Decentralised File Storage Marketplace

ICT 3144 Information Security Lab
Mini Project Final Report

Sindhu
Reg.No 220953002
Department of I&CT
Manipal Institute of Technology
Manipal Academy of Higher Education
Manipal- 576104, Karnataka, India
sindhu.mitmpl2022@learner.manipal.edu

Anushri Viraj Sakhardande
Reg.No 220953138
Department of I&CT
Manipal Institute of Technology
Manipal Academy of Higher Education
Manipal- 576104, Karnataka, India
anushri.mitmpl2022@learner.manipal.edu

Uppaluri Jahnavi
Reg.No 220953242
Department of I&CT
Manipal Institute of Technology
Manipal Academy of Higher Education
Manipal- 576104, Karnataka, India
uppaluri.mitmpl2022@learner.manipal.edu

I. Introduction

A decentralised file storage involves distributing stored data across several nodes or devices in the network instead of a central server, like in a traditional cloud server architecture. In this model, data is divided into pieces and later encrypted before being stored on the nodes. Decentralised storage means using blockchain or peer-to-peer networks. No centralised authority controls that data, thus enhancing its privacy and security. Users would keep control of their data and their respective encryption keys, a secure, resilient alternative to cloud services. One of the main benefits of decentralised storage is redundancy and reliability. Data can be fetched from other nodes even with one node offline, thereby minimising losses in any data. Popular systems include IPFS, Filecoin, Storj, and Sia, which incentivise contribution through token rewards and smart contracts, making decentralised storage cost-effective and highly resilient to failures.

The emergence of decentralised technologies has enabled novel approaches to data management, where users can securely and autonomously interact without relying on centralised authorities. This paper introduces the Decentralized File Storage Marketplace (DFSM). This blockchain-based platform empowers users to retain complete control over their data while engaging in a peer-to-peer marketplace. DFSM facilitates interactions between two types of users: data owners and data requesters. Data owners can upload files to a decentralised storage system, maintaining ownership and control over access permissions.

Data requesters seeking access to specific data can place bids within the marketplace, creating a competitive environment that encourages fair pricing and user engagement. Data owners, in turn, review these bids and grant access based on their preferences, ensuring that the data-sharing process remains user-centric and transparent. Smart contracts govern all transactions within DFSM, automating bid management, access permissions, and payments to eliminate reliance on intermediaries. This decentralised approach enhances data security, mitigates transaction costs, and aligns with a user-driven model for managing and sharing digital assets.

By leveraging a blockchain foundation, DFSM ensures transparency, auditability, and security, as every transaction is recorded immutably. This model fosters trust between users and addresses critical issues in traditional file-sharing systems, including data privacy, control, and resilience.

II. Related Works

The paper by Shangping Wang et al.[1] describes a new framework for safe and efficient data sharing in decentralised storage systems, which integrates blockchain with Attribute-Based Encryption and the InterPlanetary File System. The framework is designed to bypass the weaknesses of traditional cloud storage, such as openness to privacy attacks and dependence on central control, by distributing data in IPFS with the application of the Ethereum blockchain to enforce fine-grained access control. ABE offers flexible, attribute-based access policies that allow data owners to specify conditions under which users can access their data, thus enhancing privacy and data security. The system further supports keyword search functionality over encrypted data. Users can retrieve files relevant to encrypted search terms stored on the Ethereum blockchain. This means sensitive data would remain private yet enable an efficient retrieval. The system was evaluated on the Ethereum Rinkeby test network to demonstrate feasibility, effectiveness, and robustness in a decentralised environment. The results were that blockchain could significantly enhance the security of decentralised solutions for storage without the traditional, centralised third parties often required in current solutions. In that sense, it presents an up-and-coming alternative in safe data storage and access management cases.

The paper "A Comprehensive Survey on Blockchain-Based Decentralized Storage Networks"[2] discusses blockchain-based decentralised storage networks as a substitute for traditional clouds of storage systems with improved privacy, data ownership, and the absence of single points of failure. It outlines how blockchain facilitates decentralised storage through integrating systems such as Filecoin, Storj, and Sia to utilise distributed storage and incentivised participation through token-based rewards. These networks perform better in privacy than traditional cloud services since they leverage

blockchain regarding transparency and immutability. Storage protocols, security mechanisms, user incentives, and reliance on smart contracts for storage management and file retrieval will feature in the paper as differences in decentralised networks. Despite these benefits, the paper speaks of problems still in their infancy. It will endure in the overall adoption of the technology at scale, like latency, data integrity, and provision of high levels of network reliability. Overall, the survey shows the necessity for further development to overcome these limitations and create standardised solutions to make decentralised storage accessible and practical to a more significant extent than before.

The paper by P. Yugapuspito, E. Ekaputra et al.[3] compares the functionalities and efficiencies of two decentralised file storage solutions using Ethereum's blockchain and the other, the InterPlanetary File System (IPFS) and evaluations based on deployment, security, scalability, and cost. Ethereum is notable for robust protection and support for smart contracts, a reliable platform for managing access control and file metadata with smart contracts, but with high transaction fees, making storage costly for large-scale applications. In contrast, IPFS is a peer-to-peer distributed storage system that uses content-based addressing to find and retrieve files based on this information. Hence, IPFS proves to be highly scalable and cost-effective for data-heavy tasks. The practical approach would be to store the files on IPFS to implement efficiency with a secure, immutable ledger in Ethereum's blockchain for tracking file access permission and operations. This would balance the decentralised storage system, which uses IPFS for scalability and leverages Ethereum for security despite high transaction costs on Ethereum. The study concluded that although promising as a framework for file decentralisation, using IPFS and Ethereum, cost limitations from the perspective of the blockchain may put restrictions on its viability in certain use cases, showing the necessity to optimise so that decentralised storage can become cost-effective constantly.

In "Decentralized File Storage: Leveraging Blockchain, Polygon, Polygon, Web3, and IPFS", Jalpan Mahajan and Akshara Prachi[4] share a new file storage approach. The proposed system combines a range of technologies, such as blockchain; Polygon, a scaling solution for the Ethereum blockchain; Web3, the next iteration of the internet built on blockchain principles; and IPFS, or the InterPlanetary File System, which defines itself as a peer-to-peer hypermedia protocol. It is used to solve traditional file storage problems where decentralisation, higher security, and greater efficiency are essential. Thus, The system can ensure data integrity and immutability by using blockchain to prevent unauthorised modifications. Polygon further allows for faster processing of transactions than on the Ethereum mainnet. Web3 also provides the framework for interactions involving dApps with the storage system. Finally, IPFS ensures efficient data distribution and retrieval from a network of nodes without a centralised server. This overall approach, as presented in this paper, would likely revolutionise the storage of files to a higher plane of safety, transparency, and scalability.

K. Sivasankari and V.S. Sathyamithran have discussed in the paper "IPFS Enabled Robust Mechanism for File Storage and Retrieval Using Block Chain"[5], a novel approach to decentralised file storage powered by InterPlanetary File System and blockchain technology. The proposed system would bring out the unique strengths of both technologies by providing a robust and secure solution for file storage and retrieval. Hence, the IPFS is a decentralised data storage network allowing effective file distribution and sharing since it stores files redundantly across several nodes. However, the IPFS alone cannot guarantee the integrity or provenance of the data. This is compensated by the fact that when combined with blockchain technology, as the authors suggested, recording the file hashes and metadata on a blockchain guarantees the authenticity and immutability of files in storage. Any tampering attempt or change is traceable.

III. Method

The Decentralized File Storage Marketplace (DFSM) is designed to create a seamless interaction between data owners and requesters through a decentralised and transparent platform.

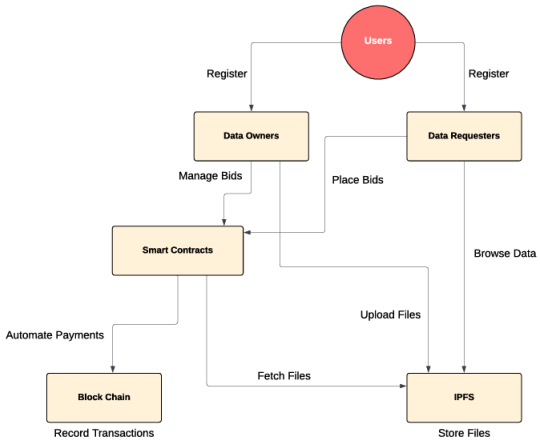

Fig. 1: Block Diagram of Decentralised File storage Marketplace

A. System Architecture

The DFSM system architecture consists of three primary components:

- **User Interface:** Provides an intuitive platform for users to interact as data owners or requesters. It allows data owners to upload files and manage permissions while requesters can browse available data and place bids.
- **Decentralised Storage System:** Utilizes IPFS to store files. IPFS provides a distributed, peer-to-peer file storage system, ensuring integrity, availability, and decentralised control over file access.

- **Blockchain and Smart Contracts:** Manages transaction records, bid placements, and access permissions. The smart contracts handle bid requests, validate permissions, and automate payments upon successful transactions.
- **Security and Transaction Validation:** The blockchain's immutable ledger ensures that all transactions are securely recorded and transparent. Smart contracts enforce transaction conditions and automate fund transfers, minimising the risk of fraud and ensuring that both parties comply with agreed terms

B. Workflow

The workflow of DFSM can be broken down into the following steps:

1) **User Registration:** Users sign in using their Metamask wallet and select a data owner or requester role.
2) **Data Upload and Metadata Generation:** Data owners upload files to decentralised storage (e.g., IPFS), generating metadata (description, size, access requirements) stored on the blockchain for file discovery.
3) **Bid Placement by Data Requesters:** Requesters browse and place bids with access details (duration, price). The blockchain records these bids for transparency.
4) **Bid Evaluation by Data Owners:** Data owners review and accept bids, triggering smart contracts to update access permissions and transfer funds.
5) **Access Grant and Data Retrieval:** Upon bid acceptance, the smart contract grants the requester access and provides a secure link to retrieve the file within the agreed period.

C. Algorithm

Algorithm 1 Decentralized File Storage Marketplace Workflow

Initialize System
User Registration:
if new user **then**
    Select Role (Data Owner / Data Requester)
end if
Data Upload (Data Owner):
    Upload file to decentralised storage
    Generate and store file metadata on the blockchain
Bid Placement (Data Requester):
for each address **do**
    Place bid with price
end for
Bid Evaluation (Data Owner):
    Review all bids
    Select the preferred bid
    Execute smart contract for fund transfer and access grant
Access Grant (Data Requester):
    Retrieve link

IV. Results

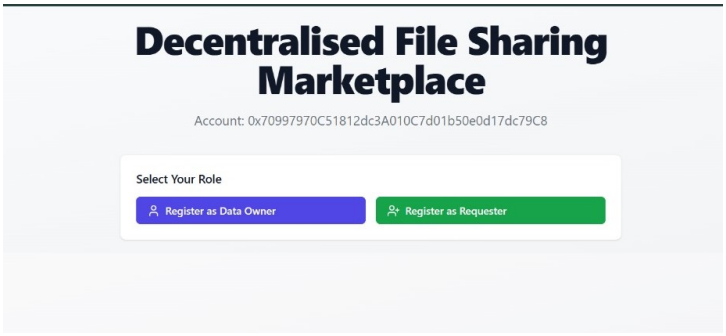

Fig. 2: Home page asking user to register

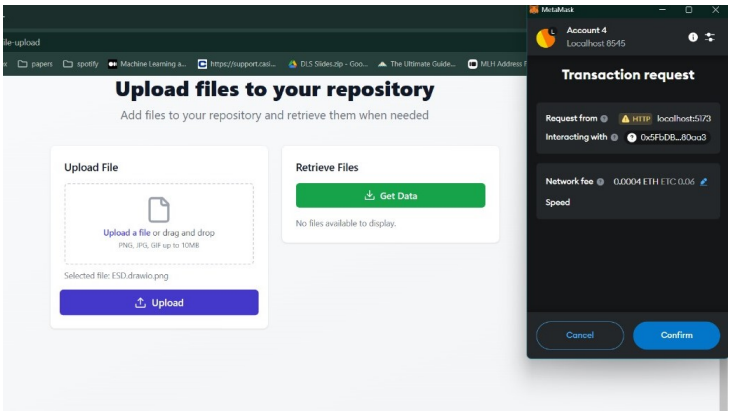

Fig. 3: Options for data owners to upload and retrieve files

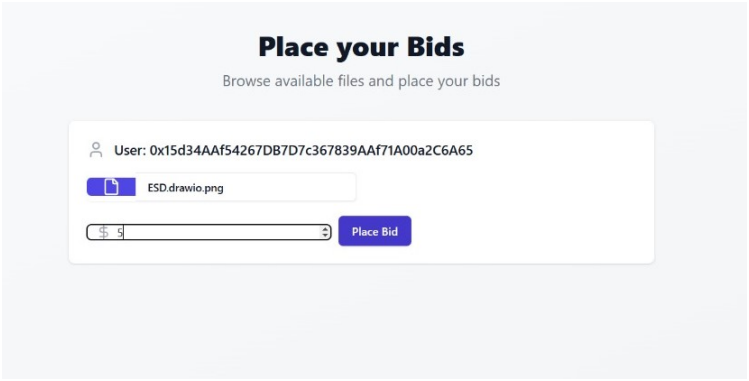

Fig. 4: Options for data requesters to place bids for data owners' files

V. Study Limitations

While these frameworks offer promising solutions, several limitations were noted across studies. First, transaction costs on blockchain networks like Ethereum remain a significant barrier to large-scale adoption, especially in high-frequency data access applications. Second, latency and network reliability issues persist, as decentralised systems can struggle to deliver the rapid response times expected in traditional

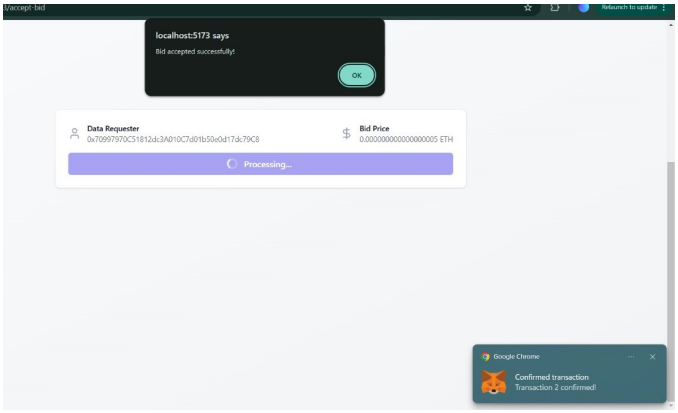

Fig. 5: Accepted bid of the data requester

cloud storage solutions. Another limitation is the dependency on public blockchain networks, which, although secure and immutable, can be slow and need more scalability when handling complex transactions or large file sizes. Additionally, concerns around data integrity, the cost-effectiveness of the technology, and limited user incentives to participate in decentralised networks such as IPFS and blockchain-based systems further indicate the need for ongoing optimisation. Finally, achieving consistent standards for interoperability across various blockchain and decentralised storage solutions is essential to enhance the scalability and usability of these technologies in a broader context.

VI. Future scope

The Decentralized File Storage Marketplace (DFSM) has promising potential for future advancements to enhance its scalability, security, and user experience. One significant development area is deploying DFSM on a production blockchain network like Ethereum mainnet or a Layer-2 solution like Polygon. This deployment would enable real-world testing, improve transaction efficiency, and prepare DFSM for broader adoption. Layer-2 solutions could help the system handle larger user bases and high-frequency transactions by reducing transaction costs and latency, making decentralised storage viable for more applications.

Time-based access can limit the time the user can retain access to the file, giving greater control to the data owner over access. Also, access revocation and blocking of future bids can be implemented to prevent bad actors. Another crucial improvement would be introducing individual bid management at the file level rather than grouping bids for all files from a data owner. By enabling data requesters to bid on specific files, the system would offer more flexibility in access control and improve the overall bidding experience for users. Dynamic constraints on bid amounts could also enhance this bidding system, allowing data owners to set minimum bid values based on factors like file size, sensitivity, or access demand. Such constraints would prevent underbidding and ensure fair compensation, supporting a healthier marketplace ecosystem.

Security is another essential area for DFSM's evolution. Implementing mechanisms to detect and prevent malpractices in transactions, such as setting flags for suspicious bid amounts, repetitive bidding patterns, or attempts to manipulate access, could significantly strengthen trust within the marketplace. Anomaly detection algorithms within smart contracts could automatically identify and block suspicious activities, further protecting the system from abuse. In addition to this, incorporating Attribute-Based Encryption (ABE) could allow data owners to specify more granular access requirements, enhancing data privacy by aligning access conditions with specific attributes or roles, making it particularly suitable for industries with stringent privacy regulations. A reputation or rating system based on users' transaction histories could be introduced to increase marketplace transparency and trust. Data owners and requesters with high ratings would build a reputation, adding reliability to their transactions. At the same time, users flagged for suspicious activities could be restricted, contributing to a safer and more trustworthy platform. Regular smart contract audits would ensure security, identify potential vulnerabilities, and align DFSM with blockchain security best practices. Enhanced features, such as multi-signature authentication for high-value transactions, would provide additional protection, securing transactions and reinforcing data owners' and requesters' confidence in the system. These future enhancements would collectively make DFSM a more robust, user-centric, and secure platform for decentralised file storage and access management. By integrating these improvements, DFSM could evolve into a highly scalable and efficient solution capable of meeting the complex needs of decentralised data storage at a larger scale.

VII. Conclusion

References

[1] Shangping Wang, Yinglong Zhang, and Yaling Zhang. A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems. *IEEE Access*, 6:38437–38450, 2018.

[2] Muhammad Irfan Khalid, Ibtisam Ehsan, Ayman Khallel Al-Ani, Jawaid Iqbal, Saddam Hussain, Syed Sajid Ullah, and Nayab. A comprehensive survey on blockchain-based decentralized storage networks. *IEEE Access*, 11:10995–11015, 2023.

[3] Pujianto Yugopuspito, Eugene Ekaputra, and Julinda Pangaribuan. Comparing decentralized file storage on ethereum with interplanetary file system. pages 1–6, 12 2023.

[4] Jalpan Mahajan and Akshara Prachi. Decentralized file storage: Leveraging blockchain, polygon, web3, and ipfs. pages 1–5, 05 2024.

[5] K. Sivasankari and V.S. Sathyamithran. Ipfs enabled robust mechanism for file storage and retrieval using block chain. In *2022 Fourth International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT)*, pages 01–05, 2022.