**E-VAULT USING BLOCKCHAIN TO STORE AND TRANSFER 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

**Mohammed Mudassir Hussain (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**

Associate Professor, School of CS&AI.



SR University, Ananthsagar,Warangal,Telagnana-506371

**SR University**

Ananthasagar, Warangal.

**

**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 Dr. M. Sheshikala**

Associate Professor, Professor & Head,

**School of CS&AI School of CS&AI,**

SR University SR University,

Anathasagar, Warangal Anathasagar, Warangal

**Reviewer-1 Reviewer-2**

Name: Name:

Designation: Designation:

Signature: Signature:

**ACKNOWLEDGEMENT**

We owe an enormous debt of gratitude toour Capstone project guide **Dr. Balajee Maram, Associate Professor** as well as Head of the School of CS&AI, **Dr. M. Sheshikala, Professor** andDean 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 industry faces challenges in securely storing, transferring, and verifying legal records with traditional systems. The "E-vault using Blockchain to Store and Transfer Legal Records" project proposes a blockchain-based solution to enhance security, integrity, and transparency in legal record management.

The E-vault system creates a secure, immutable platform for managing legal records by integrating blockchain technology. This ensures that documents remain tamper-proof, with an indisputable history of ownership and transfer. The project employs a lightweight blockchain implementation in Python, focusing on cryptographic hashing and proof-of-work consensus mechanisms.

To ensure secure document storage, the project uses AES encryption and SHA-256 hashing. Document metadata, including the document hash, name, type, owner ID, and creation timestamp, is stored on the blockchain, providing a transparent and immutable record of all document activities.

A user-friendly interface is developed using Streamlit, enabling intuitive interaction with the blockchain system. Features include user registration and authentication, document upload and storage, document viewing and verification, and secure document transfer. The blockchain explorer feature allows users to view transaction history and verify blockchain integrity.

The project plan includes Core Components Development, Integration and Testing, and Final Touches. Key objectives include developing a lightweight blockchain solution for document verification, creating a secure document storage system, establishing a transparent document transfer mechanism, and building an accessible user interface.

The E-vault blockchain project demonstrates the potential of blockchain technology to enhance the security, transparency, and efficiency of legal document management. By providing a tamper-proof, self-verifying, and immutable platform, the E-vault system addresses critical challenges faced by traditional systems, offering a scalable and practical solution for the legal industry. Future enhancements could include smart contracts for rule-based document transfers, biometric authentication, and a mobile interface for on-the-go access.

# CONTENTS

**Abstract ii**

**S. No. Chapter Page No.**

**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 06

**4** System architecture/Technical Specifications 09

4.1 System architecture 09

4.2 Technical Specifications 11

**5** Methodology 13

**6** Feature and Functionalities 17

**7** Implementation details 22

**8** Results 25

**9** Challenges and Solutions 27

9.1 Data Integration Challenges 27

9.2. Real-Time Data Fetching 27

9.3. API Rate Limits 28

9.4. Evaluation of Models 28

**10** Conclusion and Future Scope 30

10.1 Conclusion 30

10.2 Future Scope 31

References 32

# LIST OF TABLES

**S. No. Tables Page No.**

**2.1.1** Tabular representation of Literature Survey 03

**3.2.1** Existing vs Proposed Methods 08

# LIST OF FIGURES

**S. No. Figures Page No.**

**4.1.1** System Architecture Flowchart 09

**5.1** Proposed Methodology 13

**7.1** User Interface 25

**7.2** After giving input (track and artist name) 25

**7.3** Recommendations are generated as containers 26

for each model

**7.4** Recommendations given by Cosine Similarity 26

in its container

# Chapter 1

# Introduction

The legal industry is increasingly challenged by the need for secure, transparent, and tamper-proof management of legal records. Traditional document management systems often rely on centralized databases, creating single points of failure and introducing potential vulnerabilities in document integrity and security. These systems struggle to provide verifiable proof of document ownership, transparent transfer histories, and maintaining document integrity over time.

Blockchain technology, known for its decentralized and immutable nature, offers a promising solution to these challenges. By leveraging cryptographic principles and distributed ledger technology, blockchain can ensure the integrity, transparency, and security of legal records without the need for trusted third parties. This project, "E-vault using Blockchain to Store and Transfer Legal Records," aims to develop a blockchain-based platform that securely stores and transfers legal records, ensuring document integrity and providing a transparent and immutable history of document transactions.

The E-vault system integrates a lightweight blockchain implementation with advanced encryption techniques to create a secure and user-friendly platform for managing legal records. The project employs Python for blockchain implementation, focusing on cryptographic hashing and proof-of-work consensus mechanisms to validate transactions and secure the blockchain. Additionally, the system uses AES encryption and SHA-256 hashing to ensure the confidentiality and integrity of stored documents.

A key feature of the E-vault system is its user-friendly interface, developed using Streamlit. This interface allows users to interact intuitively with the blockchain system, providing functionalities for user registration and authentication, document upload and storage, document viewing and verification, and secure document transfer. The interface also includes a blockchain explorer, enabling users to view transaction history and verify the integrity of the blockchain.

## 1.1 Problem Statement

The legal industry faces significant challenges in securely managing legal records due to the limitations of traditional document management systems. These challenges include:

**Tamper-Proof Integrity:** Ensuring that documents have not been altered without detection.

**Verifiable Ownership:** Providing clear and verifiable proof of document ownership.

**Transparent Transfer Histories:** Creating transparent and immutable histories of document transfers.

**Security Vulnerabilities:** Addressing potential vulnerabilities in centralized systems, including single points of failure.

**Efficiency and Scalability:** Handling and processing large volumes of documents efficiently.

Traditional document management systems, which often rely on centralized databases and access control mechanisms, are ill-equipped to meet these challenges. They require trusted third parties for verification, introducing potential security vulnerabilities and transaction costs. Moreover, these systems struggle to 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 challenges by leveraging the security, transparency, and immutability of blockchain technology. The E-vault system aims to:

**Ensure Document Integrity:** Implement a lightweight blockchain solution for document verification using cryptographic hashing and proof-of-work.

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

**Transparent Document Transfer:** Establish a transparent and immutable document transfer mechanism.

**User-Friendly Interface:** Build an accessible interface using Streamlit to make blockchain technology accessible to legal professionals.

**Audit Trail:** Provide a comprehensive audit trail for all document activities.

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.

# 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 Healthcare Records | Data Privacy | Requirements for secure healthcare data storage | Focused on healthcare, not generalizable |
| 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

The literature survey provides a comprehensive analysis of the advancements and applications of blockchain technology across various domains. Gamage et al. (2020) offered a detailed overview of blockchain concepts, highlighting its security and transparency benefits [1]. Kaur et al. (2022) focused on the implementation of smart contracts using blockchain, emphasizing contract automation and its legal implications [2]. Ali et al. (2021) compared the benefits and functionalities of blockchain technology, identifying its efficiency and security advantages [3].

In the context of specific use cases, Ismail and colleagues explored the integration of blockchain with 6G networks, addressing potential benefits and challenges [5][6]. Sarwar et al. (2021) proposed secure data vaults for accounting systems empowered by blockchain, showcasing the technology's potential in enhancing data integrity [7]. Verma et al. (2021) introduced a blockchain-based electronic law record management scheme, demonstrating its application in judicial investigations [11].

The survey also covered early designs of secure distributed storage systems, such as the work by Paul et al. (2004), which provided foundational insights into secure storage mechanisms [8]. Hasan et al. (2007) discussed the requirements for secure storage systems specifically for healthcare records, highlighting the importance of data privacy [9].

Leveraging insights from these studies, our project aims to develop a blockchain-based E-vault system for storing and transferring legal records. By incorporating advanced encryption techniques, a custom lightweight blockchain implementation, and a user-friendly interface, the E-vault system addresses critical challenges such as document integrity, security, and scalability. The integration of a Streamlit-based interface further enhances accessibility, enabling legal professionals to interact with the blockchain system effortlessly.

# Chapter 3

# Existing Methods Vs. Proposed Method

## 3.1 Existing Methods

**Traditional Document Management Systems (DMS)** rely on centralized databases and access control mechanisms to manage documents. These systems provide basic functionalities such as document storage, retrieval, and access control but face significant limitations:

* **Centralized Trust Model:** These systems depend on a central authority for managing and verifying documents, creating single points of failure and requiring users to trust system administrators.
* **Tampering Detection:** Limited capabilities in detecting document tampering. Any modifications made to documents may not be easily traceable, leading to potential integrity issues.
* **Ownership Transfer:** Manual and often cumbersome processes for transferring document ownership, which can lead to delays and errors.
* **Audit Trail:** While audit trails exist, they can be modified by administrators, compromising the integrity of the document history.
* **Verification:** Requires third-party verification to establish document authenticity, introducing additional costs and potential delays.
* **Security:** Vulnerable to security breaches due to centralized storage, making them susceptible to hacking and data loss.
* **User Experience:** Often complex and not user-friendly, requiring extensive training for effective use.

**Blockchain-Based Document Management**

Blockchain technology offers a distributed approach to document management, using cryptographic principles to ensure data integrity. Key features of blockchain-based systems include:

* **Decentralized Trust Model:** Trust is distributed across the network, eliminating the need for a central authority and reducing single points of failure.
* **Tampering Detection:** Cryptographic hashing ensures that any tampering with documents is easily detectable, providing strong integrity guarantees.
* **Ownership Transfer:** Automated and secure ownership transfer using blockchain transactions, ensuring accuracy and efficiency.
* **Audit Trail:** Immutable audit trails that cannot be modified, ensuring a transparent and verifiable history of all document transactions.
* **Verification:** Self-verifying documents using cryptographic proofs, eliminating the need for third-party verification.
* **Security:** Enhanced security through distributed storage and cryptographic techniques, making it resilient to hacking and data loss.
* **User Experience:** Potentially more user-friendly with modern interfaces, though still in early stages of adoption in legal management.

## 3.2 Proposed Methods

The E-vault system leverages blockchain technology to address the limitations of traditional document management systems. Our proposed methods include:

**Lightweight Blockchain Implementation**

* **Custom Blockchain:** Implementation of a lightweight blockchain using Python, focusing on cryptographic hashing and proof-of-work consensus mechanisms to validate transactions and secure the blockchain.
* **Document Hashing:** Each document is hashed using SHA-256 to ensure integrity, with the hash stored on the blockchain to create a tamper-proof record.

**Secure Document Storage**

* **Encryption:** Documents are encrypted using AES (Advanced Encryption Standard) to ensure confidentiality. The encrypted documents are stored locally, with their hashes recorded on the blockchain for integrity verification.
* **Metadata Storage:** Document metadata, including the document hash, name, type, owner ID, and creation timestamp, is stored on the blockchain, providing a transparent and immutable record of all document-related activities.

**Streamlit Interface**

* **User Registration and Authentication:** Streamlit-based interface for user registration and authentication, ensuring secure access to the system.
* **Document Management:** Intuitive interface for document upload, storage, viewing, and verification, allowing users to interact seamlessly with the blockchain system.
* **Document Transfer:** Secure document transfer mechanism using blockchain transactions, ensuring accurate and efficient ownership transfer.
* **Blockchain Explorer:** Feature allowing users to view transaction history and verify the integrity of the blockchain.

**Comprehensive Audit Trail**

* **Immutable Records:** All document transactions are recorded on the blockchain, providing an immutable audit trail that cannot be modified.
* **Transparency:** Users can view the complete history of document activities, ensuring transparency and trust in the system.

**Enhanced Security**

* **Distributed Trust:** The distributed nature of the blockchain eliminates single points of failure and enhances security.
* **Cryptographic Techniques:** Use of advanced cryptographic techniques to ensure data integrity and confidentiality.

**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.

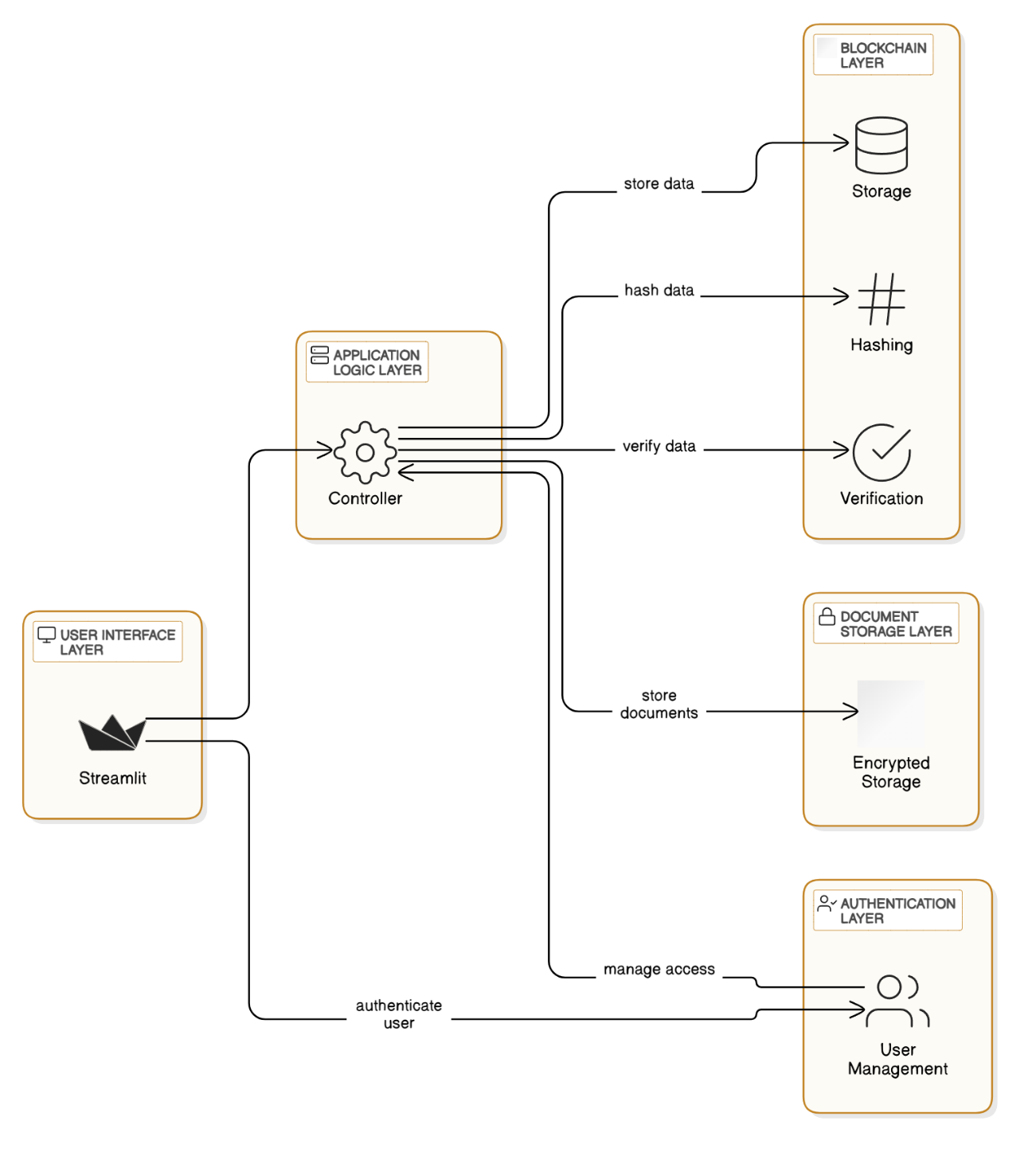
# Chapter 4

# System Architecture / Technical Specifications

## 4.1 System Architecture

The E-vault system is designed with a modular architecture to ensure scalability, security, and ease of maintenance. The architecture is divided into several layers, each responsible for specific functionalities. The key components of the system architecture include:

1. **User Interface Layer (Streamlit)**: This layer provides an intuitive and user-friendly interface for interacting with the E-vault system. It includes functionalities for user registration and authentication, document upload and storage, document viewing and verification, and secure document transfer. The interface also features a blockchain explorer for viewing transaction history.
2. **Application Logic Layer (Controller)**: This layer handles the core application logic, including user authentication, document management, and transaction processing. It acts as an intermediary between the user interface and the blockchain layer, ensuring seamless interaction and data flow.
3. **Blockchain Layer**: This layer is responsible for implementing the blockchain technology. It includes a custom lightweight blockchain, focusing on cryptographic hashing and proof-of-work consensus mechanisms to validate transactions and secure the blockchain. It ensures document integrity and provides a transparent and immutable history of document transactions.
4. **Document Storage Layer (Encrypted Storage)**: This layer manages the secure storage of documents. Documents are encrypted using AES (Advanced Encryption Standard) and hashed using SHA-256 for integrity verification. The encrypted documents are stored locally, with their hashes recorded on the blockchain.
5. **Authentication Layer (User Management)**: This layer handles user authentication and management. It ensures secure access to the system through user registration, login, and session management. User credentials are stored securely using salted password hashing techniques.
6. **Database Layer**: This layer stores non-blockchain data, such as user information and document metadata. It ensures quick retrieval and management of data required by the application logic layer.



**Figure 4.1.1:** System Architecture Flowchart

## 4.2 Technical Specifications

The technical specifications for the E-vault system include the following:

**Backend: Python**

The backend is developed using Python, leveraging its extensive libraries and frameworks for blockchain implementation, encryption, and web development.

**Blockchain: Custom Implementation**

The blockchain is a custom lightweight implementation using Python, focusing on cryptographic hashing (SHA-256) and proof-of-work consensus mechanisms.

**Encryption: AES (Advanced Encryption Standard)**

Documents are encrypted using AES to ensure confidentiality. The encryption key management is handled securely within the system.

**Hashing: SHA-256**

Document integrity is ensured using SHA-256 hashing. Each document is hashed, and the hash is stored on the blockchain to create a tamper-proof record.

**User Interface: Stream lit**

The user interface is developed using Stream lit, providing a simple and intuitive platform for users to interact with the E-vault system. Stream lit allows for rapid development and deployment of web applications.

**Database: SQLite (or any preferred lightweight database)**

The database layer uses SQLite for storing non-blockchain data, such as user information and document metadata. SQLite is chosen for its simplicity and ease of integration.

**Authentication: Salted Password Hashing**

User authentication is handled using salted password hashing techniques to ensure secure storage of user credentials.

**Development Environment:**

**Operating System:** Windows 11

**IDE:** Visual Studio Code

**Python Version:** 3.9 or later

**Dependencies:**

**streamlit:** For developing the user interface

**pycryptodome:** For encryption and hashing

**python-dotenv:** For managing environment variables

**Installation:**

The setup and installation of the development environment include creating a virtual environment, installing necessary dependencies, and setting up the project structure as outlined in the initial project setup instructions.

By adhering to these technical specifications, the E-vault system ensures a secure, scalable, and user-friendly platform for managing legal records using blockchain technology.

# Chapter 5

# Methodology

The E-vault system is designed to leverage blockchain technology for secure and transparent management of legal records. The methodology for developing the E-vault system involves several key steps, including blockchain implementation, document management, user authentication, and interface development. Each step is outlined in detail below.

**Step 1: Blockchain Implementation**

**Objective:** Develop a lightweight blockchain that can securely record transactions related to document storage and transfer.

* **Blockchain Structure:** The blockchain is implemented using Python. Each block contains an index, timestamp, list of transactions, previous block's hash, current block's hash, and a nonce value.
* **Hashing:** SHA-256 is used to hash the contents of each block, ensuring that any tampering with the block's data is easily detectable.
* **Proof-of-Work:** A simple proof-of-work algorithm is implemented to add blocks to the blockchain. This involves finding a nonce value that, when hashed with the block's data, produces a hash with a predetermined number of leading zeros.
* **Block Validation:** Each new block is validated by checking the hash of the previous block, ensuring the integrity of the blockchain.

**Step 2: Secure Document Storage**

**Objective:** Ensure documents are stored securely using encryption and hashing.

* **Encryption:** Documents are encrypted using AES (Advanced Encryption Standard) before being stored. This ensures that the contents of the documents remain confidential.
* **Hashing:** Each document is hashed using SHA-256 to produce a unique fingerprint. This hash is stored on the blockchain to ensure the document's integrity.
* **Storage:** Encrypted documents are stored locally on the system, with their metadata (including the hash) recorded on the blockchain.

**Step 3: User Authentication**

**Objective:** Implement a secure user authentication system to control access to the E-vault system.

* **User Registration:** Users can register by providing a username, email, and password. Passwords are hashed using a salted hashing technique before being stored.
* **Login:** Users can log in using their username and password. The system verifies the credentials by comparing the hashed password with the stored hash.
* **Session Management:** Once authenticated, users are granted a session token that allows them to interact with the system securely.

**Step 4: Document Management**

**Objective:** Provide functionalities for uploading, viewing, verifying, and transferring documents.

* **Document Upload:** Users can upload documents through the Streamlit interface. The system encrypts the document, hashes it, and stores both the encrypted document and its metadata.
* **Document Viewing:** Users can view their uploaded documents. The system decrypts the document for viewing while ensuring the document's integrity using the stored hash.
* **Document Verification:** Users can verify the integrity of their documents by comparing the document's current hash with the stored hash on the blockchain.
* **Document Transfer:** Users can securely transfer document ownership to other registered users. The transfer is recorded as a transaction on the blockchain, ensuring a transparent and immutable record.

**Step 5: Interface Development**

**Objective:** Develop a user-friendly interface using Stream lit for interacting with the E-vault system.

* **Stream lit Interface:** The interface includes functionalities for user registration, login, document upload, document viewing, document verification, and document transfer.
* **Blockchain Explorer:** An integrated blockchain explorer allows users to view the blockchain's transaction history and verify the integrity of the blockchain.
* **User Interaction:** The interface is designed to be intuitive and easy to use, enabling users to interact with the system without needing in-depth technical knowledge.

**Testing and Integration**

**Objective:** Ensure all components work seamlessly together and the system functions as intended.

* **Unit Testing:** Each component (blockchain, encryption, authentication, document management) is tested individually to ensure correct functionality.
* **Integration Testing:** The components are integrated, and end-to-end tests are performed to ensure the entire system works together seamlessly.
* **User Testing:** The system is tested by users to identify any usability issues and ensure the interface is intuitive and easy to use.

By following this methodology, the E-vault system is developed to provide a secure, transparent, and user-friendly platform for managing legal records using blockchain technology.

# Chapter 6

# Features and Functionalities

The E-vault system is designed to provide a comprehensive set of features and functionalities to ensure the secure, transparent, and efficient management of legal records. The following are the key features and functionalities of the E-vault system:

## 6.1 User Registration and Authentication

* **User Registration:** Allows new users to create an account by providing a username, email, and password. The system securely stores user credentials using salted password hashing techniques to ensure security.
* **User Authentication:** Facilitates user login by verifying credentials. Once authenticated, users are granted a session token for secure interactions with the system.
* **Role-Based Access Control:** Implements access control mechanisms to ensure that only authorized users can access or modify certain documents.

## 6.2 Secure Document Management

* **Document Upload:** Enables users to upload legal documents. The system encrypts each document using AES, hashes it using SHA-256, and stores the encrypted document locally. The document's metadata, including the hash, is recorded on the blockchain to ensure integrity.
* **Document Viewing:** Allows users to view their uploaded documents. The system decrypts the document for viewing and verifies its integrity using the stored hash.
* **Document Verification:** Provides functionality for users to verify the integrity of their documents by comparing the current document hash with the one stored on the blockchain.
* **Document Transfer:** Facilitates the secure transfer of document ownership to other registered users. The transfer is recorded as a transaction on the blockchain, ensuring a transparent and immutable record.

## 6.3 Blockchain Explorer

* **Transaction History:** Allows users to view the complete history of transactions recorded on the blockchain, including document uploads, transfers, and verification activities.
* **Block Details:** Provides detailed information about each block in the blockchain, including the block index, timestamp, previous hash, current hash, nonce value, and list of transactions.
* **Blockchain Integrity:** Displays the status of the blockchain, indicating whether it is valid and free from tampering.

## 6.4 User Interface (Streamlit)

* **Dashboard:** A user-friendly dashboard that provides an overview of the user's activities, including recent document uploads and transfers.
* **Upload Document:** A streamlined interface for uploading documents, where users can specify document details and upload files.
* **My Documents:** A section where users can view, verify, and transfer their uploaded documents.
* **Blockchain Explorer:** An integrated tool for exploring the blockchain, viewing transaction history, and verifying blockchain integrity.

## 6.5 Security Features

* **Encryption:** Uses AES encryption to ensure the confidentiality of stored documents. The encryption keys are managed securely within the system.
* **Hashing:** Utilizes SHA-256 hashing to ensure document integrity. Each document's hash is stored on the blockchain, making any tampering easily detectable.
* **Session Management:** Implements secure session management to ensure that user interactions with the system are protected.
* **Access Control:** Enforces role-based access control to restrict access to sensitive documents and functionalities based on user roles.

## 6.6 Audit Trail

* **Immutable Records:** Provides an immutable audit trail of all document-related activities, including uploads, transfers, and verifications. This ensures that all actions are transparently recorded and cannot be modified.
* **Activity Logs:** Maintains detailed logs of user activities, helping administrators to monitor and audit system usage.

# Chapter 7

# Implementation Details

The E-vault system is implemented using Python and Streamlit, leveraging blockchain technology for secure and transparent management of legal records. This chapter provides an overview of how to set up, run, and interact with the application, as well as details on document storage and blockchain transactions.

## 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

1. **Create a Virtual Environment:**
   * Create and activate a virtual environment to manage dependencies.

python -m venv venv

* + Activate the virtual environment:
    - On Windows:sh

venv\Scripts\activate

* + - On macOS/Linux:sh

source venv/bin/activate

1. **Install Dependencies:**

Install the required dependencies from the requirements.txt file.sh

* + - pip install -r requirements.txt

1. **Run the Application:**

Start the Streamlit application using the following command:sh

* + - streamlit run app.py

## 7.2 Usage Guide

**Registration/Login:**

* Navigate to the application in your web browser.
* Create a new account by providing a username, email, and password, or log in with existing credentials.

**Upload Documents:**

* Go to the "Upload Document" page.
* Enter the document details and select the file you wish to upload.
* Submit the form to securely store the document on the blockchain.

**View Documents:**

* Navigate to the "My Documents" page to view all your uploaded documents.
* Click the "View" button next to a document to see its content and transaction history.

**Transfer Documents:**

* Go to the "Transfer Document" page.
* Select the document you wish to transfer and enter the recipient's username.
* Securely transfer the document ownership via blockchain.

**Explore Blockchain:**

* Use the "Blockchain Explorer" feature to view the blockchain structure and verify its integrity.
* View details of transactions and blocks to ensure transparency.

## 7.3 Checking Document Storage and Blockchain Transactions

**Document Storage:**

* Uploaded documents are encrypted using AES and stored locally in the storage directory.
* The document\_storage.py file manages the document storage system, ensuring that documents are securely encrypted before storage.

**Blockchain Transactions:**

* Blockchain transactions, including document uploads and transfers, are managed by the blockchain directory.
* The blockchain.py file contains the core blockchain classes, while persistence.py handles the storage of blockchain data.
* User authentication and transaction processing are managed by auth.py and evault\_controller.py.

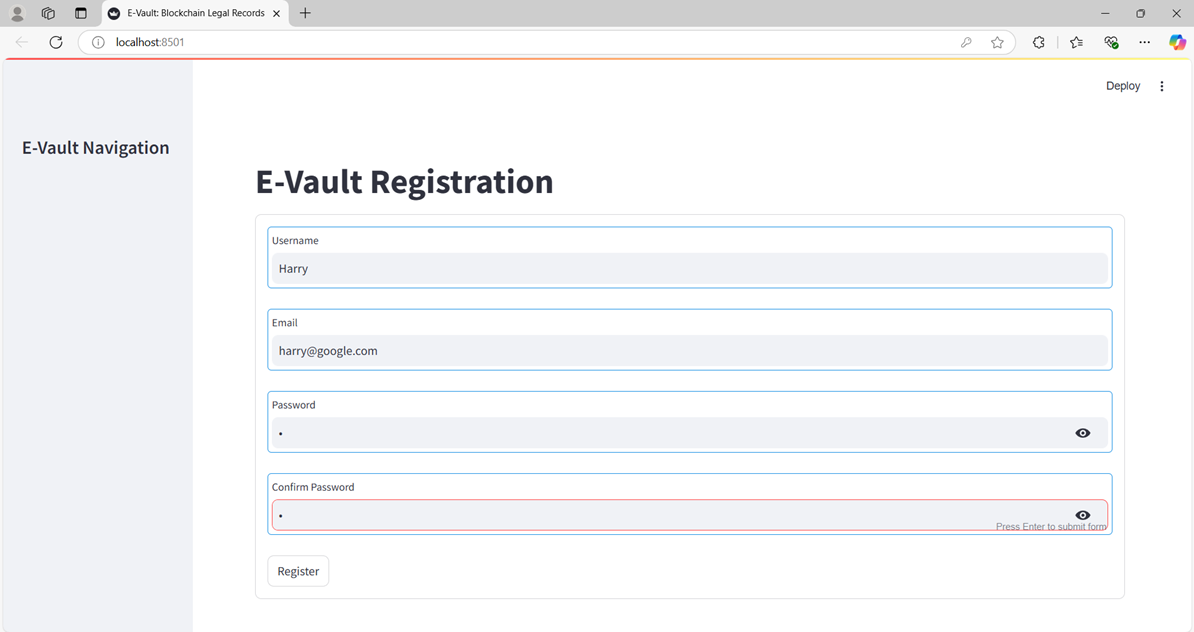
**Files and Directories:**

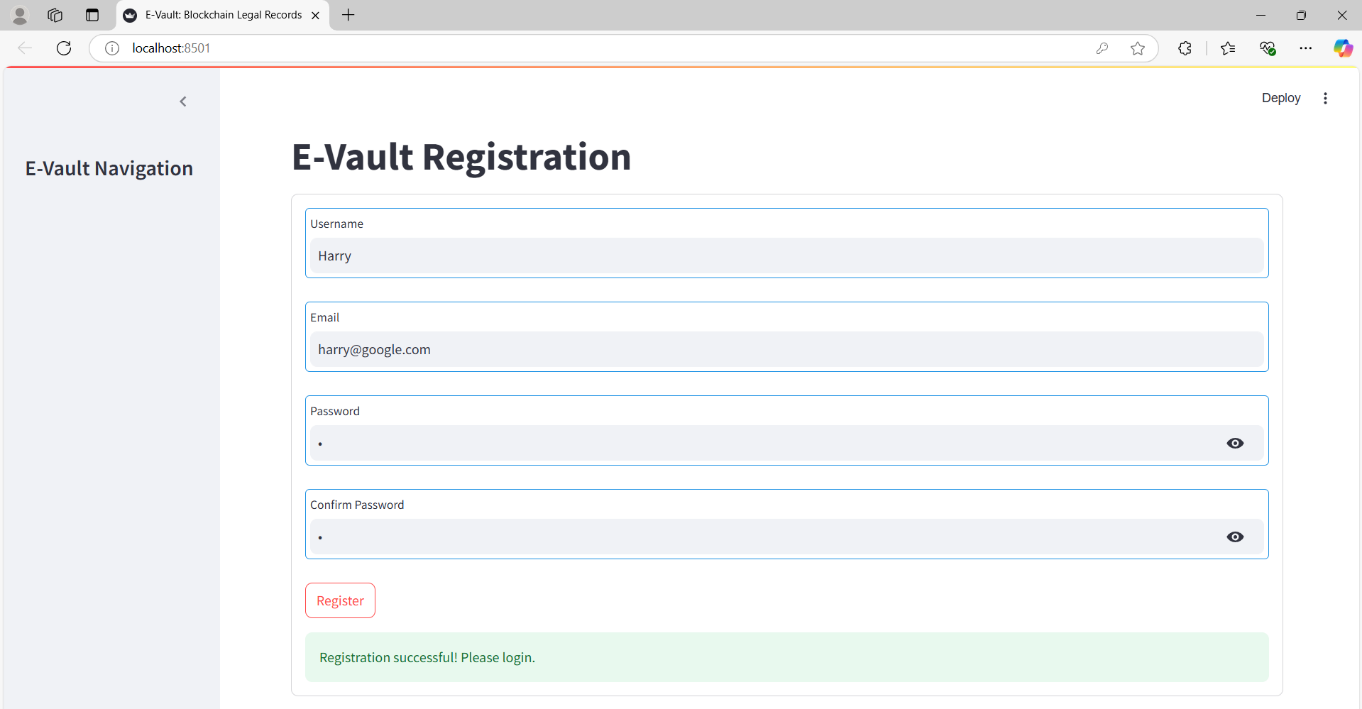
* **Main Application:** app.py
* **Blockchain Implementation:** blockchain/
  + blockchain.py: Core blockchain classes
  + persistence.py: Blockchain storage
  + auth.py: User authentication
  + evault\_controller.py: Main controller
* **Document Storage:** storage/
  + document\_storage.py: Document storage system
* **Dependencies:** requirements.txt

By following these instructions, you can set up and run the E-vault system, interact with the application through its user-friendly interface, and ensure the secure storage and transfer of legal documents using blockchain technology.

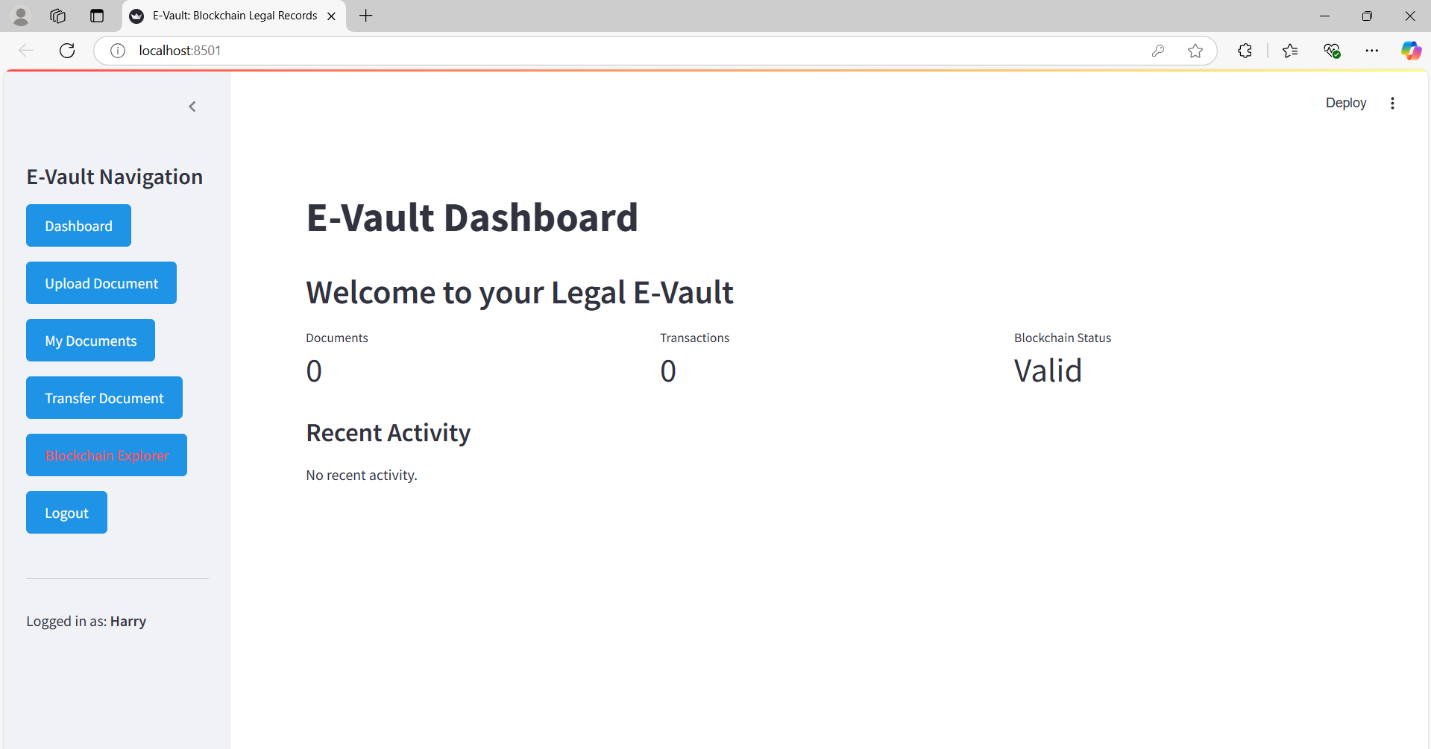
# Chapter 8

# Results

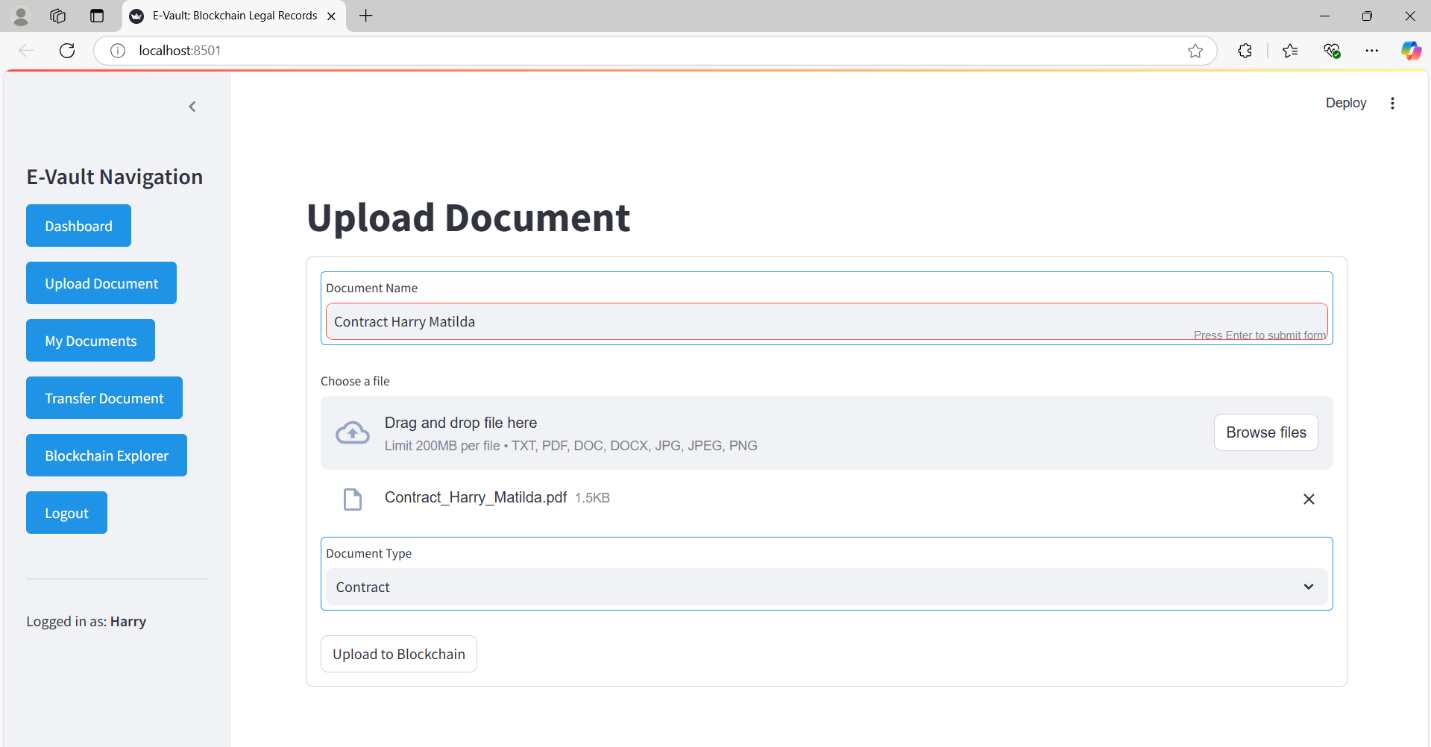
Figures 2 to 5 are the screenshots of project in run using stream lit in localhost with Description of the figure.

**Figure 8.1:** Landing Page

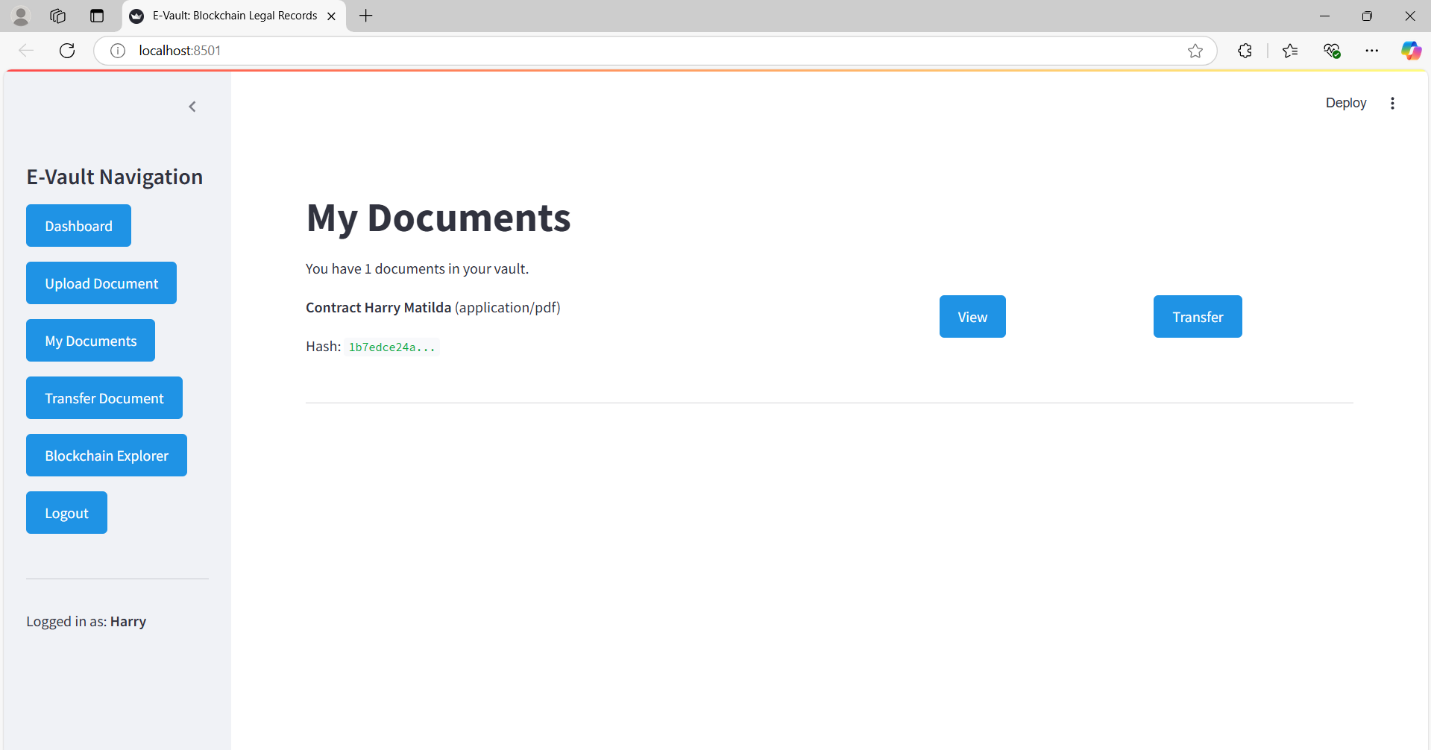
**Figure 8.2:** Registration Page: Harry registered



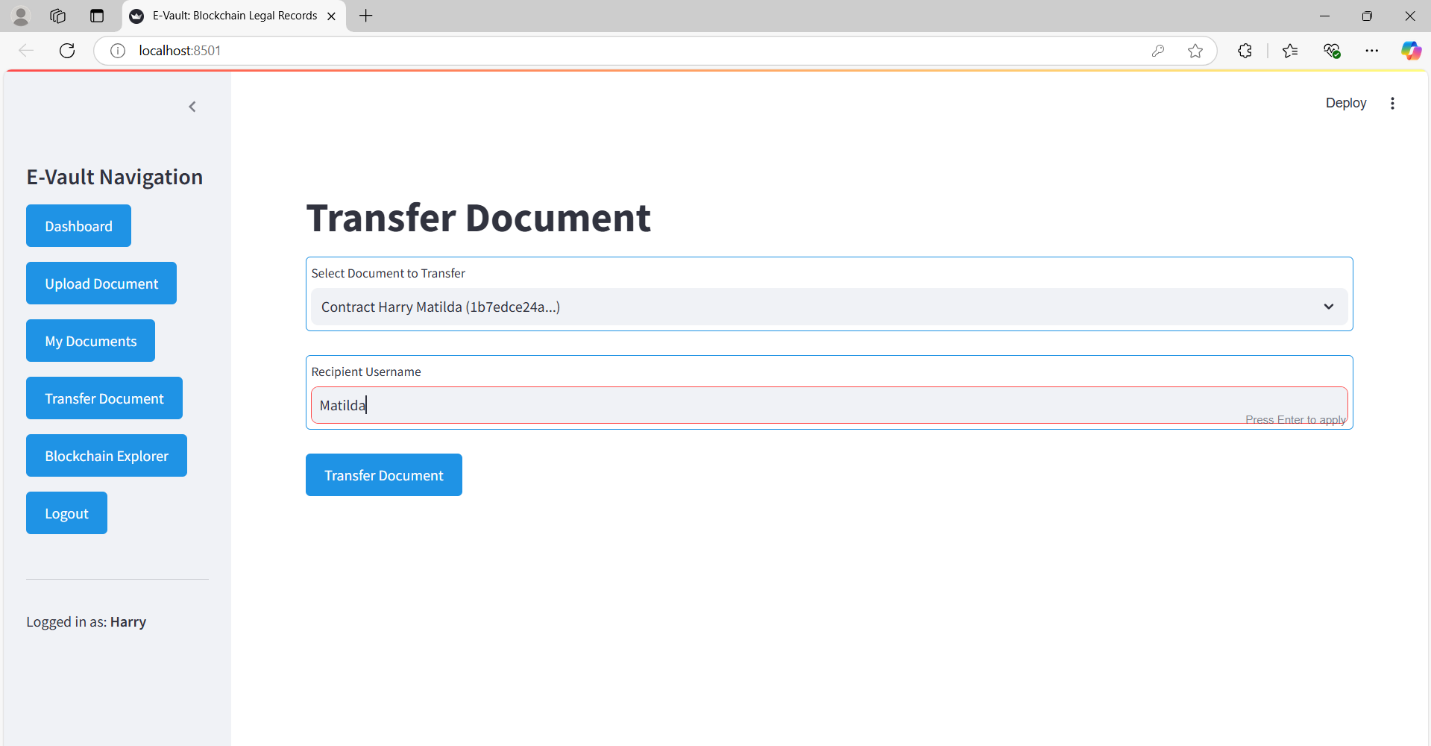
**Figure 8.3:** Initial Dashboard: Harry

****

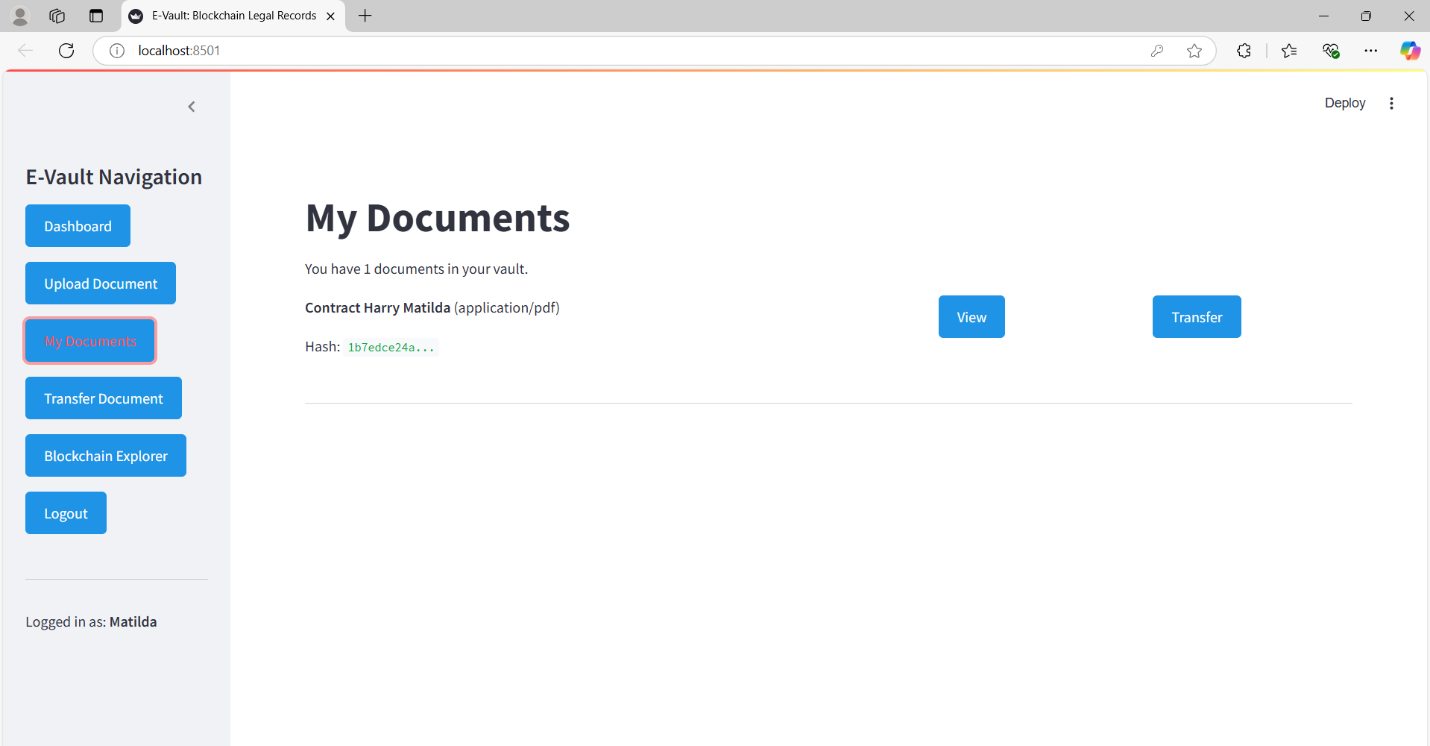
**Figure 8.4:** Uploading Document\Contract: Harry



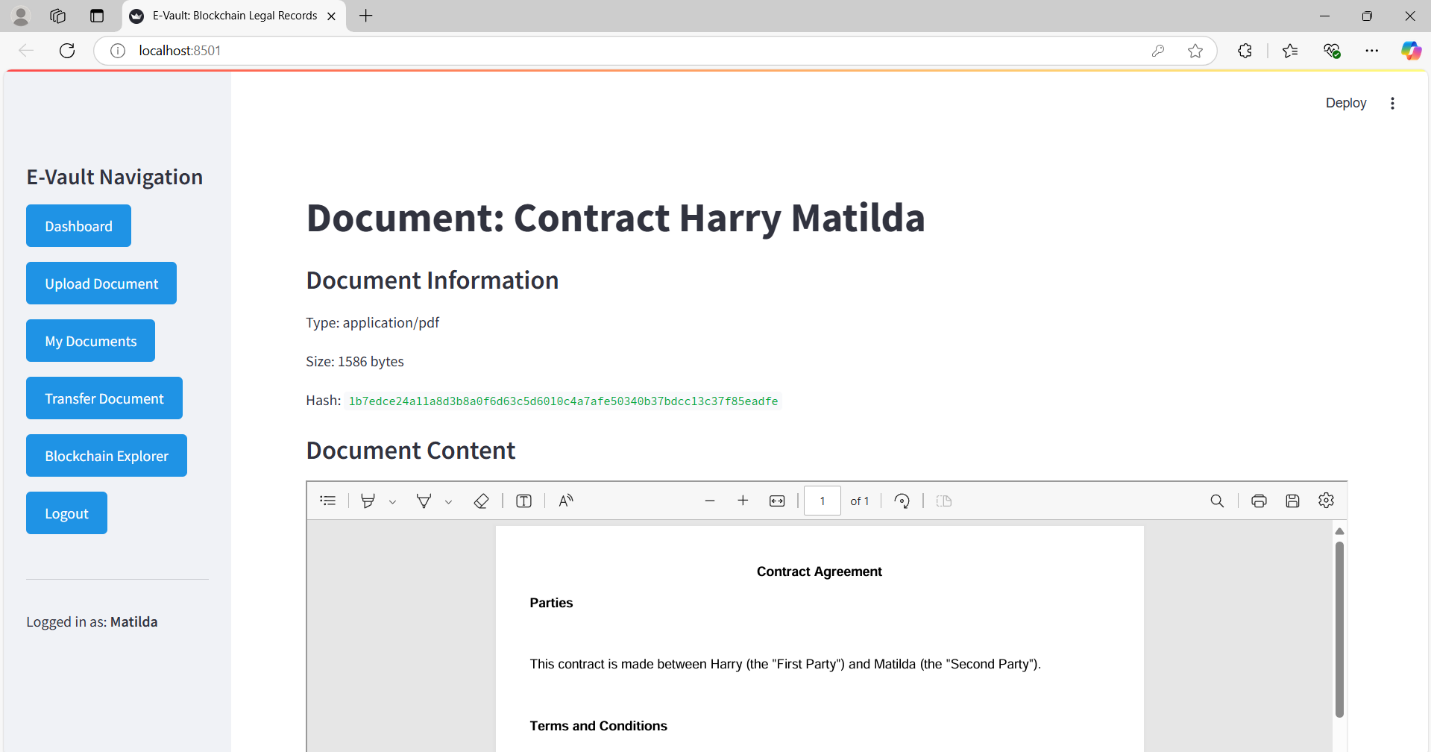
**Figure 8.5:** My Documents Page: Harry



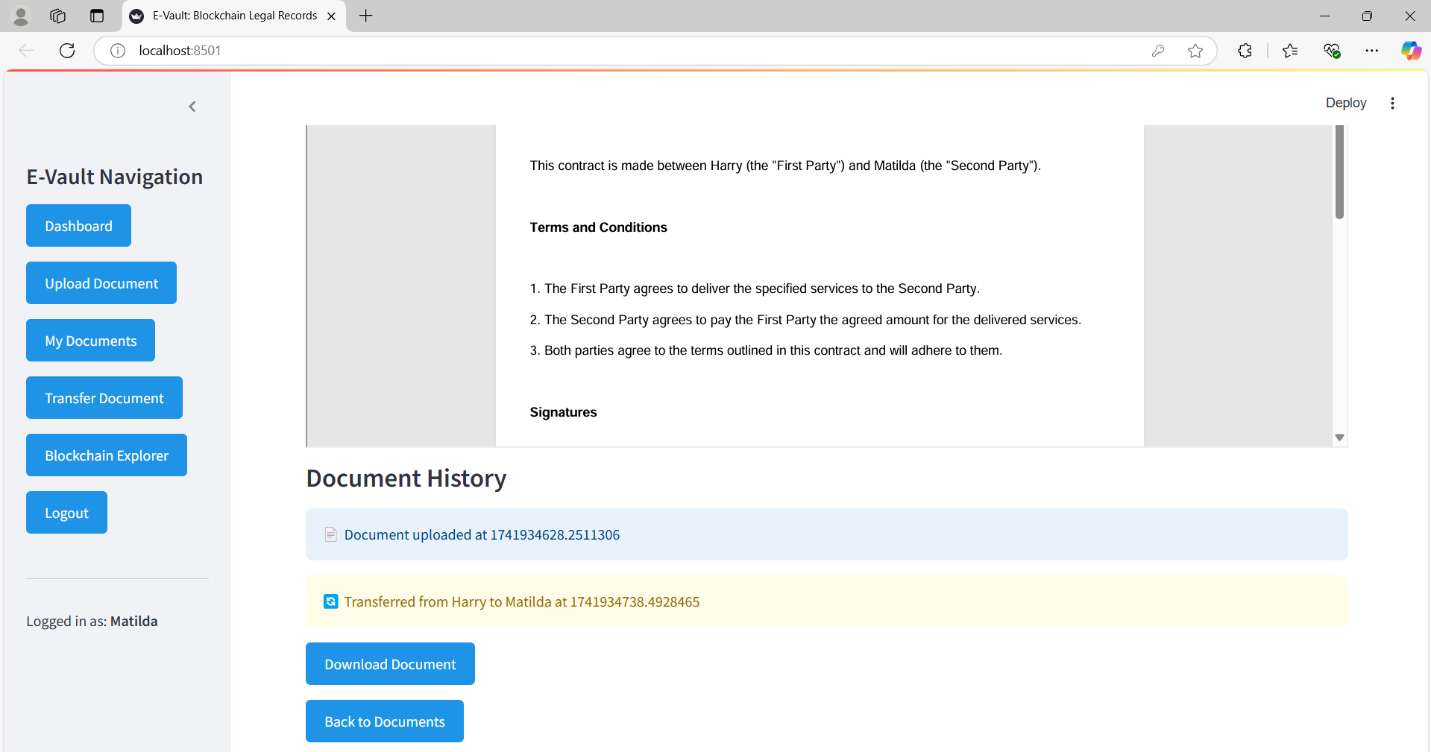
**Figure 8.6:** Transfer Document: Harry transferring to Matilda



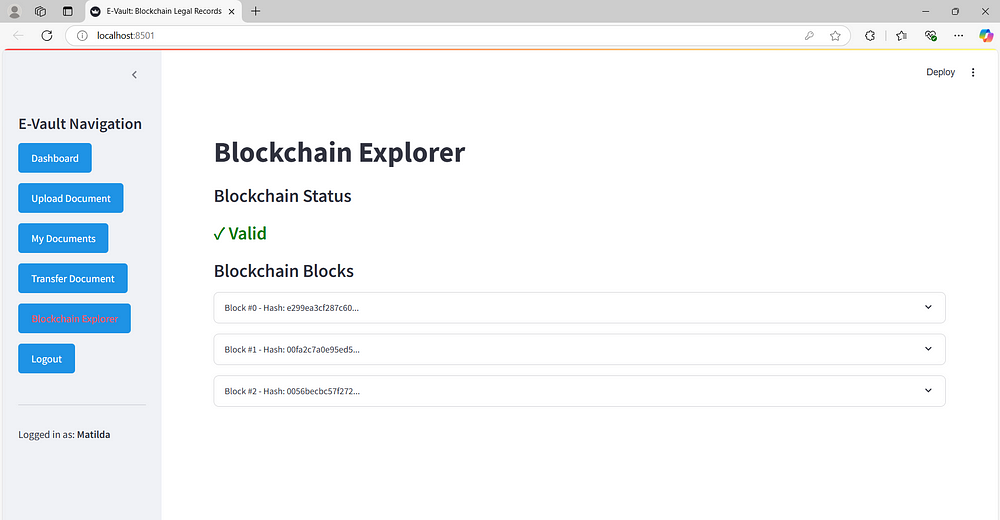
**Figure 8.7**: My Documents Page: Matilda –User 2. File Transferred



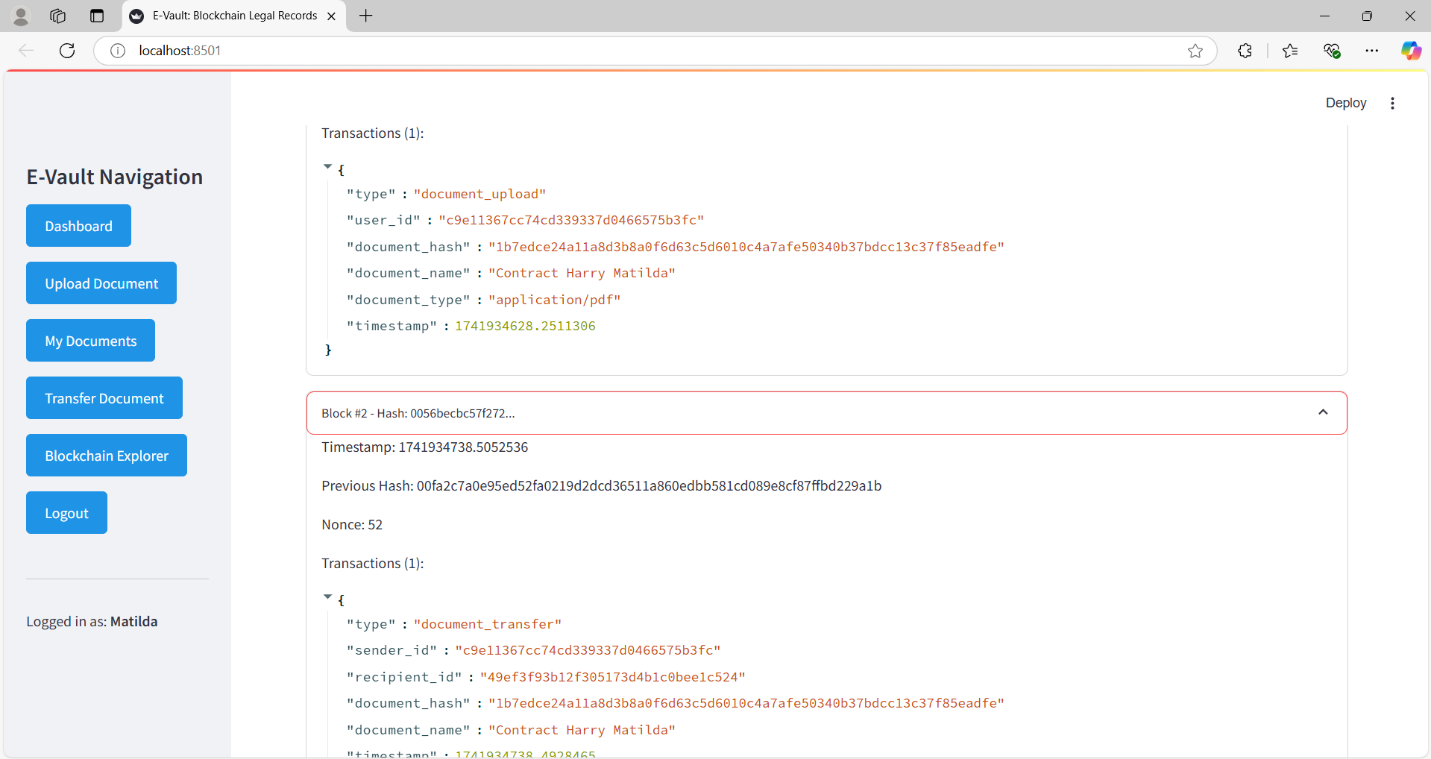
**Figure 8.8:** Viewing the Document: Matilda –User 2.



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

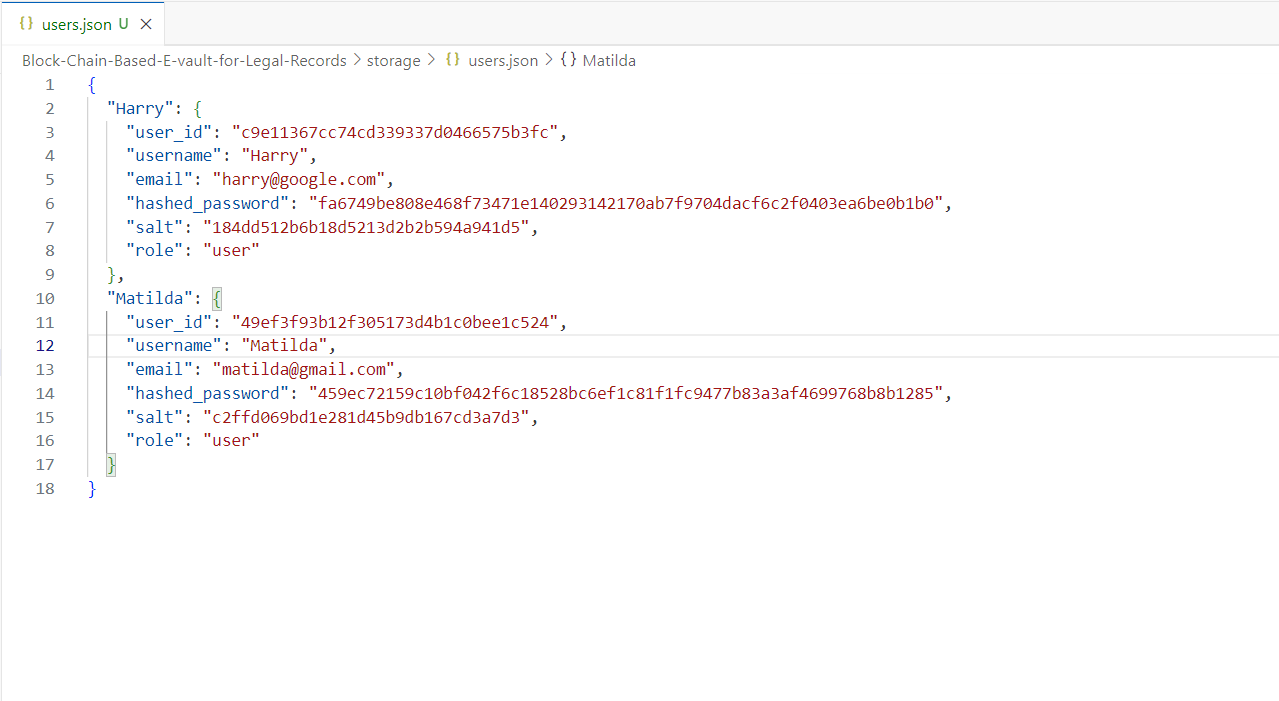


**Figure 8.10:** Blockchain Explorer Page

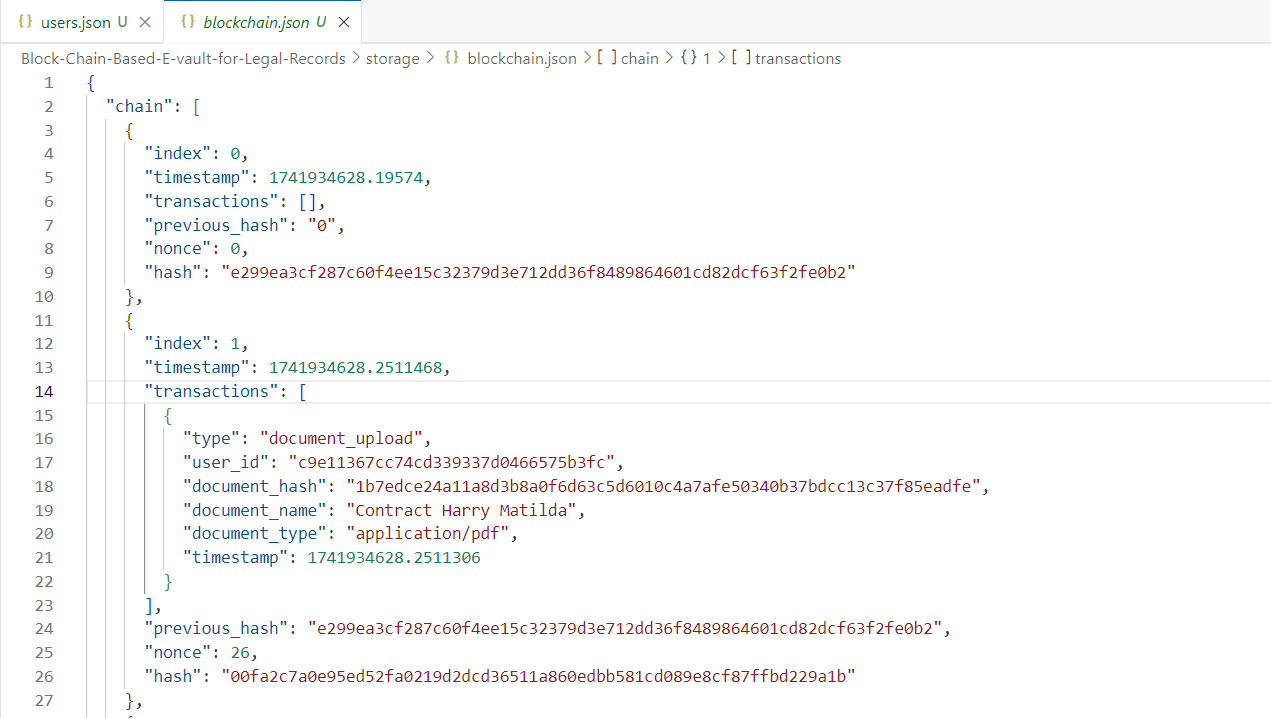


**Figure 8.11**: Blockchain explorer: Tracks all transactions

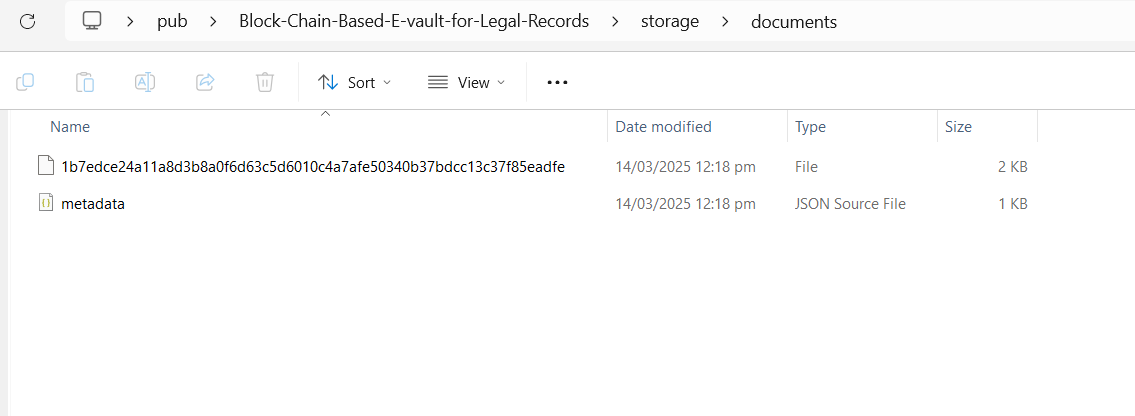
Figures 8.12 to 8.14 are the screenshots of document storage structure generated after running the application with Description of the figure.



**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:** Ensuring the integrity and security of legal documents is crucial. Traditional systems are vulnerable to tampering and unauthorized access, which can compromise the authenticity and confidentiality of legal records.

**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 often rely on manual processes for transferring document ownership, which can be inefficient and error-prone.

**Solution:**

* **Automated Ownership Transfer:** The E-vault system facilitates secure and automated document ownership transfers using blockchain transactions. This ensures accuracy and efficiency, reducing the potential for errors.
* **Transparent Transfer Records:** Each transfer is recorded on the blockchain, providing a transparent and immutable history of document ownership. This allows users to verify the transfer history and ensure the authenticity of ownership records.

## 9.3 Challenge: Ensuring System Usability and Accessibility

**Problem:** Blockchain technology can be complex and challenging for non-technical users to understand and interact with.

**Solution:**

* **Streamlit Interface:** The E-vault system uses Streamlit to provide a user-friendly interface. This simplifies the interaction with the blockchain system, making it accessible to legal professionals without requiring in-depth technical knowledge.
* **Intuitive Design:** The interface includes clear navigation and straightforward workflows for document upload, viewing, verification, and transfer. This enhances the user experience and ensures that users can easily perform necessary actions.

## 9.4 Challenge: Scalability and Performance

**Problem:** As the number of documents and transactions increases, the system must be able to handle the growing load efficiently without compromising performance.

**Solution:**

* **Lightweight Blockchain Implementation:** The custom lightweight blockchain implementation focuses on efficiency and performance, ensuring that the system can handle a large number of transactions without significant delays.
* **Optimized Storage:** The system uses efficient storage mechanisms for both encrypted documents and blockchain data, ensuring quick retrieval and processing of information.
* **Modular Architecture:** The modular design of the E-vault system allows for easy scaling and maintenance. Components can be updated or replaced independently, ensuring that the system can evolve and adapt to changing requirements.

By addressing these challenges with targeted solutions, the E-vault system ensures a secure, efficient, and user-friendly platform for managing legal records using blockchain technology.

# Chapter 10

# Conclusion and Future Scope

## 10.1 Conclusion

The "E-vault using Blockchain to Store and Transfer Legal Records" project demonstrates the potential of blockchain technology to revolutionize the management of legal records. By integrating blockchain with advanced encryption techniques and a user-friendly interface, the E-vault system addresses critical challenges faced by traditional document management systems, including document integrity, security, transparency, and efficiency.

The key achievements of the project include:

* **Secure Document Storage:** The use of AES encryption ensures the confidentiality of documents, while SHA-256 hashing guarantees their integrity.
* **Immutable Audit Trail:** The blockchain provides a transparent and immutable record of all document activities, including uploads, transfers, and verifications.
* **Automated Ownership Transfer:** The system facilitates secure and automated document ownership transfers, reducing the potential for errors and enhancing efficiency.
* **User-Friendly Interface:** The Streamlit-based interface makes the system accessible to legal professionals, allowing them to interact with the blockchain without requiring in-depth technical knowledge.
* **Enhanced Security:** The distributed nature of the blockchain eliminates single points of failure and enhances the overall security of the system.

Overall, the E-vault system offers a scalable and practical solution for managing legal records, ensuring that documents remain tamper-proof, verifiable, and securely accessible.

## 10.2 Future Scope

While the E-vault system provides a robust foundation for secure document management, there are several areas for future enhancement and development:

* **Smart Contracts:** Integrating smart contracts could automate complex legal processes, such as rule-based document transfers and conditional access control. This would further enhance the efficiency and functionality of the system.
* **Biometric Authentication:** Implementing biometric authentication methods, such as fingerprint or facial recognition, could enhance user authentication and security.
* **Mobile Interface:** Developing a mobile application would provide users with on-the-go access to the E-vault system, increasing its usability and convenience.
* **Interoperability with Other Systems:** Ensuring interoperability with other legal and document management systems through standardized APIs would enable seamless data exchange and integration.
* **Scalability Enhancements:** Further optimizing the blockchain implementation to handle larger volumes of documents and transactions efficiently as the system scales.
* **Advanced Analytics:** Incorporating advanced analytics and reporting features to provide insights into document usage, transfer patterns, and system performance.
* **Regulatory Compliance:** Ensuring compliance with evolving legal and regulatory requirements related to data protection, privacy, and digital signatures.

By exploring these future enhancements, the E-vault system can continue to evolve and adapt to the changing needs of the legal industry, providing a comprehensive and secure solution for managing legal records.

# 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](https://scholar.google.com/scholar_lookup?title=A%20survey%20on%20blockchain%20technology%20concepts%2C%20applications%2C%20and%20issues&author=H.T.M.%20Gamage&publication_year=2020&journal=SN%20Computer%20Science&volume=1&pages=1-15)
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](https://scholar.google.com/scholar_lookup?title=International%20Workshop%20on%20New%20Approaches%20for%20Multidimensional%20Signal%20Processing&author=J.%20Kaur&publication_year=2022&book=International%20Workshop%20on%20New%20Approaches%20for%20Multidimensional%20Signal%20Processing)
3. Ali, O. et al. (2021) A comparative study: Blockchain technology utilization benefits, challenges and functionalities. IEEE Access, 9, pp. 12730–12749. [Google Scholar](https://scholar.google.com/scholar_lookup?title=A%20comparative%20study%3A%20Blockchain%20technology%20utilization%20benefits%2C%20challenges%20and%20functionalities&author=O.%20Ali&publication_year=2021&journal=IEEE%20Access&volume=9&pages=12730-12749)
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](https://scholar.google.com/scholar_lookup?title=Blockchain%20Technology%3A%20Growing%20Usecases%20and%20Issues%20to%20Tackle&author=Firdous%20Sadaf%20M.%20Ismail&author=Dattatraya%20S%20Adane&publication_year=2022&journal=International%20Journal%20of%20Next-Generation%20Computing&volume=13&pages=)
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](https://scholar.google.com/scholar_lookup?title=AI%20and%20Blockchain%20Technology%20in%206G%20Wireless%20Network.%20Blockchain%20Technologies.&author=F.S.M.%20Ismail&author=S.G.M.%20Mushtaque&author=M.%20Dutta%20Borah&author=P.%20Singh&author=G.C.%20Deka&publication_year=2022&book=AI%20and%20Blockchain%20Technology%20in%206G%20Wireless%20Network.%20Blockchain%20Technologies.)
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](https://scholar.google.com/scholar_lookup?title=Role%20of%206G%20Wireless%20Networks%20in%20AI%20and%20Blockchain-Based%20Applications&author=F.%20S.%20Ismail&author=S.%20G.%20Mushtaque&author=D.%20Adane&author=M.%20Borah&author=S.%20Wright&author=P.%20Singh&author=G.%20Deka&publication_year=2023&book=Role%20of%206G%20Wireless%20Networks%20in%20AI%20and%20Blockchain-Based%20Applications)
7. Sarwar, M.I. et al. (2021) Data vaults for blockchain-empowered accounting information systems. IEEE Access, 9, pp. 117306–117324.[Google Scholar](https://scholar.google.com/scholar_lookup?title=Data%20vaults%20for%20blockchain-empowered%20accounting%20information%20systems&author=M.I.%20Sarwar&publication_year=2021&journal=IEEE%20Access&volume=9&pages=117306-117324)
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](https://scholar.google.com/scholar_lookup?title=Design%20of%20a%20secure%20and%20fault%20tolerant%20environment%20for%20distributed%20storage&author=A.%20Paul&publication_year=2004&journal=Georgia%20Tech%20Center%20for%20Experimental%20Research%20in%20Computer%20Science%20%28CERCS%29%20Technical%20Report%20GIT-CERCS-04-02.&volume=&pages=)
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](https://scholar.google.com/scholar_lookup?title=Secure%20Data%20Management.%20SDM%202007.%20Lecture%20Notes%20in%20Computer%20Science&author=R.%20Hasan&author=W.%20Jonker&author=M.%20Petkovi%C4%87&publication_year=2007&book=Secure%20Data%20Management.%20SDM%202007.%20Lecture%20Notes%20in%20Computer%20Science)
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](https://scholar.google.com/scholar_lookup?title=EduRSS%3A%20A%20blockchain-based%20educational%20records%20secure%20storage%20and%20sharing%20scheme&author=H.%20Li&author=D.%20Han&publication_year=2019&journal=IEEE%20access&volume=7&pages=179273-179289)
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](https://scholar.google.com/scholar_lookup?title=NyaYa%3A%20Blockchain-based%20electronic%20law%20record%20management%20scheme%20for%20judicial%20investigations&author=A.%20Verma&publication_year=2021&journal=Journal%20of%20Information%20Security%20and%20Applications&volume=63&pages=103025)
12. Gururaj, H.L. et al. (2020) Blockchain: A new era of technology. Cryptocurrencies and blockchain technology applications, pp. 1–24.[Google Scholar](https://scholar.google.com/scholar_lookup?title=A%20blockchain-based%20framework%20for%20data%20sharing%20with%20fine-grained%20access%20control%20in%20decentralised%20storage%20systems&author=S.%20Wang&publication_year=2018&journal=IEEE%20Access&volume=6&pages=38437-38450)
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](https://scholar.google.com/scholar_lookup?title=Web-Based%20Knowledge%20Management%20Distributed%20Application%20for%20Medical%20Certificates%20Using%20Blockchain%20Technology&author=C.%20Rupa&publication_year=2021&journal=Knowledge%20Management%20and%20Web%203.0%3A%20Next%20Generation%20Business%20Models&volume=2&pages=141)
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](https://scholar.google.com/scholar_lookup?title=Blockchain%20Technology%20for%20Real%20Estate%20Documents%20Protection%20Using%20Ethereum&author=S.S.%20Mahamure&publication_year=2020&journal=International%20Journal%20of%20Future%20Generation%20Communication%20and%20Networking&volume=13&pages=1287-1295)

**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>