iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 Issue: III Month of publication: March 2026

DOI: https://doi.org/10.22214/ijraset.2026.78285

Decentralized Web Based File Storage System Using Blockchain Technology

Prof. Mr.Gargeya M. Aware[1], Om S. Chopar[2], Vansh S. Kakde[3], Niketan W. Hambarde[4], Shailesh N. Kadu[5]
Department of Computer Science & Engineering, Prof Ram Meghe College Of Engineering & Management, Badnera – Amravati
Sant Gadge Baba Amravati University, Amravati, Maharashtra, India

Abstract: This project presents a Decentralized Web-Based File Storage System using Blockchain Technology designed to store and share files in a secure, transparent, and reliable manner. Traditional cloud storage systems rely on centralized servers where all user data is stored in a single location. This centralized approach can lead to several issues such as data breaches, server failures, unauthorized access, and lack of user control over stored data. To overcome these limitations, the proposed system utilizes blockchain technology to create a decentralized storage platform. In this system, users can securely upload, store, and share files through a web-based interface. Instead of storing files directly on a centralized server, the system uses decentralized storage along with blockchain to maintain records of file ownership, access permissions, and transaction history in an immutable and transparent manner. For enhanced security, files are encrypted before being stored, ensuring that only authorized users can access the data. Smart contracts are implemented to automatically manage file access permissions, eliminating the need for a trusted third party. The primary objective of this system is to improve data security, provide users with complete control over their files, reduce dependency on centralized storage systems, and offer a reliable and trustworthy decentralized file storage solution.

Keywords: Decentralized File Storage, Blockchain Technology, Web-Based Storage System, Data Security, Smart Contracts, Distributed Storage, File Sharing, Access Control.

I. INTRODUCTION

In the modern digital environment, the volume of data generated and exchanged through the internet has increased significantly. Every day, individuals and organizations create large amounts of digital content such as documents, images, videos, and application data. Managing and storing this data efficiently has become an important requirement for both personal and professional use. To address this need, many users rely on cloud-based storage services that allow them to store and access their files through the internet from different locations and devices.

Most traditional cloud storage systems operate on a centralized architecture. In this model, all user data is stored and managed by a single organization or service provider that controls the storage infrastructure. Centralized systems provide several advantages such as easy management, scalability, and convenient data access. However, despite these benefits, centralized storage solutions also introduce a number of critical limitations related to security, reliability, and user control.

One of the major concerns associated with centralized storage is the risk of data breaches and unauthorized access. Since large volumes of data are stored in a single location, centralized servers often become attractive targets for cyber attackers. If a central server is compromised, sensitive information belonging to many users can be exposed or manipulated. In addition, centralized systems create a single point of failure. If the server experiences technical issues, hardware failure, or cyberattacks, users may temporarily or permanently lose access to their stored files.

Another important issue is the lack of transparency and ownership control over stored data. In many centralized storage platforms, users do not have complete visibility regarding where their data is physically stored or how it is managed by the service provider. As a result, users must depend on the provider’s security policies and infrastructure management practices. This situation raises concerns regarding data privacy, data ownership, and long-term accessibility of digital information.

To overcome these limitations, researchers and developers have begun exploring decentralized technologies that distribute data across multiple nodes instead of storing it in a single centralized location. One of the most promising technologies supporting this approach is blockchain. Blockchain is a distributed ledger technology that records transactions and data across a network of interconnected nodes. Each record is stored in a block and linked to previous blocks using cryptographic techniques, forming a continuous chain of secure data.

Additionally, blockchain can be used to store metadata related to files, such as ownership information, access permissions, and transaction history. This creates a transparent and verifiable record of all file-related activities within the system. Smart contracts can also be implemented to automate file access control and enforce predefined security rules. These contracts automatically execute specific actions when certain conditions are met, ensuring secure and reliable system operations.

Based on these concepts, this project proposes a Decentralized Web-Based File Storage System using Blockchain Technology. The proposed system enables users to upload, store, and share files through a decentralized network while maintaining high levels of security and transparency. Files are stored using decentralized storage mechanisms, and blockchain technology is used to maintain secure records of file ownership and transactions. Encryption techniques are also applied to ensure that only authorized users can access the stored data.

The objective of this project is to design a storage platform that minimizes reliance on centralized servers while improving data security, transparency, and user control. By combining decentralized storage with blockchain technology, the system aims to provide a reliable and secure alternative to traditional cloud storage solutions. This approach not only enhances data protection but also ensures that users maintain greater ownership and control over their digital assets.

II. LITERATURE REVIEW

Research on decentralized storage systems using blockchain technology has increased due to the limitations of traditional centralized cloud storage systems. Centralized storage architectures rely on a single server or authority to manage and store user data, which introduces several risks such as data breaches, server failures, and lack of transparency regarding data ownership. To address these challenges, researchers have proposed decentralized storage solutions that combine blockchain technology with distributed storage networks, cryptographic techniques, and peer-to-peer communication protocols.

Satoshi Nakamoto introduced the concept of blockchain through the paper *"Bitcoin: A Peer-to-Peer Electronic Cash System"* [1]. This work presented a decentralized transaction system where transactions are recorded in blocks and connected using cryptographic hash functions to form a secure and immutable ledger. The blockchain architecture ensures transparency, data integrity, and security, which later inspired the development of several decentralized applications including decentralized storage systems.

Juan Benet proposed the InterPlanetary File System (IPFS) as a distributed file storage protocol that improves file sharing through a peer-to-peer network [2]. In IPFS, files are identified using a unique content-based hash called a Content Identifier (CID). This method ensures that files remain secure and can be retrieved efficiently without depending on centralized servers, thereby improving system reliability and fault tolerance.

Gavin Wood introduced the Ethereum platform, which extended blockchain technology by enabling smart contracts [3]. Smart contracts are self-executing programs stored on the blockchain that automatically perform operations when predefined conditions are satisfied. This capability allows developers to build decentralized applications (DApps), including blockchain-based storage systems that operate without centralized control.

Christidis and Devetsikiotis explored the use of blockchain technology and smart contracts in distributed systems such as the Internet of Things (IoT) [4]. Their research showed that blockchain can improve trust, security, and transparency in systems where multiple devices exchange data across networks. Similarly, Zheng et al. provided a comprehensive overview of blockchain technology, discussing its architecture, consensus mechanisms, and applications across different industries while identifying decentralized storage as a promising use case [5].

Further studies have integrated blockchain with distributed storage technologies. Dwivedi et al. proposed a system that combines blockchain with IPFS, where blockchain stores metadata and IPFS stores the actual file data, thereby improving storage efficiency and data integrity [6]. Patil et al. also developed a decentralized storage system where file ownership, timestamps, and transaction details are recorded on the blockchain while the file content is stored in distributed networks [7].

Khalid et al. conducted a comprehensive survey of decentralized storage networks such as Filecoin, Storj, and IPFS-based systems, analyzing their architecture and implementation challenges [8]. Ashok Kumar et al. proposed a blockchain-based platform for securely managing educational resources and enabling controlled sharing of digital content [9]. Additionally, the FileDAG project introduced a decentralized storage architecture that supports multi-version file management using a directed acyclic graph structure, which improves scalability and data availability in distributed environments [10].

Although existing studies demonstrate that blockchain-based decentralized storage systems can improve security, transparency, and reliability, several challenges still remain.

Many proposed systems focus mainly on theoretical architectures or large-scale decentralized networks and do not provide simple and practical implementations for everyday users. In addition, issues related to efficient metadata management, secure file sharing, and user-friendly web interfaces are still not fully addressed. Therefore, there is a need to design a decentralized web-based file storage system that integrates blockchain technology, smart contracts, and distributed storage networks such as IPFS to provide secure, transparent, and efficient file management while ensuring easy accessibility for users.

III. PROPOSED SYSTEM

The proposed system presents a Decentralized Web-Based File Storage System using Blockchain Technology that aims to provide a secure, transparent, and reliable platform for storing and sharing digital files. Traditional cloud storage platforms rely on centralized servers where all data is stored and controlled by a single organization. Although such systems provide convenience and easy data management, they are vulnerable to several problems including server failures, data breaches, unauthorized access, and limited user control over stored information. These issues highlight the need for a more secure and distributed storage solution.

To address these challenges, the proposed system integrates Blockchain with decentralized file storage techniques to build a secure and transparent file management platform. Instead of storing files on a single central server, the system distributes file storage across a decentralized network. Blockchain technology is used to record file metadata, ownership information, and access permissions in an immutable ledger. Because blockchain records cannot be easily modified or deleted, this approach ensures transparency, data integrity, and trust among system users.

The proposed system provides a web-based interface that allows users to upload, store, access, and share files securely. The architecture combines encryption mechanisms, decentralized storage, and blockchain-based access control to protect user data while maintaining system efficiency.

1) User Registration and Authentication

The first stage of the system involves user registration and authentication. Users are required to create an account by providing necessary identification information. After registration, users can securely log into the system using authentication credentials. Authentication ensures that only authorized users can access the storage platform.

In blockchain-based applications, user identity verification can also be performed using digital wallets such as MetaMask, which allows users to interact securely with decentralized applications. This authentication mechanism enhances system security by preventing unauthorized users from accessing stored files or performing unauthorized transactions.

2) File Upload and Data Encryption

After successful authentication, users can upload files through the web interface. The system supports various types of digital content such as documents, images, videos, and other data formats.

Before the files are stored in the decentralized storage network, they are encrypted using cryptographic techniques. Encryption ensures that file content remains confidential and protected from unauthorized access. Only users possessing the correct decryption keys are able to view or download the file. This encryption layer plays a critical role in protecting sensitive user information within the storage system.

3) Blockchain-Based Metadata Management

The system does not store large files directly on the blockchain. Instead, it stores metadata such as the file hash, owner information, and upload time. The hash value acts as a unique identifier for the file. If the file contentaredifferent, the hash will also change. Because blockchain records cannot be easily modified, this helps ensure file integrity and transparency.

The file hash acts as a unique digital fingerprint that represents the file content. If any modification occurs in the file, the hash value changes, allowing the system to detect tampering. Storing metadata on the blockchain ensures that file records remain immutable and verifiable.

4) Decentralized Storage Mechanism

The actual file content is stored in a decentralized storage network such as Inter Planetary File System. In this distributed storage environment, files are divided and stored across multiple nodes in the network.

Decentralized storage provides several advantages over traditional centralized systems. It improves data availability and reliability because files can be retrieved from multiple nodes rather than relying on a single server. Even if one node becomes unavailable due to failure or network issues, the file can still be accessed from other nodes in the network. This architecture eliminates the single point of failure commonly found in centralized storage systems.

5) Secure File Sharing Mechanism

The proposed system allows users to securely share files with other authorized users. When a file owner decides to share a file, the system updates the access permissions through blockchain transactions. The recipient user can then access or download the file based on the permissions defined by the owner.

This mechanism supports secure collaboration while maintaining full ownership control. Since the sharing activity is recorded on the blockchain, all file transactions remain transparent and traceable.

6) Administration and System Management

The system also includes an administrative module responsible for maintaining system performance and monitoring overall activities. The administrator can verify user registrations, monitor file transactions, and ensure that the platform operates efficiently.

Although the storage architecture is decentralized, administrative oversight helps maintain system integrity and prevent malicious activities. The administrator ensures that the platform remains secure while allowing users to retain ownership and control over their files.

IV. PROPOSEDARCHITECTURE

The architecture of the Decentralized Web-Based File Storage System using Blockchain Technology is designed to provide a secure and reliable way to store and share digital files. The system does not rely on a single central server, which helps reduce the risk of data loss or server failure. It combines blockchain technology with decentralized storage to improve data security and transparency. The main components of the system include a web interface, MetaMask, the Ethereum network, Smart Contracts, and Inter Planetary File System. The web interface allows users to upload and manage files easily, while MetaMask connects users to the blockchain. Smart contracts manage file access, and IPFS stores the actual files in a decentralized network.

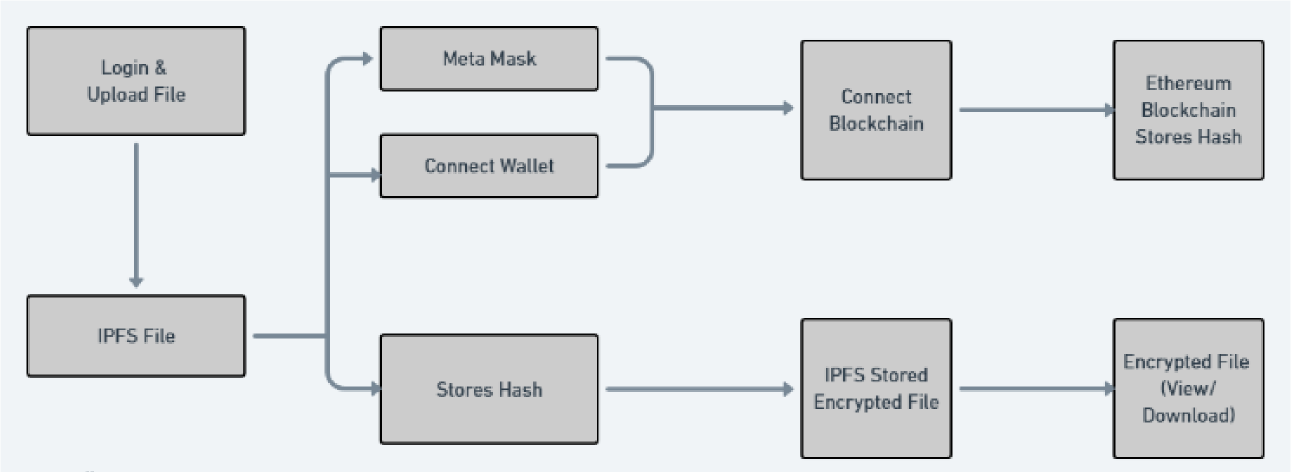


Fig1- Architecture

The architecture of the proposed decentralized file storage system is designed to provide a secure and reliable platform for storing and sharing digital files. The system uses a web-based interface that allows users to easily interact with the application. Through this interface, users can register, log in, upload files, and access stored data. The interface is designed to be simple and user-friendly so that users can perform all file operations without needing advanced technical knowledge.

When a user uploads a file, the system first connects to MetaMask, which acts as a secure gateway between the user and the blockchain network. MetaMask verifies the user’s identity and allows them to approve blockchain transactions. This step ensures that only authenticated users can perform operations such as uploading or sharing files. By using a blockchain wallet for authentication, the system improves security and reduces the risk of unauthorized access.

After the user is verified, the application communicates with the Ethereum network. In this stage, Smart Contracts are used to manage file-related activities. Smart contracts are programs stored on the blockchain that automatically execute specific actions when certain conditions are met. In this system, smart contracts store important information about the uploaded file, such as the file hash, content identifier (CID), owner details, and access permissions. Instead of saving the entire file on the blockchain, only this metadata is stored. This method helps reduce blockchain storage requirements and improves system efficiency while still maintaining transparency and security.

The actual file content is stored in Inter Planetary File System, which is a decentralized storage network. IPFS stores files across multiple nodes in a peer-to-peer network rather than relying on a single centralized server. This distributed approach improves file availability and reliability because the data can be accessed from different nodes even if one node fails. Before a file is uploaded to IPFS, the system encrypts the data to protect it from unauthorized access. Encryption ensures that only users who have the correct decryption key can view or download the file.

When a user wants to access a stored file, the system first checks the blockchain to retrieve the CID associated with that file. The CID acts as a unique identifier that helps locate the file within the IPFS network. Using this identifier, the system retrieves the encrypted file from IPFS. After the file is downloaded, it is decrypted so that the authorized user can access the original content. This process ensures secure file retrieval while maintaining user privacy.

Overall, the proposed architecture combines blockchain technology with decentralized storage to create a secure and transparent file management system. By storing metadata on the blockchain and files in a distributed storage network, the system improves data integrity, reliability, and user control. This architecture reduces dependence on centralized servers, minimizes the risk of data tampering, and provides a more trustworthy solution for managing digital files in modern applications.

.

IV. METHODOLOGY

The system explains how the decentralized file storage platform works step by step. The system uses blockchain technology, encryption methods, and distributed storage networks to create a secure environment for storing and managing files. The main objective of this methodology is to maintain data integrity, improve security, remove centralized control, and allow users to manage their files safely. Each stage of the system performs a specific function that contributes to secure file storage and retrieval.

1) System Initialization

The first stage of the system is initialization, where the decentralized environment is prepared for operation. A web-based application is developed to allow users to interact with the system through a browser. The application connects to the blockchain network using MetaMask, which acts as an interface between the user and the blockchain. During this stage, the system loads the deployed Smart Contracts that define the rules for storing file information, verifying transactions, and managing user permissions.

2) User Authentication through Blockchain Wallet

In the proposed system, user authentication is performed through blockchain wallet integration instead of traditional usernames and passwords. Users connect their digital wallet to the application, and the system verifies their identity through cryptographic signatures. This process ensures that the user is genuine and authorized to perform actions in the system. Since private keys remain with the user, the risk of centralized credential storage is eliminated, which improves overall security.

3) File Selection and Upload Process

After authentication, users can select files from their local device and upload them through the web interface. The application receives the selected file and prepares it for processing. During this stage, the system performs operations such as checking file size and generating a unique hash value. A cryptographic hash function creates a unique identifier for the file, which helps detect any modification in the file content. Even a small change in the file will produce a completely different hash value, which helps maintain file integrity.

4) File Encryption for Data Security

Before storing the file in the distributed network, the system encrypts the file to protect its content. Encryption converts the file into an unreadable format using cryptographic algorithms. This ensures that unauthorized users cannot understand the file content even if they gain access to the stored data. Only users who possess the correct decryption key can convert the encrypted file back to its original format.

5) *Distributed File Storage Using IPFS*

After encryption, the file is uploaded to the decentralized storage network known as the InterPlanetary File System. IPFS stores files across multiple nodes instead of relying on a single centralized server. When a file is stored in IPFS, the system generates a unique Content Identifier (CID) that represents the file in the network. This identifier is based on the file content, which ensures that the stored data cannot be changed without generating a new identifier.

6) *Blockchain Metadata Storage*

Although the actual file is stored in IPFS, important information about the file is stored on the blockchain. This information includes the file identifier (CID), file owner details, and upload timestamp. The metadata is recorded on the Ethereum blockchain through smart contracts. Once the information is recorded, it becomes permanent and cannot be altered without network validation. This feature improves transparency and builds trust in the system.

7) *File Retrieval Mechanism*

When a user wants to access a stored file, the system first verifies the user's permission through the blockchain. The smart contract retrieves the stored metadata, including the CID of the requested file. Using this CID, the system locates the encrypted file in the IPFS network and downloads it. After the file is retrieved, the system decrypts it using the appropriate key and provides the readable file to the authorized user through the web interface.

8) *Access Control and Permission Management*

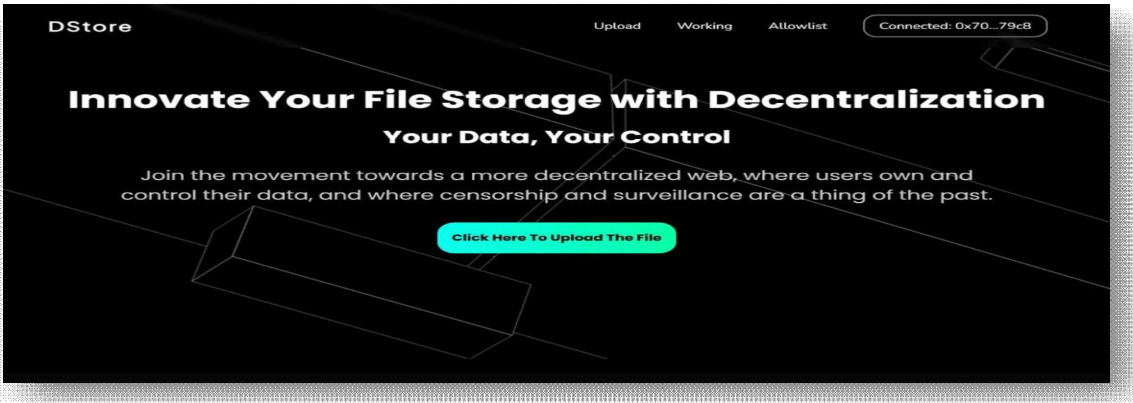
The system includes a decentralized access control mechanism that allows the file owner to manage permissions. Through smart contracts, the owner can allow or restrict other users from accessing specific files. These permission settings are recorded on the blockchain to ensure transparency and security. Since the control mechanism is decentralized, users maintain full authority over their stored data.

9) *System Integration and Workflow*

The overall system integrates three main components: the web application, the blockchain network, and the decentralized storage network. The web application provides the interface for user interaction, the blockchain manages verification and metadata storage, and IPFS handles the distributed storage of files. The workflow begins with user authentication, followed by file encryption, decentralized storage, blockchain recording, and secure retrieval of files. This integrated process ensures a reliable, transparent, and secure decentralized file storage system.

V. RESULTS

This section presents the results obtained from the implementation of the decentralized web-based file storage system. The developed system demonstrates how blockchain technology and decentralized storage networks can be used to securely store, manage, and share digital files. The interface of the system allows users to connect their blockchain wallet, upload files, manage access permissions, and store files using IPFS through the Pinata platform.



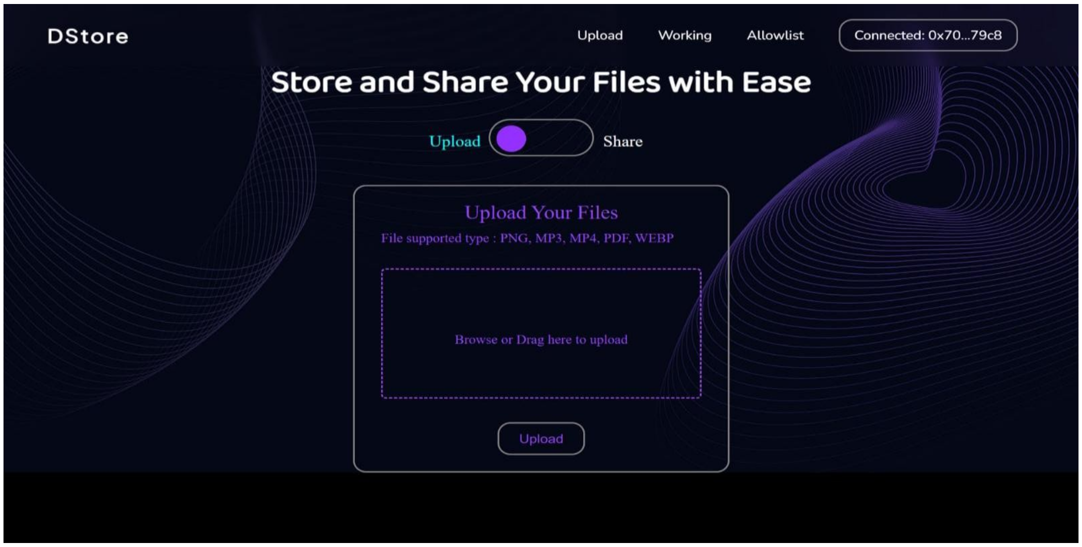
Innovate Your File Storage with Decentralization

Your Data, Your Control

Join the movement towards a more decentralized web, where users own and control their data, and where censorship and surveillance are a thing of the past.

Fig.2.1- Web Interface

Figure 2.1Decentralized file storage is a modern way of storing digital data without depending on a single central server. In this system, files are stored across many computers connected in a network instead of being kept in one location. Each computer contributes some storage space, which helps make the system more reliable. If one computer stops working, the data can still be accessed from other computers in the network. Users control their files using cryptographic keys, which gives them full ownership and privacy. This method improves security, prevents data loss, and reduces the risk of hacking. Decentralized storage also reduces censorship because no single authority controls the stored data. Overall, this technology provides a safer and more reliable way to manage digital files.



Store and Share Your Files with Ease

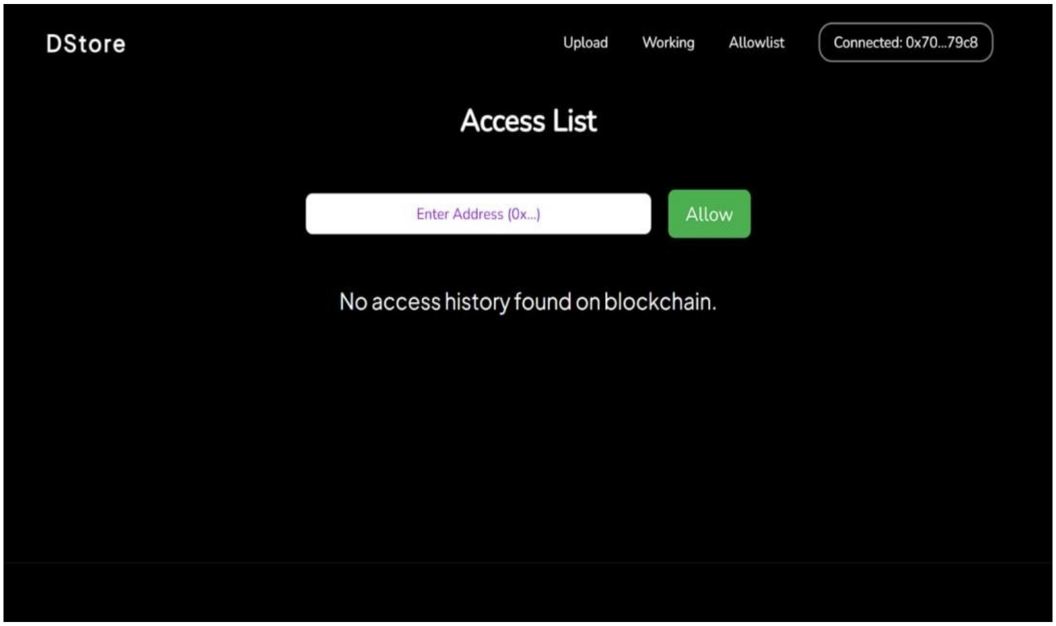
Upload Your Files

File supported type : PNG, MP3, MP4, PDF, WEBP

Browse or Drag here to upload

Fig.2.2-File Upload and store

Figure 2.2shows how users can upload and store files in a decentralized storage system. Instead of saving files on one company’s server, the system distributes them across multiple computers in a blockchain-based network. This improves security and reliability because even if one node fails, the files can still be recovered from other nodes. The wallet connection shown at the top allows users to log in using their blockchain identity. This means users control their own data rather than depending on a central authority. The upload section supports different file types such as PNG, MP3, MP4, PDF, and WEBP, making it easy for users to store different kinds of data. This design focuses on simplicity while maintaining strong security and privacy.

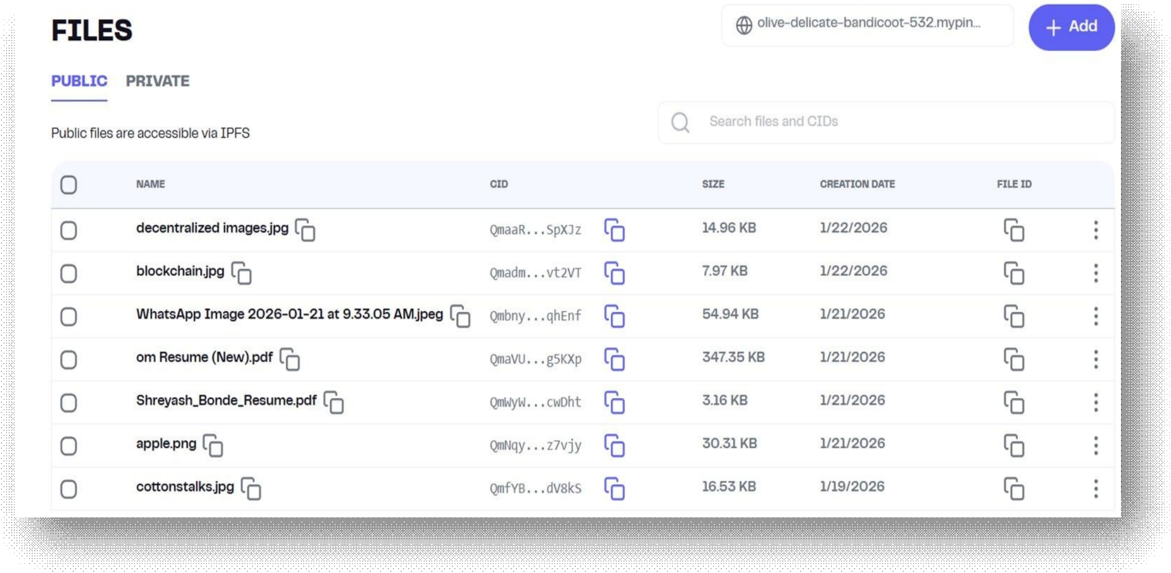


Access List

No access history found on blockchain.

Fig.2.3-Access Management

Figure 2.3 shows the access management feature of the DStore platform. This section allows users to control who can access their stored files. Users can enter an Ethereum address and grant permission by clicking the “Allow” button. The connected wallet confirms the user’s identity through the blockchain network. All access records are stored on the blockchain, which makes the system transparent and secure. Since there is no central administrator controlling permissions, users have complete control over their data. This decentralized access control improves security and prevents unauthorized access to files.



FILES

olive-delicate-bandicoot-532.mypin...

Public files are accessible via IPFS

□	NAME	CID	SIZE	CREATION DATE	FILE ID
□	decentralized images.jpg	QmaaR...SpXJz	14.96 KB	1/22/2026	
□	blockchain.jpg	Qmadm...vt2VT	7.97 KB	1/22/2026	
□	WhatsApp Image 2026-01-21 at 9.33.05 AM.jpeg	Qmbny...qhEnf	54.94 KB	1/21/2026	
□	om Resume (New).pdf	QmaVU...g5KXp	347.35 KB	1/21/2026	
□	Shreyash_Bonde_Resume.pdf	QmWyW...cwDht	3.16 KB	1/21/2026	
□	apple.png	QmNqy...z7vjy	30.31 KB	1/21/2026	
□	cottonstalks.jpg	QmfYB...dV8kS	16.53 KB	1/19/2026	

Fig.2.4-File Storage (Pinata)

Pinata is a platform that helps store files on the IPFS decentralized network. Instead of saving files on a single server, IPFS distributes the files across many computers. Each file receives a unique identifier called a Content Identifier (CID), which is created using cryptographic hashing. This identifier ensures that the file cannot be changed without detection. The Pinata dashboard shows file details such as file name, size, upload date, and CID. It also provides options for public and private storage. One important feature is “pinning,” which keeps files available on the network for a longer time. Pinata is commonly used in Web3 applications such as NFTs, decentralized applications, and blockchain-based projects. Although decentralized storage offers many benefits, it may still face challenges like slower data retrieval and storage costs.

VI. CONCLUSIONS

This research presents a decentralized web-based file storage system using blockchain technology to enhance data security and reliability. Traditional cloud storage systems rely on centralized servers, which can lead to risks such as data loss, security breaches, and lack of transparency. The proposed system addresses these issues by integrating blockchain technology with decentralized storage networks.

In the developed system, files are stored within a distributed storage network, while the blockchain records important metadata such as file ownership and storage information. This approach ensures that the data remains secure, tamper-resistant, and easily traceable. Furthermore, the use of encryption and smart contracts strengthens security and improves access control for stored files.

Overall, the proposed system demonstrates that blockchain technology can provide a more secure, transparent, and reliable approach to digital file storage compared to traditional centralized storage systems.

VII. FUTURE SCOPE

In the future, the proposed decentralized web-based file storage system can be further enhanced to improve scalability, security, and usability. The system can be expanded to support larger distributed networks, enabling it to efficiently manage a greater volume of data and users.

Advanced encryption techniques and stronger access control mechanisms can be implemented to provide higher levels of data protection. Additionally, improvements in the user interface can make the system more user-friendly and accessible for both technical and non-technical users.

The development of mobile application support will allow users to easily upload and access files from smartphones and other portable devices. Furthermore, integrating the system with other decentralized platforms and modern cloud technologies can enhance interoperability and overall system performance.

REFERENCES

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.

[2] J. Benet, “IPFS: Content Addressed, Versioned, P2P File System,”arXiv preprint arXiv:1407.3561, Jul. 2014. doi:10.48550/arXiv.1407.3561.

[3] K. Christidis and M. Devetsikiotis, “Blockchains and smart contracts for the Internet of Things,” IEEE Access, vol. 4, pp. 2292–2303, 2016. doi:10.1109/ACCESS.2016.2566339.

[4] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An overview of blockchain technology: Architecture, consensus, and future trends,” in Proc. IEEE Int. Congr. Big Data, Honolulu, HI, USA, 2017, pp. 557–564. doi:10.1109/BigDataCongress.2017.85.

[5] M. I. Khalid, I. Ehsan, A. K. Al-Ani, J. Iqbal, S. Hussain, S. S. Ullah, and N. Nayab, “A comprehensive survey on blockchain-based decentralized storage networks,” IEEE Access, vol. 11, pp. 10995–11020, 2023. doi:10.1109/ACCESS.2023.3240237.

[6] S. Jadhav and N. Pise, “Securing decentralized storage in blockchain: A hybrid cryptographic framework,” Cybernetics and Information Technologies, vol. 24, no. 2, pp. 16–31, 2024. doi:10.2478/cait-2024-0013.

[7] H.-S. Huang, T.-S. Chang, and J.-Y. Wu, “A secure file sharing system based on IPFS and blockchain,” in Proc. IEEE Int. Conf. Commun. Workshops (ICCW), 2019, pp. 1–5. doi:10.1109/ICCW.2019.8756878.

[8] Z. Zheng, S. Xie, H. Dai, and H. Wang, Blockchain Technology: Principles and Applications. Singapore: Springer, 2018. doi:10.1007/978-981-10-7276-8.

[9] S. Wilkinson, T. Boshevski, J. Brandoff, V. Buterin, and J. Preston, “Storj: A Peer-to-Peer Cloud Storage Network,”Storj Labs White Paper, 2014.

[10] C. Li, P. Li, and J. Liu, “SoK: Decentralized storage networks,” Internet of Things, vol. 25, 2024. doi:10.1016/j.iot.2024.100924.

[11] E. Daniel and F. Tschorsch, “IPFS and friends: A qualitative comparison of next-generation peer-to-peer data networks,” IEEE Communications Surveys & Tutorials, 2021. doi:10.48550/arXiv.2102.12737.

[12] S. Lamichhane and P. Herbke, “Verifiable decentralized IPFS cluster: Unlocking trustworthy data permanency for off-chain storage,” arXiv preprint arXiv:2408.07023, 2024. doi:10.48550/arXiv.2408.07023.

[13] H. Chen, Y. Lu, and Y. Cheng, “FileInsurer: A scalable and reliable protocol for decentralized file storage in blockchain,” arXiv preprint arXiv:2207.11657, 2022. doi:10.48550/arXiv.2207.11657.

[14] M. Merlec, J. Zaletelj, and M. Kovač, “Blockchain-based decentralized storage systems for sustainable data storage,” Sustainability, vol. 16, no. 17, 2024. doi:10.3390/su16177671.

[15] I. Vakilinia, J. Sengupta, and S. Sengupta, “An incentive-compatible mechanism for decentralized storage networks,” arXiv preprint arXiv:2208.09937, 2022. doi:10.48550/arXiv.2208.09937.