"Air-Talk": An IPFS and Blockchain-based Private Decentralized File Sharing and Chat Application

Anuradha Jayakody[1]
Department of Information Systems Engineering, Faculty of Computing
Sri Lanka Institute of Information Technology
Malabe, Sri Lanka

Rajitha De Silva[2]
Department of Information Systems Engineering, Faculty of Computing
Sri Lanka Institute of Information Technology
Malabe, Sri Lanka

Pirabanjan Kirupaharan[3]
Department of Information Systems Engineering, Faculty of Computing
Sri Lanka Institute of Information Technology
Malabe, Sri Lanka

Sanka Tillakarathna[4]
Department of Information Systems Engineering, Faculty of Computing
Sri Lanka Institute of Information Technology
Malabe, Sri Lanka

Chapa Vidanaarachchi[5]
Department of Information Systems Engineering, Faculty of Computing
Sri Lanka Institute of Information Technology
Malabe, Sri Lanka

Sharon Shashangan[6]
Department of Information Systems Engineering, Faculty of Computing
Sri Lanka Institute of Information Technology
Malabe, Sri Lanka

Abstract: Communication is essential for all human beings. With globalization we intensively tend to use the internet for most of our communication activities. At present, most of these communication services are controlled via a central authority. Causing data to become more vulnerable, delay in retrieving information, risk of loss and issues related to the integrity and non repudiation of data. In contrast to this, technologies like Blockchain and IPFS provide distributed and decentralized platforms where it facilitates decentralized applications (D-Apps) for communication and peer-to-peer networking for storing and sharing data in a distributed file system. In this paper the project "Air-Talk" introduces a private decentralized file sharing and chat application for communication without the aid of an intermediary third party or a central server with the use of technologies like Blockchain and IPFS. Ethereum blockchain platform is used in this project and it enables Smart contracts which are used to store the messages and hashes of the shared files inside a private Blockchain providing security and traceability into the shared content preventing any alterations to the original data. A private IPFS network, a distributed file system which avoids most of the pitfalls of centralized storage solutions is used to store the files and media of this application.

Keywords: IPFS, DApp, Blockchain, Ethereum, Decentralized networking

I. INTRODUCTION

Most of the current traditional communication systems, file sharing systems and chat applications are controlled via a central server. All the communications are handled via that central server and also all the information is stored inside a central server. Due to the traditional client-server model, most of the communication systems often suffer from service unavailability during server downtime or during the situations when servers face issues related to single point of failure or DDoS attacks [1]. If the central server fails then the whole network collapses. A decentralized communication system would be able to tackle those problems in a more comfortable manner than that of a traditional centralized server-based model.

A blockchain is essentially a fault-tolerant distributed database of records of a public ledger of all transactions that have been executed and shared among participating parties [2]. This eliminates the need for a central authority to keep tracking against manipulations. All the information transferred across the network is securely and accurately stored using cryptographic hash functions. The InterPlanetary File System (IPFS) is a protocol as well as a peer-to-peer network that allows the users to store and share data in a distributed file system [3]. This facilitates the users to communicate with each other in a more efficient way without the need of a central location to store and retrieve all the data.

In this paper, the authors of the project introduce "Air-Talk", a private communication platform developed mainly by using IPFS and Blockchain. The application is based on IPFS for distributed data storage and Blockchain's Ethereum platform to securely store the messages and hashes generated by IPFS to protect those data from manipulation. The application would allow authorized users/nodes to connect into the network and communicate and share data/information among the other connected nodes. The frontend web page would always interact with the Smart Contact of this application which is deployed on the Ethereum Virtual Machine by using web3.js library. The main objective of developing this application is to emphasize the importance of using IPFS and Blockchain technology in developing modern communication systems.

The rest of the paper is structured in the following manner – A brief background about the technologies used in this research and some related work is discussed in section two. The next section is the methodology where the system overview and the overall system design is explained. Section four discusses the testing and results. The paper concluded with a summary and discussion of the current study.

II. BACKGROUND AND RELATED WORK

This section discusses the technologies, concepts and similar work that influenced to build "Air-Talk". This contains a brief introduction about Decentralized networking, IPFS and Blockchain technologies and related work.

A. *Decentralized Networking*

In simple terms decentralized network is an architecture where the workloads are distributed among several machines instead of relying on a single central server. A decentralized network has a vast range of advantages when compared with a conventional centralized network. Some of those key advantages are increased system reliability, scalability and privacy [4]. Decentralized network has an increased reliability when compared with a centralized network because there is no real single point of failure as the nodes in the network are not reliant on a single central server to handle all the requests. Also, these types of networks are much easier to scale since all that is required is to add more nodes to the network to gain more compute power. A decentralized network architecture provides greater privacy, as the information is not passing through a single point and instead passes through a number of different points. This makes it difficult to track across a network thus providing more privacy for the information being transferred inside the network.

B. *InterPlanetary File System (IPFS)*

The InterPlanetary file system (IPFS) is a protocol as well as a peer to peer network for sharing and storing hypermedia in a distributed file system. It is a content addressed file system which uniquely identifies each file in a global namespace using content addressing. Main concepts used in IPFS are Distributed Hash Table (DHT); which is used to retrieve data across nodes in the network, Block Exchange; a peer to peer file sharing protocol which coordinates data exchange between untrusted swarms, and Markle DAG; uses a Merkle Tree or a Merkle DAG similar to the one used in the Git Version Control system[5]. It is used to track change to files on the network in a distributed system [6].

There are two types of IPFS networks; Public and Private. All the information inside a public network is accessible to everyone. But most applications and solutions require control over the data transferred inside a network. Therefore, they require more privacy. IPFS private networks help to close the network for certain entities while providing all the features given in a normal public IPFS network [7]. The described project in this paper also uses a private IPFS network to provide more privacy for the data transferred inside the network while reaping most of the features provided by an IPFS network.

C. *Blockchain*

A blockchain is essentially a fault-tolerant distributed database of records of a public ledger of all transactions that have been executed and shared among participating parties [8]. A consensus of a majority of participants in the system verifies each transaction in the public ledger. With the combination of cryptography and consensus, blockchain provides a tool for increasing data integrity. There is no central server point of control. The information is stored in blocks and each block contains a transaction, a time stamp and a link to the previous block as shown below.

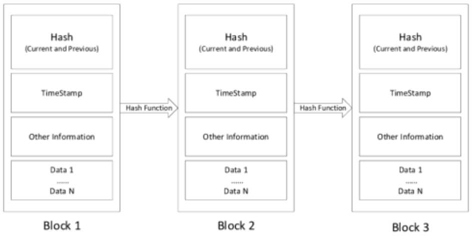


Fig.1. Blockchain Structure [9].

All blockchain structures fall into three categories; Public Blockchain architecture, Private Blockchain architecture and consortium Blockchain architecture [8]. From those three categories authors have used private blockchain architecture since those types of blockchains are controlled only by users from a specific organization or authorized users who have an invitation for participating.

Several previous works have been conducted on developing decentralized applications with the use of Ethereum and IPFS as distributed data stores. Discussed below are few of them

D. *Secure Peer-to-Peer communication based on Blockchain [10]*

This project has proposed a secure messaging solution based on blockchain technology. Throughout this research work it is explained why blockchain makes communications more secure and they have proposed a model design for blockchain based messaging maintaining the performance and security of data recorded on the blockchain, using a smart contract to verify the identities and their associated public keys, and validate the user's certificate [10]. This proposed system is entirely decentralized and allows users to exchange messages securely. Also, this guarantees the immutability of the data being shared in the network. But still this solution supports only messaging. This solution does not accommodate the transmission of large data like videos and images and also the compatibility of this solution in a private network is not discussed.

E. FileShare: Framework for secure file sharing with data provenance using Blockchain and IPFS [11]

This research introduces a decentralized application framework called FileShare for sharing files and data provenance. This solution avoids the integrity and ownership issues in the existing frameworks. This framework consists of a Decentralized application on top of Ethereum Blockchain technology which is responsible for user registration and provenance. Ethereum smart contract is used to provide traceability and visibility into the history of the shared content from its origin to the latest version. This framework still developed only for file sharing. Like text files. There are no measures taken about the exchange of videos, audios and images etc. Also, the compatibility of this solution in a private network is not discussed.

III. METHODOLOGY

This section discusses all the architectural components, design components and methodology of the project. The aim of the project "Air-Talk" is to create a file sharing application and a chat application which can be used without the aid of an intermediary third party using the technologies described in the Background section.

A. System Overview

IPFS technology has enabled a private distributed P2P network between the nodes participating in the network without an intermediary third party. The file sharing platform is built on top of this private IPFS network. Therefore, the information transferred inside the network will only be visible for the other peers who have a shared secret key. Inside a private IPFS network, each node specifies which other node it will connect to. Nodes in a private IPFS network do not respond to communications from nodes outside that network [7]. Thus, it provides the greatest level of privacy from the outside world. In addition to this, to gain more security for the information being transferred inside this network, the hash received for each information uploaded inside this network will be saved on a private blockchain. This guarantees that the data cannot be altered.

Unlike the traditional apps, the chat application introduced in "Air-Talk" avoids any single point of failure because there is no single entity which can completely control the operation. This chat application is a fully decentralized application that runs mainly using the Smart contracts deployed on the private blockchain. Each message exchange is securely stored inside the blockchain using those smart contracts.

B. System Design

Before creating decentralized applications, a private IPFS network was set up using three virtual machines with Linux Ubuntu 20.04 installed. In this phase command line was used as the main tool for installing necessary packages and configurations. All three virtual machines were given three static IP addresses during the virtual machine configurations. After installing Go and IPFS on all the nodes participating in the private network, the swarm key generation utility was installed. This swarm key allows the user to create a private network and let the peers to communicate only with those peers who share this secret key [7]. "Air-Talk" applications will run on top of this private IPFS network.

The decentralized file sharing application of this project is built mainly using Blockchain and IPFS technologies. The backend of this application is based on a Blockchain protocol called Ethereum [12]. Ethereum uses smart contracts to handle the transactions. Smart contracts are written using Solidity programming language. Angular JS is used to write the client-side application of this project. Shown below in Fig. 2 is the System Architecture diagram of the decentralized file sharing application.

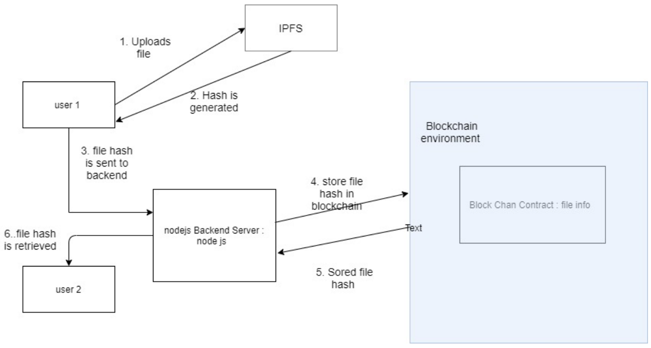

IPFS
1. Uploads file
2. Hash is generated
user 1
3. file hash is sent to backend
Blockchain environment
4. store file hash in blockchain
Block Chan Contract : file info
Text
6..file hash is retrieved
nodejs Backend Server : node js
5. Sored file hash
user 2

Fig. 2. System Architecture of file sharing application

As shown above in number 1, first the user has to upload a file to the application. When the user submits the file, the file will be stored in the IPFS. Once the file is stored in IPFS, it will provide a unique hash for that file (2). In step 3, this hash is taken to the backend server and stored in a private blockchain (4). Then the blockchain will verify the transaction before storing it in the network. To verify the transaction MetaMask [13] will be used. Once the transaction is verified successfully, the hash will be stored in the blockchain. For this the authors have used a private blockchain provided by the Ganache [14] which is a software that allows us to create a personal Ethereum blockchain which can be used to run tests and execute commands. Once the hash is saved in the blockchain no one can edit this. This adds an extra layer of security to the application. Then this hash will be retrieved from the frontend (5) and will be displayed to other users (6) so that they also can access the information.

Chat application of this communication platform is managed via Smart contracts in Blockchain. Ganache private blockchain is used in this proposal setup. Angular JS and Node JS are used to build the frontend and backend. When using this application the user has to register himself for the first time to use the application. Once a user successfully registers himself he can either use the File share application or Chat application. In the chat application the user can initiate or participate to private chats, Group chat and Broadcast chats as well. Each message exchange is handled via smart contracts written in solidity programming language. Shown below in figure 3 is the System architecture of the Chat application.

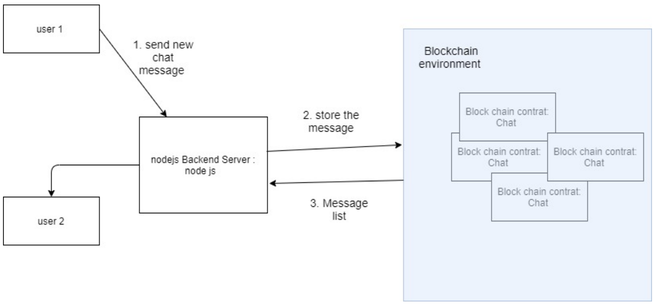
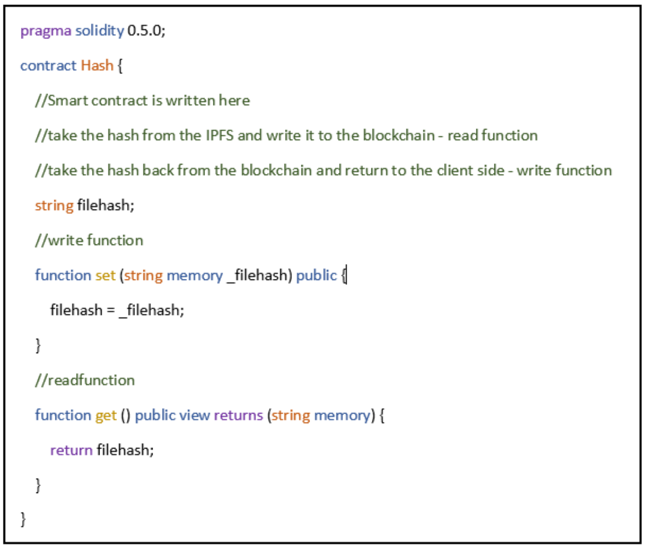

user 1
1. send new chat message
nodejs Backend Server : node js
user 2
2. store the message
3. Message list
Blockchain environment
Block chain contrat: Chat
Block chain contrat: Chat
Block chain contrat: Chat
Block chain contrat: Chat

Fig. 3. System Architecture of the chat application

Once when a user sends a message as shown in 1, it will be directly sent to the backend and then it will be stored in the private blockchain (2). Smart contract will be used to store this message and it will be stored in a message list (3) and will be retrieved from the backend to the frontend and will be displayed to the other users participating in the conversation.

Shown below in Fig. 4 is the smart contract written in the blockchain to get the hash from the IPFS and store it in the private blockchain. Similar Smart contracts are used to store the messages in the blockchain as well. This is written in Solidity programming language. Users with the hash value can view the information uploaded to the IPFS network via a unique URL given to each file inside the network.



```
pragma solidity 0.5.0;
contract Hash {
  //Smart contract is written here
  //take the hash from the IPFS and write it to the blockchain - read function
  //take the hash back from the blockchain and return to the client side - write function
  string filehash;
  //write function
  function set (string memory _filehash) public {
    filehash = _filehash;
  }
  //readfunction
  function get () public view returns (string memory) {
    return filehash;
  }
}
```

Fig. 4. Smart contract used for the blockchain

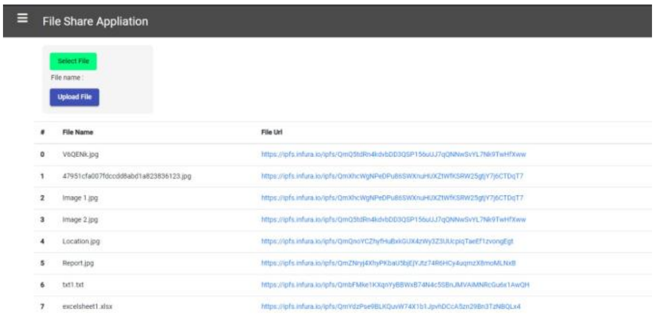
IV. RESULTS AND DISCUSSION

This section contains the testing and results of the project "Air-Talk''. In a decentralized file sharing application, a private blockchain from Ganache was used to store the hash generated from IPFS. Shown below in Table I is the private blockchain used.

TABLE I. PRIVATE BLOCKCHAIN FROM GANACHE

Blockchain Address	Balance	TX count	Index
0x3d94f3c0Fa3FeB4c0D34DA5886bDe6a76470348a	99.92 ETH	32	0
0x39146A5ABad53883a6cBC2B61780A56bEA8B5a17	100.00 ETH	0	1
0xeB4d1a5a78cAda9eB955D09678F2AbeCB49AD69E	100.00 ETH	0	2
0xAD5eE372366b558922a7426e1BeF91EE2B55F2CF	100.00 ETH	0	3
0x8616e8a736E71230363Afac27c9a66cC9Ef4f769	100.00 ETH	0	4
0x5b41D576863fA00340aD111f2a339Acbd9C7A131	100.00 ETH	0	5
0xeBC288871dB4350a50DF5ed8D275Cc92bc0B6437	100.00 ETH	0	6
0x9462FE5e15aB342645c46ef3598893111Fb565e3	100.00 ETH	0	7
0xF98e566407F015A2ebfe205c7CA995627B214Ce1	100.00 ETH	0	8
0xc7bAb69175aD8b9A41520f82b0ad87138F536f4E	100.00 ETH	0	9

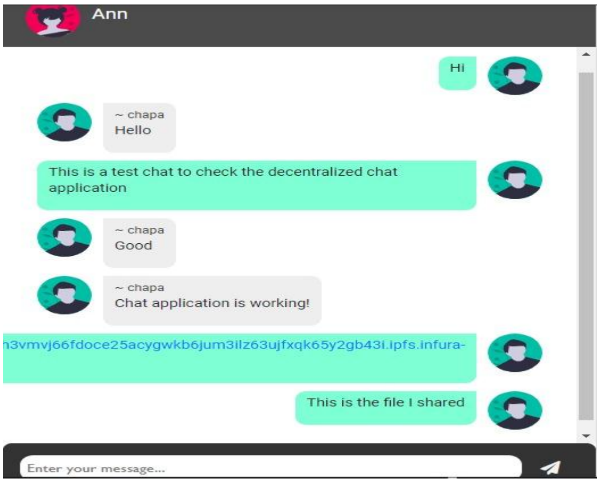
Shown below in Fig. 5 is a screenshot of the File sharing application with some files with the URLs which are uploaded to the IPFS network.



#	File Name	File Url
0	V6QENk.jpg	https://ipfs.infura.io/ipfs/QmQ5tdRn4kdvbDD3QSP156uUJ7qQNNwSvYL7Nk9TwHfXww
1	47951cfa007fdccdd8abd1a823836123.jpg	https://ipfs.infura.io/ipfs/QmXhcWgNPeDPu86SWXnuHUXZtWfKSRW25gtjY7j6CTDqT7
2	Image 1.jpg	https://ipfs.infura.io/ipfs/QmXhcWgNPeDPu86SWXnuHUXZtWfKSRW25gtjY7j6CTDqT7
3	Image 2.jpg	https://ipfs.infura.io/ipfs/QmQ5tdRn4kdvbDD3QSP156uUJ7qQNNwSvYL7Nk9TwHfXww
4	Location.jpg	https://ipfs.infura.io/ipfs/QmQnoYCZhyfHuBxkGUX4zWy3Z3UUcpiqTaeEf1zvongEgt
5	Report.jpg	https://ipfs.infura.io/ipfs/QmZNryj4XhyPKbaU5bjEjYJtz74R6HCy4uqmzX8moMLNxB
6	txt1.txt	https://ipfs.infura.io/ipfs/QmbFMke1KXqnYyBBWxB74N4c5SBnJMVAiMNRcGu6x1AwQH
7	excelsheet1.xlsx	https://ipfs.infura.io/ipfs/QmYdzPse9BLKQuvW74X1b1JpvhDCcA5zn29Bn3TzNBQLx4

Fig. 5. Interface of the file Sharing application

Shown in fig.6 is a screenshot of the decentralized chat application with a sample chat.



Ann

Hi

~ chapa
Hello

This is a test chat to check the decentralized chat application

~ chapa
Good

~ chapa
Chat application is working!

h3vmvj66fdoce25acygwkb6jum3ilz63ujfxqk65y2gb43i.ipfs.infura-

This is the file I shared

Fig. 6. Interface of the Chat application

V. CONCLUSION

In this paper, an IPFS and Blockchain based secure decentralized file sharing platform is presented. The main aim of this project is to create a decentralized platform for communication inside a private network. This system supports the secure exchange of messages, files, videos and images. At present, most of the communication and information exchange systems are controlled via a centralized authority. This causes data security issues and data availability issues. This project is leveraging on the best features of the latest trending decentralized technologies like IPFS and Blockchain to tackle those problems. Inside this platform, chats and data hashes received for each information exchange from IPFS is securely stored in a private Ethereum Blockchain via smart contracts providing data immutability and data provenance. Also, by using this model any malicious modifications to the provenance data can be prevented.

REFERENCES

[1] “What is a DDoS Attack? Types & Prevention Methods,” Sucuri, 02-Mar-2020. [Online]. Available: https://sucuri.net/guides/what-is-a-ddos-attack/#:~:text=The DDoS attack will test,zombie devices called a botnet. [Accessed: 13-Sep-2020].

[2] "MLSDev", Mlsdev.com, 2020. [Online]. Available: https://mlsdev.com/blog/156-how-to-build-your-own-blockchain-architecture. [Accessed: 28- Feb-2020]

[3] “InterPlanetary File System,” Wikipedia, 07-Sep-2020. [Online]. Available: https://en.wikipedia.org/wiki/InterPlanetary_File_System#:~:text=The InterPlanetary File System (IPFS,in a distributed file system.&text=IPFS allows users to not,a similar manner to BitTorrent. [Accessed: 13-Sep-2020].

[4] “Centralized Networks vs Decentralized Networks,” Solarwinds MSP, 10-Jun-2019. [Online]. Available: https://www.solarwindsmsp.com/blog/centralized-vs-decentralized-network. [Accessed: 13-Sep-2020].

[5] “Book,” Git. [Online]. Available: https://git-scm.com/book/en/v2/Getting-Started-About-Version-Contro. [Accessed: 13-Sep-2020].

[6] “InterPlanetary File System,” GeeksforGeeks, 20-Sep-2019. [Online]. Available: https://www.geeksforgeeks.org/interplanetary-file-system/. [Accessed: 13-Sep-2020].

[7] “Building Private IPFS Network with IPFS-Cluster for Data Replication,” Eleks Labs, 19-Jun-2020. [Online]. Available: https://labs.eleks.com/2019/03/ipfs-network-data-replication.html. [Accessed: 13-Sep-2020].

[8] "MLSDev", Mlsdev.com, 2020. [Online]. Available: https://mlsdev.com/blog/156-how-to-build-your-own-blockchain-architecture. [Accessed: 28- Feb-2020]

[9] Google Search. [Online]. Available: https://www.google.com/search?q=blockchain structure&sxsrf=ALeKk03Xa9XRcVyaQEuppBeINHOk9isDKQ:1599888287263&source=lnms&tbm=isch&sa=X&ved=2ahUKEwijrauo8OLrAhXJ63MBHZNQA7sQ_AUoAXoECA8QAw&biw=1707&bih=838&dpr=1.13#imgrc=zEE0GjpZHJjfmM. [Accessed: 13-Sep-2020].

[10] ResearchGate. 2020. (PDF) Secure Peer-To-Peer Communication Based On Blockchain. [online] Availableat: [Accessed 25 September 2020]

[11] Khatal, S., Rane, J., Patel, D., Patel, P. and Busnel, Y., 2020. Fileshare: A Blockchain And IPFS Framework For Secure File Sharing And Data Provenance. [online] Hal-imtatlantique.archives-ouvertes.fr. Available at: [Accessed 25 September 2020].

[12] “Home,” ethereum.org. [Online]. Available: https://ethereum.org/en/. [Accessed: 13-Sep-2020].

[13] MetaMask. [Online]. Available: https://metamask.io/. [Accessed: 13-Sep-2020].

[14] Truffle Suite, “Ganache,” Truffle Suite. [Online]. Available: https://www.trufflesuite.com/ganache. [Accessed: 13-Sep-2020].