IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 16, May 2023

Decentralized Drive

Prof Bajirao Shirole[1], Aditya S Dhage[2], Rohan S Randive[3], Sarika K Jagtap[4], Unnati D Bhangare[5]
Department of Computer Engineering[1-5]
Sanghvi College of Engineering, Mhasrul, Warvandi, Nashik, Maharastra, India

Abstract: *Centralized cloud-based storage has received great attention and has been extensively used by many companies in recent years. However, these cloud based storage are not secure because of the involvement of a centralized entity or a third party. On the other hand, there is a need for blockchain based decentralized storage to maximize data privacy and security. This paper proposed D-Drive, an IPFS-based decentralized storage space to solve the problem. D-Drive is a software solution trying to prove that centralized cloud-based storage applications can be decentralized, more secure, and efficient. This paper proposed developing a web-based application that provides a user interface, from which the user can directly share their data or files. Then, the user file is encrypted and stored across a peer-to-peer network using IPFS protocol instead of HTTP protocol and a cryptocurrency will be used as a payment mechanism. D-Drive's primary objective is to provide secure decentralized storage space.*

Keywords: Blockchain, Data Security, IPFS, Encryption, Cloud Storage, Decentralized storage

I. INTRODUCTION

Nowadays, huge amounts of data are produced every day. To meet the increasing demand for data storage space, cloud-based centralized storage systems have been widely used in terms of data storageand sharing. Cloud drive lets anyone upload and transfer data or files to the cloud and share them with anyone. However, centralized cloud storage has a lot of disadvantages including data leaking or breaching by malware during the process and a proprietorship of data by a single entity that increases the chances of personal data being used by third parties for their analysis or personal use. Weare all aware of information leakage cases of Facebook-Cambridge Analytica [15], [16] which motivates us to shift from centralized storage to a decentralized storage system.

Decentralization distributes data, applications, power, people, or things into a peer-to-peer rather than on a central authority. If a System is decentralized, it means that it is not controlled, or managedby a single entity or authority [5]. In addition, decentralization facilitates more benefits such as privacy, security, low price, and completely removing trust in a third party. Nowadays, the concept of Inter-Planetary File system (IPFS) [10], has been introduced. The Inter-Planetary File System (IPFS) is a version controlled decentralized file system that uses Distributed Hash Table (DHT) technology for storing data in a peer-to-peer network [7].It enables us to store and share any type and size of data over a decentralized network without any limitations. Still IFPS needs lot of research to meet specific demands of real world problem, suchas how to allow users to share data for multiple users in different organizations without any trust issues [4]. To sort out above problem cryptographic techniques [3], have been widely used in traditional storage system. This paper proposed a data storage system named D- Drive that provides decentralized, secure, and transparent means of storing and sharing data. For that, we make the use of decentralized technologies to build this system. First, we rely on advantages of IPFS network to store data of users in a decentralized manner.

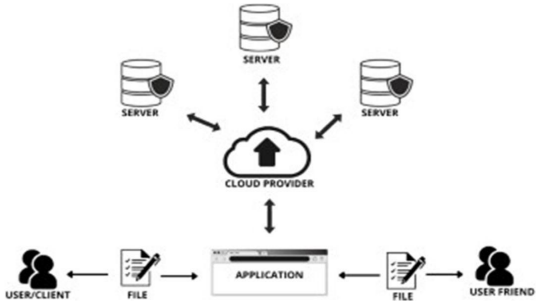

Fig. 1. Schema of centralized cloud-based storage system

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 16, May 2023

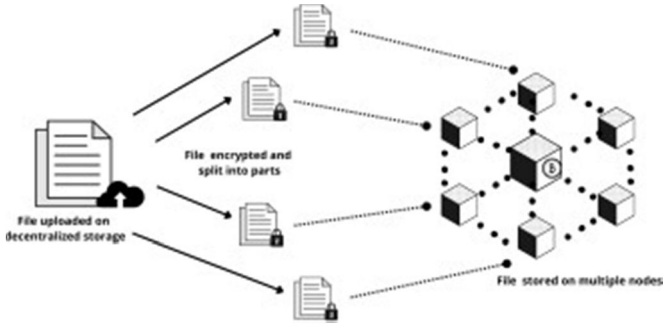

Fig. 2. Schema of decentralized storage system

1.1 PROBLEM IDENTIFICATION

Cloud-based storage pointed out the problem of data privacy and security, as there is an involvement of a centralized entity or a third party. The proposed system introduced the need for blockchain baseddecentralized storage to maximize the data privacy and security.

1.2 BACKGROUND

Blockchain Technology

There are three types of blockchain named as public, private, and consortium blockchain in decentralized systems [2]. The concept of cryptocurrency is more related to solving issues of a public blockchain. Blockchain [1], [4] is a collection of blocks, in which each block is composed by transactions and includes a hash of the previous block. Distributed technology provides immutabilityof the data because changing data in one block will affect all next blocks [8], and is beneficial for record-keeping, digital notary, and smart contracts [9]. This technology has been initially used for digital currency [6], and secure distributed transaction storage systems. Bitcoin is a great example of cryptocurrency. Ethereum[11], is another decentralized, open source, public platform basedon blockchain technology. The structure of the Ethereum is almost similar to the other blockchain networks. It has a feature called a smart contract, which facilitates online contract agreements.

Smart Contract

A smart contract is a small piece of code that executes on the blockchain platform without the involvement of any third party. The platform includes a virtual machine - Ethereum Virtual Machine(EVM) [14],which can execute scripts using an Ethereum computer network.

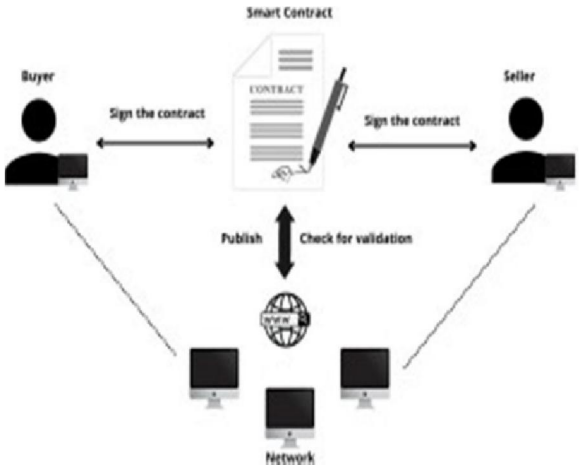

Fig. 3. Schema of blockchain transaction

Ethereum has a cryptocurrency named ”Ether” which can be transferred between accounts and used to pay miners as a gas feeto help with the calculations

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 16, May 2023

Distributed Systems and Hash Tables

Hash is the output of a hashing algorithm such as MD5 (Message Digest 5) or SHA (secure hash algorithm) [13]. It is used for several different areas such as cryptography and data indexing. A hash function generates a hash value that can only be decoded by looking up the value from a hash table. The table may be any data structure. Hash function is one-way and noninvertible.

A DHT is a distributed form of hash table. The main advantages of the DHT is that it makes blockchain faster as all nodes can be added or removed at a minimum time just by redistributing the keys [13].

IPFS

The IPFS (InterPlanetary File System) is a protocol for sharingand storing data on a peer-to-peer distributed network that uses DHT to track the information about data. Hash tables is used tostore a data package. Kademlia [12], is used to learn about data in nodes. Kademlia is a hash table for decentralized computer networks designed by Petar Maymounkov and David Mazi‘eres in 2002. Whenwe upload the data, a hash has been generated. IPFS stores the hash and then user can use the hash to get their data back. When datais uploaded on the IPFS network, the data will split into multiple pieces. These pieces of data are identified with its own hash.

II. METHODOLOGY AND ARCHITECTURE

The proposed prototype enables user to upload the data or file to the peer-to-peer network. For that, the user need to configure blockchain network(Ganache is used for local blockchain network) and integrating it into the web browser using the Metamask extension.

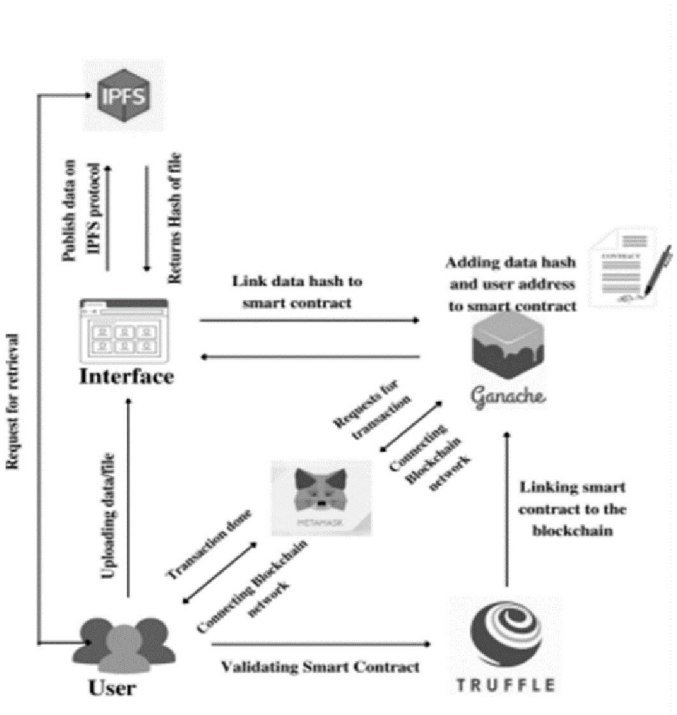

Fig. 4. Architecture of D-Drive

From the fig 4. the user needs a blockchain network, which is provided by Ganache. The accounts provided by Ganache are added to Metamask for transaction purpose. A Specific amount of Gas is needed in the form of Ether. Ether is a type of crypto token that fuels the blockchain network. Then, the user need to create an account on metamask and connect it with their wallet. Now, as our Web browser supports blockchain network, we can now upload the files through our own designed user interface. When the user select the file to upload that file goes to the IPFS and IPFS returns a hash value that will mapped with smart contract. After that the user need to pay the gas amount from their

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 16, May 2023

metamask account. After the successful payment, the smart contract allows the file to getuploaded on a peer-to-peer network

The process of retrieving the file from IPFS requires the previouslyobtained IPFS hash value, which is generated after uploading thefile.We have to put the IPFS hash in the web browser, IPFS will search for the file, and preview is shown. Thus, the file is retrieved back from the IPFS System.

III. RESULTS AND ANALYSIS

This paper proposed developing a web-based application that provides a user interface, from which the user can directly upload or share their data and files over a decentralized network. The proposed solution works in multiple segments. Firstly, the user needs to create an account on metamask and login with their credentials.

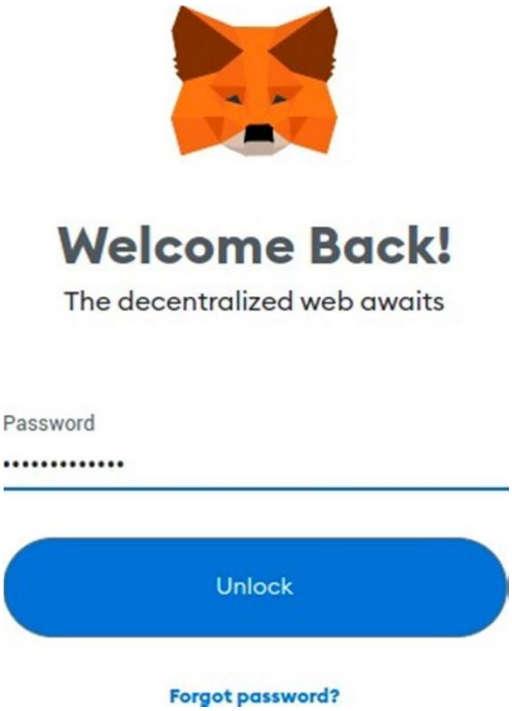

Fig. 5. Metamask login interface

Then, the user needs to connect their metamask account with their wallet. The user's account address and wallet balance arefetched in the metamask account through web3.js

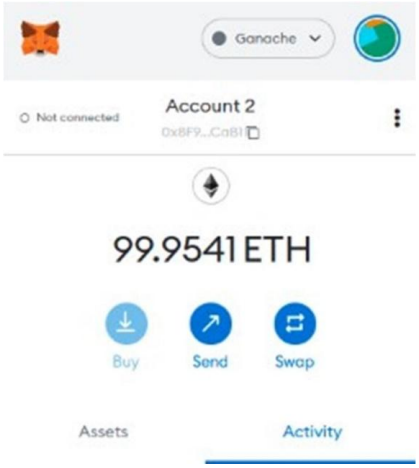

Fig. 6. Account balance fetched

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 16, May 2023

After that, the user needs to open Dapp(D-Drive) and select the files to upload.

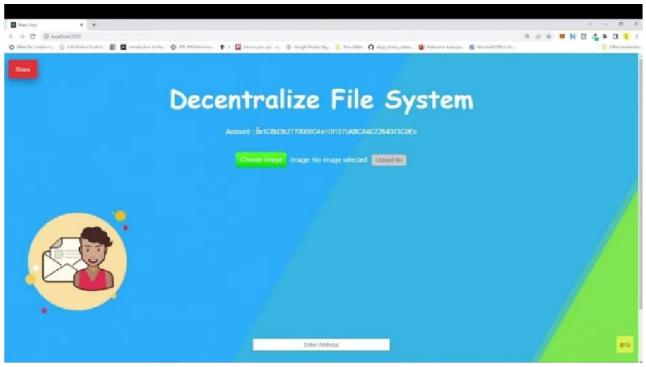

Fig. 7. User Interface

Further, the AES algorithm link the user wallet address as a keyand encrypt the uploaded file. Payment dialogue box pop-ups for the payment confirmation.

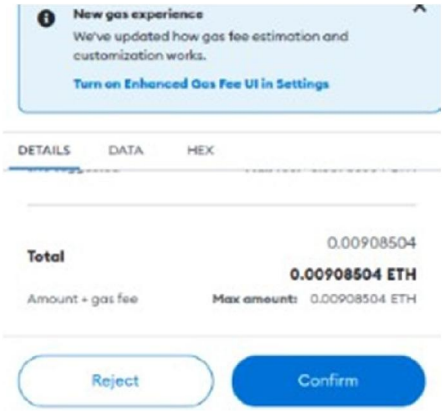

Fig. 8. Payment confirmation dialogue box

After the successful payment, the user's file stored on the peer- to-peer network using IPFS protocol. IPFS returns a hash value of the uploaded file, that will mapped with address using a smartcontract and get stored over a blockchain network.

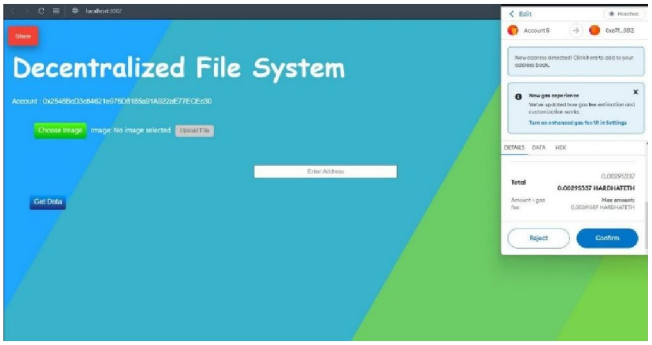

Fig. 9. File Uploaded with hash value

Further, if the user want to share their uploaded file, they just need to share the hash view with the other user, so that theycan view or download by clicking it.

Fig. 10. Hash value of a uploaded file

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 16, May 2023

type	size	date	uploader/view	hash/view/get
application/vnd.openxmlformats-officedocument.wordprocessingml.document	41 KB	5:31:25 PM 5/19/2022	0xCdE25172...	QmNt2deEzj...
application/vnd.openxmlformats-officedocument.presentationml.presentation	3 MB	5:30:43 PM 5/19/2022	0xCdE25172...	QmaLRe9gDv...
application/pdf	410 KB	5:26:55 PM 5/19/2022	0xCdE25172...	QmQ9CmC8BT...
image/jpeg	122 KB	5:25:43 PM 5/19/2022	0xCdE25172...	QmQc9ddUi4...

Fig. 11. Hash value of a uploaded file

IV. CONCLUSION

In conclusion, the project on decentralized storage has successfully implemented a reliable and efficient solution for decentralized data storage. By leveraging blockchain technology and distributed systems, the project addresses the limitations of centralized storage systems and offers improved security, data integrity, and user control. Through extensive testing, the system's functionality, performance, and robustness have been validated. The project opens avenues for further enhancements, such as advanced encryption mechanisms and decentralized file sharing capabilities. Overall, the project contributes to the advancement of decentralized storage systems, revolutionizing data storage and management in the digital age.

ACKNOWLEDGMENT

We take immense pleasure in expressing our humble note of gratitude to our project guide Prof. Bajirao Shirole Computer Engineering, Sanghvi College Of Engineering, Nashik for her remarkable guidance in doing our project

REFERENCES

[1]. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from https://bitcoin.org/bitcoin.pdf
[2]. Buterin, V. (2013). Ethereum White Paper: A Next-Generation Smart Contract and Decentralized Application Platform. Retrieved from https://ethereum.org/whitepaper/
[3]. Storj Labs Inc. (2021). Storj: Decentralized Cloud Storage. Retrieved from https://storj.io/
[4]. Filecoin Project. (2021). Filecoin: A Decentralized Storage Network. Retrieved from https://filecoin.io/
[5]. IPFS. (2021). InterPlanetary File System. Retrieved from https://ipfs.io/
[6]. Ethereum Foundation. (2021). Solidity Documentation. Retrieved from https://docs.soliditylang.org/
[7]. Hardhat. (2021). Hardhat Documentation. Retrieved from https://hardhat.org/
[8]. MetaMask. (2021). MetaMask Documentation. Retrieved from https://docs.metamask.io/
[9]. React. (2021). React Documentation. Retrieved from https://reactjs.org/docs/getting-started.html
[10]. W3C. (2021). Web Cryptography API. Retrieved from https://www.w3.org/TR/WebCryptoAPI/
[11]. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In IEEE International Congress on Big Data (pp. 557-564). IEEE.
[12]. Swan, M. (2015). Blockchain: Blueprint for a New Economy. O'Reilly Media.
[13]. Tapscott, D., & Tapscott, A. (2016). Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World. Penguin.
[14]. Antonopoulos, A. M. (2018). Mastering Ethereum: Building Smart Contracts and DApps. O'Reilly Media.
[15]. Wood, G. (2018). Ethereum: A Secure Decentralized Generalized Transaction Ledger. In B. M. Arnett, C. A. Diuk-Wasser, & D. A. Meisel (Eds.), Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data (Vol. 1, pp. 125-143). Elsevier.