IJARIIT INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X

Impact Factor: 6.078

(Volume 7, Issue 3 - V7I3-1605)

Available online at: https://www.ijariit.com

A review of decentralized storage and sharing system using blockchain

Hardik Ravindra Kajne
hardikkajne@gmail.com
Priyadarshini College of Engineering, Nagpur, Maharashtra

Rubana Khan
rubi.tarannum@gmail.com
Priyadarshini College of Engineering, Nagpur, Maharashtra

Yashwant Sharma
yashwant8530@gmail.com
Priyadarshini College of Engineering, Nagpur, Maharashtra

Manali Rahangdale
nandmanali@gmail.com
Priyadarshini College of Engineering, Nagpur, Maharashtra

Shivang Verma
verma.shivang99@gmail.com
Priyadarshini College of Engineering, Nagpur, Maharashtra

Avnish Karwa
Avikarwa0001@gmail.com
Priyadarshini College of Engineering, Nagpur, Maharashtra

ABSTRACT

A Decentralized application that would help in storing any type of files online without using any third-party software. Important documents are good to be stored online so that one can access them from anywhere in the world from any device having an internet connection, but would be helpful only when it is stored on some trusted third-party software. These third parties may peep into the documents and can use them as data for personal use. There is also a chance of restricted service or the downtime of the software. This would turn out to be a nightmare. This system proposed a solution to this problem by using Decentralized applications using Ethereum Blockchain. This Dapp stores any type of files keeping any third party away from the process of storing data. As long as this Dapp is based on Blockchain technology, it is resistant to any kind of attack because of the use of the Ethereum platform having a default hashing algorithm.

Keywords— *Decentralized Storage System, Decentralized Sharing System, Blockchain*

1. INTRODUCTION

Nowadays data is one of the most important parts of our lives. Users generate data whenever they use their phones or use the internet. All that data, especially documents, needs to be stored somewhere to be accessed. For most of the storage, cloud-based centralized storage platforms are preferred. Users trust the cloud storage providers with their data. If data is not handled in a secured way it can lead to disastrous results. But cloud-based centralized storage also has its drawbacks. All the data is stored in one place if the server gets hacked or a DOS attack happens. It can lead to all valuable data getting lost. If the server goes down then users won't be able to access their data. As users are trusting the cloud storage providers with their data it can be viewed by them. So, this system proposes a decentralized storage and sharing system that can be built using Blockchain and IPFS technologies.

2. TERMINOLOGIES USED

Ethereum: Ethereum is the community-run technology powering the cryptocurrency, ether (ETH), and thousands of decentralized applications. Ethereum may be a technology that is home to digital cash, international payments, and applications. Ethereum and its apps are open supply. Ethereum services are free and straightforward to line up, controlled by you, and work with no personal data. Ethereum is not just for digital cash. something you'll be able to own will be drawn, traded, and placed to use as non-fungible tokens (NFTs). you'll be able to tokenize your art and find royalties mechanically whenever it's re-sold. Or use a token for one thing you own to require out a loan. the chances are growing all the time.

IPFS: IPFS aims to surpass communications protocol so as to make a more robust net for all. IPFS keeps each version of your files and makes it straightforward to line up resilient networks for mirroring knowledge. IPFS powers the creation of multifariously resilient networks that change persistent accessibility with or while not net backbone property. communications protocol downloads files from one pc at a time rather than obtaining items from multiple computers at the same time. Peer-to-peer IPFS saves massive on information measure up to 60%& for video creating it doable to with efficiency distribute high volumes of information while not duplication.

Metamask: MetaMask may be a package cryptocurrency billfold accustomed to the Ethereum Blockchain. MetaMask permits users to store and manage account keys, broadcast transactions, send and receive Ethereum-based cryptocurrencies and tokens, and firmly connect with suburbanized applications through a compatible application or the mobile app's integral browser. it's accustomed to connect native Ethereum networks with personal accounts and move with sensible Contracts. It's a browser extension for Chrome.

Dapps: Dapps area unit a growing movement of applications that use Ethereum to disrupt business models or invent new ones. DApps have their backend code running on a suburbanized peer-to-peer network, as opposed to typical applications wherever the backend code is running on centralized servers. A DApp will have frontend code and user interfaces written in any language which will create calls to its backend. moreover, its front toShipping will be hosted on suburbanized storage like IPFS.

Truffle: Truffle Suite may be a development setting supported Ethereum Blockchain, accustomed to develop DApps (Decentralized Applications). Truffle may be a one-stop answer for building DApps: compilation Contracts, Deploying Contracts, Injecting it into an online app, making front-end for DApps and Testing. Truffle has integral support to Compile, Deploy and Link sensible contracts. It supports Console and net apps. It supports Network Management and Package Management with tight integration.

Ganache: Ganache may be a personal blockchain for speedy Ethereum distributed application development. Users will use Ganache across the complete development cycle; that permits them to develop, deploy, and take a look at Apps in a very safe and settled setting. It sets up ten default Ethereum addresses, complete with non-public keys and every one, and pre-loads them with a hundred simulated Ether every. One will write unit tests for his or her code, deploy sensible contracts, mess around, decide functions, so tear it all down for any simulation or new tests, returning all addresses to their initial state of a hundred Ether.

Smart Contracts: sensible contracts are merely kept on a blockchain that runs once preset conditions are met. They usually are accustomed to automatize the execution of associate agreement in order that all participants will be at once sure of the result, while not associate intermediary's involvement or time loss. they will additionally automatize an advancement, triggering following action once conditions are met. among a wise contract, there will be as several stipulations' pro re nata to satisfy the participants that the task are completed satisfactorily. to ascertain the terms, participants should verify however transactions and their knowledge area unit drawn on the blockchain, agree on the "if/when...then…" rules that govern those transactions, explore all doable exceptions, and outline a framework for resolution disputes.

3. SYSTEM WORKFLOW

This proposed system consists of Ethereum blockchain, Interplanetary File System (IPFS), peer-to-peer file storing system, and smart contracts. The proposed system is a web application developed using ReactJS (a JavaScript library for dynamic UI). It is a decentralized system for the storage and sharing of files. Smart contracts are at the center of the proposed system as are responsible for data encryption, user authentication, data management.

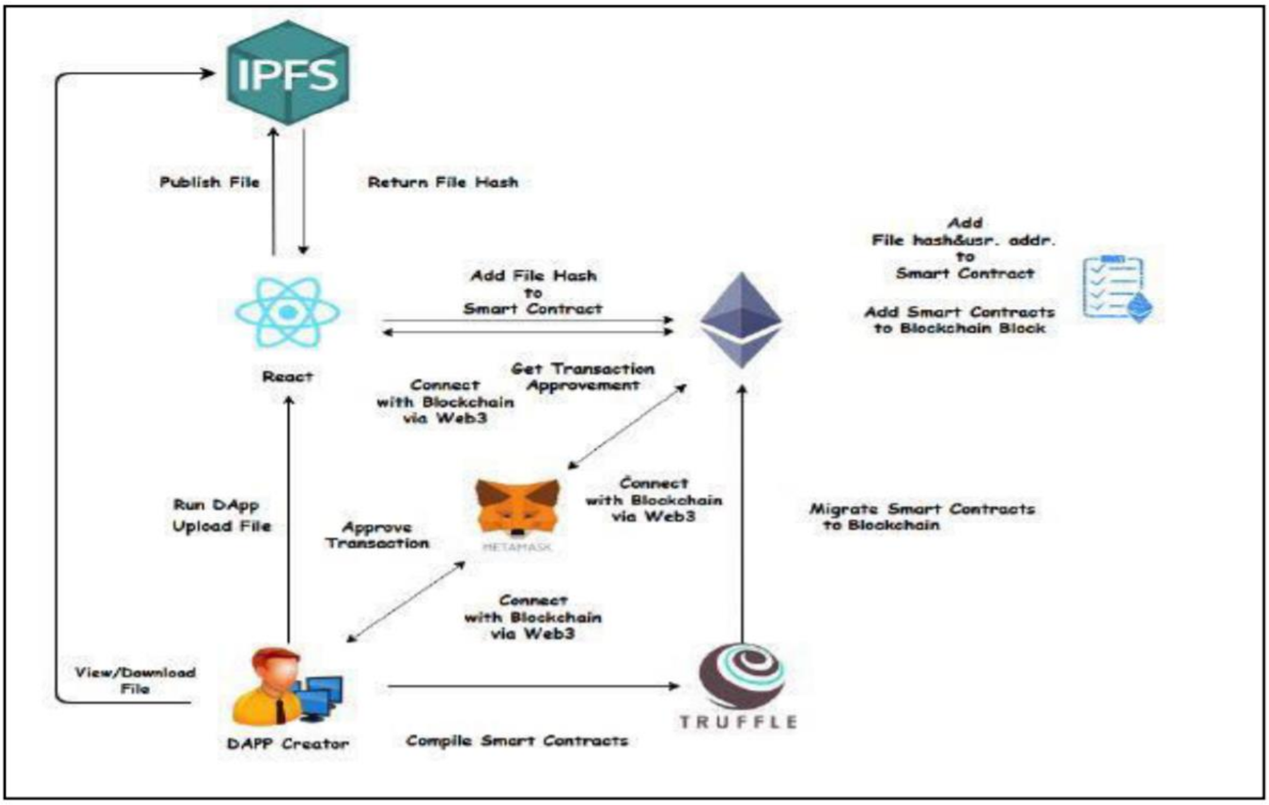
IPFS
Publish File
Return File Hash
Add File hash&usr. addr. to Smart Contract
Add File Hash to Smart Contract
Add Smart Contracts to Blockchain Block
React
Get Transaction Approvement
Connect with Blockchain via Web3
Run DApp Upload File
Approve Transaction
Connect with Blockchain via Web3
METAMASK
Migrate Smart Contracts to Blockchain
Connect with Blockchain via Web3
View/Download File
DAPP Creator
Compile Smart Contracts
TRUFFLE

Figure 1. Block diagram of the system

Author (year)	***Paper-Title***	***Geo.loc.***	***Objective***	***Research-methodology***	***Conclusion***	***Observation***
Saqib Ali **Bebo White** **Roger Leslie Cottrell** **(2018)**	A Blockchain-based Decentralized Data Storage and Access Framework for PingER	China, California	They designed a blockchain-based data storage and access framework for PingER. It is a worldwide end-to-end Internet performance measurement project. It is used to remove its total dependence on a centralized repository. The permissioned blockchain and Distributed Hash Tables (DHT) are used for this purpose. In the proposed framework, metadata of the files are stored on the blockchain whereas the actual files are stored off-chain through DHT at multiple locations using a peer-to-peer network of PingER Monitoring Agents. This provided decentralized storage, distributed processing, and efficient lookup capabilities to the PingER framework.	Permissioned blockchain, Distributed ledger technology, PingER, Decentralized system.	In the paper, they designed a decentralized data storage and access framework for PingER using permissioned blockchain technology. The proposed framework eliminates the need for the centralized repository as the upward paths from the monitoring agents are replaced by write-access data entries on the permissioned blockchain. This approach decentralizes the PingER framework and removes the project dependence upon centralized computing resources for storing, processing and uptime. The resulting architecture will help in scaling up sustainable and large-scale implementation of the project. This, in turn, will help in improving the performance monitoring of the Internet needed to maintain the quality-of-service required for present-day and future technologies of the Internet.	Our observation from this paper is: Blockchains are write-only data structures with no administrative permissions for editing or deleting data. The data structures are known as blocks and are distributed in a P2P network. Each block contains the cryptographic hash function of the previous block and acts like a link between them. The linked blocks form a complete chain, hence the term blockchain. The hash function maintains the security, integrity, and immutability of the blockchain.. The process of creating new blocks is known as mining. The new blocks are always appended at the end of the blockchain. The main components of the blockchain include Transactions, Blocks, Cryptography, Smart Contracts, Consensus Algorithms, and P2P network.
Satoshi Nakamoto (Pseudonym)	Bitcoin: A Peer-to-Peer Electronic Cash System	*********	He/They wanted to propose a purely P2P version of e-cash that would allow online payments to be sent directly from sender to receiver without going through any third party financial institution. Because of the aftermath of the 2008 Financial Crisis, the whole world wanted a decentralized system on whom they can trust, so that they will not be fooled	His/Their 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 Miners get incentive in the form of bitcoins for every single transaction	He/They proposed a solution to the double-spending problem using a P2P network. He/They created the first cryptocurrency of the world and named it Bitcoin. He/They has/have proposed a system for electronic transactions without relying on third parties. He/They started with the usual framework of coins made from digital signatures, which	Our observation from this paper is privacy: Level of privacy by limiting access to information to the parties involved and the trusted third party. The public and private keys are some random numbers. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. Suppose ‘A’ wants to send money to ‘B’. To initiate this transaction, public

			again by these banks.	validation. 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 nodes who flag the transaction as valid/invalid are called MINERS. Whenever a transaction request is generated, it goes in the pool of transactions. Miners take this transaction and check its validity, by finding the public keys of both sender and receiver and checking their balance. This process takes 10 mins to solve. The miner who does this process fast wins 12.5 BTC as a reward. This process is called Proof-of-work. In this way,new bitcoins are mined.	provides strong control of ownership, but is incomplete without a way to prevent double-spending. To solve this, he/they proposed a P2P 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. As all the transactions cannot be altered and are stored, it helps to reduce the problem of corruption. To make a transaction, it should be given a validation by another node. If these nodes flag it as INVALID, then the transaction is not added and done. For solving one complex mathematical problem, at least 10 mins are required. So to hack the whole blockchain, it will take time. Hence are secured.	keys of both are needed. Private key of the sender is also taken to create a digitally signed contract called Smart Contract. It searches the public key of the receiver. It also takes the private key of the receiver. A block is created in the blockchain, where public ids of both sender and receiver are stored and their amount sent from sender to receiver.
Yan Zhu1, **Chun Li Lv1,** **Zichuan Zeng1,** **Jingfu Wang1,** **Bei Pei2 (2019)**	Blockchain - based Decentralized Storage Scheme	China	Different from the current cloud storage solutions, which are mostly centralized storage providers, They wanted a system which can make full use of the remaining space of personal hard disks of users around the world. To create a credible and secured system where proofs and payment information would be stored in blockchain.	Their system proposes a distributed storage scheme based on blockchain. The user uploads the encrypted data to the Third party, and the third party sends the data to the storage provider and informs the user of the data storage location. After the data integrity certificate is completed between the user and the storage provider, the user uses the	Their system proposes a distributed storage scheme based on blockchain technology and introduces the system design in detail. The system uses cryptography techniques such as blockchain technology, lightning network technology, remote data integrity certification, and remote data confidentiality protection technology.	Our observation from this paper is: Data integrity: The blockchain-based distributed storage system uses a Merkel tree-based data integrity certification scheme. After the user encrypts the file data, the user generates and saves a random challenge: These random challenges correspond to the block data one by one. The block data and the random challenge are hashed together to become the Merkel leaf node, and constructed into a Merkel tree. The user saves the node information of the Merkel tree leaf and the height of the

				lightning network technology to pay the storage fee to the storage provider.		Merkel tree. During the verification phase, the user randomly selects a challenge in a random challenge: and sends it to the third party. The third party sends the challenge to the storage provider.
Prof. Rubana Khan1, **Shivang Verma2,** **Manali Rahangdale3,** **Yashwant Sharma4,** **Hardik Kajne5,** **Avnish Karwa6,**	DECENTRALIZED STORAGE AND SHARING SYSTEM USING BLOCKCHAIN	India	Data is one of the most important parts of our lives. We generate data every time we use our phones or use the internet. All that data is needed to be stored somewhere to be accessed. For most of the storage, we use cloud-based centralized storage If data is not handled in a secured way it can lead to disastrous results. But cloud-based centralized storage also has its drawbacks. All the data is stored in one place if the server gets hacked or a DOS attack happens. It can lead to all our valuable data getting lost. If the server goes down then we won't be able to access our data. As we are trusting the cloud storage providers with our data it can be viewed by them. So we are proposing a decentralized storage and sharing system that can be built using Blockchain and IPFS technologies. We are using various new and old technologies which can be used to develop a secure, privacy, and integrity-oriented system. Principles like decentralized storage, hashing algorithms like SHA-256, and peer-to-peer networking. These things are taken into consideration in developing this system using blockchain and IPFS.	ETHEREUM BLOCKCHAIN: Ethereum is a technology that lets you send cryptocurrency to anyone for a small fee. It also powers applications that everyone can use and no one can takedown INTERPLANETARY FILE SYSTEM (IPFS): A peer-to-peer hypermedia protocol designed to make the web faster, safer, and more open. Your file, and all of the blocks within it, are given a unique fingerprint called a cryptographic hash. IPFS removes duplicates across the network. SMART CONTRACT: Smart contracts are simply programs stored on a blockchain that run when predetermined conditions are met. They typically are used to automate the execution of an agreement so that all participants can be immediately certain of the outcome, without an intermediary's involvement or time loss.	The system is able to share and store files in a secured way. The combination of Ethereum blockchain and Interplanetary File System (IPFS) works together efficiently. Blockchain and InterPlanetary File System (IPFS) ensures high data security for the system. The below image will give an overview of how the web application will operate after completion:	The observations that we found after reviewing all the papers are. All the above papers have used somewhat similar uses of technologies but in our proposed solution. The developed web app uses those technologies in addition to React and different APIs working in the background. We have also used the feature of browsers that render HTML files as a web page. So if a user wants to host a single-page web page, It won't be any more effort than just uploading the HTML file and It is hosted on the web itself. This feature was not proposed in any previous solutions. Users can also share the link of the files which are stored in the blockchain. It can be done just by sharing the link which was given by the IPFS after successful completion of upload of the file, Which was also not present in any previous solutions that were referred to. If referred to the original paper of bitcoin which proposed to use blockchain for making a decentralized currency system. Our proposed solution takes a different approach of using the blockchain for creating a decentralized storage solution for anyone to store files on a decentralized network. Those files can also be accessed by anyone with a provided URL by the owner of the file.

Following is the flow of the system and all its different operations. The proposed system can perform all the stated operations in the given order to be designated as a decentralized storage system.

1. Senders are authenticated by the smart contract.
2. After the successful authentication, a new block will be added to the blockchain by the smart contract.
3. The sender’s user will use the configured web application to upload a file to the Interplanetary File System (IPFS).
4. After the successful completion of the upload process to the IPFS, an encrypted hash key is returned by IPFS. This encrypted hash key is then authenticated by the smart contract. After successful authentication of the hash key, it is added to the blockchain.
5. Encrypted hash keys of uploaded files can now be accessed by the sender using the Ethereum blockchain.
6. User will initiate the file sending operation by entering the ether (Ethereum blocks) account address (public key) of the receiver.
7. Then again authentication is processed by the smart contract.
8. Cryptographic hash keys are stored on the receiver's block by smart contracts.
9. Authenticated receivers receive a hash key sent by the sender.
10. Hash file and user address will be added to the smart contracts.
11. Users can view and download the file from the IPFS by the stored hash keys in the blockchain.

Privacy:

As this system is run by the Ethereum Blockchain platform, it has by default security features in the form of cryptography. Also, the hashing algorithms used are one-way functions. Public and Private keys of users further add to the security.

4. CONCLUSION

This paper reviews an app for storing and sharing files. The proposed decentralized application can store any type of file without interference from any third party. These third parties may peep into the documents and can use them as data for personal use. There is also a chance of restricted service or the downtime of the software. Over this, the proposed Dapp using Ethereum (whose functionality at first was just to save files online, later added with the sharing of files concept) is beneficial. This type of network would be resistant to the peeping eyes of any third party. Thus, privacy can be easily maintained.

5. REFERENCES

[1] Shanping Wang, Yinglong Zhang, Yaling Zhang. “A Blockchain-Based Framework for Data Sharing With Fine-Grained Access Control in Decentralized Storage Systems” Institute of Electrical and Electronics Engineers, Digital Object Identifier 10.1109/ACCESS.2018.2851611, Vol. 6, 2018.

[2] S. Nakamoto. (2008). Bitcoin: A Peer-to-Peer Electronic cash system. [online]. Available: http://bitcoin.in/pdf/bitcoin.pdf

[3] G. Wood, ‘‘Ethereum: A secure decentralized generalized transaction ledger,’’ Yellow Paper. Accessed: Jan.2021. [Online].Available:https://ethereum.github.io/yellowpaper/paper.pdf

[4] G. Wood, ‘‘Ethereum: A secure decentralized generalized transaction ledger,’’ Yellow Paper. Accessed: Jan. 25, 2021. [Online].Available:https://ethereum.github.io/yellowpaper/paper.pdf

[5] Blockchain for Financial Services. Accessed: Jan. 25, 2021.[Online].Available:https://www.ibm.com/blockchain/ HYPERLINK "http://www.ibm.com/blockchain/%EF%AC%81nancial-services"fi HYPERLINK "http://www.ibm.com/blockchain/%EF%AC%81nancial-services"financial-services

[6] Blockchain for Supply Chain. Accessed: Jan. 25, 2021. [Online].Available:https://www.ibm.com/blockchain/supply-chain

[7] C. Fromknecht and D. Velicanu. (2014). A DecentralizedPublic Key Infrastructure With Identity Retention.[Online]. Available: https://eprint.iacr.org/2014/803.pdf

[8] Proof of Existence. Accessed: Jan. 25, 2021. [Online]. Available: https://proofofexistence.com

[9] S. Wilkinson, T. Boshevski, J. Brandoff, and V.Buterin, ‘‘Storj a peer-to-peer cloud storage network,’’ White Paper. Accessed: Jan. 25, 2021. [Online]. Available:https://storj.io/storj.pdf

[10] J. Benet. (2014). ‘‘IPFS-content addressed, versioned, P2P file system.’’ [Online]. Available: https://arxiv.org/abs/1407.3561

[11] P. Labs. (2018). Filecoin: A Decentralized Storage Network. [Online]. Available: https://filecoin.io/filecoin.pdf

[12] Ethereum Homestead Documentation. Accessed: Jan. 25, 2021. [Online] Available: https://readthedocs.org/projects/ethereum-homestead

[13] Ethereum Blockchain App Platform. Accessed: Jan.25, 2021. [Online]. Available: https://www.ethereum.org

Abbreviations

SHA = Secure Hashing Algorithm
IPFS = Interplanetary File System
DOS = Denial of Service
DAPP = Decentralized Application
ETH = Ether