Blockchain Based Decentralized Data Storage Solution

TINURANJEN T
Department of Electronics and Communication Engineering
National Engineering College,
Kovilpatti,India

ABDUL AZIZ A
Department of Electronics and Communication Engineering
National Engineering College,
Kovilpatti,India

HARISANKAR M
Department of Electronics and Communication Engineering
National Engineering College,
Kovilpatti,India

ARIVIGNESH G
Department of Electronics and Communication Engineering
National Engineering College,
Kovilpatti,India

PRASANNA VENKATESAN K J
Asso. Prof
Department of Electronics and Communication Engineering
National Engineering College,
Kovilpatti,India

***Abstract*— Blockchain-based decentralized data storage solution (BDDSS) uses the new capabilities of blockchain technology to create a secure, transparent, and efficient system. BDDSS addresses the limitations of centralized data storage systems by distributing data across a network of nodes, ensuring data integrity and better access. The immutability of blockchain data makes the data im- mutable and prevents illegal interception, instilling trust in the storage ecosystem. Through smart contracts, BDDSS automates data management, complements data connectivity and management, while protecting data privacy and security. The design process includes integrated integration and smart contract algorithms to support robust and flexible data. BDDSS aims to transform the data storage system, liberate data, eliminate failures, and give users full ownership and control over their data. BDDSS represents an advancement in data storage. Traditional centralized data storage systems have long suffered from security vulnerabilities, data loss, and restricted access. However, BDDSS leverages the transformative power of blockchain technology to create a secure, transparent, and efficient storage ecosystem that promises to revolutionize the way we store and manage information. One of the main advantages of BDDSS is the use of blockchain technology to ensure that information cannot be changed and its immutability. Once data is stored in the system, it is tamper-proof and protected against unauthorized changes.**

***Keywords* -blockchain Technology, Decentralized Datastorage, Smart contract Automation, Data privacy.**

I. INTRODUCTION

Today, the world has become dependent on information, and this dependence is increasing at an unprecedented pace. From personal memories to important financial information to important business information, information stored in the cloud has become the lifeblood of our digital lives. But traditional centralized data storage has long been full of gaps and limitations. BDDSS emerged in response to these short- comings and has enabled a revolution in the way we store, manage, and protect data. Centralized data storage, as the name suggests, relies on a central organization or organization to store large amounts of data. Although this model has worked well for the last three years, it has weaknesses. One of the most obvious problems is that one cannot fail. In the central system, if the central organization collapses, the data will not be accessible. Additionally, centralized locations often become attractive targets for criminals, leading to frequent data breaches. These vulnerabilities are especially common at a time when data breaches can cause serious harm to individuals and organizations. BDDS solves this problem by using a decentralized data storage method. In this model, data is not stored in a non-persistent environment. Instead, it is distributed throughout the network of nodes, each contributing to the overall impact of the system. This means that even if one of the nodes fails or is compromised, most data is still accessible. The redundancy inherent in this decentralized architecture ensures uninterrupted availability even in the face of network outages or cyber-attacks. This change is a game changer and provides peace of mind to users who regularly rely on their data.

II. PROBLEM IDENTIFICATION

Cloud-based storage creates data privacy and security issues due to the involvement of central organizations or third parties. The proposed system highlights the need for blockchain-based decentralized storage to ensure data privacy and security.

III. BLOCKCHAIN TECHNOLOGY

A. Blockchain Technology

There are three types of blockchains in decentralized systems: public blockchains, private blockchains, and consortium chains. The concept of cryptocurrency is related to the solution of public blockchains. Blockchain is a

collection of blocks where each block contains a transaction and contains the hash of the previous block. Decentralized technology ensures immutability of data as changing data in one block will affect all subsequent blocks and help manage data storage, digital notarization, and smart contracts. Technology began to be used in the digital money and securities market. Ethereum is another distributed, open-source, public platform based on blockchain technology. The structure of Ethereum is almost the same as other blockchain net- works. It has features called smart contracts that facilitate online contracts.

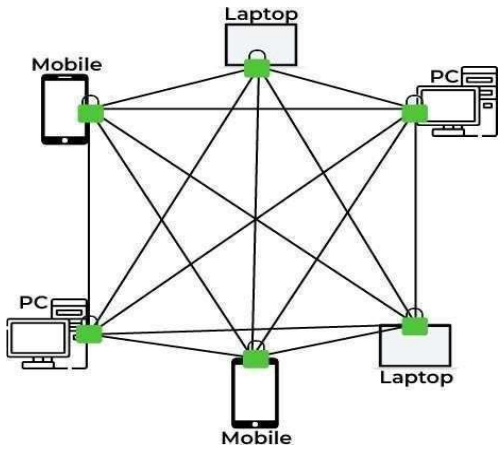

Fig. 1. Blockchain Structure

B. Smart contract:

A smart contract is a small set of rules executed on the blockchain platform without the involvement of third parties. The platform includes a virtual machine (Ethereum Virtual Machine (EVM)) that can process scripts using the Ethereum computer network. Ethereum has a cryptocurrency called “Ether” that can be exchanged between currencies and used to pay miners. Fat feet help in calculation.

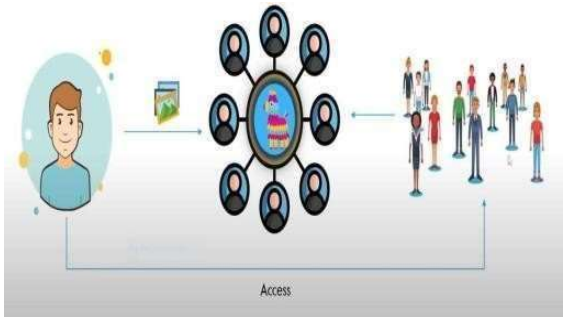

Fig. 2. Smart Contract

C. IPFS

IPFS (Interplanetary File System) is a system for sharing and storing files on a peer- to-peer decentralized network. It uses DHT to track data files. Hash tables are used to store data packets. Kademlia is used to understand the information in nodes. Kad- emlia is a hash table for computer collaboration created in 2002 by Petar Maymoun- kov and David Mazi'eres. When we upload the file, the hash value is created. IPFS stores hashes and users can use these hashes to store data. When data is transferred to the IPFS network, the data is split into multiple pieces. This file is identified by the hash value.

IV. METHODOLOGY AND ARCHITECTURE

The design allows users to send data or information to apeer-to-peer network. To do this, users need to configure the blockchain network (Hardhat is used for traditional blockchain networks) and embed it in the web browser using the MetaMask extension.

Users need a blockchain network provided by Hardhat. The money provided by Hardhat was added to MetaMask for the marketplace. Some gas must be present in the form of ether. Ethereum is a cryptographic token that powers blockchain networks. Users then need to create an account on MetaMask and link it to their wallet. Now that our web browser supports blockchain networks, we can now send data through our own user interface. When the user selects a file to upload the file will go to IPFS and IPFS will return a hash based on the smart contract. After that, users must pay the fuel fee from their MetaMask account. Once the payment is completed, the smart contract allows data to be sent to the peer-to-peer network.

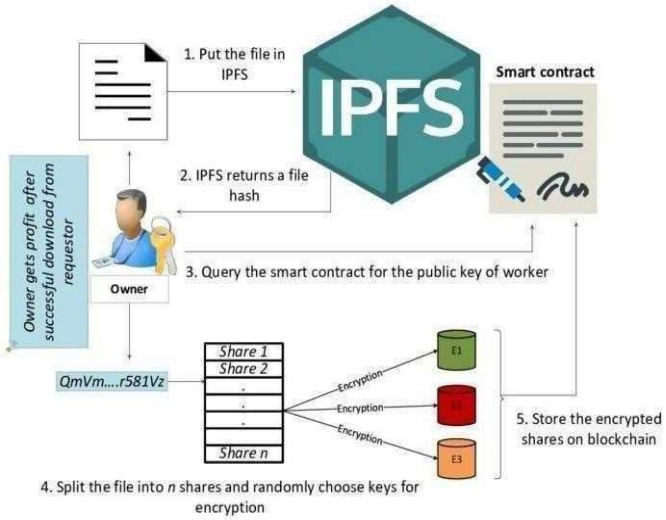

Fig.3.Data sharing in IPFS Network

The process of retrieving data from IPFS must have already retrieved the IPFS hash generated after the archive was loaded. IPFS hash needs to placed in the web browser and IPFS will first access the file and display it. Therefore, data storage is provided by the IPFS system.

V. RESULT AND ANALYSIS

This article describes the development of a web-based application that provides a user interface through which users can directly upload or share their data and information. The solution works in many areas.

First, users must create an account on MetaMask and log in using their credentials.

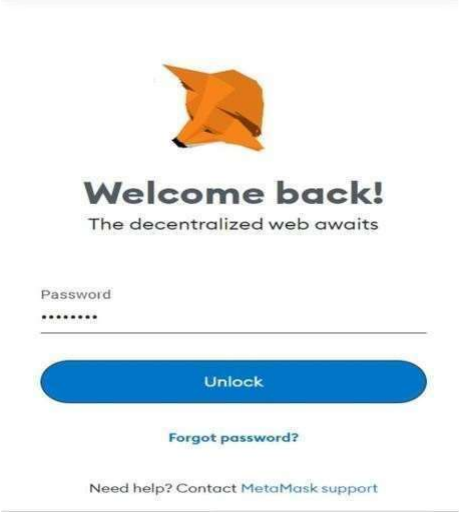

Fig. 4. Meta Mask Login

The user needs to create a security mask and then link the MetaMask code to their wallet.

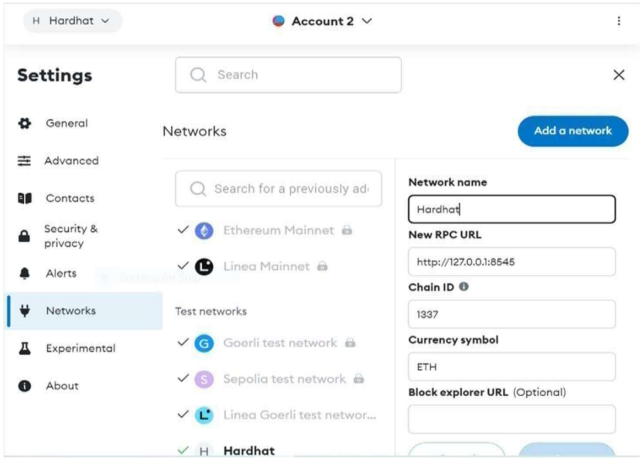

Fig. 5. Account in Hardhat

After that the user needs to open the decentralized drive and select the archive to load.

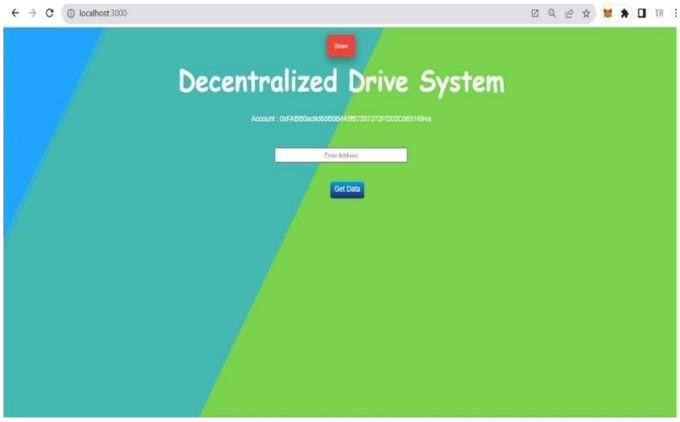

Fig. 6. Decentralized Drive System

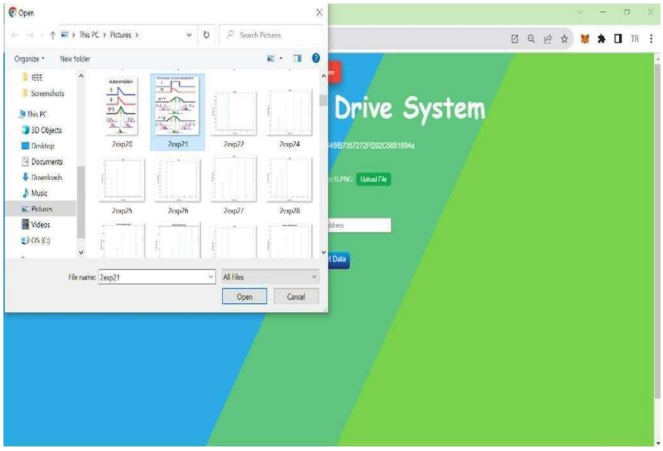

Fig. 7. Uploading Images on Decentralized Drive

Payment box opens to confirm payment.

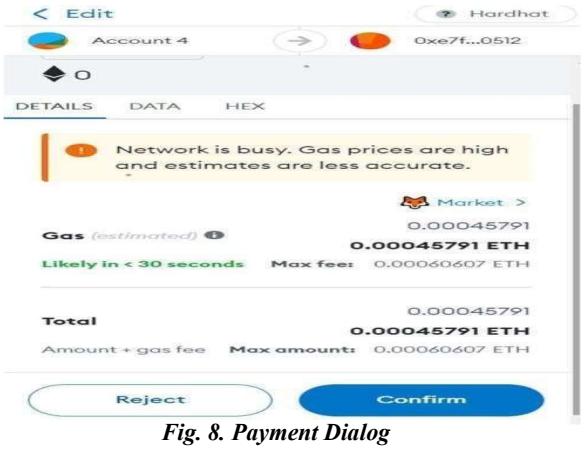

Fig. 8. Payment Dialog

Once payment is completed, the user's data is stored on a peer-to-peer net- work using the IPFS protocol.

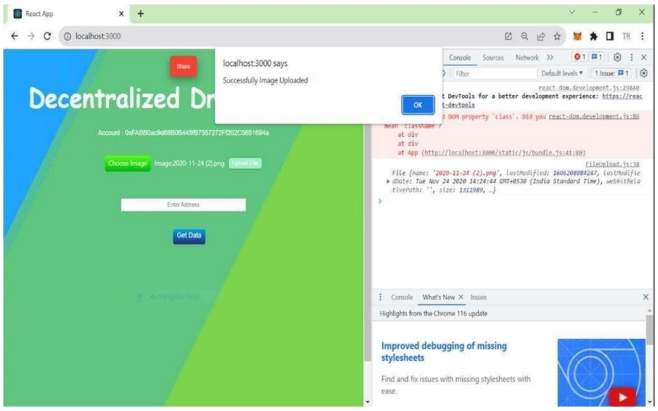

Fig. 9. Image Successfully Uploaded

Additionally, if users want to view the files they have uploaded, they can simply click the "Get data" button.

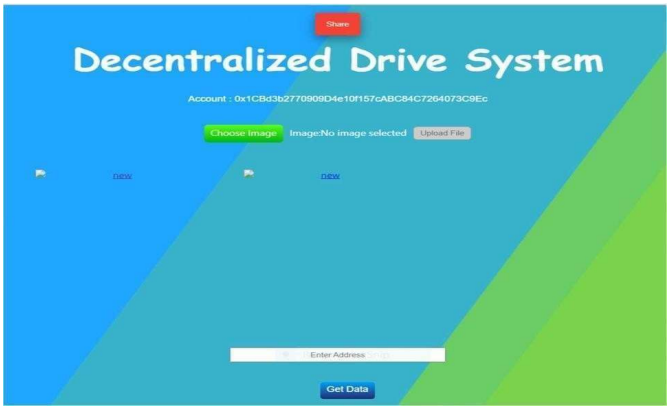

Fig. 10. Images Displayed on the screen.

Additionally, if the user wants to allow access to other users, he or she can do so by clicking the share button and providing the user's address.

Fig. 11. Share Access to the Accounts in IPFS Network

Additionally, if users want to see who has access, they can do so by clicking “People with Access”.

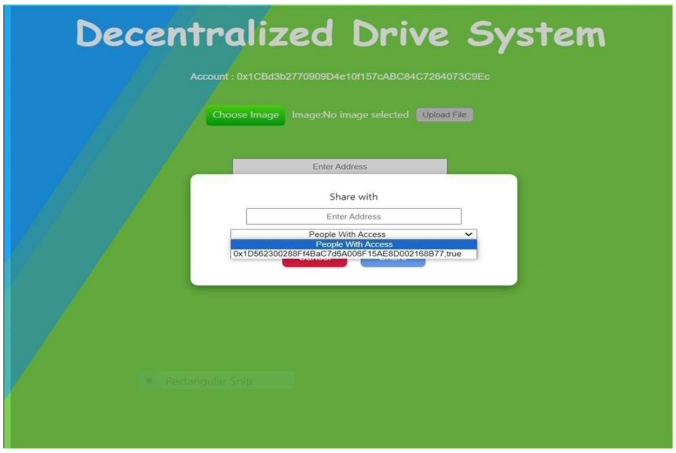

Fig.12.Account with Share Access

VI. CONCLUSION AND FUTURE SCOPE

This article introduces a new evolution based on IPFS, called decentralized disk drive. The proposed system ensures data security by distributing our data in a distributed manner over a peer-to-peer network. The system uses the IPFS protocol to ensure the confidentiality of user data. In addition to these advantages, accuracy and speed also need to be improved. IPFS protocol is used in the planning process, but if a better system becomes available in the future, it can also be used.

References

[1] D. Kraft, “Blockchain-Based Consensus Systems for Complex Governance,” Peer-to-Peer Networks and Applications, vol. 9. No. 2 H. 397-413, March 2016.

[2] D. Dias, J. B. Silva, and L. Veiga, “Storj: Peer-to-peer cloud storage network,” hauv 2014 IEEE 33rd International Symposium on Dependable Distributed Systems, p. 522-523, October 2014.

[3] P. Zhong et al., “Blockchain-based decentralized storage and security framework for IoT data,” IEEE Internet of Things Magazine, vol. 5. No. 4, p. 2651-2662, 2018.

[4] L. Ren et al., “MIDAS: A multilayer incentive mechanism for blockchain-based decentralized storage,” Phau ntawv Journal of Parallel and Distributed Computing, vol. 139, p. 63-73, 2020.

[5] V. L. Lemieux, “Blockchain thiab decentralized ledgers as trusted recordkeeping systems: A framework for evaluating archival theory.” Future Technology Conference (FTC), vol, 2017, 1-11 pm, 2017.

[6] M. E. Peck, "Blockchain World - Do you need Blockchain? This guide will show you whether the technology can solve your problem," IEEE Spectrum, p. 54, no. 10,p. 38-60, November 2017.