholar

[5] Ismail, F.S.M., Mushtaque, S.G.M. (2022). Comprehensive Evolution of Pharmaceutical Industries by Pioneering Blockchain Technology with 6G Wireless Networks Amalgamation. In: Dutta Borah, M., Singh, P., Deka, G.C. (eds) AI and Blockchain Technology in 6G Wireless Network. Blockchain Technologies. Springer, Singapore.Google Scholar

[6] Ismail, F. S., Mushtaque, S. G., & Adane, D. (2023). Struggles, Potential, and Research Angles in the Amalgamation of Blockchain Technology With 6G Networks. In M. Borah, S. Wright, P. Singh, & G. Deka (Eds.), Role of 6G Wireless Networks in AI and Blockchain-Based Applications (pp. 167–196). IGI Global. Google Scholar

[7] Sarwar, M.I. et al. (2021) Data vaults for blockchain-empowered accounting information systems. IEEE Access, 9, pp. 117306–117324.Google Scholar

[8] Paul, A. et al. (2004) Design of a secure and fault tolerant environment for distributed storage. Georgia Tech Center for Experimental Research in Computer Science (CERCS) Technical Report GIT-CERCS-04-02.Google Scholar

[9] Hasan, R. et al. (2007). Requirements of Secure Storage Systems for Healthcare Records. In: Jonker, W., Petković, M. (eds) Secure Data Management. SDM 2007. Lecture Notes in Computer Science, vol 4721. Springer, Berlin, Heidelberg.Google Scholar

[10] Li, H. and Han, D. et al. (2019) EduRSS: A blockchain-based educational records secure storage and sharing scheme. IEEE access, 7, pp. 179273–179289.Google Scholar

[11] Verma, A. et al. (2021) NyaYa: Blockchain-based electronic law record management scheme for judicial investigations. Journal of Information Security and Applications, 63, p. 103025.Google Scholar

[12] Gururaj, H.L. et al. (2020) Blockchain: A new era of technology. Cryptocurrencies and blockchain technology applications, pp. 1–24.Google Scholar

[13] Rupa, C. et al. (2021) Web-Based Knowledge Management Distributed Application for Medical Certificates Using Blockchain Technology. Knowledge Management and Web 3.0: Next Generation Business Models, 2, p. 141.Google Scholar

[14] Mahamure, S.S. et al. (2020) Blockchain Technology for Real Estate Documents Protection Using Ethereum. International Journal of Future Generation Communication and Networking, 13(3), pp. 1287–1295.Google Scholar

Software and Libraries

1. **Python:** General-purpose programming language used for the entire project.
2. **Streamlit:** Web app framework for developing the user interface. Documentation**:** https://docs.streamlit.io/
3. **PyCryptodome:** Library for cryptographic operations, including AES encryption and SHA-256 hashing. Documentation: https://www.pycryptodome.org/
4. **SQLite:** Lightweight database for storing user information and document metadata.

GitHub Repository: Source code and project repository. GitHub: https://github.com/Naveed-4/Block-Chain-Based-E-vault-for-Legal-Records