International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 04 | Apr 2020 www.irjet.net p-ISSN: 2395-0072

A Comprehensive Study on Blockchain Technology

Shiv Suraj Oberoi[1], Yashika Varyani[1], Dr. Deepak Chahal[2]

[1]MCA Student, Department of IT, Jagan Institute of Management Studies, Sector -05, Rohini, New Delhi. India
[2]Professor , Department of IT, Jagan Institute of Management Studies, Sector -05, Rohini, New Delhi. India.

Abstract: Online transactions were always thought to be very safe and secure but with the ever-changing technology, a lot of ways were figured out to compromise financial transactions via the internet. As a solution to this, Blockchain was developed as it provided a way to safely execute financial transactions. It is purely a peer-to-peer version of electronic cash to go from one party to another without involving a middleman. Blockchain was proposed as a solution to the double spending problem.

Keywords: Blockchain, Double-spending problem, Blocks, Transaction, Mining, Consensus Mechanism.

Introduction

Technological innovations such as robotics, machine learning, cloud technology etc. have established themselves very fast over the last few years and have now become a key element of the commercial and social economy[1]. Similarly, block chain will also become a indispensable part of our lives in near future. Block chain is term that has come to us in many things to many people and captures the imagination and fascinates many [1].Over the past few decades the information technology has undergone a lot many changes to better facilitate exchange of raw data, information and monetaryfunds in varying ways. With the internet coming into picture, digital communication emerged, allowing all forms data exchange via the internet such as financial transactions for receiving and making payments.Online transactionsinvolve 3 parties, the person sending the money/funds (Sender), the person receiving the money/funds (Receiver) and the middle party through the which the transaction is made, which in most of the cases is a Bank. The process of online transaction is very simple and easy but it requires the Sender and the Receiver to trust to bank completely. Although online transactions are most of the times very safe and secure but it can also create a very well know problem, known as "The Double Spending problem". According to this problem, a person can make an electronic transaction more than once using the same digital money. This problem was not solved until the first blockchain cryptocurrency which was introduced in 2009 called as Bitcoin.

Bitcoin can be intrinsically linked to the blockchain technology. It is one of the most controversial cryptocurrencies as it introduced a multi-billion-dollar global market of anonymous transactions without any governmental control.

Blockchain

This technology got name it's as"blockchain" because down to its most basic level, it is nothing but a collection of blocks. The word "blockchain" can be broken down in two parts: blocks and chains, where block refers to "Information (Digital)" and chains refer to "Public Databases". Blockchain can be defined as: "A blockchain is, in the simplest way can be defined as, a time-stamped series ofrecords of data that are immutableand are managed by a cluster of computers not owned by any single entity. Each of these blocks of data (i.e. block) is secured and bound to each other using cryptographic principles (i.e. chain) [1].The technical definition of blockchain that is based on its working pattern is that it is a public ledger for all transactions that are made and are shared among participating parties. Each transaction that is stored in the public ledger and is verified on a general agreement by a majority of the participants in the system and once the information is stored, it can never be erased. It contains a record of every verifiable transaction that has ever been made without involving any trusted centralized party. Each transaction is digitally signed by the owner with the private key.

To keep a track of multiple transactions that are occurring at the same time, such transactions are combined together in a structure called "block" and is uniquely identified by its hash and timestamp. Some of the most widely known blockchains allows

user to make instant transactions on a decentralized network. Transactions made on blockchain are completely secure and cryptographic encryption algorithms make sure no record of a transaction can be altered once it has been saved.

Structure

The structure of blockchain can be represented as a list of blocks with transactions in a particular order. These lists can be stored in a simple database or a Flat file.

The two most prominently used data structures in blockchain are pointers and linked list. Logically the first block in the chain does not contain a pointer because it is the first block in the chain and similarly the last block in the chain will also not contain a pointer because it is going to be the final block in the chain. All blockchain architecture falls into three categories: ***Public Blockchain Architecture***, ***Private blockchain architecture, Consortium blockchain architecture.***

A public blockchain architecture means that the data and the access to the system is publicly available, it is open-ended and is decentralized. It provides an open platform for various individuals and organizations to join, transact and mine. No restriction is imposed on this type of blockchain, that is why a Public Blockchain is also called a "Permission-less Blockchain". Everyone who is a part of the blockchain is given full authority to read and write transactions, perform auditing and review a blockchain at any given time. In the Public blockchain there is no such thing as "Validator nodes". All users are allowed to collect the transaction and begin with the mining process and collect their rewards. The copy of the entire blockchain is available with all the nodes and is synchronized, which makes the blockchain immutable.

A private blockchain architecture is operated only by users from a specific organization, it considered to be more centralized as it is controlled by a specific group with increased privacy. It is also called a "Permissioned Blockchain" because unknown users can't get access to it unless they are given a special invitation. Each nodes participation is decided by a set of rules or by the network in-charge to control its access. Unlike in a public blockchain, the access of a node to write a transaction is restricted in a private blockchain.

A consortium blockchain architecture can be called a "Semi-private system" and it works across multiple organizations. It can be considered as "Partially private" and "permissioned" blockchain, where a set of pre-determined nodes is responsible consensus and block violation. These pre-determined nodes get to decide that who can be a part of the network and who can do the mining process. To validate a block, a multi-signature scheme is used, according to which a block is only valid if it is signed by the selected nodes. The read and write permissions is decided by consortium that whether they are going to be public or limited to participants of the network.

Core Components of Blockchain Architecture

The Core components of Blockchain architecture include***: Node, Transaction, Block, Chain, Miners, Consensus.***

A Node can be defined as the user or the computer within the blockchain architecture. They store and preserve data, theoretically it can be stated that the blockchain exists on nodes. A full- node is a computer that has all the transaction history of the blockchain.

Transactions represent the current state of the blockchain, which is continuously generated by nodes on network. The state of the blockchain changes after each transaction is made. With transactions being generated in a huge amount, it is important to validate and verify the genuine ones and discard the fake ones.

Minersget paid for the work they do as auditors, as they are doing the job of verifying the previous bitcoins transactions that were made. By doing this, Miners also help avoid the "Double spending problem". A miner needs to verify 1MB worth of Bitcoin transactions to be eligible to get rewarded with some quantity of bitcoin but sometimes the "Miners" don't get paid also. To earn bitcoins, a miner needs to fulfil two conditions. The first conditions states that 1MB worth of bitcoin transaction data must be verified and according to the second condition, the Miner should be the first

one to arrive at the right answer to a numeric problem, this process is called as "*Proof-of-work*".

Consensus Mechanism

When the nodes begin to share and exchange data through a blockchain platform, there is no centralized party to solve disputes or provides safe-guards against security violations, and a mechanism to keep of flow of funds. All the nodes involved should agree on a common content uploading protocol for the ledger to maintain a consistent state and the blocks should not be simply included in the blockchain without majority consent, this is called "Consensus Mechanism".

Consensus Algorithms

Since there is no centralized party to resolve disputes, therefore we can say that consensus is a decentralized network with distributed users. Consensus Mechanism has the following algorithms: "*Proof-of-work*" and "*Proof-of-state*".

Proof of Work

The first decentralized network which was developed by Satoshi Nakamoto is called "Proof of Work", it was designed to achieve security and consistency in the Bitcoin. Currency exchange in bitcoin happens in decentralized manner thus it requires authentication and block validation. In bitcoin network, the nodes compete with each other to try and figure out the hash code for the next block. Once the solution is obtained, every node in the network has to mutually agree to it before the block can be added to the existing blockchain.

One of the main disadvantages of Proof-of-work is "Huge expenditure". The process of mining requires specialized computer hardware to properly execute the complicated mining algorithms. Such machines are very expensive and increase the overall cost.

Proof of State

Proof of State was designed to overcome the problems which were there in Proof of State such as "High expenditure Costs".Ethereum is also one of the main projects that implement Proof-of-state. POS proposes the idea to buy cryptocurrency and invest that money in the network, instead of investing all the resources to run algorithms that require high computation to calculate the hash functions. The money invested is directly proportional to the chance of becoming a block validator. To attain consensus, validator is randomly selected.

Conclusion

Blockchain is becoming increasingly popular because it provides a way to make online transactions happen in safest way possible as all the transactions are stored as records in an online ledger. One can think about the blockchain as a ledger of transactions [2]. This paper talks about the Block chain architecture, types of Block chain, the Core components of blockchain and the Consensus mechanism.

References

1. Chahal D. et al. The Developing Role of Block Chain(R) Evolution, EPRA International Journal of Multidisciplinary Research (IJMR), Volume: 4 | Issue: 11 | November 2018.

2. Kharb L et al, International Journal of Computer Science and Mobile Applications, Vol.5 Issue. 11, November- 2017, pg. 1-8].