International Journal for Research in Engineering Application & Management (IJREAM)
ISSN : 2454-9150 Special Issue - CTRD - 2018

Decentralized Chat Application using Blockchain Technology

[1]Abhishek P. Takale, [2]Chaitanya V. Vaidya, [3]Suresh S. Kolekar

[1,2]UG Student, [3]Assistant Professor, Rajendra Mane College Of Engineering And Technology, Ambav, India.

[1]abhishektakale1995@gmail.com, [2]chaitanya95vaidya@gmail.com, [3]kolekarss@rmcet.com

Abstract — Decentralized application make use of peer-to-peer networks, this ensures that no network failure can occur due to central node failure. Blockchain serves as an immutable ledger which allows messaging to take place in a decentralized manner. A decentralized application for communication and resource sharing is need in today's world, where keeping data on a centralized server can be risky and costly experience. With the help of various consensus, we can implement different ways to share resources and communicate. Together with Blockchain and Decentralized Applications, we can create a secure and reliable messaging application that overcomes the drawbacks of traditional messaging applications.

Keywords — blockchain, centralized, consensus, decentralization, immutability, ledger

I. INTRODUCTION

As we all know, traditional chat applications are centralized i.e., all the data is stored on a centralized server. Therefore major problem of this structure is, if the central server fails then whole network collapses. For example, WhatsApp server stored all the data on a central server, if in case that server is destroyed then there can be a loss of user data, or they can even leak the user information stored on the server.

To overcome this, our project makes the use of decentralized Application approach (dApps). In our application all the user data is stored on a block which is connected to other blocks forming a chain. As the name suggests, a decentralized application does not have a centralized server. It is basically a peer-to-peer network. Also the data that is stored in block is almost impossible to view as a very secure encryption and hashing functions (256 bits) are used. Also is a hacker tries to make changes to the information in block then, he/she will have to make changes to all the copies of that block on whole blockchain network and that can be quite impossible. Though block are on all nodes, they cannot access the information in it, only the person for whom the information if can access it.

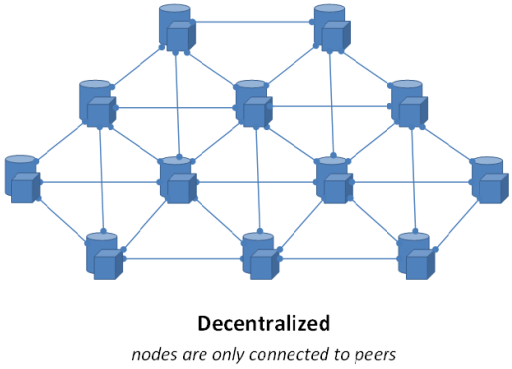

Figure 1.1 Decentralized Application Structure

Decentralized Application consists of multiple nodes connected to each other in a mesh topology type network. They are connected to each other in a Peer-to-Peer fashion. Blockchain is a sequence of blocks, which holds a complete list of transaction records like conventional public ledger.

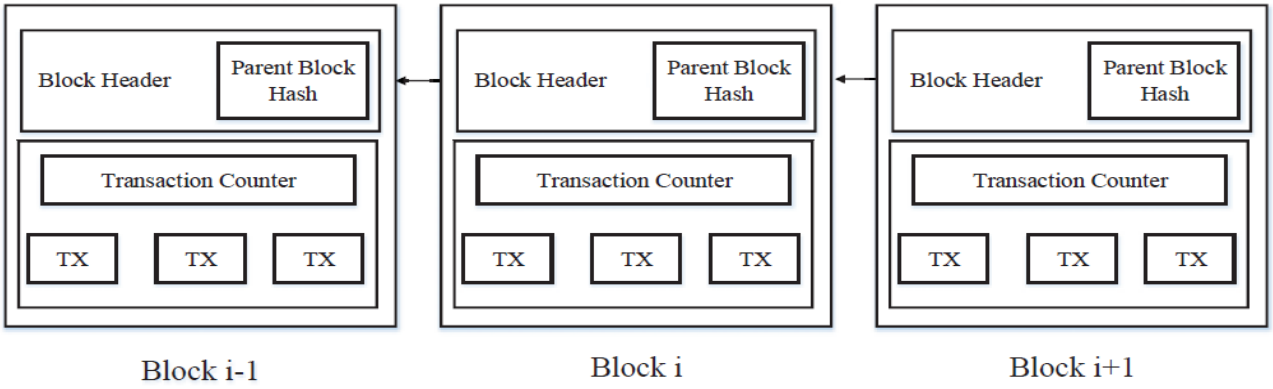

Figure 1.2 an example of blockchain which consists of a continuous sequence of blocks

The four main components of any blockchain ecosystem are as follows:

1. a node application
2. a shared ledger
3. a consensus algorithm
4. a virtual machine

- Node Application

Each Internet-connected computer needs to install and run a computer application specific to the ecosystem they wish to participate in. Using the case of Bitcoin as an example ecosystem, each computer must be running the Bitcoin wallet application.

- Shared Ledger

This is a logical component. The distributed ledger is a data structure managed inside the node application. Once you have the node application running, you can view the respective ledger (or blockchain) contents for that ecosystem.

- Consensus Algorithm

This, too, is a logical component of the ecosystem. The consensus algorithm is implemented as part of the node application, providing the 'rules of the game' for how the ecosystem will arrive at a single view of the ledger.

- Virtual Machine

The virtual machine is the final logical component implemented as part of the node application that every participant in the ecosystem runs. To understand the capabilities added to an ecosystem by including a virtual machine let's take a quick look at what a virtual machine is.

II. AIM AND OBJECTIVES

- To provide more secure environment for chatting and resource sharing.
- To reduce the possibility of immutability.
- To provide more efficient system that works even if a node in the network fails.

III. LITERATURE SURVEY

[1] Is a paper in which author has introduced all the uses and possible ways the blockchain can be used along with decentralization. Also the author emphasizes on, what the future blockchain applications will be. There is also a detailed report on advantages it provides, different areas in which blockchain can improve computing and how it is better and the current traditional systems.

IV. PROBLEM STATEMENT

The systems we currently use have a centralized approach to resource sharing and communication. Here, all the data is stored on a centralized server. This may lead to loss of data if the server collapses. Also, there are countless counterfeit information and product publishing on social networking without any known root transgressor (like on WhatsApp, hike). The information shared can be hacked which is stored on the centralized server.

V. SCOPE

To develop software that can provide all the features provided by currently available chat applications as well as overcome the drawbacks that they have. The resultant software will be more secure and reliable than the currently available ones.

VI. PROPOSED SYSTEM

In our application all the user data is stored on a block which is connected to other blocks forming a chain. As the name suggests, a decentralized application does not have a centralized server. It is basically a peer-to-peer network. Also the data that is stored in block is almost impossible to view as a very secure encryption and hashing functions (256 bits) are used. Also is a hacker tries to make changes to the information in block then, he/she will have to make changes to all the copies of that block on whole blockchain network and that can be quite impossible. Though block are on all nodes, they cannot access the information in it, only the person for whom the information if can access it.

VII. SYSTEM ARCHITECTURE

The block body is composed of a transaction counter and transactions. The maximum number of transactions that a block can contain depends on the block size and the size of each transaction. Blockchain uses an asymmetric cryptography mechanism to validate the authentication of transactions. Digital signature based on asymmetric cryptography is used in an untrustworthy environment. We next briefly illustrate digital signature.

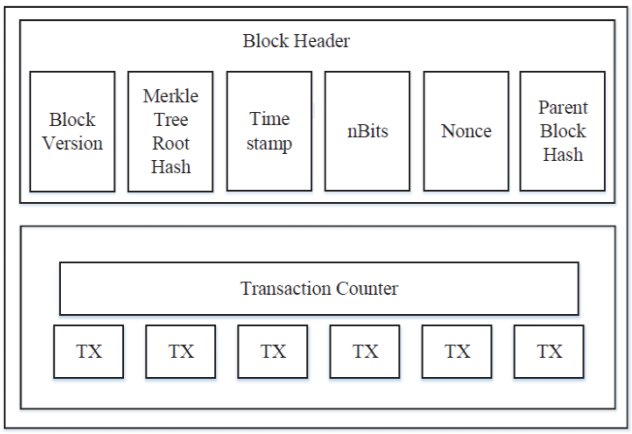

Figure.3 Block structure

Block

A block consists of the block header and the block body as shown in Figure 3. In particular, the block header includes:

i. Block version: indicates which set of block validation

rules to follow.

ii. Merkle tree root hash: the hash value of all the transactions in the block.
iii. Timestamp: current time as seconds in universal time since January 1, 1970.
iv. nBits: target threshold of a valid block hash.
v. Nonce: a 4-byte field, which usually starts with 0 and increases for every hash calculation.
vi. Parent block hash: a 256-bit hash values that points to the previous block.

VIII. ADVANTAGES

1. Immutability: Since records are stored on a large number of participants, it is nearly impossible to tamper transactions in a public blockchain.

2. Efficiency: It takes plenty of time to propagate transactions and blocks as there are a large number of nodes on public blockchain network.

3. Decentralization: Consensus algorithms in blockchain are used to maintain data consistency in decentralized network.

IX. CONCLUSION

In this project, we are developing an application that makes use of blockchain in a very efficient way. Blockchain has shown its potential for transforming traditional industry. Also, by eliminating the centralized approach, we can assure the safety and availability of data and communication. Decentralized applications tend to make the interaction between two people more efficient and simple. The chatting process nowadays have a mediating node, while our software does not have any mediating device/node i.e., every person is connected by peer-to-peer network.

REFERENCES

[1] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends", 2017 IEEE 6th International Congress on Big Data.

[2] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[3] G. W. Peters, E. Panayi, and A. Chapelle, "Trends in crypto-currencies and blockchain technologies: A monetary theory and regulation perspective," 2015. [Online]. Available: http://dx.doi.org/10.2139/ssrn. 2646618

[4] G. Foroglou and A.-L. Tsilidou, "Further applications of the blockchain," 2015.

[5] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in *Proceedings of IEEE Symposium on security and Privacy (SP)*, San Jose, CA, USA, 2016, pp. 839–858.

[6] B. W. Akins, J. L. Chapman, and J. M. Gordon, "A whole new world: Income tax considerations of the bitcoin economy," 2013. [Online]. Available: https://ssrn.com/abstract=2394738

[7] Y. Zhang and J. Wen, "An iot electric business model based on the protocol of bitcoin," in *Proceedings of 18th International Conference on Intelligence in Next Generation Networks (ICIN)*, Paris, France, 2015, pp. 184–191.