Decentralised File Storage System for Enhanced Security

[1]Devanshi Padhy [2]Maaz Shaikh [3]Siddhi Mardhekar [4]Vineesh Naringrekar
[12]Bharatiya Vidya Bhavans Sardar Patel Institute of Technology

Abstract - **This research proposes a novel decentralized file storage system that leverages blockchain technology and peer-to-peer networks to enhance data security and privacy. The system eliminates centralized control, distributing data across multiple nodes for resilience against attacks and data loss. Advanced encryption techniques and access control mechanisms based on smart contracts safeguard data confidentiality and enable granular sharing permissions. The decentralized architecture ensures data availability and integrity through replication across nodes. Evaluations demonstrate the system's superior performance in data security, privacy, and reliability compared to centralized solutions, making it suitable for domains prioritizing these aspects, such as healthcare and finance.**

Key Words- Decentralized file storage, blockchain, peer-to-peer networks, data security, data privacy, encryption, access control, smart contracts, data availability, data integrity, resilience, centralization risks, performance evaluatio

I. INTRODUCTION

In the digital age, the need for secure and decentralized file storage solutions has become paramount. Centralized systems are vulnerable to single points of failure, data breaches, and privacy concerns. This research proposes a novel decentralized file storage system that facilitates secure file uploading and downloading on the blockchain through the utilization of Solidity for smart contract development and React for the front-end interface.

The proposed system empowers users to securely upload files to the InterPlanetary File System (IPFS) and manage access permissions by leveraging the capabilities of smart contracts. This innovative solution ensures the immutability and decentralization of stored files while providing a seamless and user-friendly experience for interacting with blockchain technology.

By combining the power of Solidity and React, the system offers a robust platform for individuals to securely share their files while maintaining control over who can access them, thereby enhancing privacy and security in the realm of decentralized file sharing. Smart contracts govern access control, enabling users to grant or revoke permissions dynamically, ensuring that sensitive data remains confidential and accessible only to authorized parties.

The decentralized nature of the system mitigates the risks associated with centralized storage solutions, such as data loss, unauthorized access, and service disruptions. By distributing data across a peer-to-peer network, the system achieves resilience against single points of failure and enhances data availability and integrity.

This research presents a comprehensive analysis of the system's architecture, security mechanisms, and performance evaluations, highlighting its potential for adoption in various domains where data security, privacy, and decentralization are critical, such as healthcare, finance, and government sectors.

II. BACKGROUND AND RELATED WORK

Decentralized systems and blockchain technology have emerged as powerful solutions for addressing the challenges associated with traditional centralized architectures. This section provides an overview of the fundamental principles and concepts underpinning decentralized file storage systems, as well as a discussion of related work in this domain.

A. Principles of Decentralized Systems and Blockchain Technology

Decentralized systems are characterized by the absence of a central authority or single point of control. Instead, they rely on a distributed network of nodes, each contributing to the overall functionality and decision-making process. This distributed nature enhances resilience, as there is no single point of failure, and ensures that no single entity has complete control over the system.
Blockchain technology, which gained widespread attention with the advent of cryptocurrencies like Bitcoin, is a key enabler of decentralized systems. A blockchain is a distributed, immutable ledger that records transactions in a secure and transparent manner. It operates on the principles of consensus mechanisms, where multiple nodes validate and agree upon the state of the ledger, preventing tampering or manipulation.

The combination of decentralization and blockchain technology offers several advantages, including enhanced security, transparency, and trust. By distributing data and computations across a network of nodes, the risk of data breaches and single points of failure is mitigated. Additionally, the immutable nature of blockchain transactions ensures data integrity and provides an auditable trail of activities.

B. InterPlanetary File System (IPFS)

The InterPlanetary File System (IPFS) is a decentralized file storage and sharing protocol that plays a crucial role in the proposed file storage system. IPFS operates on a peer-to-peer network, where files are split into smaller chunks and distributed across multiple nodes. Each chunk is identified by a unique cryptographic hash, ensuring content addressing and facilitating efficient retrieval and verification.

IPFS offers several advantages over traditional centralized file storage systems. First, it enhances data availability and redundancy, as files are replicated across multiple nodes, reducing the risk of data loss. Second, it improves performance by enabling efficient content distribution and retrieval through content addressing and peer-to-peer sharing. Third, IPFS promotes censorship resistance, as there is no central authority controlling the storage and distribution of files.

C. Related Works

Numerous research efforts have explored the potential of decentralized file storage systems, leveraging blockchain technology and peer-to-peer networks. These solutions aim to address the limitations of centralized storage, such as data breaches, censorship, and single points of failure.

One notable example is the InterPlanetary File System (IPFS), which has been extensively studied and implemented in various projects. IPFS provides a decentralized and distributed file system, enabling efficient content addressing, retrieval, and sharing. However, IPFS lacks built-in access control mechanisms, which are essential for ensuring data privacy and security.

Other research projects have focused on integrating blockchain technology with decentralized file storage systems to address the access control and data ownership challenges. For instance, the Storj project combines blockchain-based smart contracts with distributed storage nodes to enable secure and decentralized file storage. Similarly, the Sia project employs blockchain technology and cryptographic proofs to facilitate secure and decentralized storage contracts between hosts and renters.

While these existing solutions have made significant strides in decentralized file storage, there are still challenges and limitations that need to be addressed. These include scalability concerns, performance bottlenecks, and the complexity of integrating multiple technologies (e.g., blockchain, peer-to-peer networks, and access control mechanisms) into a cohesive and user-friendly system.

The proposed decentralized file storage system, Dgdrive3.0, aims to build upon the strengths of existing solutions while addressing their limitations. By combining the power of blockchain technology, IPFS, and advanced security mechanisms, Dgdrive3.0 seeks to provide a secure, resilient, and censorship-resistant file storage solution that empowers users with enhanced privacy and control over their data.

III. PROPOSED SYSTEM ARCHITECTURE

Dgdrive3.0 is a decentralized file storage system that leverages the power of blockchain technology, the InterPlanetary File System (IPFS), and a user-friendly front-end interface to provide a secure, resilient, and censorship-resistant solution for file storage and sharing. This section outlines the system's overall architecture, key components, and the roles played by various technologies.

A. System Overview and Key Components

The proposed system architecture consists of three main components: the Ethereum blockchain, IPFS, and the React-based front-end interface. These components work in tandem to facilitate secure file uploads, access control, and retrieval while ensuring data privacy, integrity, and availability.

1. *Ethereum Blockchain*: The Ethereum blockchain serves as the foundation for the system's decentralized nature and secure transaction management. Smart contracts deployed on the Ethereum network govern the access control mechanisms, ensuring that only authorized users can upload, access, and modify files. These smart contracts are responsible for validating transactions, enforcing permissions, and maintaining an immutable record of all file-related activities.
2. *InterPlanetary File System (IPFS)*: IPFS is a decentralized, peer-to-peer file storage system

integrated into the proposed architecture. It provides a robust and distributed storage solution, ensuring data redundancy and availability. Files uploaded to the system are encrypted, split into smaller chunks, and stored across multiple nodes in the IPFS network, eliminating the risk of a single point of failure.

3. *React Front-end Interface*: The front-end interface, developed using React, a popular JavaScript library for building user interfaces, serves as the gateway for users to interact with the decentralized file storage system. This user-friendly interface abstracts away the underlying complexities of blockchain and IPFS, enabling seamless file uploads, access control management, and file retrieval.

B. Utilization of Solidity for Smart Contract Development

Solidity, a contract-oriented programming language, plays a crucial role in the development of smart contracts that govern the system's access control mechanisms. These smart contracts are responsible for enforcing permissions, validating transactions, and maintaining an immutable record of file-related activities on the Ethereum blockchain.

The smart contracts are designed to ensure secure and transparent file management, enabling users to grant or revoke access permissions to specific files or groups of files. They also handle the storage and retrieval of file metadata, such as file hashes, ownership information, and access control lists (ACLs).

C. Integration of IPFS for Decentralized Storage

The InterPlanetary File System (IPFS) is a crucial component of the proposed system architecture, providing a decentralized and distributed file storage solution. IPFS operates on a peer-to-peer network, where files are split into smaller chunks, encrypted, and distributed across multiple nodes. Each chunk is identified by a unique cryptographic hash, enabling efficient retrieval and verification of file integrity.

By integrating IPFS, the system benefits from enhanced data availability, redundancy, and censorship resistance. Files are no longer stored on a central server, mitigating the risks of data breaches, censorship, and single points of failure. Additionally, IPFS's content-addressing mechanism enables efficient file retrieval and sharing, improving overall system performance.

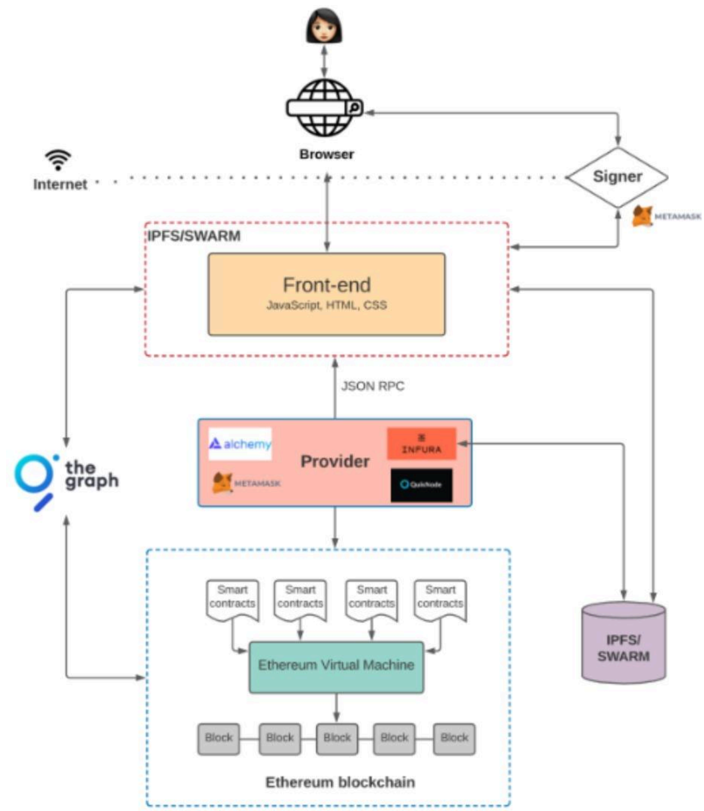

Figure 1: Flowchart for the architecture of the proposed solution

D. ROLE OF REACT FOR THE FRONT-END INTERFACE

The front-end interface, developed using React, a popular JavaScript library for building user interfaces, plays a vital role in providing a seamless and user-friendly experience for interacting with the decentralized file storage system. React's component-based architecture and efficient rendering mechanisms ensure a responsive and intuitive interface, enabling users to easily upload, manage, and retrieve files.

The front-end interface abstracts away the complexities of blockchain technology and IPFS, presenting a simplified and intuitive user experience. It handles file selection, initiates transactions on the Ethereum blockchain, communicates with the smart contracts for access control management, and facilitates file uploads and retrieval from the IPFS network.

By leveraging React's extensive ecosystem of libraries and tools, the front-end interface can be easily extended and customized to meet specific user requirements, ensuring a consistent and engaging user experience across various platforms and devices.

The integration of Ethereum's blockchain, IPFS, and the React front-end interface forms a robust and secure decentralized file storage system that empowers users with enhanced privacy, data resilience, and censorship resistance. This architecture combines the strengths of each component, creating a cohesive and efficient solution for decentralized file storage and sharing.

IV. SYSTEM COMPONENTS

A. Smart Contracts:

Developed using Solidity, smart contracts govern access control mechanisms on the Ethereum blockchain. They handle file ownership, permissions, and maintain an immutable record of activities. These contracts enforce rules and validate transactions for secure file uploads, access, and modifications.

B. InterPlanetary File System (IPFS):

A decentralized, peer-to-peer file storage system integrated into the architecture. IPFS ensures data redundancy and availability by distributing encrypted and chunked files across multiple nodes. Content-addressing facilitates efficient retrieval and verification of data integrity. IPFS enhances censorship resistance and eliminates single points of failure.

C. Front-end Interface:

Built with React, the user-friendly interface provides a seamless experience for interacting with the system. It abstracts underlying blockchain and IPFS complexities, handling file selection, transaction initiation, access control management, and file uploads/retrieval. Cross-platform compatibility ensures a consistent experience across devices.

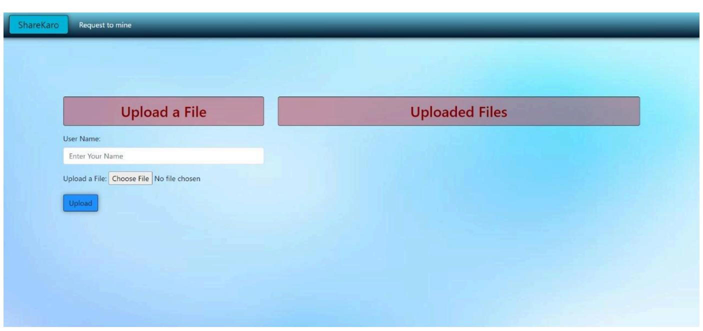

Figure 2: Front- End of DgDrive 3.0

The smart contracts govern access control, IPFS enables decentralized storage with data integrity, and the front-end interface facilitates user interactions, forming a secure and reliable file management solution within a decentralized ecosystem.

V. SYSTEM INTERACTION

A. Document Upload Process

The document upload process begins with the user initiating an upload via the frontend interface. This action triggers a blockchain transaction containing the file metadata. A smart contract then validates the transaction and facilitates the storage of the file on the InterPlanetary File System (IPFS). The file is encrypted, chunked, and distributed across the IPFS network, with the successful upload being recorded on the blockchain for transparency and auditability.

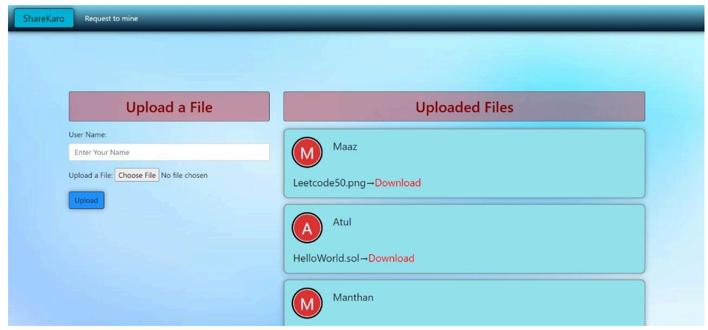

Figure 3: Three Files uploaded onto DgDrive 3.0

B. Document Access and Permissions

When a user requests access to a document through the front end, the system checks the user's permissions against the smart contract. If the user is granted access, the smart contract retrieves the file hash from IPFS, allowing the file to be fetched, decrypted, and displayed on the front end. However, if the user lacks the necessary permissions, access is denied, ensuring data security and privacy.

. *C. Document Download*

To download a document, an authorized user initiates the request through the frontend. The system checks the user's permissions against the smart contract, and if access is granted, the smart contract retrieves the file hash from IPFS. The file is then fetched, decrypted, and made available for download to the user. This process ensures that only authorized users can access and download the documents, maintaining data security and integrity.

The system interaction architecture effectively leverages blockchain technology for secure transactions, IPFS for decentralized and resilient storage, and smart contracts for granular access control. By combining these elements, the system ensures data integrity, transparency, and security throughout the document lifecycle, enhancing trust and reliability in document management processes.

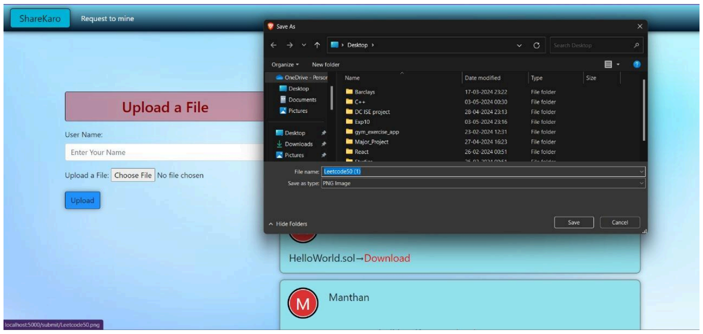

Figure 4: Option to download files

VI. USE CASES AND APPLICATIONS

Dgdrive 3.0 offers versatile applications in healthcare, finance, and government. It enables secure storage and sharing of sensitive data, streamlining document management and enhancing transparency. The system's decentralized nature provides greater user control, data security, and resilience. However, it faces challenges like scalability, user adoption, and regulatory compliance.

The system's benefits include data control, security, and resilience. Challenges include scalability and user adoption. Compliance with regulations is crucial. Understanding these aspects helps stakeholders assess Dgdrive 3.0's impact on document management and data security across industries.

Dgdrive 3.0's decentralized architecture ensures data availability and reduces the risk of data loss. The system's distributed storage and blockchain-based access control mechanisms combat censorship, guaranteeing data integrity and availability. By understanding the potential use cases, benefits, advantages, challenges, and limitations, stakeholders can better assess Dgdrive 3.0's applicability and impact, paving the way for enhanced document management practices and data security.

VII. CONCLUSION

In conclusion, the exploration of Dgdrive 3.0 has revealed a groundbreaking decentralized document management system that leverages blockchain, IPFS, and smart contracts to enhance data security, privacy, and accessibility. The system's key findings include its potential applications across sectors such as healthcare, finance, and government, offering benefits like enhanced privacy, resilience, and censorship resistance. Dgdrive 3.0's contributions lie in empowering users with greater control over their data and fostering a transparent, censorship-resistant document sharing ecosystem.

Despite its strengths, Dgdrive 3.0 faces challenges such as scalability, user adoption, and regulatory compliance. Addressing these limitations is crucial for optimizing the system's performance and usability. Potential improvements could focus on enhancing scalability through optimized network architecture, increasing user education and onboarding processes to drive adoption, and implementing robust compliance measures to meet evolving regulatory requirements.

Looking ahead, future research in the field of decentralized document management systems could explore advanced encryption techniques to further enhance data security, develop user-friendly interfaces to simplify interaction with blockchain technologies, and investigate novel consensus mechanisms to improve system efficiency and scalability. Additionally, research efforts could focus on exploring the integration of artificial intelligence and machine learning algorithms to automate document management processes and enhance user experience in Dgdrive 3.0 and similar systems. By addressing the identified limitations, pursuing potential improvements, and exploring future research directions, the evolution of Dgdrive 3.0 and decentralized document management systems holds promise for revolutionizing data management practices, ensuring data integrity, security, and accessibility in diverse industries and applications.

VIII.REFERENCES

[1] H. Huang, J. Lin, B. Zheng, Z. Zheng and J. Bian, "When Blockchain Meets Distributed File Systems: An Overview, Challenges, and Open Issues," in IEEE Access, vol. 8, pp. 50574-50586, 2020, doi: 10.1109/ACCESS.2020.2979881.

[2] H. Li and D. Han, "EduRSS: A Blockchain-Based Educational Records Secure Storage and Sharing Scheme," in IEEE Access, vol. 7, pp. 179273-179289, 2019, doi: 10.1109/ACCESS.2019.2956157.

[3] H. Li and D. Han, "EduRSS: A Blockchain-Based Educational Records Secure Storage and Sharing Scheme," in IEEE Access, vol. 7, pp. 179273-179289, 2019, doi: 10.1109/ACCESS.2019.2956157.