DECENTRALIZED STORAGE AND SHARING SYSTEM USING BLOCKCHAIN

Prof. Rubana Khan[1], Shivang Verma[2], Manali Rahangdale[3], Yashwant Sharma[4], Hardik Kajne[5], Avnish Karwa[6],
Professor[1], B.E Students[2,3,4,5,6]
Department of Computer Technology
Priyadarshini College of Engineering, Nagpur, Maharashtra, India

ABSTRACT

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 the cloud based centralised storage has also its drawbacks. As all the data is stored at one place if the server gets hacked or 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 decentralised storage and sharing system which can be built using Blockchain and IPFS technologies. We are using various new and old technologies which can be used to develop a more secure, privacy and integrity oriented system. Principles like decentralized storage, cryptography,hashing algorithms like SHA-256 and peer to peer networking.These things are taken into consideration in developing this system using blockchain and IPFS.

I. INTRODUCTION

Currently most of the data is stored in cloud based decentralized storage systems. As the amount of data is increasing every day the cloud providers are also charging fees for storing the data. The exponential increase in the amount of data has led to the growth of many digital cloud based storage systems. These storage systems have also turned out to be the most reliable and convenient systems for storing data. A major advantage of a centralized cloud based storage system is that it makes it very easy to maintain and store data at one place which can be accessed by any number of devices. Which also leads to its single point of failure. If the server goes down or succumbs to denial of service attack will lead to unavailability or loss of the stored data on the cloud. Developing a system with decentralized storage will help in storing data at different places which will overcome the above stated problems like data unavailability or prevention from DOS attacks.

As the data uploaded on the IPFS is stored in a decentralized manner and the encrypted

hash returned by the IPFS will be stored in the Ethereum blockchain. As for accessing the data stored on the IPFS only the authenticated user can access the particular data on IPFS by successful decryption of an encrypted hash key stored in the Ethereum blockchain.

II. PROPOSED METHODOLOGY

We are proposing a decentralised storage and sharing system which can be built using Blockchain and IPFS technologies.

- We are using various new and old technologies which can be used to develop a more secure, privacy and integrity oriented system.
- Principles like decentralized storage, cryptography,hashing algorithms like SHA-256 and peer to peer networking.

They can also automate a workflow, triggering subsequent action when conditions are met. Smart contracts

work by following simple "if/when…then…" statements that are written into code on a blockchain. A network of computers executes the actions when predetermined conditions are met and verified. These actions could include releasing funds to the acceptable parties, registering a vehicle, sending notifications, or issuing a ticket. The blockchain is then updated when the transaction is completed. That means the transaction cannot be changed, and only parties who have been granted permission can see the results.

III. WORKING

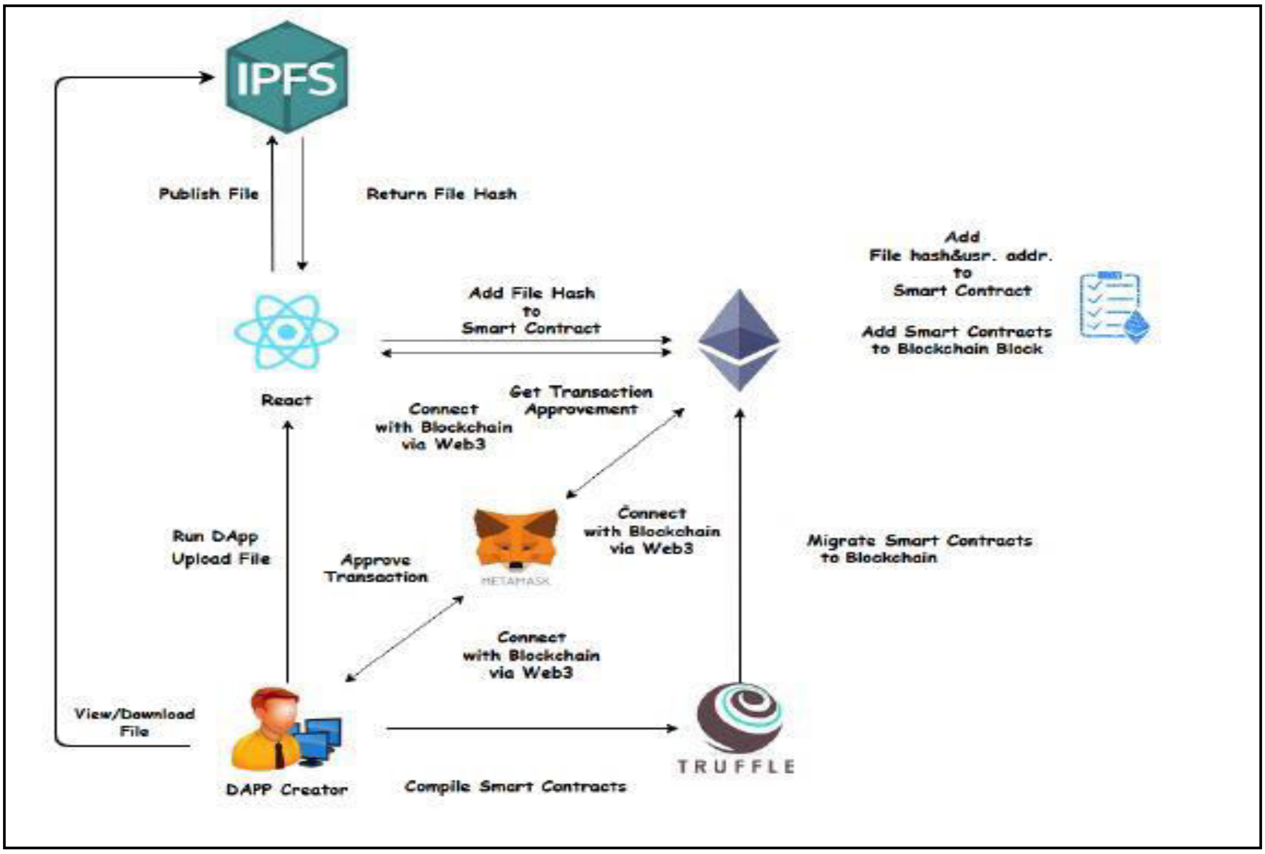

IPFS
Publish File
Return File Hash
Add File Hash to Smart Contract
Add File hash&usr. addr. to Smart Contract
Add Smart Contracts to Blockchain Block
React
Connect with Blockchain via Web3
Get Transaction Approvement
Run DApp Upload File
Approve Transaction
METAMASK
Connect with Blockchain via Web3
Migrate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

The proposed system will consist of Ethereum blockchain, Interplanetary File System (IPFS) peer to peer file storing system and smart contracts. The proposed system will be a web application developed using ReactJS, a javascript library for dynamic UI. It will be a decentralised system for storage and sharing of files. Smart contracts are at the center of the proposed system as it will be responsible for the data encryption , user authentication, data management. Following is the flow of the system and all its different operations. The proposed system should be able to perform all the stated operations in the given order to be designated as a decentralised storage system.

1. Senders should be authenticated by the smart contract.

2. After the successful authentication of the sender a new block will be added to the blockchain by smart contract.

3. The sender 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 smart contract. After successful authentication of the hash key it is added to the blockchain.

5. Encrypted hash key of uploaded file can now be accessed by sender using 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 smart contract.

8. Cryptographic hash keys are stored on receivers 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.

TECHNOLOGY USED

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 take down. It's the world's programmable blockchain. Ethereum builds on Bitcoin's innovation, with some big differences. Both let you use digital money without payment providers or banks. But Ethereum is programmable, so you can also use it for lots of different digital assets – even Bitcoin! This also means Ethereum is for more than payments. It's a marketplace of financial services, games and apps that can't steal your data or censor you

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, is given a unique fingerprint called a cryptographic hash. IPFS removes duplicates across the network. Each network node stores only content it is interested in, plus some indexing information that helps figure out which node is storing what. When you look up a file to view or download, you're asking the network to find the nodes that are storing the content behind that file's hash. You don't need to remember the hash, though — every file can be found by human-readable names using a decentralized naming system called IPNS.

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 any intermediary's involvement or time loss.

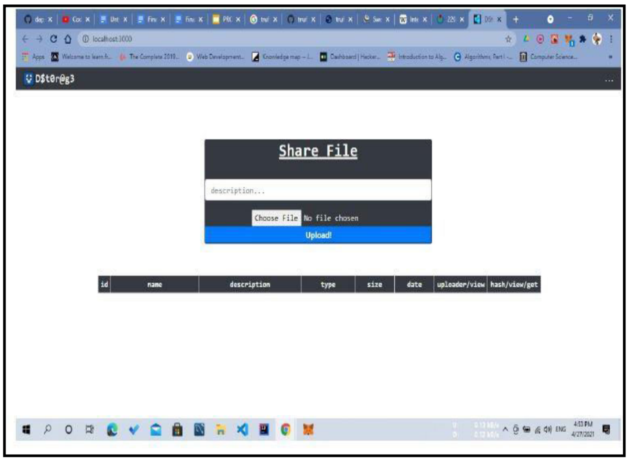
IV. RESULT AND DISCUSSION

The proposed software is a web application where any person can store and share their data so that it can not be seen or altered by anyone as it is encrypted. This system aims to develop a web application which ensures the security, integrity and privacy of the data.

V. CONCLUSION

The system is able to share and store files in a secured way. 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 how the web application will operate after completion:



id	name	description	type	size	date	uploader/view	hash/view/get

ACKNOWLEDGEMENT

Priyadarshini College of Engineering is a well established & renowned institute and follows a goal of creating technocrats and brings it into reality. We wish to avail this opportunity to express our sincere thanks to our Guide Prof. RUBANA KHAN who continuously supervised our work with utmost care and zeal. She has always guided us in our endeavor to present our project on "DECENTRALIZED STORAGE AND SHARING SYSTEM USING BLOCKCHAIN".

VI. 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 decentralised generalised transaction ledger,’’Yellow Paper.Accessed: Jan.2021.[Online].Available:https://ethereum.github.io/yellowpaper/paper.pdf

[4] G. Wood, ‘‘Ethereum: A secure decentralised generalised 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/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