Report On

EVault: A Decentralized File System on IPFS

Submitted in partial fulfillment of the requirements of the Course project in Semester VII of Fourth Year Computer Engineering

By
Hrushikesh Shetty(Roll No. 66)
Kshitij Shetty (Roll No. 74)
Nikita Mundaye (Roll No. 73)

Supervisor
Prof. Dinesh Patil

University of Mumbai

Vidyavardhini's College of Engineering & Technology

Department of Computer Engineering

(2023-24)

Vidyavardhini's College of Engineering & Technology
Department of Computer Engineering

CERTIFICATE

This is to certify that the project entitled “EVault: A Decentralized File System on IPFS” is a bonafide work of "Hrushikesh Shetty (Roll No. 66), Kshitij Shetty (Roll No. 74), Nikita Mundaye (Roll No. 73) submitted to the University of Mumbai in partial fulfillment of the requirement for the Course project in semester VII of Fourth Year Computer Engineering.

.

Supervisor

Prof. Dinesh Patil

Dr. Megha Trivedi
Head of Department

Abstract

This comprehensive project embarks on a revolutionary journey, harnessing the potential of blockchain technology to redefine the landscape of file storage and management. With a strong focus on practical implementation, it sheds light on the capabilities of Hardhat, a crucial development tool in the blockchain domain. At its core, the project features a meticulously crafted smart contract, an exhaustive testing suite, and a deployment script, all working harmoniously to establish a decentralized and highly secure file storage system.

As you immerse yourself in this exploration of blockchain-based file storage, you'll gain valuable insights into the groundbreaking project at hand. It pioneers a new era in data management and security, offering a vision of what's possible when blockchain technology and file storage merge. Developers and blockchain enthusiasts, both novice and seasoned, are invited to delve into this project to uncover innovative solutions and embark on their own journey towards blockchain-based file storage.

Contents **Page No.**

1 Introduction

1.1 Introduction

In an era defined by an unprecedented surge in data creation and consumption, the way we manage and store files has become a paramount concern. While centralized cloud storage services have dominated this landscape for years, there's an emerging paradigm shift that's set to revolutionize file storage – blockchain technology. "Revolutionizing File Storage with Blockchain Technology: An In-Depth Project Exploration" introduces a groundbreaking endeavor that seeks to bridge the gap between traditional file storage solutions and the decentralized, secure world of blockchain.

This project stands at the intersection of innovation and practicality, showcasing the transformative potential of Hardhat, a vital tool in the blockchain developer's toolkit. It presents a hands-on experience that unveils the magic of blockchain-based file storage. At its core, you'll discover a meticulously crafted smart contract, a comprehensive testing suite, and an efficient deployment script. These components collectively pave the way for a decentralized and ultra-secure approach to file storage.

As we embark on this journey, we'll unravel the fascinating capabilities of this project, ushering in a new era of data management and security. Developers and blockchain enthusiasts, regardless of their expertise level, will find inspiration in this exploration and the innovative solutions it unveils. This is the dawn of a new chapter in file storage, and you're invited to join us as we dive deep into this transformative project.

1.2 Problem Statement

In the context of our project, we confront the formidable challenges presented by the current state of data storage and retrieval within a rapidly evolving digital ecosystem. These challenges arise from the limitations of traditional data management systems, which require innovative solutions to ensure efficient, secure, and accessible data handling.

The existing data storage systems often lack transparency, making it difficult for users to verify the authenticity and integrity of stored information. Moreover, concerns about data security and custody emerge due to the prevalent reliance on centralized, third-party data custodians, leaving data vulnerable to theft and fraud risks. Furthermore, the management of diverse data types, spanning from structured to unstructured data, necessitates data handling across multiple platforms and technologies, contributing to complexity and inefficiency.

Navigating the intricate landscape of data regulatory compliance poses another substantial challenge, as data governance requirements vary across jurisdictions, making it onerous for users to ensure data compliance and adherence to pertinent regulations. Additionally, the accessibility of data management tools remains largely restricted to specialized or institutional users, excluding a wider and diverse audience from harnessing these resources.

Interoperability issues between various data management systems and platforms, including traditional and emerging technologies, hinder the seamless and efficient flow of data. Data integrity within centralized systems is at constant risk, owing to vulnerabilities that expose data to manipulation or unauthorized alterations.

This solution is designed to mitigate the aforementioned issues by offering enhanced transparency, robust security measures, improved accessibility, and cost-efficiency. Our project seeks to empower a diverse range of users, ensuring compliance with regulatory requirements, preserving data integrity, and providing scalable data management solutions.

1.3 Project Scope

The scope of the blockchain-based file storage project is to address the limitations inherent in traditional file management systems, particularly in a rapidly evolving digital landscape. The primary issues include concerns related to transparency, security, accessibility, and the increasing operational costs. To resolve these challenges, the project aims to develop a blockchain-based decentralized file storage system.

This system will offer enhanced transparency, fortified security measures, and optimized operational efficiency. It will provide a decentralized, user-friendly platform for file storage, ensuring compliance with various regulatory frameworks. The project will also explore potential integrations with other decentralized applications and services to create a seamless and interconnected network for data management.

Ultimately, the blockchain-based file storage project seeks to empower users to have greater control over their data while ensuring a trusted and censorship-resistant platform for their storage needs within the blockchain ecosystem.

2. Requirement Analysis

2.1 Hardware Requirements

Hardware Required:

Recommended:

- 16 GB RAM

Minimum:

- 8 GB RAM

2.2 Software Requirements:

- Visual Studio Code
- Pinata Cloud
- React Js & Node JS
- Metamask Wallet
- Solidity

2.3 Functional Requirements

User Registration and Authentication:

- Users should be able to create accounts securely using a username and password or by providing a cryptocurrency wallet address for enhanced security.
- Multi-factor authentication (MFA) should be implemented to enhance user account security.
- Users must have the ability to log in and log out of their accounts securely.

File Upload and Storage:

- Enable users to upload a variety of file types, including images, documents, and media files, for secure storage within the blockchain-based system.
- Implement data encryption and secure storage mechanisms to safeguard uploaded files against unauthorized access and data manipulation.

File Management:

- Users should be able to manage their files effectively, including organizing, renaming, editing metadata, and categorizing files.

- Implement version control features to track changes and revisions in file content, allowing users to revert to previous versions when necessary.

Blockchain Integration:

- Utilize smart contracts within the selected blockchain network to securely store file metadata and ensure data integrity.
- Implement blockchain-based timestamping to provide users with a method to verify the authenticity of uploaded files and their timestamps.

Access Control:

- Define access control policies that allow users to specify who can view and access their stored files.
- Enable users to revoke access permissions at any time, ensuring they maintain control over their data.

Search and Retrieval:

- Implement a robust search and retrieval system to enable users to quickly locate their stored files, including search by file name, metadata, and timestamps.
- Optimize search capabilities to accommodate a growing volume of stored files efficiently.

User Documentation and Help Center:

- Develop comprehensive user documentation and a help center to provide users with guidance on system usage, including file upload, management, and blockchain-based features.

These functional requirements aim to create a robust, secure, and user-friendly blockchain-based file storage system, enhancing data management while ensuring data security and accessibility for users.

2.4 Nonfunctional Requirements

Performance: The DApp should be able to handle a large number of transactions and users simultaneously without any significant degradation in response time.

Security: Given the sensitive nature of the data, the DApp should ensure that all data is encrypted and secure from unauthorized access. It should also be resistant to common web vulnerabilities.

Reliability: The DApp should be available for use at all times, with minimal downtime for maintenance or updates.

Usability: The user interface should be intuitive and easy to use, even for individuals who are not familiar with blockchain technology.

Scalability: The DApp should be able to scale and accommodate an increasing number of users and transactions over time.

Maintainability: The codebase should be well-documented and modular to allow for easy updates and bug fixes.

3. System Design

3.1 System Design

User Interface: The frontend is created on ReactJs with a user friendly interface where the users can store files by just the click of a button.

IPFS Nodes: These nodes are part of the IPFS network and store and distribute the files. They act as the backbone of the decentralized file system.

Pinata Cloud: Pinata Cloud is a service that allows you to pin content on IPFS. It can be used to ensure that your files remain accessible even if there are no other nodes currently hosting them on IPFS.

Blockchain Integration: To make the system more decentralized and secure, we integrated blockchain technology for storing metadata and managing access control.

Smart Contracts: On the blockchain, smart contracts manage access control, file ownership, and incentivize participants in the network.

File Encryption: Implement encryption techniques to ensure the security and privacy of files stored in the system.

Decentralized Identity: Used decentralized identity solutions to manage user authentication and authorization.

Metadata Storage: Stored file metadata on IPFS or the blockchain. Metadata can include information such as file names, file sizes, and access permissions.

3.2 Diagram

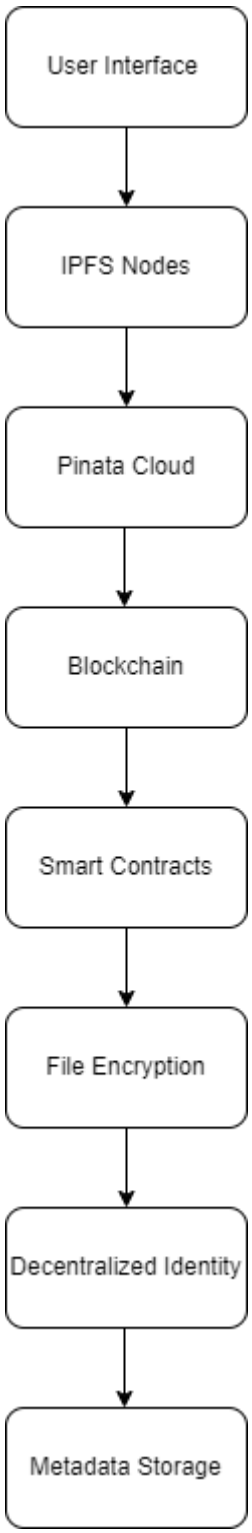


Fig. 1

The above Fig. 1 shows the working of the system in a sequential manner.

3.2 Module Description

User Interface: This module provides the user with a graphical or command-line interface to interact with the decentralized file system. Users can upload, download, and manage files through this interface.

IPFS Nodes: These nodes store and distribute the actual file content using the IPFS protocol. They ensure that files are available even when no users are actively requesting them.

Pinata Cloud: Pinata Cloud is a service that helps to pin content on IPFS. It ensures high availability and reliability of files by hosting them on IPFS nodes.

Blockchain Integration: The blockchain provides a decentralized and secure way to manage file metadata and access control. It can be integrated to enhance the system's trustworthiness.

Smart Contracts: Smart contracts on the blockchain handle tasks like access control, ownership management, and possibly even incentivize participants in the network.

File Encryption: This module ensures that files are stored securely by encrypting them. Decryption keys can be managed through the blockchain's access control.

Decentralized Identity: This component manages user identity in a decentralized way, ensuring that users are who they claim to be.

Metadata Storage: Metadata about the files, including information like file names, sizes, and access permissions, can be stored on IPFS or the blockchain for reference.

4. Implementation

4.1 Methodology

Project Inception and Planning:

In this phase, the project team established the foundation for the decentralized file system on IPFS with Pinata Cloud. Key activities included:

- **Project Goals and Objectives:** Clearly defined the purpose and scope of the project.
- **Stakeholder Identification:** Identified all relevant stakeholders and their respective roles.
- **Project Schedule:** Created a detailed project schedule with milestones and deadlines.
- **Resource Allocation:** Determines the budget and allocated resources, including human resources and technology.
- **Project Management:** Defined project management protocols and established communication channels for efficient collaboration.

Requirement Analysis:

During the requirement analysis stage, we gathered and documented the essential requirements for the decentralized file system:

- **User Requirements:** Collected and documented user needs and expectations.
- **Functional Specifications:** Defined the features and functionalities of the file system.
- **Performance and Scalability Requirements:** Identified performance benchmarks and scalability considerations.
- **Security and Privacy Considerations:** Documented security measures and privacy requirements.
- **Regulatory and Compliance Requirements:** Addressed regulatory constraints and compliance standards.

Blockchain Technology Selection:

Selecting the right blockchain technology is pivotal to the success of the project. The following steps were taken:

- **Research and Evaluation:** Researched various blockchain platforms (Ethereum, Binance Smart Chain, etc.) based on project requirements.
- **Platform Selection:** Chose Ethereum as the blockchain technology for its robustness, developer support, and compatibility with smart contracts.
- **Considered Factors:** Evaluated factors like scalability, consensus mechanism, and developer ecosystem to ensure it aligns with the project's objectives.

Architecture and Design:

The architecture and design phase involved detailed planning of the decentralized file system:

- **Technical Architecture:** Designed the overall system architecture, including user interface, IPFS nodes, Pinata Cloud integration, blockchain components, and more.
- **Technical Diagram:** Created a comprehensive technical architecture diagram for reference.
- **Database Schema:** Defined the database schema for storing metadata and access control information.
- **Security and Encryption:** Planned security mechanisms, including file encryption and access control using blockchain-based smart contracts.
- **API and Communication:** Specified API endpoints and communication protocols for effective interaction between system modules.

4.3 Code

```
// SPDX-License-Identifier: GPL-3.0

pragma solidity >=0.7.0 <0.9.0;

contract Upload {

  struct Access{
    address user;
    bool access; //true or false
  }
  mapping(address=>string[]) value;
  mapping(address=>mapping(address=>bool)) ownership;
  mapping(address=>Access[]) accessList;
  mapping(address=>mapping(address=>bool)) previousData;

  function add(address _user,string memory url) external {
    value[_user].push(url);
  }
  function allow(address user) external {//def
    ownership[msg.sender][user]=true;
    if(previousData[msg.sender][user]){
      for(uint i=0;i<accessList[msg.sender].length;i++){
          if(accessList[msg.sender][i].user==user){
              accessList[msg.sender][i].access=true;
          }
      }
    }else{
        accessList[msg.sender].push(Access(user,true));
        previousData[msg.sender][user]=true;
    }

  }
```

```
  function disallow(address user) public{
     ownership[msg.sender][user]=false;
     for(uint i=0;i<accessList[msg.sender].length;i++){
        if(accessList[msg.sender][i].user==user){
           accessList[msg.sender][i].access=false;
        }
     }
  }

  function display(address _user) external view returns(string[] memory){
     require(_user==msg.sender || ownership[_user][msg.sender],"You don't have
access");
     return value[_user];
  }

  function shareAccess() public view returns(Access[] memory){
     return accessList[msg.sender];
  }
}
```

5. Results:

5.1 Results:

The implementation phase of the decentralized file system project on IPFS with Pinata Cloud has yielded significant outcomes and accomplishments.

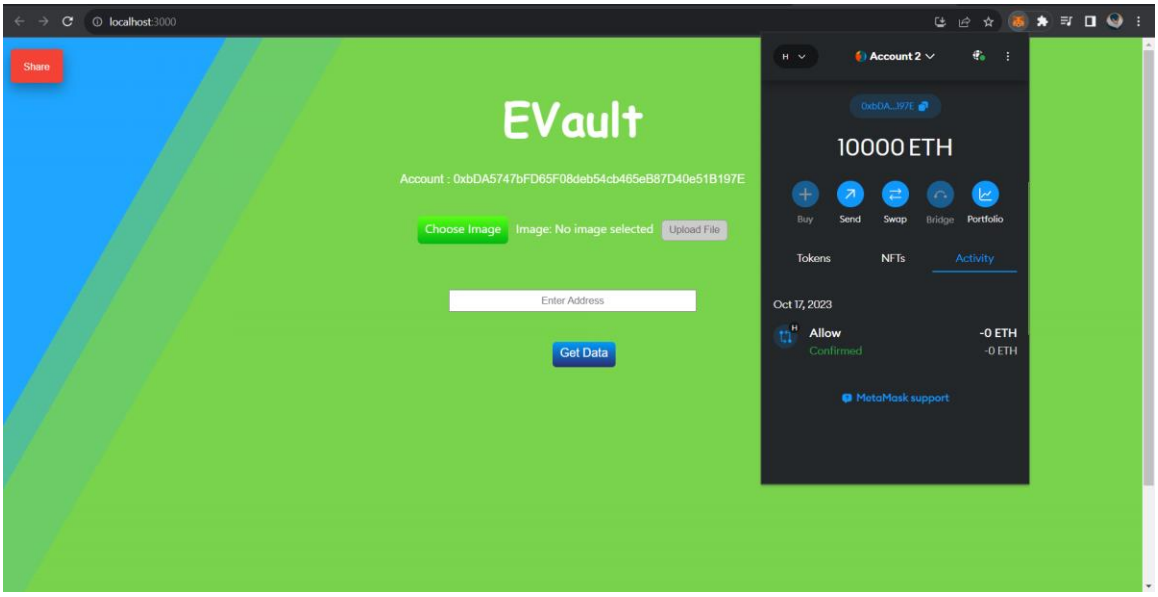


Fig. 2

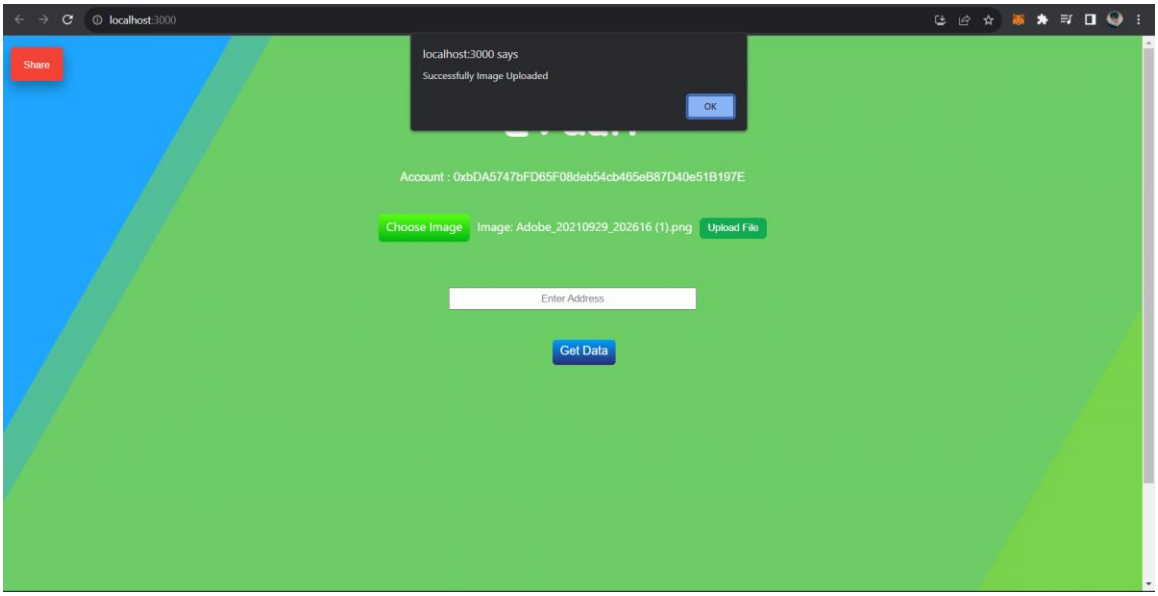


Fig. 3

Fig. 4

The above figures display the user interface and the modules it has for the users.

Fig. 2 shows the MetaMask integration with the blockchain and user interface where we can switch from different accounts.

Fig. 3 shows the successful uploading of the file to the IPFS on Pinata through the provided API.

Fig. 4 shows the Share Access module where one user can give access to other users in the same blockchain network.

5.2 Conclusion:

In conclusion, the proposed blockchain-based decentralized file storage system represents a pioneering solution in the ever-evolving landscape of data management. The project was born out of a necessity for a more transparent, secure, accessible, and cost-efficient approach to file storage, addressing the limitations of traditional systems.

Throughout the development process, we have strived to build a system that ensures transparency and security are at the forefront. The implementation of a decentralized infrastructure fosters trust and confidence, enhancing data integrity while minimizing the risk of unauthorized access or manipulation.

Moreover, this project sets its sights on offering an interconnected network for data management by exploring potential integrations with various decentralized applications and services. This approach aims to create a seamless and vibrant ecosystem where users can not only store data but also interact with it in novel and meaningful ways.

Ultimately, the proposed system empowers individuals and organizations to regain control over their digital assets, making data management more user-centric and secure. By providing a trusted and censorship-resistant platform, we are not only adapting to the changing digital landscape but also driving innovation and setting new standards for the future of data storage and management.

References:

[1] Ismail, A., Toohey, M., Lee, Y. C., Dong, Z., & Zomaya, A. Y. (2022, August). Cost and Performance Analysis on Decentralized File Systems for Blockchain-Based Applications: State-of-the-Art Report. In 2022 IEEE International Conference on Blockchain (Blockchain) (pp. 230-237). IEEE.

[2] Nizamuddin, N., Salah, K., Azad, M. A., Arshad, J., & Rehman, M. H. (2019). Decentralized document version control using ethereum blockchain and IPFS. Computers & Electrical Engineering, 76, 183-197.

[3] Shah, M., Shaikh, M., Mishra, V., & Tuscano, G. (2020, June). Decentralized cloud storage using blockchain. In 2020 4th International conference on trends in electronics and informatics (ICOEI)(48184) (pp. 384-389). IEEE.

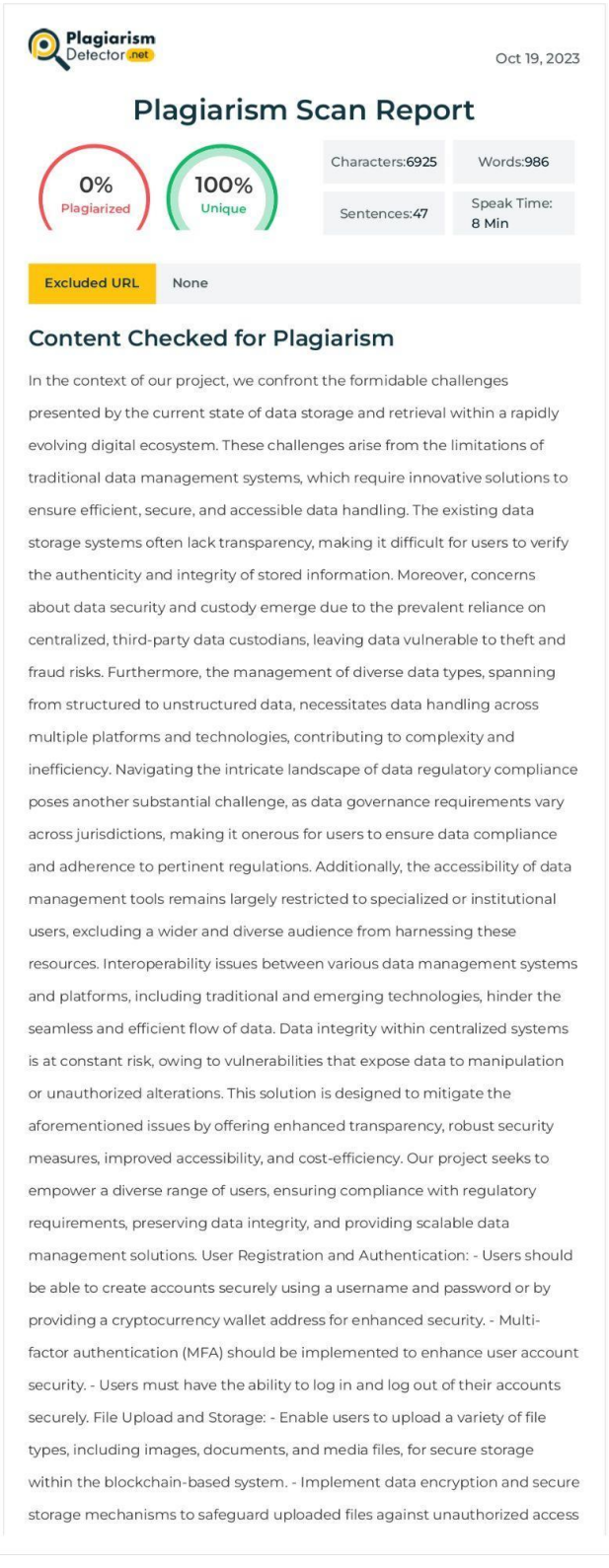
[4] Leka, E., & Selimi, B. (2020). Bcert–a decentralized academic certificate system distribution using blockchain technology. International Journal on Information Technologies & Security, 12(4).

[5] Huang, H., Lin, J., Zheng, B., Zheng, Z., & Bian, J. (2020). When blockchain meets distributed file systems: An overview, challenges, and open issues. IEEE Access, 8, 50574-50586.

[6] Huang, H. S., Chang, T. S., & Wu, J. Y. (2020, July). A secure file sharing system based on IPFS and blockchain. In Proceedings of the 2nd International Electronics Communication Conference (pp. 96-100).

[7] Naz, M., Al-zahrani, F. A., Khalid, R., Javaid, N., Qamar, A. M., Afzal, M. K., & Shafiq, M. (2019). A secure data sharing platform using blockchain and interplanetary file system. Sustainability, 11(24), 7054.

Plagiarism:



Plagiarism Detector .net

Oct 19, 2023

Plagiarism Scan Report

0% Plagiarized

100% Unique

Characters:6925 | Words:986

Sentences:47 | Speak Time: 8 Min

Excluded URL: None

Content Checked for Plagiarism

In the context of our project, we confront the formidable challenges presented by the current state of data storage and retrieval within a rapidly evolving digital ecosystem. These challenges arise from the limitations of traditional data management systems, which require innovative solutions to ensure efficient, secure, and accessible data handling. The existing data storage systems often lack transparency, making it difficult for users to verify the authenticity and integrity of stored information. Moreover, concerns about data security and custody emerge due to the prevalent reliance on centralized, third-party data custodians, leaving data vulnerable to theft and fraud risks. Furthermore, the management of diverse data types, spanning from structured to unstructured data, necessitates data handling across multiple platforms and technologies, contributing to complexity and inefficiency. Navigating the intricate landscape of data regulatory compliance poses another substantial challenge, as data governance requirements vary across jurisdictions, making it onerous for users to ensure data compliance and adherence to pertinent regulations. Additionally, the accessibility of data management tools remains largely restricted to specialized or institutional users, excluding a wider and diverse audience from harnessing these resources. Interoperability issues between various data management systems and platforms, including traditional and emerging technologies, hinder the seamless and efficient flow of data. Data integrity within centralized systems is at constant risk, owing to vulnerabilities that expose data to manipulation or unauthorized alterations. This solution is designed to mitigate the aforementioned issues by offering enhanced transparency, robust security measures, improved accessibility, and cost-efficiency. Our project seeks to empower a diverse range of users, ensuring compliance with regulatory requirements, preserving data integrity, and providing scalable data management solutions. User Registration and Authentication: - Users should be able to create accounts securely using a username and password or by providing a cryptocurrency wallet address for enhanced security. - Multi-factor authentication (MFA) should be implemented to enhance user account security. - Users must have the ability to log in and log out of their accounts securely. File Upload and Storage: - Enable users to upload a variety of file types, including images, documents, and media files, for secure storage within the blockchain-based system. - Implement data encryption and secure storage mechanisms to safeguard uploaded files against unauthorized access

Page 1 of 3