An Overview of Blockchain Technology

Karthik C
Department of Computer Science and Engineering
School of Engineering and Technology, Jain University
Bangalore, India
karthikcy06@gmail.com

Abstract—Blockchain Technology is an emerging technology nowadays. The Blockchain was first used as a Peer-to-Peer ledger for registering Bitcoin transactions. The blockchain is a singly linked list which consists of a number of transactions. The blockchain is a decentralized distributed ledger which consists of a number of blocks organized in the form of a chain. A block in blockchain consists of two parts data and hash pointer. The first block in the blockchain is known as genesis block. The transactions and data in the block are secured by cryptography. The data inside a block in blockchain can be anything like bank transactions, backup data etc., which are recorded chronologically and publicly. The Hash pointer of a block is a unique code generated by a hash function like SHA256, SHA-3 etc., the hash function used in bitcoin blockchain. A block consists of a public key and a private key, using hash function digital signature is generated to the block. This is how the data inside the blockchain is so secured. The blocks are added into the blockchain by verifying the transaction in the block, the transactions are verified by miners. The miners use consensus algorithm to solve the blocks.

Key words: Blockchain, Bitcoin, cryptocurrencies, Proof-of-Elapsed, Federated

I. INTRODUCTION

The Blockchain was first used as a Peer-to-Peer ledger for registering Bitcoin transactions. A transaction in a bitcoin blockchain represents a transfer of the bitcoin cryptocurrency[1]. New transactions on a blockchain are relayed to all peers of the blockchain, which is used to check their validity. Multiple Valid transactions are stored into a block and stored in the blockchain in a way that altering the block is nearly impossible, as it would require large computational power to tamper a block in blockchain[2]. Some peers store the entire history of the blockchain, and they are called as full nodes. Each attempt of add a not valid transaction in the blockchain or changing the data in the block is detected by the nodes in the blockchain and can be avoided[3].

There are three types of blockchain:

A. Public Blockchain: As the name suggests this is the blockchain 'for the people, by the people, and of the people'. Here in this type of blockchain no one is in charge and anyone can perform reading/ writing/ editing the blockchain. These types of blockchain are open and transparent so that anyone can review anything at a given point of time on the blockchain. The miners for this blockchain can be anyone who is part of the blockchain. Example: Bitcoin, Litecoin, Ethereum, etc.

B. Private Blockchain: As the name suggests it is a private chain of an individual or an organization. This type of blockchain is same as a centralized system. Unlike the public blockchain here there is an organization in-charge who looks after of important information such as transactions inside the blocks. The miners for this blockchain is decided by the same organization. It is still debatable if such a private chain can be called a 'Blockchain' because it fundamentally defeats the whole purpose of blockchain. Example: Bankchain.

C. Federated or Consortium Blockchain: A federated blockchain tries to remove the autonomy which gets vested in just one entity by using private blockchains. This type of blockchain is built on two or more organizations. Basically, a group of organizations or representatives come together and make decisions for the best benefit of the whole network. Example: r3, EWF, Hyperledger.

Miners: Miners are members of the same blockchain who perform mining. The miners are the validators after solving a block i.e., transactions the transaction fees will be created by the blockchain itself and this process is called as Mining. Mining in the blockchain technology is the process of adding solved blocks to the large distributed decentralized public ledger of existing blocks known as the blockchain. The miners use an algorithm to solve the transactions and add it to the blockchain and it is known as the Consensus Algorithm. A block consists of a number of transactions in a single block, each transaction will be solved by different miners so that the block reward will be divided as transaction reward/fees amongst the miners.

Consensus Algorithm: Consensus algorithm is the fundamental of blockchain. A Consensus algorithm in blockchain technology is a process used to achieve agreement on a data value among distributed organization or systems. In Consensus algorithm group of people or nodes comes to a common decision how blocks should be added to the blockchain. Consensus algorithms are designed to achieve reliability in a network involving multiple unreliable nodes.

There are three types of Consensus Algorithm:

Proof-of-Work: This is the most popular algorithm being used by currencies such as Bitcoin and Ethereum, each one with its own differences. In Proof of Work, an actor to be elected as a leader and choose the next block to be added to the blockchain, the actor have to find a solution to a particular transaction of the

block before it is added to the blockchain. The major drawback of this algorithm is when a single organization own 51% of mining power then the organization can alter the transaction details. For example, Ghash is a mining company which owns the majority of hashing power in Bitcoin Blockchain once in a while it can own 51% of bitcoin then it can alter the transactions in Bitcoin.

Proof-of-Stake: The miner of a new block is chosen in a deterministic way, depending on its money investment, also called a stake. No coin creation exists in proof-of-stake hence a miner invests in the ICO of the system. The chance of being picked to solve the block depends on the fraction of the ICO in the system the participant owns. Different proof-of-stake systems vary in how they handle the commitment of the created block of the blockchain. A person with nothing to lose has no reason not to behave badly, this is called nothing at stake problem. Most efficient proof-of-stake is known as Delegated Proof-of-Stake. Delegated Proof-of-Stake is Faster, most efficient, most decentralized and most flexible consensus model. Deterministic selection of block allows blocks to be confirmed in an average time of the blockchain. The consensus protocol is designed to manage the average time of the blockchain and to protect all nodes against unwanted regulatory interference.

Proof-of-Elapsed Time: Intel developed its own consensus algorithm called proof-of-elapsed time. The algorithm is similar to proof of work but consumes less power. This type of algorithm uses a Trusted Execution Environment(TEE) such as Software Guard Extension (SGX) to ensure blocks get varified in a random lottery fashion, but without doing the required work. The approach is based on a wait time generated through the Trusted Execution Environment.

Hashing: Hashing means giving an input data like string, number of any length and getting an output string of a fixed length. In many of the cryptocurrencies like Bitcoin, the transactions of the bitcoin ICO is taken as an input and is is run through a hashing algorithm which gives an output string of fixed length. There are many hash function like SHA-3, SHA-224, SHA-256 etc., to generate a hash value to a block SHA-256(Secure Hashing Algorithm 256) is a hash function used in Bitcoin Blockchain which converts text, number and any kind of data to a 256-bits(32 bytes) string known as hash value. SHA-3 (Secure Hashing Algorithm) is a hash function used in Ethereum Blockchain. To calculate target hash i.e., the hash of a mined block [Target Hash=(Merkel Root Hash+Nonce)] is the formula. Target hash is the hash value of the block which is mined. More the miners in the blockchain more complex will be the target hash. Merkel Root Hash is the hash of the entire block, in a block we have more than one transaction and each transaction has it's own hash value by Merkel root algorithm a single and unique hash value will be generated to a block known as Merkel root hash. Nounce is a random number calculated by brute force technique, the very first value of the nonce is zero.

Branches in Blockchain: As and when the blocks are solved by different miners there are chances that more than one block is solved at the same time. Because of this reason branches are formed in such cases. After adding branches to the chain when a next block is to be added to the blockchain the miners should simply build on top of the first branch that they recieve. Different participants may have received the branches in different order. They will build the new block on the branch they first receive. The tie of creation of branches gets broken when the next block is solved, because it is very rare for this situation to happen more than one time in a row. Blockchain quickly stabilizes in this situation. The general rule in blockchain is to continue with the longest chain available. The transactions which are in shortest branch will go back to the unconfirmed transactions pool and will be picked later in the block by the miners.

II. Motivation And Research Problem

The blockchain is a secured decentralized distributed ledger. For many years people were exchanging values from many technological institutions like legal systems, corporations, and marketplaces. As the society grows more complex and trade route grow more distance more formal institutions were built up like barter system, banks for currency etc. In the early days, people were exchanging the values by barter system and banks came into existence. As the uncertainty and complexity grow up personal control was much lower, eventually by using internet bank institutions were put online. Nowadays banks have been charging high transactions fees and it's been very expensive exchanging the values. But there is a new technological institution that will fundamentally change how to exchange value and its called the Blockchain. As humans find ways to lower the uncertainty about one and another so that exchanging values becomes easier. For the first time uncertainty can be lowered by not just with political and economic institutions but can be done with technology alone and that is by Blockchain Technology. The Blockchain is an open source ledger the transactions are openly done with the public. If any changes to be made to the transactions then it must be done with the permission of the members in the blockchain. The Double-spending problem in a digital scheme can be solved by the Blockchain technology. Smart Contracts is another advantage of the Blockchain. With Smart Contracts, agreement between two or more organization can be automatically validated, signed and enforced through a Blockchain construct. This smart contract eliminates the need for middle mens and saves the company time and money. Currently many governments are looking to implement blockchain in there elections. One live example is that the government of Moscow implemented blockchain in there local elections to test the effectiveness of blockchain.

III. COMPARATIVE STUDY

Below table is the comparison of different types of blockchain :

TABLE I: COMPARISON OF DIFFERENT TYPES OF BLOCKCHAIN

Characteristics	Public Blockchain	Private Blockchain	Consortium/ Federated Blockchain
What is it?	Anyone anywhere in the world can read and write on the network. Data validated by every participant (node) in the network, thus making it the very secure	Permissions to read and write data onto the Blockchain a rusted' organization predetermined the owner of there controlled by a single Thighly blockchain	Permissions to verify read and write on the organization predetermined nodes. blockchain controlled by a few The choice of predetermined nodes can be different for every entity on the blockchain
Network Type	Decentralized	Partially Decentralized	Partially Decentralized, hybrid between private and public blockchain
Access	Anyone can access	Single Organization	Multiple selected organization
Participants	Permissionless	Permissioned	Permissioned
Security	Consensus mechanism, eg: Proof of Work, Proof of Stake etc	Pre-approved participants like voting/multiparty consensus	Pre-approved participants like voting/multiparty consensus
Transaction Speed	Slow	Lighter and Faster	Lighter and Faster

Below table is the comparison of types of consensus algorithm :

TABLE II: COMPARISON OF TYPES OF CONSENSUS ALGORITHM

Characteristics	Proof-of-Work	Proof-of-Stake
Node identity management	open	open
Energy saving	no	partial
Tolerated power of adversary	< 25% computing power	< 51% stake
Example	Bitcoin	Peercoin

IV. CONCLUSION

Blockchain development is in its infancy. But already the technology is old enough that the community has bifurcated both culturally and technically. This should not be viewed as a bad thing. When the first blockchain was invented it sought to solve one very specific problem. Today, players in the space are stretching to reorganize every fact of the digital terrain. As the problems take on more definition, it becomes clear that there is not a single solution. At the same time, if the efficiencies gained by one successful blockchain project are to be shared across domains, then developers and industry managers will have to

think about interoperability from the very beginning. The above proposals seek to study and identify the bifurcations in the blockchain space while finding new ways to link them together.

REFERENCES

[1] Morgen Peck, Freelance Technology Writer, Contributing Editor of IEEE Spectrum Magazine Special Edition "Blockchain World", 2017.

[2] Nicola Dimitri Professor in Siena-Italy University "THE BLOCKCHAIN TECHNOLOGY: Some Theory and Applications", 2017.

[3] Maaruf Ali, Department of Computer Science and Technology, University of Suffolk, Ipswich, Suffolk, UK "Applications of Blockchain Technology beyond Cryptocurrency", 2017.

[4] "Mastering Bitcoin" 2nd Edition, published by O'Reilly publications in July 2017.

[5] Nir Kshetri, IT professional , "Can Blockchain Strengthen the Internet of Things?", May 2017.

[6] Mahdi H. Miraz, "Blockchain: Technology Fundamentals of the Trust Machine," University of Hong Kong, 2017.

[7] Don Tapscott "Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World", 1st Edition. New York, USA.

[8] "Blockchain Beyond Bitcoin,", Sarah Underwood Communications of the ACM, November 2016.

[9] Catalini C, Gans J, "Some Simple Economics of the Blockchain", MIT SLoan School of Management, 2016.

[10] Narayanan A, Bonneau J, Felten E, Miller A, Goldfeder S., "Bitcoin and Cryptocurrency Technologies", Princeton University Press, 2016.

[11] Mahdi H. Miraz and Maaruf Ali, "Blockchain Enabled Enhanced IoT Ecosystem Security", London, UK, 23 August 2018.

[12] Bonneau J, Miller A, Clark J, Narayanan A, Kroll J, Felten W, "SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies", IEEE Symposium on Security and Privacy, 2015.

[13] "Blockchain: Enigma, Paradox Opportunity", Deloitte Limited, 2016.

[14] Nomura Research Institute, "Survey on Blockchain Technologies and Related Services", 2016.

[15] Satyavolu P and Sangamnerkar A, "Blockchain's Smart Contracts: Driving the Next Wave of Innovation Across Manufesturing Value Chains", Cognizant, 2016.

[16] Tschorsch F., Scheuermann B., "Bitcoin and Beyond: A Technical Survey on Decentralized Currencies", 2016.

[17] Walport M, "Distributed Ledger Technology: Beyond Blockchain", HM Government Office of Science, .2015.