Decentralized File Storing and Sharing System using Blockchain and IPFS

Mihir Nevpurkar[1], Chetan Bandgar[2], Ranjeet Deshmukh[3], Jay Thombre[4], Rajashri Sadafule[5], Suhasini Bhat[6]

[1,2,3,4]Student, Dept. of Information Technology Engineering, P.E.S's Modern College of Engineering, Pune, Maharashtra, India
[5,6]Asst. Professor, Dept. of Information Technology Engineering, P.E.S's Modern College of Engineering, Pune, Maharashtra, India

---***---

Abstract – *Data is considered as the basic building block for any system. If data is not handled in secured way then this insecurity may lead to many threats for existing system. It is necessary to provide a system which can overcome security loopholes of current systems being used so that those systems will be able to store and share most valuable data of the users in a secured way. In the proposed methodology, the design and implementation of a decentralized file storage and sharing system is carried out using Blockchain and IPFS technologies. Various principles of smart contracts, decentralized storage, cryptographic hashing algorithms, peer to peer networking are taken into consideration while developing system using blockchain and IPFS. The web application is designed such that any person can store and send their data in secured way. The aim of this system is to develop a web application which ensures security, authenticity and integrity of data.*

Keywords: **data, security, decentralized, blockchain, IPFS.**

1. INTRODUCTION

Most software systems rely on cloud data storage for management of the data. With expeditious growth of digital world cloud storage has turned out into most reliable and convenient way of storing data [1]. Data stored using cloud storage is stored in centralized manner. A major advantage of traditional cloud storage is, it is not only easy to handle but also easy to access the data. The data stored on cloud storage can be easily accessed by number of devices at a time. This way of storing data can cause single point failure, denial of service attack which may further lead to unavailability of data [1]. Developing a system with decentralized storage of data can definitely overcome problems like single point failure, data unavailability etc. File uploaded on IPFS [11] is stored in decentralized manner and cryptographic hash key returned by IPFS is stored on Ethereum blockchain. Further, only authenticated user can access that particular data on IPFS by successful decryption of cryptographic hash key stored on Blockchain.

1.1 Literature Review

In traditional mechanism of centralized data handling system, it inevitably inherits the single point of failure drawback of relying on third party services. In some cases, cloud storage systems are backed up to avoid data unavailability. In many cases data security is at stake because cloud storage services providers need to suffer from unnecessary disputes such as political censorship. It may also lead to users would be unable to access their own data [1]. . The cost of centralized cloud storage services comes mainly from employee wages, legal costs and data centre rentals etc. If respective fixed costs are gradually increased then, overall cost of the centralized cloud storage services will be higher. Also, single point failure most of the times leads to data unavailability and eventually to collapse the system.

These facts suggest that, In the future there is a need of decentralized storage approach to provide people with data storage and sharing services. Decentralized data redundancy is proposed in this system which will ensure that copies of the data are maintained on each and every node in a peer to peer network. Various applications are created using blockchain for file transfer but most of them are done using distributed cloud and multi chain framework, files are stored on distributed cloud. In the proposed system Ethereum blockchain framework will be used for creating the blockchain and IPFS will be used for decentralised file storage. Proposed system will be a web application and the data operations will be authenticated by smart contract.

2. DESIGN AND ARCHITECTURE

The proposed system consists of Interplanetary File System (IPFS), Ethereum blockchain and Smart Contracts. This architecture depicts exact file sharing mechanism proposed by this decentralized web application. Smart Contracts in the system are kept centre because they are responsible for carrying out different data operations in a secured manner. Numbers above all the arrows depicts overall flow of the system with different operations.

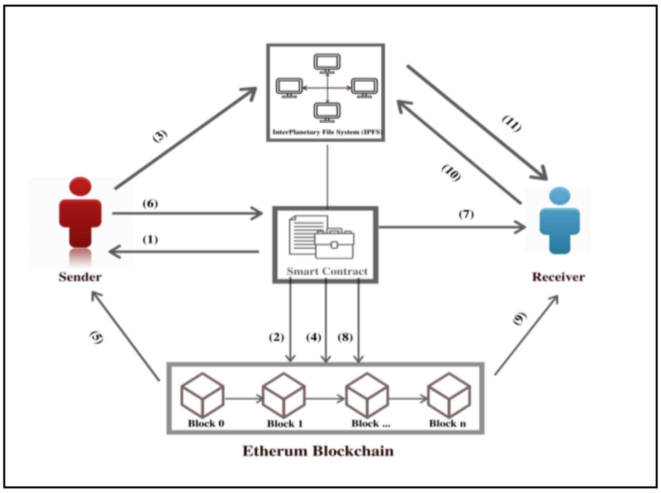

Figure 2.1 – Block diagram of system

Function of each operation number and flow of the system are explained below:

(1) Sender is authenticated by smart contract.
(2) New user block is added to blockchain by smart contract after successful authentication of user.
(3) Sender uploads a file to Interplanetary File System (IPFS).
(4) IPFS returns cryptographic on successful storage of file. If hash key returned by IPFS is trusted then it is stored on blockchain. This authentication is done by Smart Contract.
(5) Cryptographic hash key of uploaded file now can be accessed by sender using blockchain.
(6) User initiates file sending operation by entering ether account address (public key) of receiver.
(7) Authentication of particular receiver is checked by smart contract.
(8) Cryptographic hash key is stored on receivers block by Smart Contract.
(9) Authenticated receivers receives hash key sent by sender.
(10) Receiver requests a particular file to IPFS.
(11) Receiver gets access to file, if and only their private key pair matches with public key which was used for encryption of a file while sending it

2.1 Technologies used in the proposed system

2.1.1 Ethereum Blockchain

In recent years, decentralized cryptocurrency (such as Bitcoin [2], Ethereum [3], Zcash [4], etc.) have become hot topics and the blockchain, being the underlying technology of cryptocurrency, has been paid more attention. There are many fields in which data security is the main aim of the system. Blockchain is being used nowadays for achieving data security in number of fields. It plays major role in ensuring data security in the financial field [5]. Along with this, blockchain is being used in many other non-financial fields. Such as: decentralized supply chain [6], identity-based PKI [7], decentralized proof of document existence [8], decentralized IOT [9], decentralized storage [10]–[12], etc.

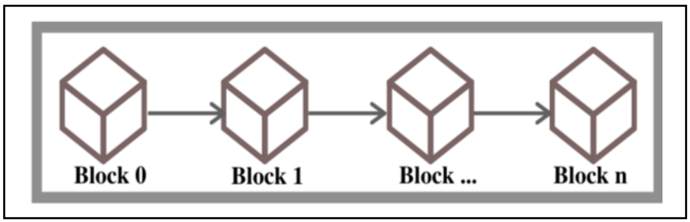

Figure 2.2 – Structure of a blockchain

Ethereum [3], [13], [14] is a new decentralized application platform of smart contract. Smart Contracts can be created, deployed and executed with the help of Ethereum. Once the smart contract is deployed, it starts executing automatically according to the logic written within it.

In the proposed system, blockchain is used for authentication of users as well as to ensure integrity of data. As there are number of blocks in blockchain connected with each other in a chain like structure blockchain is called as Immutable way of storing data.

2.1.2 Interplanetary File System (IPFS)

InterPlanetary File System (IPFS) [11] is a peer-to-peer distributed file system. IPFS uses content-based addressing mechanism. Problem of single point failure can be solved by using IPFS. The advantage of IPFS over traditional data storage system is that there is no central server. Also, data is distributed and stored at different (nodes) on the network. Proposed system uses IPFS to store the data. When user uploads file to IPFS that files gets divided into number of chunks and stored on all peers of the network. After storing the file, IPFS returns cryptographic hash key [11] for a particular file.

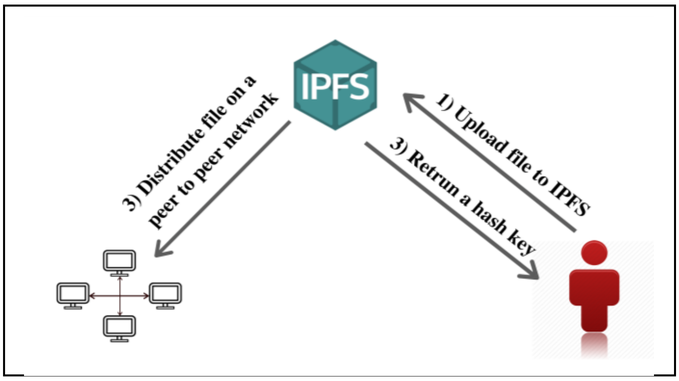

Figure 2.3 – IPFS

2.1.3 Smart Contract

Smart contracts [3], [14] are a kind of computer protocols that can be self-executed and self-verified once formulated and deployed without the need for human intervention.

Smart contract is deployed in the proposed system to check whether user is authentic or not. Smart contract prevents system from eavesdropping attack. It is highly difficult for threat agents to breach the system due to smart contracts. Data integrity is also ensured by the smart contract in the proposed system.

Deployment of smart contract [1] is as shown in fig 2.4

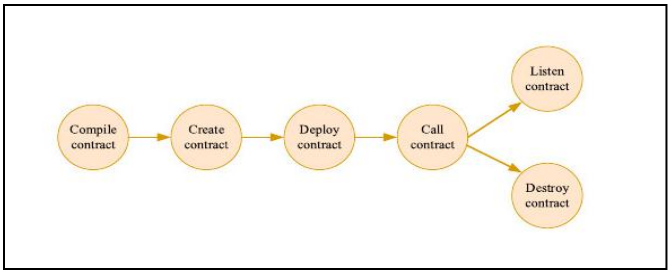

Figure 2.4 – Deployment of smart contract

3. RESULTS

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.

4. FUTURE ENHANCEMENT

The system can further be improved by adding more functions in it. Thus, system can be used for as a regular social networking application. Sharing photos, videos and communication facilities like highly secured voice calling, video calling can also be added to the system in the future. Along with this, security model used in the system can be implemented for system to ensure data security.

5. CONCLUSION

This paper proposes the design and architecture of an advanced as well as secured web application for storing and sharing the data. A simple, affordable, easy to use and most secured system is proposed to solve the data security issues like integrity, authenticity and data unavailability.

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: Mar. 25, 2018.[Online].Available:https://ethereum.github.io/yellowpaper/paper.pdf

[4] D. Hopwood, S. Bowe, T. Hornby, and N. Wilcox, “Zcash protocol specification,” Zerocoin Electric Coin Company, Oakland, CA, USA, Tech. Rep. 2016-1.10, 2016.

[5] Blockchain for Financial Services. Accessed: Mar. 25, 2018.[Online].Available:https://www.ibm.com/blockchain/financial-services

[6] Blockchain for Supply Chain. Accessed: Mar. 25, 2018. [Online].Available:https://www.ibm.com/blockchain/supply-chain

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

[8] Proof of Existence. Accessed: Mar. 25, 2018. [Online]. Available: https://proofofexistence.com

[9] A Decentralized Network for Internet of Things. Accessed: Mar. 25, 2018. [Online]. Available: https://iotex.io

[10] S. Wilkinson, T. Boshevski, J. Brandoff, and V. Buterin, “Storj a peerto-peer cloud storage network,” White Paper. Accessed: Mar. 25, 2018. [Online]. Available: https://storj.io/storj.pdf

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

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

[13] Ethereum Homestead Documentation. Accessed: Mar. 25, 2018. [Online]. Available: https://readthedocs.org/projects/ethereum-homestead

[14] Ethereum Blockchain App Platform. Accessed: Mar. 25, 2018. [Online]. Available: https://www.ethereum.org

BIOGRAPHIES

Mihir Nevpurkar
Student at Dept. of Information Technology, P.E.S. Modern College of Engineering, Pune, Maharashtra, India

Chetan Bandgar
Student at Dept. of Information Technology, P.E.S. Modern College of Engineering, Pune, Maharashtra, India

Ranjeet Deshmukh
Student at Dept. of Information Technology, P.E.S. Modern College of Engineering, Pune, Maharashtra, India

Jay Thombre
Student at Dept. of Information Technology, P.E.S. Modern College of Engineering, Pune, Maharashtra, India

Rajashri S Sadafule
Asst. Professor at Dept. of Information Technology, P.E.S. Modern College of Engineering, Pune, Maharashtra, India

Suhasini L. Bhat
Asst. Professor at Dept. of Information Technology, P.E.S. Modern College of Engineering, Pune, Maharashtra, India