International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 03 | Mar 2019 www.irjet.net p-ISSN: 2395-0072

Blockchain based Secure Data Storage

Kumar Bhosale[1], Kadaya Akbarabbas[2], Jadhav Deepak[3], Awani Sankhe[4]

[1,2,3]Student, Dept. of Computer Engineering, University of Mumbai, India
[4]Professor, Dept. of Computer Engineering, University of Mumbai, India

---

Abstract - *Today's cloud storage is completely dependent exclusively on large storage providers. These storage providers act as trusted third parties, which transacts the data for storing, sending and receiving the data from an organization. This type of model poses a number of issues like high operational cost, data availability and data security.*
In this paper, we introduce a project that uses blockchain technology to provide a secured distributed data storage. The system allows the user to upload the data through Inter Planetary File System (IPFS), which distributes the data content to cloud nodes at global level network and ensures data availability by fetching that data files through URLs using the hash values of the files uploaded to IPFS. So the one who has the hash value of that particular data which was uploaded on IPFS network can only access the file from IPFS network. Finally, the system supports the privacy of data by ensuring the immutability property of the blockchain by storing them on distributed global network. The project is implemented using smart contracts and tested on Ethereum blockchain platform using Ganache Blockchain.

Key Words: **Inter Planetary File System, Cloud storage, Ethereum, Ganache, Blockchain, Smart contracts etc.**

1. INTRODUCTION

In the current era, there has been a problem of storing the huge amount of data for big organizations, which work globally. So, these organizations have turned to cloud storage, which has excellent properties for storing and transferring the data. But these cloud storage providers act as trusted third party organization. This results in various security and confidentiality problems. To overcome this problem this paper presents the system which provides the storing of data with the help of Blockchain based Inter Planetary File System.

1.1 What is Blockchain?

A blockchain,[1][2][3] originally block chain,[4][5] is a growing list of records or data, called blocks, which are linked to each other using cryptography.[1][6] Each block contains a cryptographic hash of previous block,[6] a timestamp, and transaction data.

By design, a blockchain does not allow modification of the data i.e. blockchain is immutable. It is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way".[7] A blockchain is typically managed by a global peer-to-peer network collectively bonding to a protocol for communication between inter-node and validation of new blocks, to use this distributed ledger. Once stored, the data in any block cannot be changed retroactively without alteration of any of the blocks within a blockchain, which requires validation by consensus (a general agreement) of the network majority. Even if blockchain records are not unalterable, blockchain may be considered secured by its design and illustrating a distributed networked computing system with high Byzantine fault tolerance. Decentralized consensus for validating has been claimed with a blockchain.[8]

1.2 What is IPFS?

IPFS is Inter Planetary File System, which is open source. Creator of IPFS is Juan Benet. It is an open source distributed protocol, which works with the function of providing global file system for all computing devices. Using IPFS within a blockchain transaction, you can place immutable, permanent links. In other words IPFS is a protocol and network designed to create a content-addressable, peer-to-peer method of storing and sharing Hypermedia in a distributed file system.[9]

Each file and all blocks within it are given a unique identifier, which is a cryptographic hash. File structures in IPFS are linked to each other using Merkle links and every file can be found by using a decentralized naming system called IPNS, which gives human-readable names. The implementation of this Merkle Directed Acyclic Graphs (DAGS), which illustrates the linking of the files, is important to the underlying functionality of the IPFS protocol, but it is more complex than the scope of this paper.

2. IMPLEMENTATION

2.1 Installing Dependencies

There are some dependencies, which are needed to be installed and configured in order to further get started with the project building.

2.1.1 Ganache

Fig -1: Ganache

This dependency is a personal blockchain, which is a local development blockchain that can be used to act as a public blockchain. Ganache is used to deploy smart contracts and for running tests. Here you have a personal blockchain network running. Ganache provides 10 accounts with 100Ether to test our smart contracts on local blockchain bases.

2.1.2 Node.JS

Since we have a private or local blockchain running, we need to configure our environment for developing smart contracts. For that, we will require Node Package Manager or NPM, which includes Node.js

2.1.3 Truffle Framework

Fig -2: Truffle framework

Truffle Framework is an essential tool for developing Ethereum smart contracts. It uses the Solidity programming language to develop smart contracts. Truffle framework provides following functionalities:

- Client Side Development
- Script Runner
- Network Management
- Development Console
- Deployment & Migrations
- Smart Contract Management
- Automated Testing

2.1.4 Metamask

Fig -3: Metamask

Since current browsers do not support the connection to blockchain networks. Adding Metamask extension to the browser, converts the browser into a blockchain browser. Using Metamask, we can connect our Ganache accounts to deploy our project. MetaMask is also used to manage the personal accounts, which are used to connect to the blockchain and transaction purposes.

MetaMask is an extension or plugin that allows us to visit the distributed web in your browser. It allows you to run Ethereum Decentralized applications right in your browser without running a full Ethereum blockchain.

MetaMask includes a secure identity vault, providing a user interface to manage your identities on different sites and sign blockchain transactions. We can install the MetaMask add-on in Chrome, Firefox and Opera.[10]

2.2 Project Setup

Our proposed system involves a user who wants to upload the data or any file to the IPFS. We are configuring private local blockchain provided by Ganache and integrating it to web browser using Metamask extension.

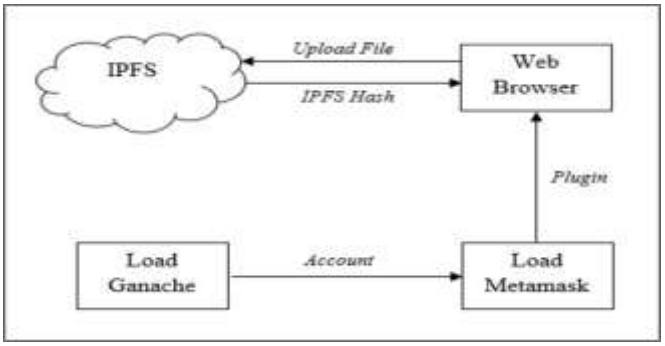

Fig -4: File Upload

Workflow: As mentioned above first the user needs a local blockchain network, which is provided by Ganache. The accounts provided by Ganache are added to Metamask for transaction purpose. Per transaction, a specific amount of Gas is needed in the form of Ether. Ether is a type of crypto token that fuels the blockchain network.

Ganache provides 10 accounts; each account has 100Eth, which can be used for transactions. Using these accounts, we can run tests, execute commands and inspect state while controlling how the chain operates on a personal Ethereum blockchain. From these 10 accounts, any one account is used to log on in Metamask using the private key provided by the particular account in Ganache.

Now, as our Web browser supports blockchain network, we can now upload the files through our own designed user interface (UI).

In our user interface, the files are uploaded on to the Inter Planetary File System (IPFS). When a file is selected for uploading process a popup is generated by Metamask, which verifies the transaction. After confirming the transaction the Ether from our account is deducted, else we can reject the transaction. Since the file is uploaded, IPFS generates a unique IPFS hash value of that file which is obtained in console of web browser.

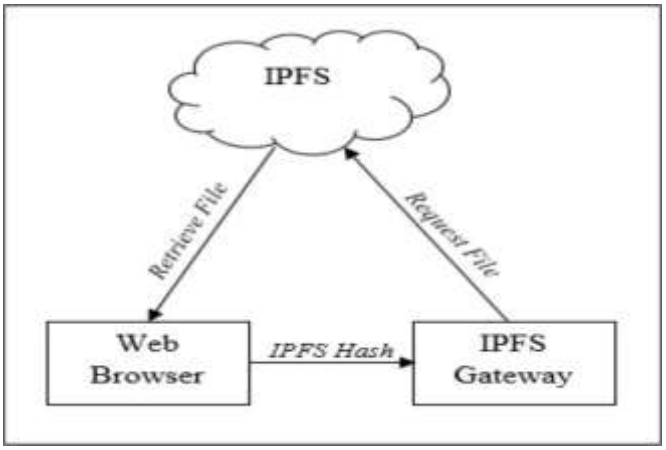

Fig -5: File Retrieval

The process of retrieving the file back from IPFS requires the previously obtained IPFS hash value, which is generated after uploading the file. IPFS Gateway (https://ipfs.io/ipfs/) is required. We have to put the IPFShash in the URL, IPFS will search for the file, and preview is shown. Thus, the file is retrieved back from the IPFS System.

3. RESULTS

As we are using Linux Mint Cinnamon 19.1 for this project implementation so the below results are been tested on the linux operating system. Following screenshots are the steps for usage of the project, which shows the actual procedure of uploading a file on IPFS system using Blockchain successfully. Uploaded file can be retrieved using the IPFS Gateway (https://ipfs.io/ipfs/).

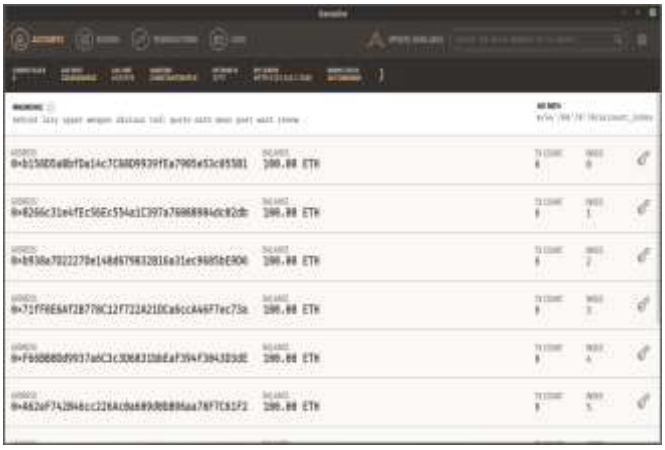

Fig -6: Initiating Local Blockchain

First, we need to initiate the blockchain by starting the Ganache. Then we need to choose an account from these 10 accounts as shown in fig.6 provided by Ganache to be logged in to Metamask.

Fig -7: User Interface

After login in to Metamask, try uploading a file from user interface as shown in fig.7.

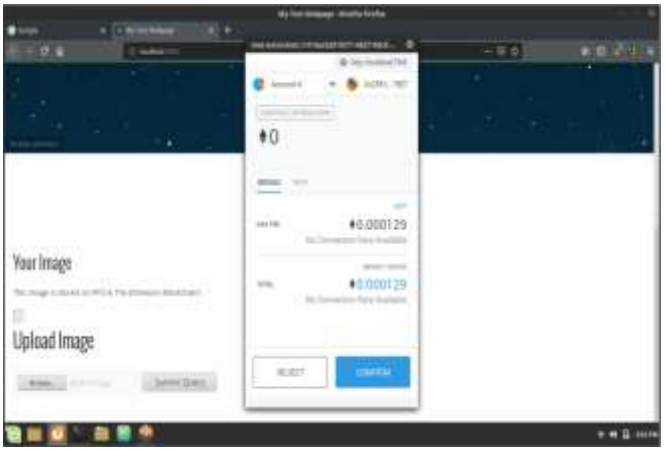

Fig -8: Transaction verification

Submitting of file needs to be verified. Metamask as shown in fig.8 does this verification process.

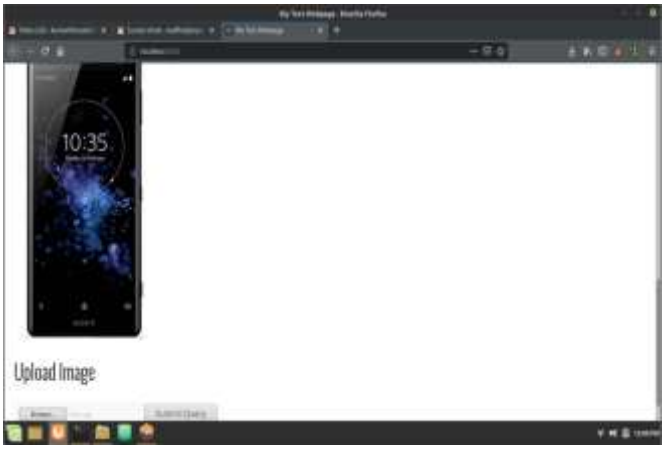

Fig -9: Transaction verification

As soon as the transaction is confirmed, the file is uploaded on to the IPFS. After uploading the file, IPFS gives back the hash value of that file so that it can be retrieved back. In fig.8 an image file is uploaded which is previewed by using the hash value as shown in fig.9 provided by IPFS as it was uploaded.

4. CONCLUSION

Project outlined in this paper is our own implementation of Data Storage using IPFS and local blockchain. Although still, there remains much to do in terms of development and improvement in this model. Blockchain based Secure Data Storage is created as a model with IPFS as storage by using the dependencies viz. NPM, Truffle, Metamask and Ganache. Files are stored in the IPFS and the hash obtained after uploading is use to retrieve the File back again. Thus a victorious result is obtained and is implemented as per the idea described in the paper. It also clear the concept how IPFS and Blockchain network can be integrated to develop a Decentralized Storage application.

REFERENCES

[1] "Blockchains: The great chain of being sure about things". The Economist. 31 October 2015. Archived from the original on 3 July 2016. Retrieved 18 June 2016. M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[2] Morris, David Z. (15 May 2016). "Leaderless, Blockchain-Based Venture Capital Fund Raises $100 Million, And Counting". Fortune. Archived from the original on 21 May 2016. Retrieved 23 May 2016.K. Elissa, "Title of paper if known," unpublished.

[3] Popper, Nathan (21 May 2016). "A Venture Fund With Plenty of Virtual Capital, but No Capitalist". The New York Times. Archived from the original on 22 May 2016. Retrieved 23 May 2016.

[4] Brito, Jerry; Castillo, Andrea (2013). Bitcoin: A Primer for Policymakers (PDF) (Report). Fairfax, VA: Mercatus Center, George Mason University. Archived (PDF) from the original on 21 September 2013. Retrieved 22 October 2013.

[5] Trottier, Leo (18 June 2016). "original-bitcoin" (self-published code collection). github. Archived from the original on 17 April 2016. Retrieved 18 June 2016." This is a historical repository of Satoshi Nakamoto's original bit coin sourcecode"

[6] Narayanan, Arvind; Bonneau, Joseph; Felten, Edward; Miller, Andrew; Goldfeder, Steven (2016). Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton: Princeton University Press. ISBN 978-0-691-17169-2.

[7] Iansiti, Marco; Lakhani, Karim R. (January 2017). "The Truth About Blockchain". Harvard Business Review. Harvard University. Archived from the original on 18 January 2017. "Retrieved 17 January 2017. The technology at the heart of bitcoin and other virtual currencies, blockchain is an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way."

[8] Raval, Siraj (2016). "What Is a Decentralized Application?". Decentralized Applications: Harnessing Bitcoin's Blockchain Technology. O'Reilly Media, Inc. pp. 1–2. ISBN 978-1-4919-2452-5. OCLC 968277125. Retrieved 6 November 2016 – via Google Books.

[9] Finley, Klint (20 June 2016). "The Inventors of the Internet Are Trying to Build a Truly Permanent Web". Wired.

[10] Metamask. "https://metamask.io/"