Vol-06 Issue 06, June -2022 ISSN: 2456-9348
Impact Factor: 5.004

iJETRM
International Journal of Engineering Technology Research & Management

SECURE STORING & SHARING OF FILES USING BLOCKCHAIN

Mohit Arora, Mohd. Salar Khan, Ankit Negi
Department of Information Technology
Dr. Akhilesh Das Gupta Institute of Technology & Management, Shastri Park, Delhi

Abstract:
Data is the most important part of one's life nowadays. This data needs to be stored with security and should be easily accessible. Cloud is an emerging technology which provides solution to this problem. Cloud storage seems to be efficient but it is not risk free. The cloud technology is not safe as it uses centralized storage approach resulting in continuous data breaches, data leakages. Blockchain can be used to store data securely but large files cannot be efficiently stored on Blockchains. IPFS is a file sharing system that solves this problem of storing and sharing large files efficiently. IPFS does not allow users to share files with selected parties. Therefore, this paper proposes a modified version of the Inter Planetary Filesystem (IPFS) that uses Ethereum smart contracts to provide access-controlled file sharing.

Keywords:
Security, Storage, Cryptography, Blockchain, Smart Contract, Ethereum

1. INTRODUCTION

With the rapid growth in the fields of Information Technology, information has become the most valuable asset for anyone. Organizations around the world create and use huge amounts of data. This data needs to be securely stored and should be easily accessible. For this purpose Databases are being used to store data. With the adoption of cloud storage, organizations do not need to manage their data locally and can also make this data available anytime anywhere through the internet. Cloud storage seems to be efficient but it is not risk free. The centralized storage approach of cloud computing is not secure resulting in continuous data breaches, data leakages. Blockchain can be used to solve this issue. But large files cannot be efficiently stored on Blockchain because it makes Blockchain bloated with data that has to be propagated within the network. IPFS is a file sharing system that solves this problem of storing and sharing large files efficiently. Users cannot share files with selected parties using IPFS. Therefore, this proposed system leverages Ethereum smart contracts to provide access controlled file sharing.

1.1) PROBLEM STATEMENT

Many cloud storage companies ensures the data availability and safety but most of them have terms that allow the company to access, change, delete, view and analyze your content. Data stored to a private owned database gives several access rights to that company and is not always secure. It is sometimes risky to store sensitive data only on local machine or drives because once they are stolen, lost or destroyed by any other means, user cannot make a recovery. Moreover, most of the Cloud Storage companies do not take responsibility in case of data loss due to catastrophic failure. So, completely relying on data storage on your local machine only or on the cloud storage is just not always safe and genuine. Furthermore, storing sensitive data of users to the cloud is not considered a good option when it comes to the high potential value of that data. Sensitive information here means: user passwords, secret keys of cryptocurrencies wallet, secret and confidential documents, sensitive information, papers, records of banking transactions, etc. loss or manipulation of which can bring a huge disaster for any organization or individual.

1.2) OBJECTIVES

The objectives of this research are:

- To develop a decentralized application.
- To utilize storage spaces efficiently.
- To let user store files/data securely without compromising privacy on IPFS.

iJETRM
International Journal of Engineering Technology Research & Management

- To leverage the security of the storage application by using Blockchain.
- To share data with other people in a permissioned manner by sharing the link for document with the intended user.
- To provide transparency as Blockchain-based cloud storage also facilitates immutable transaction records to verify ownership and identity.
- To make storage more secure & decrease the data breaches & several attacks.

2. LITERATURE SURVEY

In 2008, after the global financial crisis, a new paper brought about by a person or group named Satoshi Nakamoto introduced a concept of a peer-to-peer distributed currency with a paper titled "Bitcoin: A peer-to-peer Electronic Cash System". With there usually being a central authority bearing a higher power in a system may it be in economics, finance, technological or general, there exists a risk of the central authority misusing its power for one's gain while other's loss. The paper talked about a distributed digital crypto-currency which could improve how we did things and many regarded as a better system. However, taking this step further, Blockchain allows for what is known as a Distributed Autonomous Organization where it is an organization self-sustained by members without a central authority and trust built around what is known as "Smart contracts"[2]. Hence, using Blockchain technology we can build a cloud platform where you are storing your data. You will trust the server of the given cloud service provider to hold the data without tampering and betrayal of trust and make it available for use any time you want. This trust is built by the company itself with continuous service and a good policy. However, in a distributed service this is hard to do as there is no central authority. The same kind of trust people put in data storage services like a dedicated server or even simple cloud storage applications like Google Drive.

The IPFS is a decentralized storage architecture, which helps to provide decentralized cloud storage based on the principles of P2P networking and content addressing. The internet infrastructure is based on centralized cloud storage and management. The cloud providers control most of today's Internet traffic, which results in a substantial centralization of data and traffic [3]. To counteract this, several initiatives and groups have focused on developing decentralized alternatives. However, the decentralized architecture of such networks may also add new challenges and types of complexity [3].

The work by Trinh Viet Doan, Yiannis Psaras, Jörg Ott & Vaibhav Bajpai discusses both the benefits and challenges — in relation to IPFS, a protocol for decentralized cloud storage [3]. IPFS is a set of protocols that combines different existing concepts from P2P networking, Linked Data, and other fields to allow users to exchange information, similar to torrent. It provides persistence of names, deduplication, and integrity-checks for files through Content Identifiers (CIDs), censorship resistance, network partition tolerance, and ultimately decentralization, among other properties. But IPFS has yet to overcome challenges such as access control, participation incentives, or persistent availability, storage of large data and replication of content. Integration of IPFS and Filecoin aims to overcome some of IPFS' challenges with regard to incentives and content availability. Together with the native support of IPFS in the Opera [8] browser as well as the addition of the IPFS scheme in Mozilla Firefox [9], these are important steps in stimulating the growth of the network and moving towards a more decentralized Internet in the future.

In their work [12], Jatin Ahuja, Dr. Neha Agrawal & Dr. Meenu Garg compares IPFS with Blockchain based file system. The work discussed advantages and disadvantages of both Blockchain and IPFS based file systems. For a beginner user Blockchain based system is extremely handy and easy to use and can be operated by anyone while the IPFS still requires you to have some understanding of how to use it and installation can be quite time consuming. Sharing of data is easy in Blockchain based files system as compared to IPFS. Whereas, IPFS is better in terms of: Fault Tolerance - If one node crashes, the file remains accessible as long as there are other nodes hosting it. Persistent Storage - IPFS objects can be stored permanently without being changed since data blocks are stored locally across the network and can be cached forever. Censorship Resistance - Since content is spread through an entire network, no single authority can delete it until it has been submitted to IPFS. Scalability - The more nodes hosting files, the better and more accessible they become to network users.

The work concluded that IPFS is much more decentralized, established, secured and provides much more use cases. IPFS is the preferred choice over a purely Blockchain based system as explained in the paper.

One major disadvantage of IPFS is that it content on it is open to the public. Anyone who has the content hash will access the content. Currently, IPFS lacks a built-in workaround for saving private data. In this paper we examined the advantages and disadvantages of both these systems [12]. This problem is solved in our research where we used Blockchain in order to save the hash of the file stored in the IPFS which can only be accessed by the user.

There are few such examples of distributed database using Blockchain. We here discuss BigchainDB, Storj.io and MaidSafe as it is more somewhat related to our project. BigchainDB: a scalable Blockchain database that uses Blockchain technology

iJETRM
International Journal of Engineering Technology Research & Management

to store the data of users in various nodes. BigchainDB inherits characteristics of modern distributed databases: linear scaling in throughput and capacity with the number of nodes [11]. Being built on an existing distributed DB, it also inherits enterprise hardened code for most of it's codebase.

Storj is the first decentralized, end-to-end encrypted cloud storage that uses Blockchain technology and cryptography to secure users files. Storj is a platform, cryptocurrency, and suite of decentralized applications that allows you to store data in a secure and decentralized manner. Storj does not support smart contracts on the Blockchain that set the rules and requirements for storage; Storj users pay what they use. This particular payment model means that if a user disappears, the host will no longer be paid for lending their space, a potential problem for those who will be renting their storage space [11]. Storj, MaidSafe are all built with a native storage marketplace where users and hosts can buy and sell storage space. All use mining to provide computing power for the network.

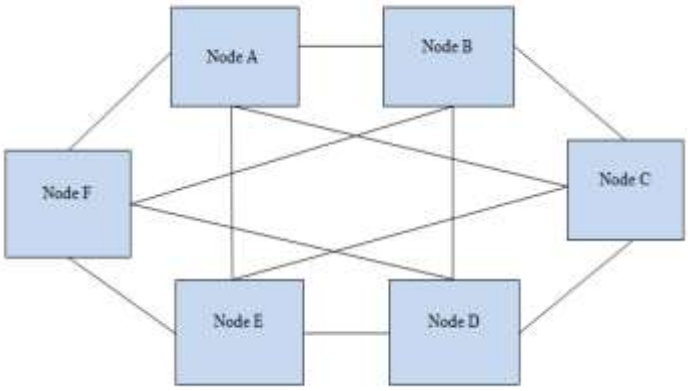
3. PROPOSED WORK

This application is more advanced and is better than other existing systems. Some of the features of our proposed system are:

- It is more focused on storing of keys, passwords, secret keys of cryptocurrency wallets, credentials, etc. It is more focused on securing users' data than just providing mass data storage.
- As we are developing it over Ethereum Blockchain, Ether coins can be used to pay and receive in transaction. Since it is widely used currency. Users do not have to invest on buying coins specifically for this system.
- The time taken by the transaction in Ethereum is less (20 seconds in ideal case), it will be relatively faster than other systems like Storj, MaidSafe.

4. METHODOLOGY

4.1) Building P2P network

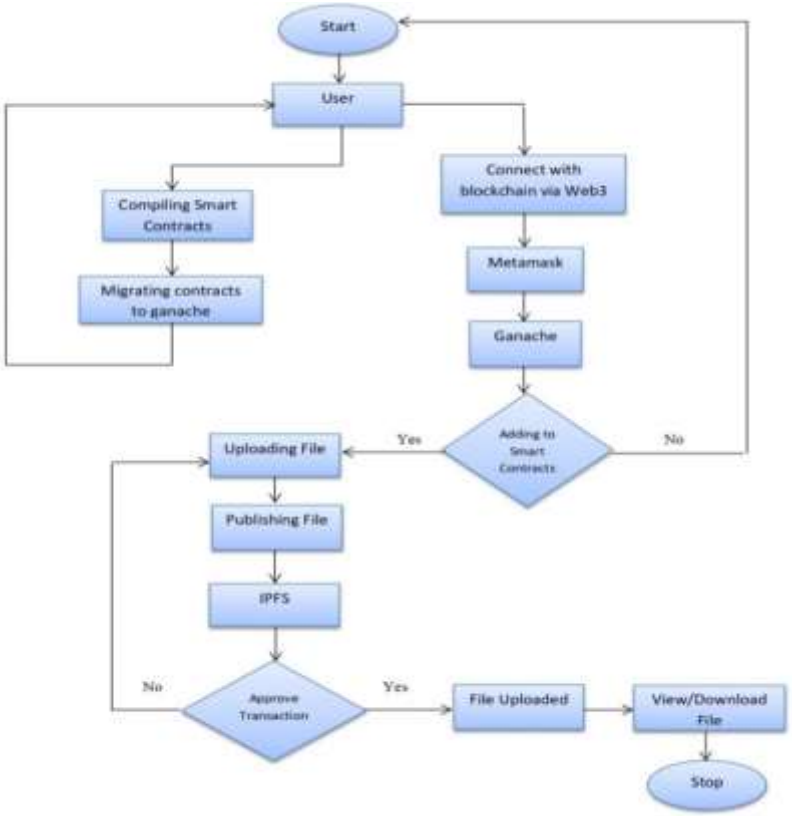


Peer to Peer network is a distributed network in which each node communicates with each other directly or via other nodes. There is no client and server machine to fetch the resource. Each node can act as a host or client according to the needs. There is no centralized server to control the system flow and other nodes.

4.2) File Processing

The main function of the application is to encrypt and decrypt the file. The encryption is done by splitting the file into user defined parts and uploading them on nodes. Similarly, when downloading the file, fetch the parts of the file from nodes, merge the chunks into a single file and then decrypt to get the original file.

iJETRM
International Journal of Engineering Technology Research & Management



4.3) Flowchart of Proposed System

These are the roles in our smart contract:

• Node: stores client data and gets tokens.

• Client: stores data on node and pays tokens.

This flowchart shows the workflow of the proposed system. User first connects to the Blockchain via Web3. Metamask is a chrome extension used to interact with Ethereum Blockchain.

User can select any type of file to upload. After the file is selected, it is stored in IPFS.

IPFS returns a hash which is stored in the Blockchain via smart contracts.

User having ether in their Ethereum accounts can interact with the contract. We have defined our own currency or tokens. In order to store data in our system, client must pay agreed amount of tokens.

During this process, client and user come to agreement based on storage size, bandwidth, time of transaction and token amount.

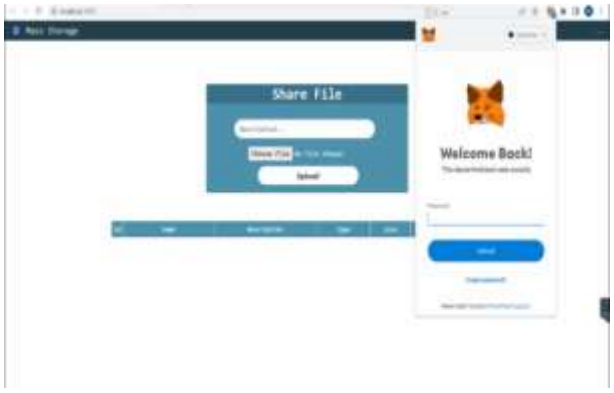
When agreement is completed, all details of agreement between client and node is written in Smart contract which gets deployed to Blockchain.

User can later on view the file or share the hash of that particular file with the intended someone.

5. RESULTS

Home Page: Initially, the application requires users to be authenticated. Users can login with the credentials. The Login is provided by the Metamask which is a chrome extension it is used to connect the app to the ganache (local Blockhain running on our device).

iJETRM
International Journal of Engineering Technology Research & Management

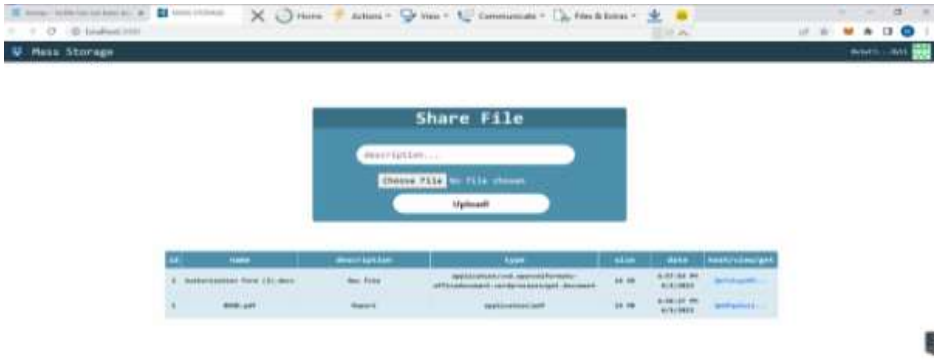


Uploading file: User can upload any type of file using MASS crypto. We have added MASS which is a currency made by us that is imported with ganache through a private key.

File selected: As soon as the user selects a file, an alert is given and he has to confirm the notification whether he allows this operation or not. Also, he needs to confirm the transaction from Metamask. Once the transaction gets completed, the file is uploaded to the cloud. Finally, the log is stored on Blockchain for file creation.

File uploaded: Once the file is uploaded, user can view/download the file. This also requires the same approval from the user which will also trigger Metamask transaction & the operation log details will be written to the Blockchain.

iJETRM
International Journal of Engineering Technology Research & Management



6. CONCLUSION

In this research, we studied the traditional ways of storing data using local disks and cloud storage and the challenges faced with them. This paper proposes the system design of a Blockchain-based storage application which combines security and scalability with its interlinked blocks, hashing functions, and decentralized architecture. Various cryptography techniques like Blockchain technology, lightning network technology, remote data integrity certification, and remote data confidentiality protection technology are used in the system. The system we propose provides value to existing cloud storage systems. It provides better and efficient way to store data than keeping encrypted documents on the cloud. The proposed work uses IPFS and Blockchain which makes it near to impossible to third party to change or damage the stored data. If it happens then the hashes stored in next blocks in Blockchain also changes which can be detected by other nodes in the Blockchain network. It not only eliminates the problems faced in the centralized cloud storage applications where the central server is in charge of users' data but also provides the user the ability to share and give access to the files to only selected individuals. Sharing of data is secure as it uses two-factor authentication in which the first step is to share the link with trusted entity and the second is approving the notification for granting permission to prevent unauthorized access. This makes our system cheap, secure and fast. The agreement is bound by Smart Contract and uses MAAS token as a value for service. The two layers of the proposed work can also be used separately as individual components for different use cases. The businesses can reduce their IT expenditure and enhance the security by incorporating Blockchain technology in cloud storage. In any case, we are still in the beginning phase of the development of Blockchain, and these impediments will be overcome later on, opening the way for some energizing potential outcomes.

7. REFERENCES

[1] M. Crosby, P.Pattanayak, S. Verma and V. Kalyanaraman "Blockchain technology: Beyond bitcoin," Applied Innovation, vol. 2, pp. 6–10, 2016.
[2] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.
[3] Trinh Viet Doan, Yiannis Psaras, Jörg Ott & Vaibhav Bajpai, "Towards Decentralised Cloud Storage with IPFS: Opportunities, Challenges, and Future Considerations", 2022
[4] S. Wilkinson, T. Boshevski, J. Brandoff, and V. Buterin, "Storj a peer-to-peer cloud storage network," 2014.
[5] T. McConaghy, R. Marques, A. Müller, D. De Jonghe, T. McConaghy, G. McMullen, R. Henderson, S. Bellemare, and A. Granzotto, "Bigchaindb: a scalable blockchain database," white paper, BigChainDB, 2016.
[6] Qiwu Zou, Yuzhe Tang, Ju Chen, Kai Li, Charles A. Kamhoua, Kevin Kwiat, Laurent Njilla, ChainFS: Blockchain-Secured Cloud Storage, IEEE 11th International Conference on Cloud Computing (CLOUD), 2018.
[7] Fran Casino, Thomas K. Dasaklis, Constantinos Patsakis,A systematic literature review of blockchain-based applications:Current status,classification and open issues , Elsevier, 2018
[8] R.Gowthami Saranya, A. Kousalya, "A comparative analysis of security algorithms using cryptographic techniques in cloud computing", IEEE, 2017.
[9] Protocol Labs, "IPFS in 2021: The Backbone of Web3's Mainstream Momentum," 2022, accessed 2022-03-31.[Online]. Available: https://blog.ipfs.io/2022-01-11- IPFS-in-2021/

iJETRM
International Journal of Engineering Technology Research & Management

[10] M. Conca, "Extensions in Firefox 59 | Mozilla Addons Blog," 2018, accessed 2022-03-31. [Online].Available:https://blog.mozilla.org/addons/2018/01/26/ extensions-firefox-59/
[11] Shakya, Subarna & Bhusal, Sagar & Shrestha, Anish & Chhetri, Sumit & Khatiwada, Bipin. (2018). DECENTRALIZED SECURE CLOUD STORAGE USING BLOCKCHAIN. 10.13140/RG.2.2.30153.98403.
[12] Shubham Desai, Rahul Shelke, Omkar Deshmukh, Harish Choudhary, Prof. S. S. Sambhare Blockchain Based Secure Data Storage and Access Control System using Cloud IEEE – ICCUBEA 2019.
[13] Ilya Sukhodolskiy, Sergey Zapechnikov, A Blockchain Based Access Control System for Cloud Storage, IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus), 2018.
[14] Xiaoqi Li, Peng Jiang, Ting Chen, Xiapu Luo, Qiaoyan Wen,A Survey on the Security of Blockchain Systems,beijing university China, 2018.
[15] Sangsuree Vasupongayya -Blockchain-Based AccessControl Model to Preserve Privacy for Personal Health Record Systems , Research Article, 2019.
[16] Rongzhi Wang, Research on data security technology based on cloud storage, 13th Global Congress on Manufacturing and Management, GCMM, 2016.
[17] Zibin Zheng1, -An Overview of Blockchain Technology: Architecture, Consensus, National Engineering research center of China, [IEEE] 2017
[18] Y. Tang, T. wang, L. Liu, X. hu, and J. Jang, "Lightweight authentication of freshness in outsourced key-value stores", in proceedings of the 30th annual computer security applications conference, new Orleans, Louisiana, USA, 2014, pp.176-185.
[19] P. Labs, "IPFS is the Distributed Web", IPFS. [Online]. Available: https://ipfs.io/.
[20] A. Narayanan, J.Bonneau, E. W. Felten, A. Miller, and S.Goldfeder, "Bitcoin and Cryptocurrency Technology (manuscript). 2015".
[21] R. Kumar and R. Tripathi, "Implementation of Distributed File Storage and Access Framework using IPFS and Blockchain," 2019 Fifth International Conference on Image Information Processing (ICIIP), 2019, pp. 246-251, doi: 10.1109/ICIIP47207.2019.8985677.
[22] C. Udokwu, A. Kormiltsyn, K. Thangalimodzi, A. Norta, The state of the art for blockchain-enabled smart-contract applications in the organization, 2018 Ivannikov Ispras Open Conference (ISPRAS), IEEE, 2018, pp. 137144.
[23] F. Casino, E. A. Politou, E. Alepis, and C. Patsakis, "Immutability and decentralized storage: An analysis of emerging threats," IEEE Access, vol. 8, pp. 4737– 4744, 2020. [online] Available: https://doi.org/10.1109/ ACCESS.2019.2962017
[24] Justin S. Gazsi, Sajia Zafreen, Gaby G. Dagher, Min Long, "VAULT: A Scalable Blockchain-Based Protocol for Secure Data Access and Collaboration", *2021 IEEE International Conference on Blockchain (Blockchain)*, pp.376-381, 2021.
[25] Saad M, et al. (2020) Exploring the Attack Surface of Blockchain: A Comprehensive Survey, IEEE Communications Surveys & Tutorials, 22(3):1977-2008
[26] Nawari, o.n. and Ravindran, S. (2019). Blockchain And the Built Environment: Potentials and Limitations. Journal of Building Engineering, 1-16.
[27] Beck, R. (2018). Beyond Bitcoin: The Rise of Blockchain World. Published by The IEEE Computer Society, pp.54-58.
[28] Jin Ho Park, -"Blockchain Security in Cloud Computing: Use Cases, Challenges.", Seoul National University of Science and Technology, SoongSil University,Korea;Research Article,2017
[29] Naresh vurukonda, B.Thirumala Rao, -"A Study on Data Storage Security Issues in Cloud Computing", 2nd International Conference on Intelligent Computing, Communication & Convergence, (ICCC-2016), 2018.
[30] Wood G. Ethereum: A secure decentralised generalised transaction ledger [J]. Ethereum project yellow paper, 2014, 151: 1-32.