[1]

Decentralized File Storage Platform using IPFS and Blockchain

***Abstract*— This paper presents a pioneering web application that combines InterPlanetary File System (IPFS) and Blockchain technology to meet the increasing demand for secure, scalable, and decentralized data storage. The system utilizes locally-hosted Digital Ocean droplets as gateways, eliminating reliance on third-party companies and maintaining decentralization. By integrating blockchain technology, the application enhances security through transaction authentication and access permission management. It offers features such as access control, file integrity checking using IPFS hashes, and the potential for future enhancements like a custom cryptocurrency for transactions. This innovative system provides a practical, decentralized alternative to mainstream cloud storage services, ensuring data privacy, security, and integrity while granting users greater authority over their data.**

***Index Terms*— File Storage, Blockchain, Decentralized, IPFS , Access Control, Private Gateway**

I. Introduction

The dawn of the digital age has significantly transformed how individuals and organizations manage, store, and share their data. Traditional methods, often centralized and susceptible to security risks, have increasingly become inadequate and insecure as the digital world grows exponentially in size and complexity. This project endeavors to address these challenges and revolutionize data storage and management practices through an innovative application that combines the importance of the InterPlanetary File System (IPFS) and blockchain technology.

In recent years, decentralization has emerged as a key theme within the digital arena. The advent of blockchain technology, underpinning cryptocurrencies such as Bitcoin, has showcased the potential of decentralized systems in ensuring transparency, security, and independence from central authorities. Extending this concept to data storage, this project introduces a groundbreaking web application that leverages the principles of decentralization to provide robust and secure file storage.

The application utilizes IPFS as its underlying framework, which is a decentralized file system that aims to link all computing devices using a unified file system. Rather than relying on specific addresses like URLs, IPFS establishes connections between users and files through a network of nodes. This approach guarantees file redundancy and availability, even when network disruptions occur. The concept of decentralized storage is smoothly incorporated into the application, offering users a reliable and effective way to safeguard and manage their information.

To enhance the security and integrity of the system, blockchain technology is employed as an additional layer of security. By incorporating blockchain technology for verifying transactions, the application guarantees the authenticity of interactions within the system. This implementation of a blockchain layer establishes an unchangeable record of all transactions, effectively thwarting any unauthorized modifications to stored data and enhancing the overall security of the system.

Built using ReactJS, a popular and powerful JavaScript library known for its efficiency and flexibility, the application offers a user-friendly and intuitive interface. Its user-centric design makes it accessible to a variety of users, from individuals seeking secure personal storage to organizations requiring robust data management solutions.

Unlike existing systems that rely on third-party services for storage, this application stands on its own, hosted on a dedicated Digital Ocean droplet. This approach upholds the true spirit of decentralization, as it eliminates dependence on third-party services, further ensuring the privacy and control of user data.

Apart from secure file storage, the system also features controlled file sharing capabilities. Users can share files or even entire drives with their contacts and can seamlessly manage the access rights to their shared files. This feature, often overlooked in mainstream data storage services, enhances the collaborative potential of the application.

An additional special function is the 'file integrity checker' that employs IPFS hashes to authenticate the genuineness of files. This procedure guarantees that the files users retrieve remain unchanged from their original state at the time of upload, thereby enhancing trust and dependability in the system.

In essence, this project heralds a new era in file storage and data management. By integrating the principles of decentralization with the efficiency of modern web technologies, the application offers a secure, reliable, and user-friendly solution to the challenges of digital data storage and sharing. This introduction is just the tip of the iceberg. The following sections will explore in more detail the reasons behind the application's development, its goals, and distinctive characteristics, offering a thorough comprehension of this innovative undertaking.

[1]

II. Related Work

A. *Integrating Blockchain and the Interplanetary File System, a resilient platform for storing students' file*

Roychaudhary et al. [1] proposed a decentralized application model that combines blockchain and IPFS to enable secure file storage for students. The model utilizes a private blockchain for enhanced privacy and transparency, while IPFS addresses the issue of trust for large file storage. When a student uploads a file, it is stored on IPFS, and a transaction hash is generated. Access to the file is granted through the hash, which acts as a password. The model aims to provide a tamper-proof platform in response to increasing cyber-attacks and data breaches. By leveraging IPFS for decentralized storage and blockchain for immutability, the model offers secure, transparent, and scalable file storage, with potential applications across various industries in the future.

B. *Web 3.0 in Education & Research*

Lal et al. [3] examine the evolution of the World Wide Web, from Web 1.0 to Web 3.0. The development of online learning has progressed over the years, and with the emergence of Web 3.0, it has introduced enhanced features like intelligence, customization, compatibility, and virtual experiences. The authors discuss the potential of these technologies in creating immersive online classrooms, blurring the boundaries between physical and virtual realms. By integrating Web 3.0 technologies with best practices in online education, a reliable and efficient learning environment can be established.

C. *Blockchain-based, decentralized access control for IPFS*

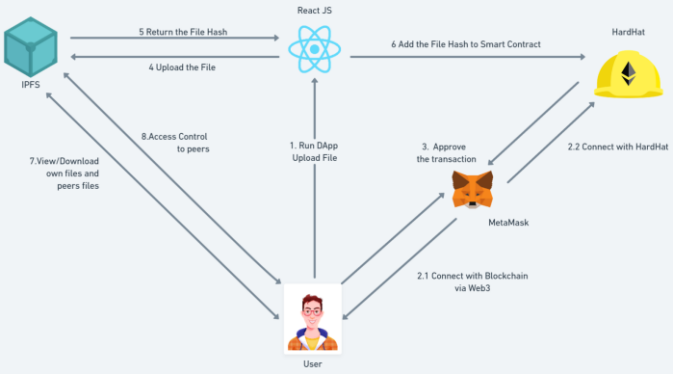
Steichen et.al [6] proposes the use of Ethereum smart contracts to offer access-controlled file sharing on a modified version of IPFS. Due to the expense of processing, transporting, and keeping the data, blockchains are not effective for storing huge files. IPFS, a file-sharing platform, utilizes cryptographic hashes for efficient storage and distribution of large files, without allowing direct file exchange between specific individuals. The maintenance of permissions is handled by a smart contract and enforced through regular updates to the IPFS software. Using an experimental configuration, the effects of this access-controlled IPFS are examined and addressed.

The author suggests acl-IPFS, a blockchain-based IPFS plugin that offers user access for sharing bigger files with sensitive data. Users may register files, grant or cancel access to them, and manage the list of permissions using Acl-IPFS, which manages it using Ethereum smart contracts. The access control list-stored permissions are enforced by the upgraded IPFS software, which also communicates with the blockchain network. The effectiveness of the system in comparison to unmodified IPFS is demonstrated through experiments and some use cases for acl-IPFS. It is demonstrated that the additional time brought on by interacting with the blockchain is negligible for operations.

The customizable permissions package allows integration with different blockchains or access control systems without modifying the IPFS code. It maintains a record of transactions and verifies their execution through content identifiers. It provides regular updates on the status of these identifiers. Additionally, to optimize memory usage, the package employs a concurrent go method that deletes outdated transaction data at specific intervals.

III. Materials And Methods

A. *System Architecture:*



This diagram depicts a user's experience with the blockchain-based file storage system. It starts with MetaMask user authentication and then uses a test blockchain network (Hardhat) for transactions. The user has the ability to upload, download, share, and revoke file access. Transactions involve the payment of a gas price in ETH. File hashes are securely distributed on a private IPFS gateway located on a DigitalOcean cluster.

The workflow is as follows:

- The user arrives at the webpage.
- Front-end authentication is implemented by MetaMask to verify user identity.
- For file transactions, the user connects with the test blockchain network (Hardhat).
- Transactions include uploading, downloading, sharing, and revoking access to files and folders.
- Each transaction is authenticated by paying a gas price in ETH.
- Files are hashed and uploaded to IPFS through the private gateway hosted on a DigitalOcean cluster.

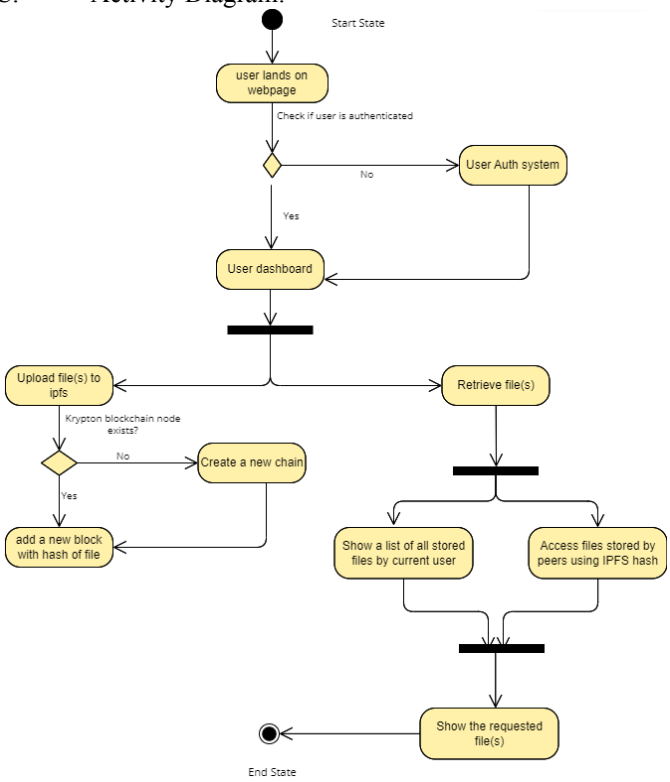
B. High Level Architecture:

When a user lands on the webpage, they have the ability to perform various actions such as retrieving files, adding files, and provide access control to their files. To guarantee the

security and integrity of transactions on the blockchain network, user approval via MetaMask authentication is required prior to any transaction execution. This measure guarantees that only individuals with proper authorization can start transactions, thereby strengthening the security protocols of the blockchain network.

Once a file is added, a private IPFS gateway in implemented, which is hosted on a DigitalOcean droplet. This configuration consists of five micro-servers that serve as IPFS swarm nodes. Each server keeps several pieces of information relating to the uploaded file(s), enabling for efficient file retrieval when necessary. They also pin and replicate the files. This distributed storage approach improves the system's file reliability and availability.

C. Activity Diagram:

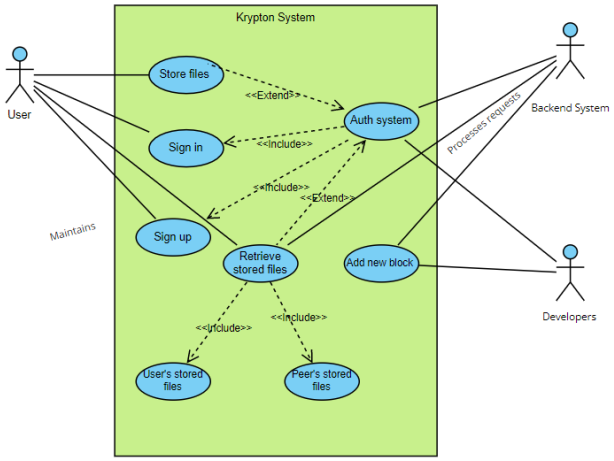


The activity diagram for the project illustrates the various activities and processes involved in the platform's operation. The diagram begins with the system's initiation, where users can authenticate themselves. Once authorised, users can utilise the platform to do tasks such as uploading files, downloading files, and access control to files.

The diagram also depicts the internal processes that occur as a result of these actions. When a person uploads a file, the system secures the information by converting it into a coded form and divides it into smaller parts. These parts are then dispersed across the IPFS network for storage in a decentralized manner. The method generates a unique hash for each piece while simultaneously storing the metadata on the blockchain for verification and immutability.

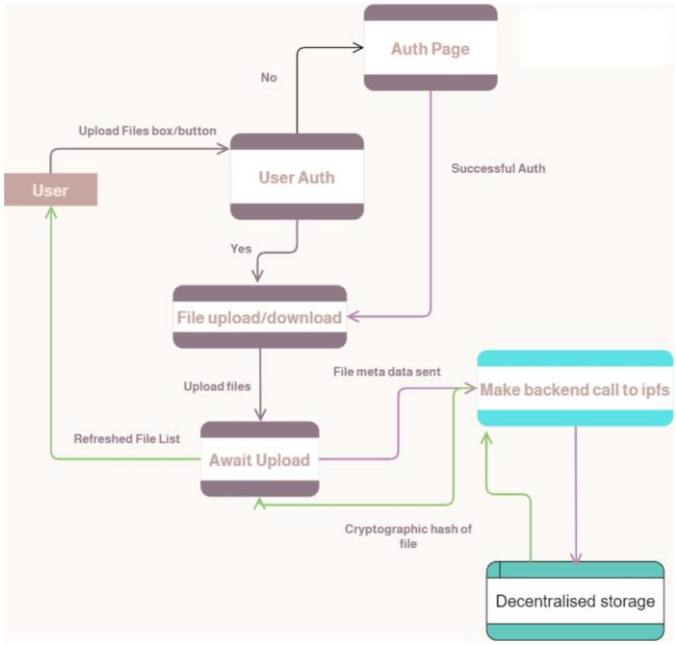
When a user wants to download a file, they start the process by supplying the relevant information, such as the file's hash. The system obtains the relevant metadata from the blockchain, locates the chunks across the IPFS network, and reassembles the file for download. This ensures that data is retrieved from the decentralised storage system in a secure and efficient manner. Users have the capability to securely exchange files with authorized individuals, ensuring restricted and protected data sharing within the system.

D. Use Case Diagram:



A use case diagram depicts the interactions between actors and the system visually. The major actors in this context are users and peers, and the system includes features such as sign-in, sign-up, storing files, authentication system, retrieving data, and accessing user and peer files. The user authentication and registration processes are involved in the sign-in and sign-up use cases. The storage feature allows users to upload their data to the platform, where it is securely stored using the IPFS protocol. The authentication system ensures that only users with proper authorization can access their files. Users can fetch and download their stored files.

E. Dataflow Diagram:



In the file upload and retrieval process, user data is authenticated using MetaMask. Upon successful authentication, the system generates a Content ID (CID) using IPFS algorithms. The information about the file is transferred to a specialized contract for safekeeping, while the actual file is placed on IPFS nodes hosted by DigitalOcean droplets. The system returns a cryptographic hash value to the user on the frontend for future reference. To retrieve files, the user requests a file using its hash, triggering a backend call to fetch the metadata for display or download. This process ensures secure file storage and retrieval, utilizing IPFS and blockchain technology.

IV. Results and Discussion

A. Web Application Development:

The frontend interface is a web application, developed leveraging the efficient and flexible JavaScript library, ReactJS. The design is user-centric, facilitating effortless file uploading, storing, and retrieval. In addition, the platform includes a functionality that enables individuals to securely exchange files with their blockchain connections while maintaining full control over the permissions and access privileges.

B. Private IPFS Gateway Setup:

The implementation of the infrastructure is kickstarted by setting up Digital Ocean droplets, serving as the self-hosted IPFS gateway for the system. Digital Ocean, a renowned cloud infrastructure provider, offers flexible and scalable droplets that can be customized according to the project's requirements. The droplet allocated for this project is specifically configured with the essential hardware and software specifications to ensure seamless operation of the IPFS gateway. This optimized configuration facilitates the efficient functioning of the gateway and supports its intended functionalities. This self-hosted gateway forms the heart of the decentralized file storage system, responsible for the efficient storing and retrieval of files.

C. IPFS Functionality:

Rather than storing the entire file on the blockchain, the files are passed through the IPFS protocol which splits the data into multiple chunks which are stored across multiple IPFS nodes. Every file has a distinct Content ID (CID) that is utilized to access the file distributed via the IPFS protocol.

IPFS CIDs (or IPFS hash) are stored on the blockchain, enabling transparent and auditable tracking of file integrity and access history. This method ensures that only authorized users with verified credentials on the blockchain can access specific files.

File Upload: The system's main function is to enable users to upload files to IPFS. Users utilize the web interface to select a file for uploading. The file is then sent to the IPFS gateway, which generates a unique IPFS hash for the file. This hash serves as an address pointing to the file data and is stored on the Ethereum blockchain, creating a link for future file retrieval.

File Retrieval: Users input the unique IPFS hash of a file through the web interface to retrieve it. The system forwards the hash to the IPFS gateway, which locates the file data and sends it back to the user. This process ensures quick and secure file access.

File Sharing: The system also offers a feature for sharing files. Users can share files with other system users by providing the recipient's blockchain contact information (metamask ID). The Ethereum blockchain is then updated with a smart contract that grants the specified user access to the file.

Access Revocation: If a user wants to revoke another user's access to a shared file, they can do so using the web interface. The system generates a new smart contract on the Ethereum blockchain, effectively denying the specified user access to the file. This demonstrates a significant advantage of integrating blockchain technology, as it allows for dynamic and secure control over file access.

D. Blockchain and Metamask:

The Ethereum blockchain and Metamask integration within the system facilitates secure and transparent transaction authentication. Metamask, a browser-based Ethereum wallet, allows users to interact directly with the Ethereum blockchain. Solidity programming language is used to write the code for blockchain which provides the functionality of authenticating the user via MetaMask, adding the hashes to the blockchain, displaying the IPFS hashes, adding and removing contacts.

Users can share files, revoke access, and perform other transactions using their Metamask ID. These transactions are recorded on the Ethereum blockchain through smart contracts, providing a secure, transparent, and immutable record of all activities within the system. This effectively enhances the security and reliability of the system, contributing to a

trustworthy decentralized file storage solution.

By combining private IPFS clusters, blockchain authentication, and secure file access controls, our proposed system provides a robust and decentralized storage solution. It allows users to maintain ownership and control over their data while leveraging the benefits of IPFS and blockchain technologies.

V. CONCLUSION

The application developed in this project represents a substantial leap forward in the realm of secure and private data storage, leveraging cutting-edge technologies, such as the InterPlanetary File System (IPFS) and blockchain. This project has successfully provided an efficient, decentralized solution to the data storage problem, offering an unprecedented level of privacy, security, and control over user data.

One of the standout features of the application is its unique ability to manage access permissions. This particular functionality addresses a notable drawback found in popular data storage services, where users often have limited control over who can access their shared files. With the controlled access mechanism in place, users have the power to grant or revoke file access, ensuring their data remains private and under their control.

Additionally, a remarkable accomplishment of this project is the creation and implementation of the 'file integrity checker', which significantly enhances data security. This tool utilizes IPFS hashes to verify the authenticity and integrity of stored files, making it exceedingly challenging for unauthorized individuals to manipulate user data.

Moreover, the application hosts its IPFS gateway on a dedicated Digital Ocean droplet. This self-contained approach reduces dependencies on third-party providers and enhances the decentralization aspect of the application. Users can be confident that their data is not held hostage by any centralized entity.

The use of ReactJS for building this application not only ensures a dynamic and responsive user interface but also provides a stable and robust architecture for the overall system. By incorporating ReactJS, a popular JavaScript library known for its efficiency and flexibility, the application has ensured a scalable and maintainable codebase, setting a strong foundation for future enhancements.

The inclusion of blockchain technology in verifying transactions has marked a substantial advancement in enhancing the system's security during interactions. Each transaction is recorded on the blockchain, making it immutable and transparent, thereby increasing the trustworthiness of the application.

In summary, this endeavor signifies a significant step forward in the direction of a future where individuals possess greater authority and possession over their data. It's not just a file storage system; it's a significant advancement in the field of data storage and retrieval, offering users an innovative, secure, and private alternative to traditional, centralized storage systems. The innovative use of the InterPlanetary File System (IPFS), blockchain technology, and the unique features of controlled access and file integrity checker, sets this application apart and showcases the transformative potential of decentralized technologies.

REFERENCES

[1] Roychowdhury, Reema, et al. "Integrating Blockchain and the Interplanetary File System, a resilient platform for storing students' file."

[2] Zhu, Yan, et al. "Blockchain-based decentralized storage scheme." Journal of Physics: Conference Series. Vol. 1237. No. 4. IOP Publishing, 2019.

[3] Lal, Manohar. "Web 3.0 in Education & Research." BVICAM's International Journal of Information Technology 3.2 (2011).

[4] Xu, Haimei, et al. "Content sharing network based on ipfs and blockchain." IOP Conference Series: Materials Science and Engineering. Vol. 1043. No. 5. IOP Publishing, 2021.

[5] Nizamuddin, Nishara, Haya R. Hasan, and Khaled Salah. "IPFS-blockchain-based authenticity of online publications." International conference on blockchain. Springer, Cham, 2018.

[6] Steichen, Mathis, et al. "Blockchain-based, decentralized access control for IPFS." 2018 Ieee international conference on internet of things (iThings) and ieee green computing and communications (GreenCom) and ieee cyber, physical and social computing (CPSCom) and ieee smart data (SmartData). IEEE, 2018.

[7] Zheng, Qiuhong, et al. "An innovative IPFS-based storage model for blockchain." 2018 IEEE/WIC/ACM international conference on web intelligence (WI). IEEE, 2018.

[8] Alizadeh, Morteza, Karl Andersson, and Olov Schelén. "Efficient decentralized data storage based on public blockchain and IPFS." 2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE). IEEE, 2020.

[9] Trautwein, Dennis, et al. "Design and evaluation of IPFS: a storage layer for the decentralized web." Proceedings of the ACM SIGCOMM 2022 Conference. 2022.

[10] Baumgart, Ingmar, and Sebastian Mies. "S/kademlia: A practicable approach towards secure key-based routing." 2007 International conference on parallel and distributed systems. IEEE, 2007.

[11] Ciriello, Raffaele, Roman Beck, and Jason Thatcher. "The paradoxical effects of blockchain technology on social networking practices." Available at SSRN 3920002 (2018).

[12] Arquam, Md, Anurag Singh, and Rajesh Sharma. "A blockchain-based secured and trusted framework for information propagation on online social networks." Social Network Analysis and Mining 11.1 (2021): 1-16.

[13] Jiang, Le, and Xinglin Zhang. "BCOSN: A blockchain-based decentralized online social network." IEEE Transactions on Computational Social Systems 6.6 (2019): 1454-1466.

[14] Hisseine, Mahamat Ali, Deji Chen, and Xiao Yang. "The application of blockchain in social media: a systematic literature review." Applied Sciences 12.13 (2022): 6567.

[15] Murimi, Renita M. "A blockchain enhanced framework for social networking." Ledger (2019).