IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 4, April 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204153 |

Decentralized File Storing and Sharing DAPP Using Blockchain

Dasi Raja, Kompella Sai Sriram Kashyap, Donga Sandeep Reddy, Mrs. S. Tejaswi

Student, Department of CSE, Anurag University, Hyderabad, India

Student, Department of CSE, Anurag University, Hyderabad, India

Student, Department of CSE, Anurag University, Hyderabad, India

Assistant Professor, Department of CSE, Anurag University, Hyderabad, India

ABSTRACT: The "Decentralized Worldwide Cloud: A Blockchain-Powered Disk Space Renting System" project introduces a groundbreaking paradigm for global cloud storage. At its core, the system aims to tap into the unused disk space of individuals globally, creating a decentralized peer-to-peer network attached to a blockchain registry. Unlike traditional centralized cloud models, this innovative approach empowers users worldwide to rent out their idle disk space, with future prospects for extending the concept to include computing power and memory. The integration of blockchain data structures enhances network security by reducing the risk of a single point of failure and fortifying defenses against unauthorized access through the use of individual cryptographic keys.

KEYWORDS: Solidity, VSCode , Ethereum, Metamask, File Storage, File Sharing

I. INTRODUCTION

An unparalleled era of data generation and storage has been brought about by the digital age. Cloud storage solutions have become a viable and scalable approach to handle this constantly expanding amount of data. This dependence on centralized storage providers, however, brings up serious issues with censorship and data privacy. Users give their data to organizations that can be open to security lapses or that have the power to impose access restrictions due to internal regulations. This project seeks to transform conventional cloud storage paradigms by putting forth a fresh way to file sharing. The project uses blockchain technology to build a decentralized file storage solution, in contrast to well-known centralized solutions like Google Drive. This results in a number of significant benefits:

Decentralization: Information isn't kept on a single, corporately-controlled server. Rather, it is dispersed and encrypted over a computer network, increasing its resistance to data breaches and censorship.

Security: Strong security characteristics are provided by blockchain technology. To guarantee that only authorized individuals may access your data, files are encrypted and access permissions are managed via smart contracts.

Privacy: User privacy is the project's main concern. No central body has access to your data without your consent, so you maintain control over your files.

The project describes creating an approachable application using the Ethereum blockchain's smart contracts implemented in Solidity and React on the front end. It also looks at using the decentralized storage network IPFS to distribute files.

II. LITERATURE SURVEY

S. Nakamoto, "bitcoin: A peer-to-peer electronic cash system," 2008.

A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof- of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204153 |

pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone. We have proposed a system for electronic transactions without relying on trust. We started with the usual framework of coins made from digital signatures, which provides strong control of ownership, but is incomplete without a way to prevent double-spending. To solve this, we proposed a peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power. The network is robust in its unstructured simplicity. Nodes work all at once with little coordination. They do not need to be identified, since messages are not routed to any particular place and only need to be delivered on a best effort basis. Nodes can leave and rejoin the network at will, accepting the proof-of-work chain as proof of what happened while they were gone. They vote with their CPU power, expressing their acceptance of valid blocks by working on extending them and rejecting invalid blocks by refusing to work on them. Any needed rules and incentives can be enforced with this consensus mechanism.

Naz M, Al-zahrani FA, Khalid R, Javaid N, Qamar AM, Afzal MK, Shafiq M. A secure data sharing platform using blockchain and interplanetary file system. Sustainability. 2019 Dec 10;11(24):7054.

In a research community, data sharing is an essential step to gain maximum knowledge

from the prior work. Existing data sharing platforms depend on trusted third party (TTP). Due to the involvement of TTP, such systems lack trust, transparency, security, and immutability. To overcome these issues, this paper proposed a blockchain-based secure data sharing platform by leveraging the benefits of interplanetary file system (IPFS). A meta data is uploaded to IPFS server by owner and then divided into n secret shares. The proposed scheme achieves security and access control by executing the access roles written in smart contract by owner. Users are first authenticated through RSA signatures and then submit the requested amount as a price of digital content. After the successful delivery of data, the user is encouraged to register the reviews about data. These reviews are validated through Watson analyzer to filter out the fake reviews. The customers registering valid reviews are given incentives. In this way, maximum reviews are submitted against every file. In this scenario, decentralized storage, Ethereum blockchain, encryption,and incentive mechanism are combined. To implement the proposed scenario, smartcontracts are written in solidity and deployed on local Ethereum test network. The proposed scheme achieves transparency, security, access control, authenticity of owner, and quality of data. In simulation results, an analysis is performed on gas consumption and actual cost required in terms of USD, so that a good price estimate can be done while deploying the implemented scenario in real set-up. Moreover, computational time for different encryption schemes are plotted to represent the performance of implemented scheme, which is shamir secret sharing (SSS). Results show that SSS shows the least computational time as compared to advanced encryption standard (AES) 128 and 256.

Liu J, Li X, Ye L, Zhang H, Du X, Guizani M. BPDS: A blockchain based privacy-preserving data sharing for electronic medical records. In2018 IEEE Global Communications Conference (GLOBECOM) 2018 Dec 9 (pp. 1-6). IEEE.

Electronic medical record (EMR) is a crucial form of healthcare data, currently drawing a lot of attention. Sharing health data is considered to be a critical approach to improve the quality of healthcare service and reduce medical costs. However, EMRs are fragmented across decentralized hospitals, which hinders data sharing and puts patients' privacy at risks. To address these issues, we propose a blockchain based privacy-preserving data sharing for EMRs, called BPDS. In BPDS, the original EMRs are stored securely in the cloud and the indexes are reserved in a

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204153 |

tamper-proof consortium blockchain. By this means, the risk of the medical data leakage could be greatly reduced, and at the same time, the indexes in blockchain ensure that the EMRs can not be modified arbitrarily. Secure data sharing can be accomplished automatically according to the predefined access permissions of patients through the smart contracts of blockchain. Besides, the joint-design of the CP-ABE-based access control mechanism and the content extraction signature scheme provides strong privacy preservation in data sharing. Security analysis shows that BPDS is a secure and effective way to realize data sharing for EMRs.

III. METHODOLOGY AND APPROACH

This project provides a disruptive decentralized file storage and sharing application (dApp) in response to the growing concerns over the vulnerabilities of centralized storage solutions. Through the utilization of the Ethereum blockchain and the Inter Planetary File System (IPFS), the dApp ushers in a new era of data management marked by improved security, resistance to censorship, and user empowerment. By spreading file fragments throughout a network of interconnected nodes, the decentralized structure of this dApp ensures data availability and integrity, in contrast to typical centralized platforms where data is vulnerable to single points of failure and potential breaches. Additionally, using blockchain technology makes it easier to maintain tamper-proof records, ensuring accountability and transparency in file transactions. Fundamentally based on user governance, the dApp gives people the ability to maintain control over their data, allaying worries about arbitrary censorship and privacy violations. The project aims to rethink file storage and sharing paradigms by utilizing this novel approach, providing a reliable and user-friendly substitute for conventional centralized solutions.

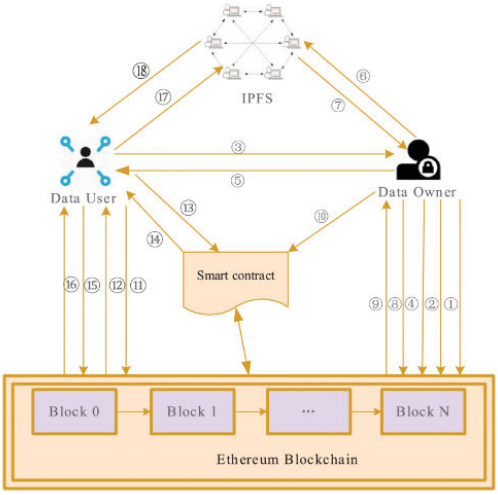

Figure 1. System Framework

Modules

Smart Contracts:

Self-executing contracts, or smart contracts, are implemented on the Ethereum blockchain and are designed to carry out predetermined actions automatically in response to specific events. Smart contracts are essential for handling user interactions, file storage, access control, and data integrity in the context of the decentralized file storage and sharing dApp.

User Registration: By safely storing user data on the blockchain, including public keys and user IDs, smart contracts handle user registration. Users can safely access the dApp's features and authenticate themselves because of smart contracts.

File Upload and Storage: Smart contracts manage the blockchain's storage of file metadata, like as hashes, timestamps, and access permissions, when users submit files to the dApp. This guarantees that critical data about submitted files is tamper-proof and safely stored.

Access Control: Smart contracts manage who can view and download shared files by enforcing user-defined access control policies. This stops illegal access and data breaches by giving users fine-grained control over the security and privacy of their files.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204153 |

File Retrieval and Sharing: By giving users safe access to IPFS links and stored file information, smart contracts make it easier to retrieve and share files. This preserves data security and confidentiality while enabling users to exchange and retrieve files with ease.

User Registration:

Users register to create accounts on the decentralized file storage and sharing network, which is the first step in the process. Users give the system the information it needs to identify them, including passwords, email addresses, and usernames, upon registration.

To improve the security of user accounts, more security methods like biometric or two-factor authentication may be used.

File Upload

The file upload process can be started by users once they have registered and logged in. They choose one or more files from their local devices to upload to the platform using an easy-to-use interface. Users can be informed about the status of their uploads using progress indicators, which guarantee a seamless and open experience.

Hashing Files

The system uses strong hashing algorithms like SHA-256 to automatically create a unique cryptographic hash for every file when it is submitted. By digitally identifying every file and guaranteeing data integrity throughout storage and exchange, these file hashes act as digital fingerprints. The uploaded files are protected from tampering attempts and illegal modifications by the system's ability to detect hashes of the file content.

IPFS Storage

The technology uploads the real file content to the Inter Planetary File technology (IPFS) network in tandem with smart contract exchanges. Across dispersed network nodes, IPFS provides effective and fault-tolerant file storage through the use of a decentralized, content-addressed storage paradigm. A unique content identifier (CID) is assigned to every uploaded file, acting as its IPFS network address and enabling sharing and retrieval.

File Sharing

Lastly, by providing access permissions through the implemented smart contracts, users can exchange files with other people. Smart contracts provide access control policies that specify who can download and access shared files, guaranteeing safe and private file sharing. Users can enable public, private, or permissioned sharing according to their needs and preferences, with fine-grained control over access rights.

IV. RESULTS AND DECLARATION

Here you can see the website after redirecting to the web browser

Figure 2. User Interface

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204153 |

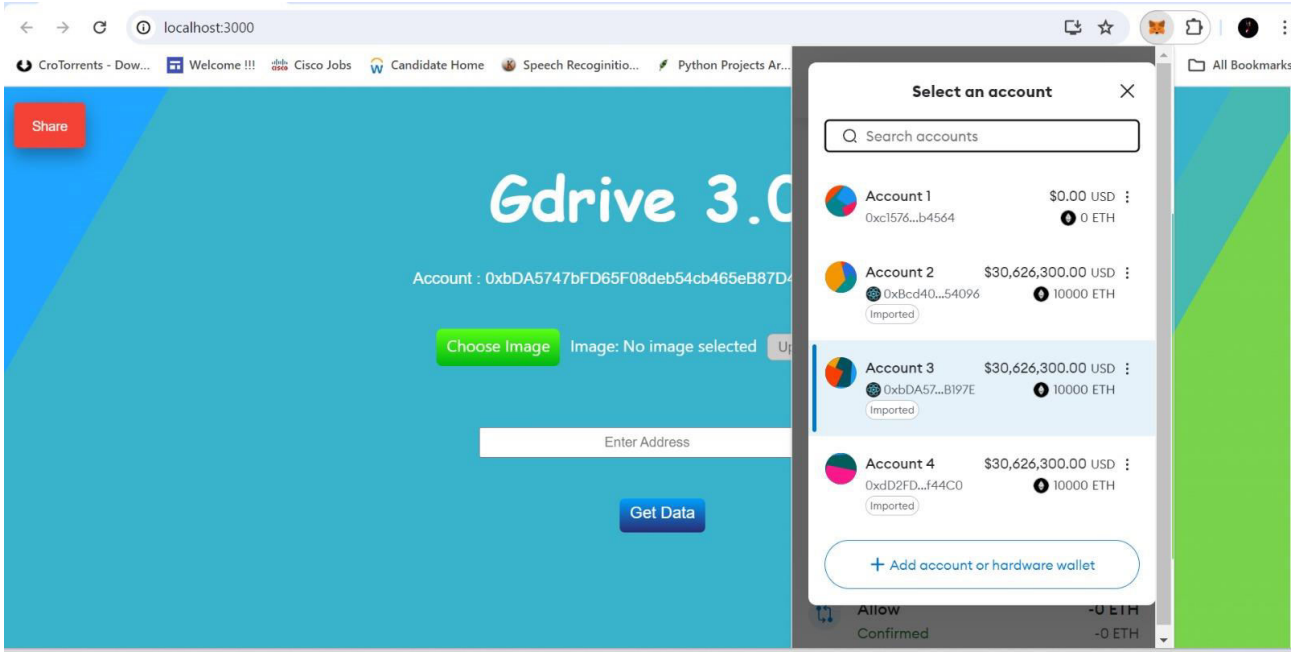

Figure 3. Accessing Metamask Accounts

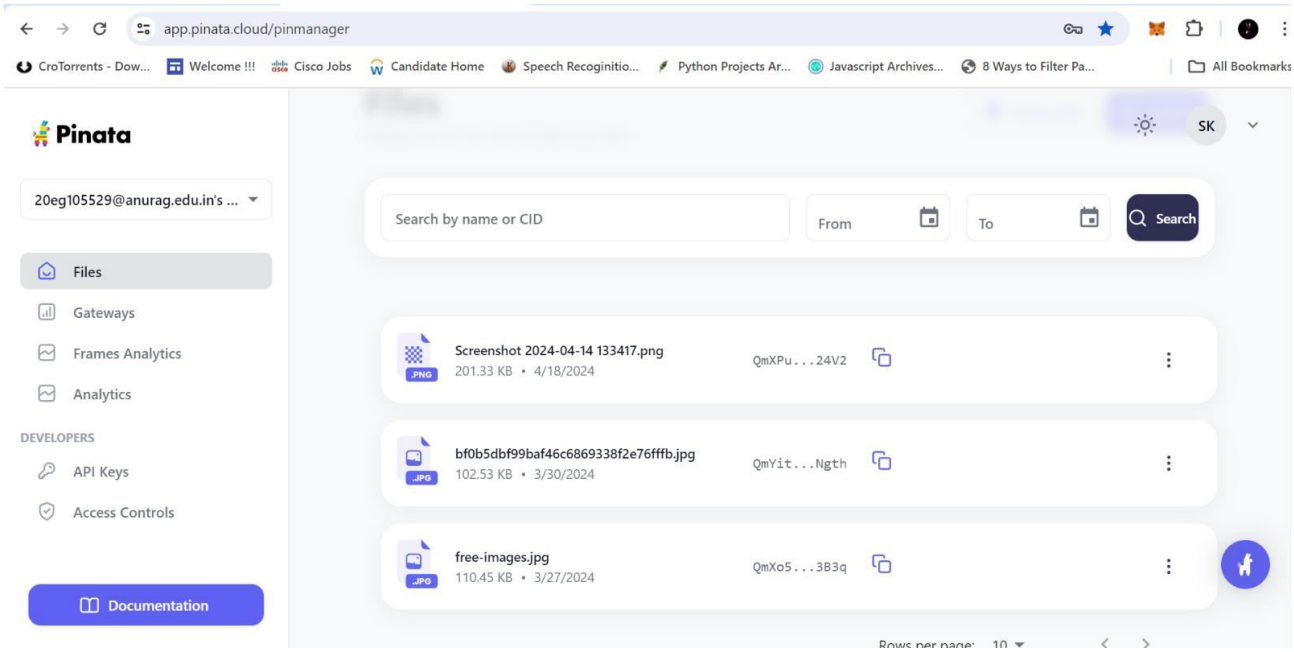

Figure 4. Pinata Storage

V. CONCLUSION

This study looked at how blockchain technology might be used to develop a safe and user-friendly file-sharing program. The suggested method overcomes the drawbacks of conventional cloud storage options by utilizing the fundamental blockchain features of decentralization, immutability, and transparency.

A user-friendly application, safe smart contracts, and IPFS's distributed storage network were all outlined in the study paper's description of the system architecture. We demonstrated in-depth features including data integrity checking optionally, smart contract-based access control management, and file upload with cryptographic hashing. We also talked about how to improve user experience and make advantage of the current bitcoin infrastructure by

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204153 |

integrating MetaMask, a well-known cryptocurrency wallet. blockchain technology's ability to develop a safe and user-friendly file-sharing program. To overcome the drawbacks of conventional cloud storage solutions, the suggested approach makes use of the fundamental decentralization, immutability, and transparency provided by blockchain technology.

REFERENCES

[1] S. Nakamoto, “bitcoin: A peer-to-peer electronic cash system,” 2008.
[2] ”Hyperledger Fabric Documentation, Release main”, ttps://readthedocs.org/projects/hlf/downloads/pdf/latest/, accessed on Dec 2022
[3] Naz M, Al-zahrani FA, Khalid R, Javaid N, Qamar AM, Afzal MK, Shafiq M. A secure data sharing platform using blockchain and interplanetary file system. Sustainability. 2019 Dec 10;11(24):7054.
[4] Liu J, Li X, Ye L, Zhang H, Du X, Guizani M. BPDS: A blockchain based privacy-preserving data sharing for electronic medical records. In2018 IEEE Global Communications Conference (GLOBECOM) 2018 Dec 9 (pp. 1-6). IEEE.
[5] YSari L, Sipos M. FileTribe: blockchain-based secure file-sharing on IPFS. InEuropean Wireless 2019; 25th European Wireless Conference 2019 May 2 (pp.1-6). VDE.
[6] Benet J. Ipfs-content addressed, versioned, p2p file system. arXiv preprintarXiv:1407.3561. 2014 Jul 14.
[7] ”Hyperledger Caliper Documentation, Getting Started”, ”https://hyperledger.github.io/caliper/v0.5.0/getting-started/”, accessed onDec 2022
[8] ”Apache Couch Database Documentation: Release 3.3.0”, ”https://docs.couchdb.org/ /downloads/en/latest/pdf/”, accessed on Dec2022
[9] Buterin, Vitalik. ”A next-generation smart contract and decentralizedapplication platform.” white paper 3, no. 37 (2014): 2-1.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details