A Foretaste of Blockchain Technology, Bitcoin and Ethereum

[1]Sainath Acharya, [2]Sudarshana K

Department of Information Science and Engineering
Alva's Institute of Engineering and Technology
Moodbidri, India

***Abstract*: A peer-to-peer network, distributed consensus and cryptography all these contained in a unique technology known as Blockchain. Blockchain is about enabling peer to peer transaction in a decentralized network. As our day to day life shifting towards digitization and we depending more and more on online methods "money" isn't left behind either. Online transaction is gaining more popularity over the past few years. A decade ago, an approach towards this online transaction led to the creation of "Bitcoin". To create many such applications similar to bitcoin and other different applications "Ethereum" was created with Blockchain Technology acting as the base for both of them.**

***Keywords:* Blockchain, Bitcoin, Ethereum, transaction, blocks, nodes, EVM, decentralized.**

I. INTRODUCTION

A blockchain can be defined as a time-stamped series of immutable record of data that is managed by cluster of computers and not owned by any single entity. Each of these blocks of data (i.e. block) are secured and are bound to each other using cryptographic principles (i.e. chain). The blockchain network has no central authority which means that it itself is the very definition of a democratized system. The information in Blockchain is open for anyone and everyone to see because of the fact that it is a shared and immutable ledger. Hence, anything that is built on the blockchain is by its very nature transparent and everyone involved is responsible for their actions. A blockchain brings with itself no transaction cost. The blockchain is a simple yet creative way of passing information from user A to user B in a fully automated and safe manner. Single party to a transaction initiates the process by creating a block. This block is verified by thousands or perhaps millions of computers distributed around the internet. Then this verified block is added to a chain, which is stored across the internet, creating not just a unique record but also a unique record with a unique history. Forging a single record would mean forging the entire chain in millions of instances which is virtually impossible.

II. TYPES OF BLOCKCHAIN

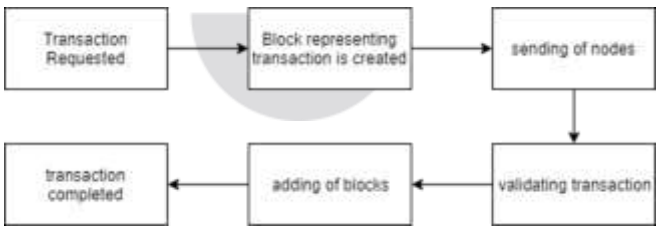
A. Public Blockchain

A public blockchain can be said as a blockchain that any person in the world can read, send transactions to and expect to see them included if they are valid, and any person in the world can participate in the consensus process i.e. determining what blocks get added to the chain and what the current state is. Here, in Public Blockchain ledgers can be 'public' in two senses: 1) Any person, who can write data, without permission granted by another authority. 2) Any person, who can read data, without the permission granted by another authority. Normally, when people talk about Public Blockchains, they mean anyone-can-write.

B. Private Blockchain

A fully private blockchain is a blockchain where write permissions are kept centralized to single organization. Read permissions can be public or restricted to an uninformed extent. Likely applications include database management, auditing, etc are internal to a single company, and so public readability may not be necessary in many cases at all, though in other cases public auditability is desired.

C. Working of Blockchain Technology

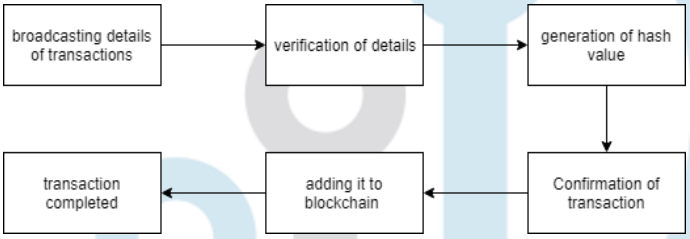


Initially, a transaction is being requested by a client who wants to perform exchange of money. After the transaction is requested, a block is created which will represent that particular transaction.in the next step, the block representing the transaction is sent to every other node that resides inside the distributed network. The nodes validate the transactions that they receive and give the results. These nodes receive rewards as a proof of their work. After this step, the block is then added to the existing Blockchain.

III. BITCOIN BLOCKCHAIN

Bitcoin and Blockchain are two completely different entities but they are closely related. Bitcoin, simply is a digital currency. On the other hand, Blockchain is the technology that is used by Bitcoin to allow secure, public and anonymous transactions to occur. The Bitcoin blockchain is a database (known as a "ledger" – a collection of financial accounts) that consists only of Bitcoin transaction records. There is no central location that holds the database, instead it is shared across a huge network of computers. So, for new transactions to be added to the database, the nodes must agree that the transaction is real and valid. This group agreement is also known as a "consensus". It occurs during the process of mining. (Mining is the process in which nodes verify transactional data and are rewarded for their work. It covers their running costs i.e. electricity and maintenance etc. and a small profit too for providing their services. It is not just a part of bitcoin but also a part of all blockchains).

Once the nodes agree that the transaction is real, it is then added to a "block" (which is why it is called a blockchain) and is placed below the previous block of transactions in the ledger. For a transaction to be valid, the computers on the network must confirm that: 1) The account holds the amount of bitcoin that the user wants to send. 2) The amount hasn't already been sent to someone else. This means that nobody can ever spend the same money twice. The sole purpose of Bitcoin is to act as a store of value. It allows for peer-to-peer transactions that do not need a third party, such as PayPal or a bank. The distribution of data works on a peer-to-peer basis. Peer-to-peer is like a gossip network where everyone tells a few other people the news (about new transactions and new blocks), and eventually the message gets to everyone in the network. For example, when you make a bitcoin payment (transaction), a payment instruction is sent to the network. This instruction is validated by the computers on the network and then it is relayed to other computers. After certain period of time has passed, in of the block-updates the payment gets included and then it is added to The Bitcoin Blockchain File on all computers across the network. Bitcoins are associated with "bitcoin addresses". Bitcoins themselves are not stored; but rather the keys or passwords needed to make payments are stored, in "wallets" (also called as Bitcoin Wallets) which are apps that manage the addresses, keys, balances, and payments.



When a user wants to send bitcoins to someone else, they broadcast the details of the transaction (public key, the recipient's public key, and the bitcoin amount to be transferred) to a network of interlinked nodes. This transfer information is independently verified by other computers in the network, corresponding to having witnesses present when signing a contract. A "digital signature" is used by these other nodes for the purpose of authenticating a transaction. A long, complex string of letters and numbers is generated from a combination of a user's private and public keys, along with the transaction message itself. This alphanumeric pattern is unique to every transfer and can't be used twice, to further safeguard against fraud. Once it's been confirmed that the transaction message is genuine, the transaction data itself must be added to the blockchain to be considered as "confirmed"

IV. ETHEREUM BLOCKCHAIN

Ethereum is an open blockchain platform that lets anyone build and use decentralized applications that run on blockchain technology. Like Bitcoin, Ethereum is a distributed public blockchain network. But there is a significant difference between them. A peer-to-peer electronic cash system which enables online bitcoin payments, is offered by Bitcoin which is one particular application out of the several applications of Blockchain Technology. While the Bitcoin blockchain is used to track the ownership of digital currency (bitcoins), on the other hand the Ethereum blockchain focuses on running the programming code of any decentralized application. In Ethereum blockchain, miners work to earn Ether, instead of mining for bitcoin. Ether is a type of crypto token that funds the Ethereum network. Ethers are also used to pay for transaction fees and services on the Ethereum network by Application developers. There is a second type of token that is used to pay miner's fees for including transactions in their block, it is called gas, and every smart contract execution requires a certain amount of gas to be sent along with it to tempt miners to put it in the blockchain. Smart contract is a code that can ease the exchange of money, content, property, shares, or anything of value. When a Smart Contract runs on a blockchain, it becomes like a self-operating computer program that executes automatically when certain conditions are met. All blockchains have the ability to process code but most of them are severely limited. Ethereum is different. Ethereum allows developers to build whatever operations they want, rather than providing a limited set of operations. This means developers can build thousands of different applications. The Ethereum Virtual Machine (EVM) can be said as a complete Turing software that runs on a network known as Ethereum network. Regardless of any programming language and if given enough time and memory EVM enables anyone to run any program on it. The Blockchain application creation process is made much easier and efficient with the use of EVM. Instead of having to build an entirely original blockchain for each new application, Ethereum enables the development of potentially thousands of different applications all on single platform.

V. CONCLUSION

In this paper, we discuss about the Blockchain Technology, the working of blockchain technology and types of blockchain technology. Further, we also discussed about the two applications out of many applications of Blockchain Technology – Bitcoin and Ethereum. The world is becoming more digitalized day by day and also the digital currency gaining rapid momentum Bitcoin has become successful as it is a decentralized form of online currency transaction therefore widely accepted by the world for internet transactions. And these transactions are stored in a distributed database called Blockchain that keeps a permanent and tamper-proof ledger of transaction data. Ethereum, an open blockchain platform that lets you build and deploy applications that run on blockchain technology. Because of this, Ethereum has gained immense popularity since its release in 2015. Some of the apps, platforms and markets using Ethereum are Metamask, MyEtherWallet, Augur, Ujo. Both Bitcoin and Ethereum with Blockchain Technology is a big revolutionary in the IT industry and is bound to change the digital world.

REFERENCES

[1] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system, J. Consulted, 2008.

[2] SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies Joseph Bonneau, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A. Kroll, Edward W. Felten Princeton University, Stanford University, Electronic Frontier Foundation, University of Maryland, Concordia University.

[3] Florian Tschorsch and BjörnScheuermann: "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies" https://eprint.iacr.org/2015/464.pdf.

[4] http://liquidthink.net/pros-cons-decentralized-currency.

[5] Vitalik Buterin, "Ethereum and The Decentralized Future". Future Thinkers Podcast. 2015-04-21. Retrieved 2016-05-13.

[6] F. Ametrano, "Bitcoin, Blockchain, and Distributed Ledger Technology" http://ssrn.com/abstract=2832249.