A REVIEW ON BLOCKCHAIN-BASED DATA SHARING

Vikas Pitambar Narkhede
M.E CSE Student
Deparment Of Computer Engineering
SSBT's COET,Bambhori
vikaspn@hotmail.com

Satpalsing Rajput
Assistant Professor
Deparment Of Computer Engineering
SSBT's COET,Bambhori
rajputsatpal@gmail.com

Abstract

In traditional cloud storage system has centralized storage system. if failure then collapse all the systems. Decentralized storage system no problem if failure. In development system of blockchain technology has distributed ledger technology (DLTs) these technology solve the problem of centralized storage failure. In this paper blockchain technology implements a data sharing system over decentralized storage. In this system data sharing between data owner and data user. data owner share with encrypted data to data user without opening the key.

Keywords: *Blochchain, Smart Contract, IPFS*

1. Introduction

A blockchain is a sequence of block that use to distribute trust records across the network control by p2p network so the record is valid transaction and secured because every block has its own hash and previous block hash it does not any change or modify its hash. It is not centrally control or managing.All the transaction are transparent and trust to any other. [1].

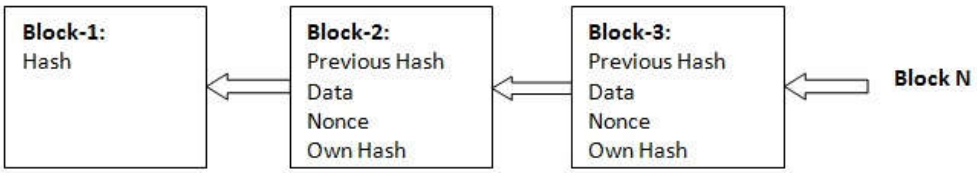

Fig. 1 Structure of BlockChain

Details of blockchain components are

- Index(Block 1) - The position of First block has index 0 or Genesis block .
- Previous Hash- Check it is valid or not previous block.
- Time Stamp- When the new block is added the information store at that time.
- Data - The information store on block.
- Nonce - Number generation of new block.
- Hash - hash is generated for current block.

All the block are connected sequentially the above component index, previous hash, data, nonce, own hash used to creation of block. [1].

IPFS is a InterPlanetary File System protocol design by Juan Benet and the protocol transfering the file between server to client over internet IPFS using P2P

method for storing. It is content addressable storage system combine with distributed hash table .The main advantage of IPFS is data immutability and speed. Single node did not depends on any nodes in case failure.IPFS consume low bandwidth. And prevent from DDos attrack.

Normally Contract is in document form or agreement between the parties. but Smart contract is a computer Program the concept is given by Nick Szabo. Smart contract integrated with blockchain. Solidity is programming language to make smart contract in Ethereum blockchain. A program made to specific rules and term of contract stored in blockchain, not a central authority like decentralized and transfer asset through smart contract.Smart contract is open distributed ledger, no trust issue not any involved third party. A program fully automatically excecuting.

2. Related Work

Yue Fu et al. in 2017 [4] described Blockchain will be directly applied on cloud-storage model. Every node is either space requirement or provider. Due to the large volume of data, we have to place key metadata of these data into blockchain system instead of store large data. Any node wants to store data they request to the provider.Provider put the information of key as a metadata in blockchain and the key decrypt them by its private key and get the information about location of data.

LI Yue et al. in 2017 [5] described using the smart contract solving the security problem self executing the instruction it is decentralized model for data sharing system without involve trusting any other parties.

H. Shafagh et al. in 2017 [6] described The P2P cloud storage (e.g., STORJ, Sia, Filecoin) is an interesting application of blockchain as it provides a decentralized data storage facility without involving any trusted third party or a client server architecture. The decentralized data storage will help to eliminate the most traditional data failures and outages by increasing the security, privacy, and control of the data.

Xia et al. 2017 [7] proposed a blockchain-based data sharing system access the medical record to data user and data owner from shared storage shows its identity and keys were confirmed.They used the work of secure cryptographics procedures to ensure proficient access control to delicate shared information. The system that adequately addresses the entrance control difficulties identified with delicate information store on inside the cloud.

Elena Kara 2017 [8] describe store the medical and health event on metadata just like an indetity of supplier, visit, patient. And all other record store in separate cloud for example if patient visits a two hospital they will store the data about him in two database. If hospital have to communicate they will use mediator like web services,email. In scenario where blockchain is applied,all the record are store in universal health cloud.and then hospital create a blockchain transaction with metadata and url to the record in the cloud. When the patient visits the second hospital, it provide the key in order to read the Blockchain transactions.

3.Problem Defination

Blockchain is decentralized model framework that is kept up by all node inside the system. User encrypt the data and metadata. Every node should store the copy inside the blockchain. if unmanageable size of data store in blockchain tragically, known as blockchain bloat. Subsequently, some key data of the information are store into block rather than full information. The information is in hash. At that point, full information are store in cloud.

problem statement along with its solution for the work contained in this mechanism is provided. Metadata using with blockchain-based architecture. Blockchains aren't general purpose databases. It is not to store data on the blockchain because it can quickly scale to an unmanageable size and cause the matter of Blockchain Bloat [4]. Therefore, use the blockchain to manage the identity and access management on the network by storing small quantity of metadata information of data files.

an overview of the problem statement along with its solution for the work contained in this information is provided. In Metadata, Additional information that can be stored along with the transaction. this is where relevant information can be added.

4.Proposed Work

Blockchain as a metadata store. data is store on within the blockchain forever and may be retrieved using hash as an identifier. we storing only small amount of instead of full data. this can be done by sending a simple transaction with metadata. we are able to store its hash, file location, and the other data that we have a tendency to view as essential. For privacy and security reasons we are able to cipher this data before we have a tendency to insert it into the blockchain. A sample of this data size in KB.

Data-sharing method is data are encrypted by data owners. Firstly the data user request to the data owner .the data owner encrypt the data and upload to cloud secondly the information about data are enclosed in encrypt key and store in metadata of blockchain.user decrypt the key and get the information of data location and then download the data and decrypt.

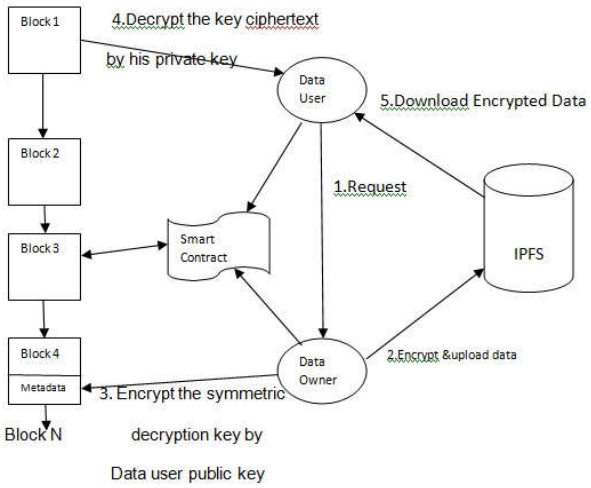

Figure 2 Proposed System Architecture

5.Conclusion

Blockchains are an important new form of information technology, a decentralized infrastructure and organizational system that is universal, global, secure, and granular. Blockchain ensures data trustability, and the automated execution of the smart contract provides protection for data security sharing. The decentralized storage approach can solve single point of failure in traditional cloud storage systems. At the same time, compared to centralized storage, it also has a series of advantages such as low price and high throughput.

6. References

[1] S. S. N. L. Priyanka and A. Nagaratnam, “Blockchain evolution - a survey paper," IJSRSET, 2018.

[2] S. Wilkinson and J. Lowry, “Metadisk: Blockchain-based decentralized file storage application," http://metadisk.org/metadisk.pdf

[3] S. Wang, Y. Zhang, and Y. Zhang, “A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems," IEEE, 2018.

[4] Y. Fu, “Meta-key: A secure data-sharing protocol under blockchain-based decentralized storage architecture," cs.DC, 2017.

[5] Li. Yue, H. Junqin, Q. Shengzhi, and W. Ruijin, “Big data model of security sharing based on blockchain," IEEE, 2017.

[6]Hossein Shafagh,Hossein Shafagh,Lukas Burkhalter,Simon Duquennoy,"Towards Blockchain-based Auditable Storage and Sharing of IoT Data",ACM Nov 3, 2017.

[7] Q. Xia, E. B. Sifah, A. Smahi, S. Amofa, and X. Zhang, “Bbds:blockchain-based data sharing for electronic medical records in cloud environments," Information, vol. 8, no. 2, p. 44, 2017.

[8] Elena Kara_loski and A. Mishev, “Blockchain solutions for big data challenges," IEEE EUROCON, 2017.

[9] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, “Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," IEEE, 2016.

[10] M. Gosavi and T. Maktum, “Security and e_ciency enhancement in attribute based distributed data sharing," IJSTE, 2017.

[11] P. M. Salunke and S. Kumar, “Decentralized and secured data sharing in distributed cloud environment," IJETT, 2016.

[12] S. K. Sangode and H. K. Barapatre, “Generate distributed metadata using blockchain technology within hdfs environment," IRJET, 2018.

[13] Garca-Barriocanal, S. Sanchez-Alonso, and M.-A. Sicilia, “Deploying metadata on blockchain technologies," researchgate, 2017.