IOSR Journal of Engineering (IOSR JEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 55-58

Storage Management using Blockchain

Burhanuddin Rampurawala[1], TejPatel[2], Amar Pendhari[3], Foram Shah[4]
[12 3 4](Computer Engineering, Atharva College of Engineering/ University of Mumbai, India)

Abstract: *Blockchain technology is known to be the driving force of the next fundamental revolution in information technology. Cloud data is metadata that records the history of the creation and operations performed on a cloud data object. Secure data provenance is crucial for data accountability, forensics and privacy. In this paper,in the proposed system a smart contract will store the metadata like the file size, type of file, created timestamp, updated timestamp, deleted timestamp, and the hash of the file which will act as a unique identity of the file. This unique identity will help us to fetch the file and will be the proof that the file was not tampered with. The data is stored on a peer-to-peer network of nodes, using a data structure called Directed acyclic graph. DAG breaks the files and stores it in small pieces across the nodes. The storage system makes the files available even if central websites go offline or government authorities censor the content. One can also get a good network speed as it gets the file from the node that is closer to you.*

Keywords: *Blockchain, peer to peer, Decentralized network, IPFS,* ***,*** *Ethereum.*

I. Introduction

Decentralisation is understood as the transfer of authority from a central entity to a more localized and 'liberal' system. The concept itself has been around for a while and an earlier concept could be paralleled to the introduction of the Internet where the spread of information was democratized. The term is now being coined against Blockchain technologies and applications like Bitcoin and Ethereum which are decentralized financial transactions and computing power. Each block contains a cryptographic hash of the data of the previous block. The nonce is calculated by the miners by solving a cryptographic puzzle to propose the next block in the chain. It is known as proof of work. The blockchain is said to be immutable because of its cryptographic properties. But this does not mean that changing the data is impossible. It means that it is extremely hard to change the data and any change can be easily detected. A merkle tree is a binary tree with hash pointers.

A merkle tree is a structure that allows for efficient and secure verification of content in a large body of data. The advantage of using merkle trees is that proving membership requires O(log(n)) steps. Also, in a sorted merkle tree, non-membership can also be proved in O(log(n)) steps. The first block is known as the genesis block.Theblockchain is essentially a distributed account database,which is composed of a chain of data blocks generated through cryptographic correlation. Each data block contains information which is valid for multiple network transactions.Once the data has been verified and added to the blockchain,it will be permanently stored unless someone can control more than 51% of the nodes at the same time. The modification of the database on a single node is invalid, this property makes the data stability and reliability of the blockchain excellent.

The first blockchain was conceptualized by Satoshi Nakamoto 2008 and is currently used primarily in digital currencies similar to Bitcoin. The distributed and non-tampering features of blockchain make it favored in many industries, especially in the financial sector. However, until now, only a small number of applications have been put into use in the realistic environment.Therefore, in the face of the tracking data about agricultural products, we hope that we can use blockchain technology to prevent tampering to ensure data security. However, compared with other industries, the internet of things has a greater amount of data and storage pressure. In order to achieve the consensus of distributed nodes, the block generation speed and transaction processing capacity of blockchain are limited, so it is not possible to directly apply the blockchain technology to store a mass of sensor data.On the other hand, the blockchain system, which focuses on the transactions of users, we can store the data by writing it into transactions, but with the transaction rate limit of blockchain, there is a bottleneck in data throughput.More importantly, relying on the blockchain itself, it is hard to quickly store or query all the hash bulk data in different blocks through the identity defined by us

II. Related Work

2.1 Secured Data Storage Scheme based on Blockchain for Agriculture[1]

Their proposed system uses blockchain to track agriculture products . Here Idea is to use blockchain technology with Internet of things to ensure data security. Agricultural products are bound with an IOT sensor module, so that the sensor can acquire the data of the products and upload it to the server in real-time. The server then uses a data structure to store data on blockchain, concurrently the system can efficiently query the data and provide it to the front-end application.

2.2 BlockStore: A Secure Decentralized Storage[2]

This Blockstore provides a decentralized framework for file storage. The system's primary motivation is to efficiently utilize storage resources of users. Users often have un-utilized or underutilized storage on their devices. They can choose to host their storage resources when they are not in use. Users rent storage from the host for a fee for a fixed period and release back after the time expires.

2.3 Endolith: A Blockchain-based Framework to Enhance Data Retention in Cloud Storage[3]

Endolith, an auditing framework for verifying file integrity and tracking file history without relying on third party, uses a smart contract-based blockchain system. Endolith hashes file on creation or modification and stores metadata to keep track of these files. Endolith uses a File System API for creation, modification and deletion of files.

III. Methodology

Agile Practice Development is being used, to meet the ever changing business needs for the product, product has to be made iteratively all the while also providing an efficient and quality output. Also scaling up the development process as the product reaches its completion phase. Other methodologies that will be used are:

3.1 Smart-Contracts:

The main logic of the system depends on the smart contract. Ethereum smart contracts are immutable computer programs that run on blockchain. A smart-contract will be the brain of our system, it will have the tasks to store file meta-data on the blockchain.

3.2 Responsive User Interface:

A Responsive User Interface is the key to a good application. The issue with web applications is that different browsers have different bugs, for example memory leaks, layout issues, clicking issues etc, all these have to be taken care of during development for users seamless experience. Also, the website layout on mobile browsers might look smaller as compared to the desktop browsers, sometimes some layout might be missing or the views get arranged in a disorderly fashion, due to size of the mobile screen. All these issues should also be taken into consideration during development.

3.3 State Channel:

State channels are basically two-way pathways opened between two users that want to communicate with each other in the form of transactions. Each participant in the channel signs these transactions with his private key to ensure that they are undeniably true and authorized. After all the transactions are complete, the final state of the state channel is stored in the blockchain, ignoring all the previous transactions. This reduces fees as now the fee will be charged for only one transaction.

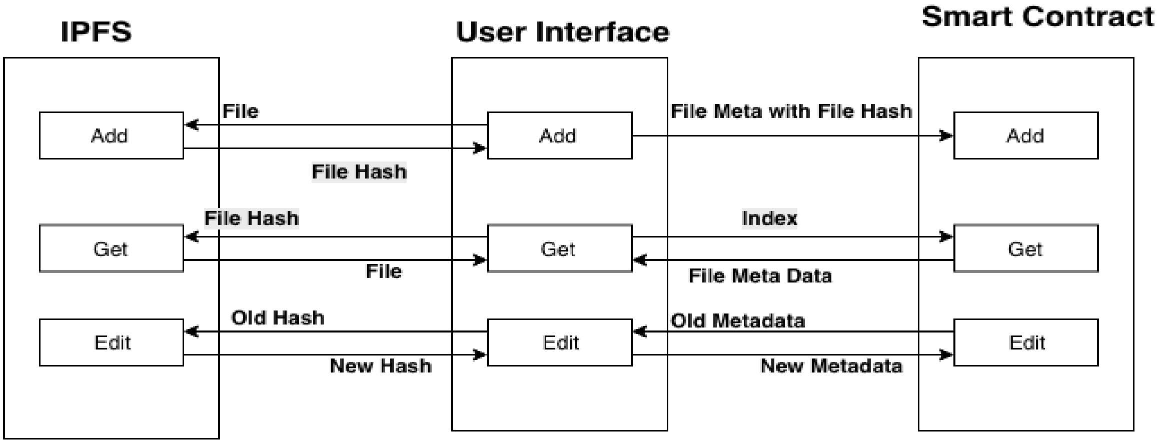
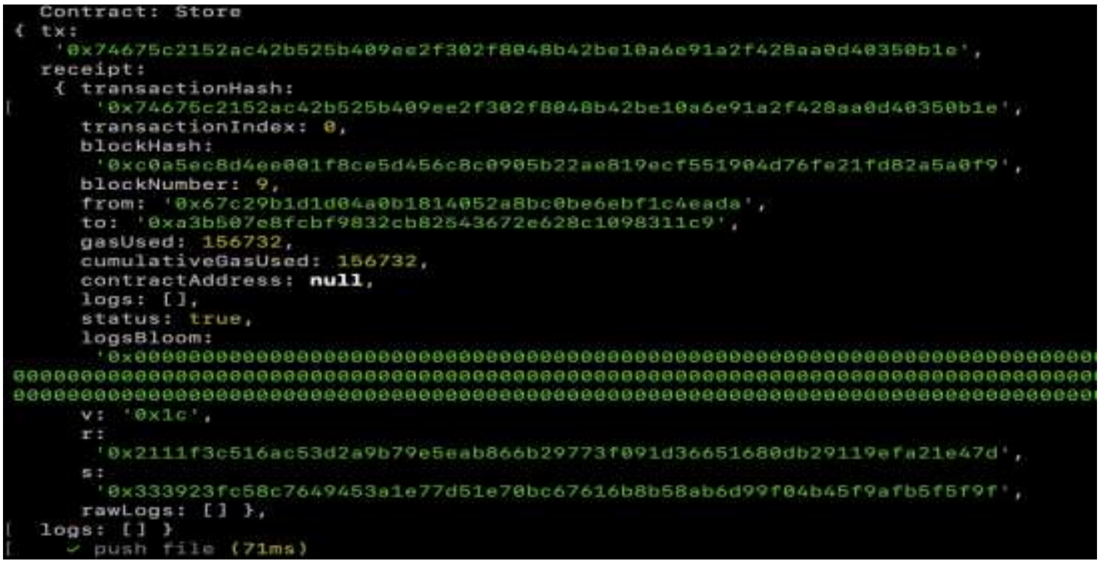


Fig 1. Working of Storage Management using IPFS(Inter Planetary File System

IV. Results

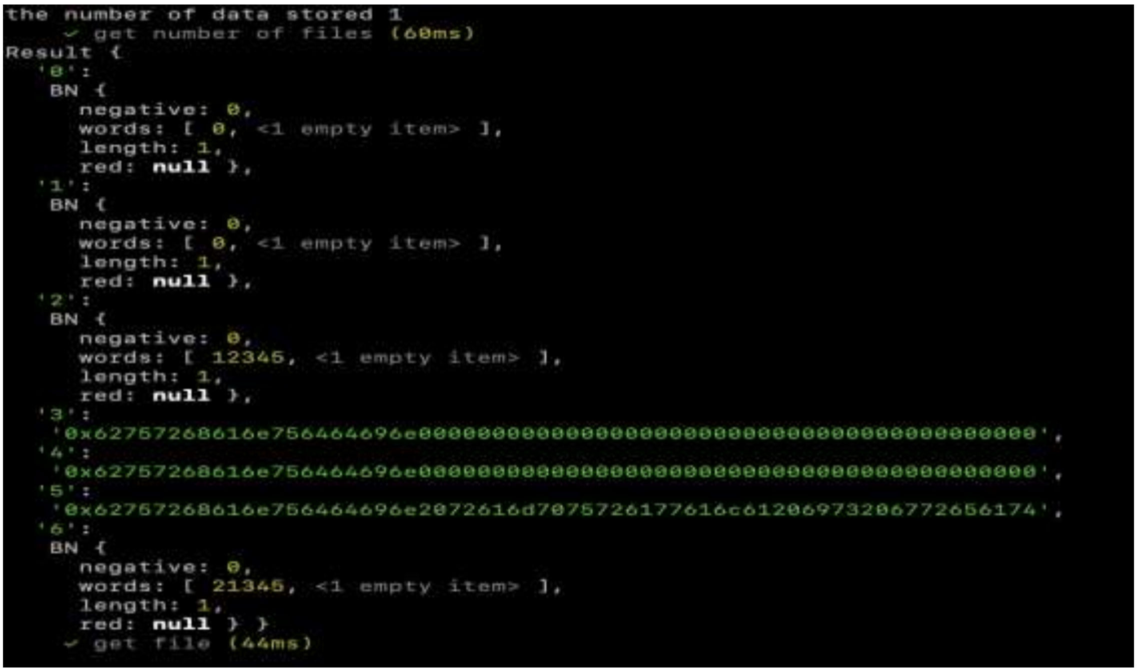
We store the metadata on the ethereumblockchain and wrote the below tests. Below Fig 2(a) & (b) shows test on application for storage of file metadata, to fetch the number of files stored and to fetch the file's metadata. When we store file metadata we get all the details of the transaction (A function call to change the state of blockchain is called a transaction). This transaction takes some fees which is calculated in gas and paid with ethereum. When a function to get number of files is called we get a length of the file metadata array in

Integer type. To retrieve files we call getFile function with the index of file, this index is of type integer. The function returns metadata mapped with the provided index in the function parameter.



```
   Contract: Store
{ tx:
   '0x74675c2152ac42b525b409ee2f302f8048b42be10a6e91a2f428aa0d40350b1e',
   receipt:
    { transactionHash:
[      '0x74675c2152ac42b525b409ee2f302f8048b42be10a6e91a2f428aa0d40350b1e',
      transactionIndex: 0,
      blockHash:
       '0xc0a5ec8d4ee001f8ce5d456c8c0905b22ae819ecf551904d76fe21fd82a5a0f9',
      blockNumber: 9,
      from: '0x67c29b1d1d04a0b1814052a8bc0be6ebf1c4eada',
      to: '0xa3b507e8fcbf9832cb82543672e628c1098311c9',
      gasUsed: 156732,
      cumulativeGasUsed: 156732,
      contractAddress: null,
      logs: [],
      status: true,
      logsBloom:
       '0x000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
      v: '0x1c',
      r:
       '0x2111f3c516ac53d2a9b79e5eab866b29773f091d36651680db29119efa21e47d',
      s:
       '0x333923fc58c7649453a1e77d51e70bc67616b8b58ab6d99f04b45f9afb5f5f9f',
      rawLogs: [] },
[  logs: [] }
[    ✓ push file (71ms)
```

Fig. 2(a) Output of metadata fetching



```
the number of data stored 1
    ✓ get number of files (60ms)
Result {
  '0':
   BN {
     negative: 0,
     words: [ 0, <1 empty item> ],
     length: 1,
     red: null },
  '1':
   BN {
     negative: 0,
     words: [ 0, <1 empty item> ],
     length: 1,
     red: null },
  '2':
   BN {
     negative: 0,
     words: [ 12345, <1 empty item> ],
     length: 1,
     red: null },
  '3':
   '0x62757268616e756464696e000000000000000000000000000000000000000000',
  '4':
   '0x62757268616e756464696e000000000000000000000000000000000000000000',
  '5':
   '0x62757268616e756464696e2072616d7075726177616c6120697320677265617 4',
  '6':
   BN {
     negative: 0,
     words: [ 21345, <1 empty item> ],
     length: 1,
     red: null } }
    ✓ get file (44ms)
```

Fig. 2(b) Output of metadata fetching

V. Conclusion

Blockchain technology is going to be the future of the internet, also known as ‘WEB 3.0’. The storage that we provide can help users to upload files, edit files, share files and also at some point files like music, videos, pictures etc could be sold and bought using Ethereum or any other cryptocurrency. Also, the storage can be used to host websites same as hosting files. Finally all the meta-data is stored on the blockchain and the data is impossible to manipulate as the chain becomes bigger and bigger.

References

[1]. Chao Xie, Yan Sun and Hong Luo “Secured Data Storage Scheme Based on BlockChain for Agricultural Products Tracking”, *2017 3rd International Conference on Big Data Computing and Communications (BIGCOM), Pp. 45-50*, 10 August 2017.

[2]. SushmitaRuj, Mohammad ShahriarRahman, AnirbanBasu, and ShinsakuKiyomoto “BlockStore: A Secure Decentralized Storage Framework on Blockchain”, *32nd International Conference on Advanced Information Networking and Applications (AINA),Pp. 1096-1103*, 16 May 2018.

[3]. Thomas Renner, Johannes Müller and Odej Kao "Endolith: A Blockchain-Based Framework to Enhance Data Retention in Cloud Storages", *26th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP), Pp. 627-634,* 21 March 2018.

[4]. https://bitcoin.org/bitcoin.pdf,*Bitcoin White Paper*

[5]. https://github.com/ethereum/wiki/wiki/White-Paper, *Ethereum White Paper.*

[6]. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system,http://bitcoin.org/bitcoin.pdf," 2008.

[7]. P. Maymounkov and D. Mazieres, "Kademlia: A peer-to-peer information system based on the XOR metric," in Peer-to-Peer Systems, First International Workshop, 2002.

[8]. H. Shacham and B. Waters, "Compact proofs of retrievability," J. Cryp-tology, vol. 26, 2013.

[9]. S. Wilkinson, T. Boshevski, J. Brandoff, and V. Buterin, "Storj a peer-to-peer cloud storage network," 2014.

[10]. I. Miers, C. Garman, M. Green, and A. D. Rubin, "Zerocoin: Anonymous distributed e-cash from bitcoin," in 2013 IEEE Symposium on Security and Privacy, 2013.