Blockchain

I.P. Yuvashree[1], Sarathkumar.M[2], Mutharasan.P[3]

[1,2,3] Sri Krishna Adithya College Of Arts And Science

Abstract- *Blockchain is an undeniable innovation which acts as a core mechanism for the Bitcoin. Blockchain enables the creation of suburbanized environment, in which transactions and data are privatised and not under the control of any third-party organization. The transaction records are recorded in a public ledger in a secured and verifiable way with time stamp and other details. The Blockchain is alleged to be best invention in the technical world, which will be the foundation for the unfold able future technology it also provides different verticals and use case with far reaching effect.*

I. INTRODUCTION

Blockchain lime lighted in the popular media recently. Blockchain is shared data base bewildered by private enterprises, to amaze and wonder about a new technology that has a potential to create economic or social change.

Blockchain is the digital currency system which enhances monetary transaction between two parties and not under the control of any third party. It acts as a tool for financial services to increase the efficiency and reduce cost within the industry. As a retort, blockchain contributors are created all over the world and developed independently or sponsored by the innovation labs, bank and other entities.

II. HISTORY

Technologies are sprouting in our day to day life, we are now in the midst of another revolution:" Blockchain", a dispersed database that manages a continuous growing list of sorted records called "Block". The research was started by the scientist Stuart Haber and W Scott Stornetta the idea of block chain was introduced in early 1991. Stuart Haber and W Scott Stornetta did the first work on a secured chain of blocks for getting a solution for practical computational time-stamping digital documents. This is a cryptographical system which contains a chain of blocks to store the time-stamped documents. Then on the next year 1992 block chain technology improved by incorporating Markle trees which enables that the multiple documents that can be stored in a single block. By storing multiple documents in a single block which increases the blockchain efficiency. After 10 years later in 2002 the innovations are:

a) First innovation

The first innovation was "Bitcoin", a digital currency experiment which is been used by millions of people for monetary transaction.

b) Second innovation

The second innovation was "Blockchain" which is been used for all kinds of other interorganizational cooperation. Almost all the financial institution in the world were doing research on Blockchain and expected to be used by 15% of banks in 2017.

c) Third innovation

The third innovation was "Smart contract" which builds coding directly into the Blockchain and these coding allows the financial instructions such as loans and bonds.

The Ethereum smart contract platform has a market cap of around billion dollars and hundreds of projects headed towards the market.

Keyword: Ethereum – Blockchain system

d) Fourth innovation

The fourth innovation was "proof of stake" which is used to count largest total of computing power makes the decision and provides security to vast data centres.

e) Fifth innovation

The fifth innovation was "Blockchain scaling" which secures and figure out how many computers are necessary for a particular Financial transaction and it also divides the work efficiently.

These innovations are ten years of work which changed the economy of the world and still the world economy is waiting for the active future in the Blockchain.

III. BLOCKCHAIN

Blockchain is a chain of block that contains information. A Blockchain is a distributed ledger that is completely open to anyone. When some data inside a blockchain, is recorded then we cannot easily able to change it.

Each block contains some

1. Data: -

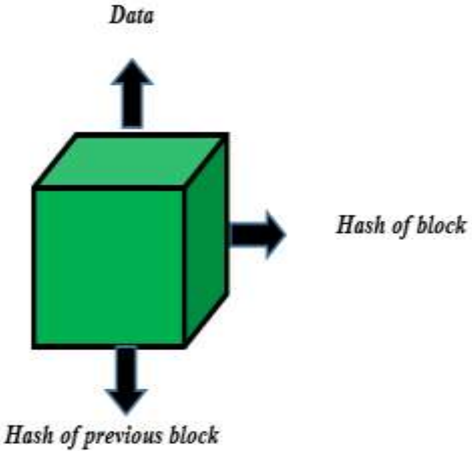
The data that is stored inside a block depends on the type of blockchain.

2. The hash of the block: -

Hash identifies a block and all of its contents and it's always unique, just as a fingerprint. Once a block is created, its hash is being calculated. Changing something inside the block will cause the hash to change. So, in other words hashes are very useful when you want to detect changes to blocks. If the fingerprint of a block changes, is no longer in the same block.

3. The hash of the previous block: -

Each block has the hash of the previous block. This effectively creates a chain of blocks and this technique that makes a blockchain so secure.



Block diagram

Changing a single block, it will make all following blocks invalid. Hashes is not enough to prevent tampering. Computers is a very fast device that can calculate many hashes per second effectively and could effectively tamper with a block and recalculate other blocks hashes to make a blockchain valid again. To mitigate this, something that in a blockchain called proof-of-work. This mechanism that slows down new creation of blocks. In Bitcoins to calculate the required proof-of-work and add a new block to the chain it takes about 10 minutes. You'll need to recalculate the proof-of-work for all the following blocks to tamper with one block. So, this mechanism is very hard to tamper with the blocks. The blockchain security comes from its creative use of hashing and the proof-of-work mechanism. Blockchains secure themselves and that's by being distributed. Blockchain uses peer-to-peer network instead of using a central entity to manage the chain and anyone is allowed to join. The full copy of the blockchain will get by the person when he joins this network. To check that everything is still in order the node can use this to verify. The new block will be sent to everyone on the network while creating a new block. The block is verified by each node to make sure that it hasn't been tampered with. Each node adds this block to their own blockchain if everything is checked out. All the nodes in this network create consensus. Other nodes in the network will rejects the block that aren't tampered with and they agree what blocks are valid. So, you'll need to tamper with all blocks on the chain to successfully tamper with a blockchain.

IV. TYPES OF BLOKCHAIN

There are three types of Blockchain. They are:

- Public Blockchain
- Private Blockchain
- Consortium or federated Blockchain
- Public Blockchain: -

A public blockchain has absolutely no access restrictions. Anyone with an internet connection can send proceeding to it as well as become a validator (i.e., participate in the execution of a generally accepted protocol)Usually, such networks offer economic incentives for those who secure them and utilize some type of a Proof of Stake[proof of stake(pos) is a type of algorithm by which a crypto currency block chain network aims to achieve distributed consensus.in pos-based cryptocurrencies the creator of the next block is chosen via various combinations of random selection and wealth or age.] or Proof of Work algorithm[A proof-of-work system is an economic measure to deter denial of service attacks and other service abuses such as spam on a network by requiring some work from the service requester, usually meaning processing time by a computer.

Example: - Bitcoin and Ethereum,

- Private Blockchains: -

Private block chain as its name suggests is a private property of an individual or an organization. A private blockchain is permissioned. know One cannot able to join the network without the permission of the network. Participant and validator access is Limited. This type of blockchains can be considered an intermediate position or area of compromise or possible agreement between two opposing views for a companies that are interested in the blockchain technology in general but are not comfort with a level of control offered by public networks. Typically, they seek to include something as part of something larger block chain into their accounting and record-keeping procedures without sacrificing the rights of an organization.

Example: Bitcoin, Litecoin etc,

- Consortium Blockchains: -

This type of blockchain tries to remove the sole the rights or condition which gets inalienably in just one entity by using private blockchains. An organization of several business or group joins together as a group for shared purpose in blockchain is often said to be semi-decentralized. A multiple company controlling it on such a network instead of controlling by a single company. The administrators of a organization of several business or group joins together as a group for shared purpose of chain limited users reading right.

Example: - quorum, Hyperledger and Coda.

V. BENEFITS OF BLOCKCHAIN

Decentralized & Trustless: -

Blockchain is a public ledger of all transaction on the network which is maintained by different decentralized nodes. Decentralized and trust less peer-to-peer network is enabled by blockchain technology. where the peers do not need a trusted intermediary for interacting with each other we do not need trusted intermediary by the peers. Since a blockchain network is not controlled by a central authority and all the transactions are verified and validated by a consensus among the peers, the peers do not need to trust each other.

Resilient:

Blockchain network is resilient, because with no single point of failure as it is a decentralized peer-to-peer network. When the data that is recorded inside a blockchain then it cannot be easly able to delete or alternate it.

Scalable:

Blockchain network is maintained by a network of peers and this network is naturally highly scalable. The computing capability of the network scales up as more peers (or miners) joins the network.

Secure & Auditable:

A strong cryptography is used to secure the transactions in blockchain. Furthermore, the public ledger is transparent in nature it is maintained by a blockchain network. And this network makes it secure and auditable. All the transactions in the network will knows by everyone on the network and the transactions cannot be disputed.

Autonomous:

Blockchain can enable different entities (e.g. lodevices) to communicate with each other and do transaction autonomously.

VI. CONCLUSION

Blockchain is a chain of block that contains information. Each block contains some Data. The data that is stored inside a block depends on the type of blockchain. The hash identifies a block and all of its contents and its always unique, just as a fingerprint. If the fingerprint of a block changes is no longer in the same block. Each block has the hash of the previous block. Changing a single block, it will make all following blocks invalid. Computers is a very fast device that can calculate many hashes per second effectively and could effectively tamper with a block and recalculate other blocks hashes to make a blockchain valid again. In Bitcoins to calculate the required proof-of-work and add a new block to the chain it takes about 10 minutes. Blockchain uses peer-to-peer network instead of sing a central entity to manage the chain and anyone is allowed to join. So, you'll need to tamper with all blocks on the chain to successfully tamper with a blockchain.

REFERENCES

[1] https://r.search.yahoo.com/_ylt=AwrPhmqBc1RcDG8ACDq7HAx.;_ylu=X3oDMTByajVjNzRjBGNvbG8Dc2czBHBvcwM0BHZ0aWQDBHNlYwNzcg--/RV=2/RE=1549067265/RO=10/RU=https%3a%2f%2fwww.coindesk.com%2finformation%2fwhat-is-blockchain-technology/RK=2/RS=ABg50_DxOvLCr9I5Eo7CLkUj0VQ-

[2] https://r.search.yahoo.com/_ylt=AwrPiFJWdFRciTgAjs.7HAx.;_ylu=X3oDMTByaW0wdmlxBGNvbG8Dc2czBHBvcwMyBHZ0aWQDBHNlYwNzcg--/RV=2/RE=1549067479/RO=10/RU=https%3a%2f%2fwww.slideshare.net%2fFerdinando1970%2f20161110-rome-icc-intro-to-blockchain/RK=2/RS=..R5E1LveNpF5nwX7mXaerIjMMo-

[3] https://r.search.yahoo.com/_ylt=AwrPiFJWdFRciTgAls.7HAx.;_ylu=X3oDMTBycnYxMDN2BGNvbG8Dc2czBHBvcwM2BHZ0aWQDBHNlYwNzcg--/RV=2/RE=1549067479/RO=10/RU=https%3a%2f%2fwww.sketchbubble.com%2fen%2fpresentation-blockchain.html/RK=2/RS=qMb0TCjM.30vsi1KbmlBDUEpe9I-

[4] https://r.search.yahoo.com/_ylt=AwrPhOqtdFRc1zcAJ0u7HAx.;_ylu=X3oDMTByaW0wdmlxBGNvbG8Dc2czBHBvcwMyBHZ0aWQDBHNlYwNzcg--/RV=2/RE=1549067565/RO=10/RU=https%3a%2f%2fwww.sec.gov%2fspotlight%2finvestor-advisory-committee-2012%2fslides-nancy-liao-brief-intro-to-blockchain-iac-101217.pdf/RK=2/RS=hZriR2cpXuWDA6k33mz9Q_QFn3s-