International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 09 | Sep 2020 www.irjet.net p-ISSN: 2395-0072

Block chain Technology: Architecture, Types, characteristics, Challenges and Possible Future Directions

Sharique Ali Sayed

Department of Master of Computer Applications, Vivekananda Education Society's Institute of Technology

---

Abstract - *Block chain is a digital ledger system which is decentralized serving as the foundation on which Bitcoin as well as other cryptocurrencies operate. Block chain keep track of digital transactions, such as cryptocurrency using wide network. Additions or changes are added linearly and connected together, hence referred to as chain. Thus it cannot be edited or changed surreptitiously. The Parties involved cannot alter or reverse it without mutual agreement, once transaction becomes part of the network and is encoded.*

Key Words: Block chain, immutable decentralized, peer to peer, consensus, scalability, public block chain, private block chain, consortium block chain

1. INTRODUCTION

Current modern trend is all about technology, thus there is a need of increasing need for modernization in our day-to-day lives. People welcome and accept new technologies. Technologies ranging from controlling devices to using voice notes for giving commands (Alexa); modern technology is involved in our day to day lives. Some of the recent technologies like augmented reality and IoT has gained more and more attention in the last decade and one technology that is gaining more and more focus recently is Block chain Technology.

Block chain - Block chain technology that has impacted many different industries was introduced to the market with its first modern application i.e. Bitcoin

There is a misconception that Block chain and Bitcoin are same, which is not true. Creating cryptocurrencies is one such application in Block chain and Bitcoin, however, there are numerous other applications too that are developed using Block chain technology.

Each Transaction on a block chain proves its authenticity using digital signature mechanism. Thus, with the use of encryption and digital signatures, the data stored on the block chain cannot be changed or tampered.

Block chain allows all participants in the network to reach an agreement, known as consensus. Data are recorded digitally and all network participants share a common history. Thus, with the elimination of Third-party, the chances of fraudulent or duplication activity is least possible.

Using Block chain to Transfer Money is much easier and secure than using a bank to transfer money. With the elimination of Third Party, there is no extra fee involved, funds are directly processed by you. Also the Block chain Database is decentralized making it not limited to any single location, which means that all records and information's are kept on the block chain are decentralized and public. Hence information is not stored in a single place, resulting in no chance of corruption of information by hacker.

A block chain is basically a chain of blocks containing information or data. Satoshi Nakamoto, discovered the first popular and successful application of block chain technology in 2009. He created Bitcoin, first digital cryptocurrency using Block chain technology

Thus, here's how block chain allows transactions to take place:

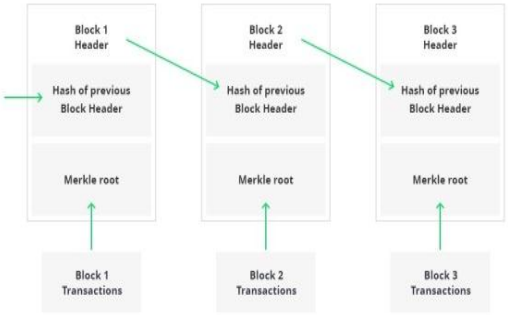
- Public and Private Keys are used to form a digital signature which ensures security and consent.
- Once the authentication is done using these keys, need for authorization arises.
- Block chain ensure all participants reach consensus to agree on particular value by allowing participants to perform mathematical verification.
- During a transfer, sender announces transaction over the network using their private key. A block is formed having information such as timestamp, DS and receiver's public key.
- This Block is broadcasted over the network and process of validation starts.
- Miner's uses their computing power to start solving the mathematical puzzle related to the transaction in order to process this information.
- On solving the puzzle firstly, the miner are rewarded in the form of bitcoins. Such problems are termed as proof-of-work Mathematical problem.

- Upon coming on a consensus by majority of the nodes in the network, the block is time stamped and added to the existing block chain.

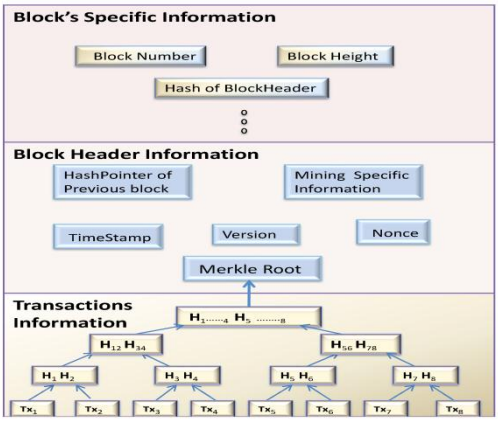
- The block information ranges from money to data to messages.

- Existing copies of block chain are updated after the new block is added to the chain, for all the nodes on the network.

2. BLOCKCHAIN ARCHITECTURE



Block chain consists of a continuous sequence of blocks.



For Beginners, Block chain technology is chain of blocks containing specific database information, in a genuine and secure manner which is grouped together in a peer-to peer way. Thus, Combination of computers linked together to each other in a decentralized manner is what we call as Block chain.

Core Components of Block Chain are:

- Node - a specific computer or a user within the block chain network architecture (each one of which has a independent copy of the whole block chain ledger).
- Transaction – small building block of block chain serving as the purpose of block chain (information, records, etc.).
- Block - A data structured in a way for keeping set of transactions in a distributed manner to all participating nodes in the network.
- Chain - a block sequence in a specific order.
- Miners - Specific nodes responsible to perform the block verification process prior to adding to the block chain structure.
- Consensus - set of arrangement and rules to be followed and agreed upon by every node to carry out the block chain operations.

2.1. Block

The block is divided into six components which are:

The version number of the software:-

Software number is least mattered in most of the case. However, which protocol decisions is to be supported is signalled by the miner with a particular version number.

The hash of the previous block:-

The hash of the previous block is basically, so to speak to, the block chains. Because previous hash block is stored in new block hash, all blocks in the block chain are built on each other. There will be no chronology and connection between blocks, if this component is absent.

The root hash of the Merkle Tree:-

- Every Transactions in a block are aggregated to a hash. This hash is the root hash of the merkle tree.

The Goal of the current difficulty:-

- The Goal indications small portion of new hash that can claim validity. To Simplify, every hash has a size in bits. Lower the goal in bits, harder it is to find matching hash. A hash without zeroes is bigger than a hash with many zeroes at the beginning, resulting in difficulty to find out the proof of work.

The Nonce:-

- A variable that is incremented by proof of work. Thus, miner predicts a valid hash which is smaller than the target.

- This Six Components forms the Block Header of the Block chain. Thus, by connecting all the blocks together, it plays a fundamental role in Bitcoin.

2.2. Block Body:

- The Block body consists of transaction counter and Transactions. Maximum number of transactions a block can uphold depends on the size of each transaction and block size.

- Block chain validates authentication of transactions using asymmetric cryptography mechanism. Digital Signature is one such asymmetric cryptography used in an untrustworthy environment.

2.3. Digital Signature

Every User or node has a pair of public and private key. The Private Key is kept confidential, only to be used to sign the transactions. These Signed Digital transactions are broadcasted throughout the entire network. The Digital signature is completed in two phases: Signing phase and verification phase. For Example, Alice, an user, wants to send some message to bob, another user.(1) In the Signing phase, Alice encrypts data using her private key and broadcasts the encrypted result and original data .(2)In the verification phase, Bob validates using Alice's public key. This way, bob checks if the data was corrupted or tampered along the way.

Key Characteristics of Block chain

Block chain has following key characteristics:-

- The Data which is stored in Block chain cannot be changed easily and is immutable as explained earlier. And also data is added to only when it is approved by every node/user in the network, thus resulting in secure transactions. The one responsible to validate the transactions and add them in the block are known as miners.
- As mentioned earlier, Block chain is as open ledger system operating in a decentralized manner. Ledger is what is known as record of transactions done and it being visible to everyone, it is known as open ledger. Decentralization results in No individual or organization being in charge of any transaction. Every connection in the block chain has same copy of ledger.

- Block chain has peer to peer network. This means, that at a given transaction, only two parties are involved i.e. Sender and Receiver. Thus, removing third party authorization as everyone is able to authorize the transactions.

- Every transaction refers to its previous unspent transactions. Once a new transaction is admitted into the block chain, State of those previous unspent transactions switches from unspent to spent. Thus, transactions can be easily be verified and tracked.

3. Taxonomy of Block chain

3.1. Public block chains

People who have interacted with cryptocurrency, may have chances that they have interacted with block chain as well. These contributes to the majority of all the distributed ledgers that exist today. These ledgers can be viewed by anyone, hence termed as public, joining it is simply downloading the necessary software.

We often use term like "permission less" alongside public. In this, anyone can engage with the consensus mechanism, there is no gatekeeper that can stand in the way of participation. Since anyone is free to join, miners are rewarded for their role in achieving consensus.

Since anyone can view the transaction, we would expect a public block chain to be more censorship oriented than a private. As it is visible to anybody, the protocol must incorporate certain mechanism to prevent and stop any malicious action to happen during the transaction.

In public chain, the security oriented approach come with trade off on performance front, however throughput is relatively weak and scaling obstacles. Moreover, pushing changes to network can be a difficult challenge, as it is rare that all users agree on the purposed changes.

3.2. Private Block chains

In Contrast to permission less nature of public block chain, private block chain establishes set of rules on who can see and write to the chain. This prohibits Decentralized systems, as there is some amount of control over the transaction. They are distributed, though, as many nodes maintain copy of the block chain.

Private Block Chain are suited to enterprise settings, where organization want to use block chain technology within the network and not accessible externally.

Proof of work is a waste, but can be necessary for an open environment, given the security model. Even though PoW deters, Each node identity is known and control is maintain in secure manner.

A Systematic approach involves appointing validators, which are responsible to take control on certain functions for transaction validation. This involves agreement among all nodes to select validator node. If the Validator node starts acting maliciously, they can quickly be identified and removed from the network. Thus making it easy to coordinate reversal

3.3. Consortium Block chains

Consortium Block chain is the middleware of the public and the private block chain, combining from both. Instead of open system where validation is done in open or closed one where only a single entity appoints block validators, consortium sees handful of equally powerful parties function as validators.

In consortium, rules are flexible, where visibility can be limited to validators or viewable to authorized individuals or by all .Changes can be rolled out only when validator's reaches consensus .As for functionality, system will not run into any problem as long as certain threshold of these parties is behaving honestly.

Consortium Block chain is most suited where multiple organization operate in the same industry and requires common ground to carry out transaction or relay information .This type of block chain can be beneficial to an organization, allowing them to share insights into their industry with other players

Which one is better?

Fundamentally, public, private, and consortium block chains are not at same – they're different technologies:

- Public chain which are well-designed tends to excel owning to censorship-resistance, at the cost of throughput and speed. Suitable for greater security assurances based on transaction settlements.
- Private Chain prioritizes system's speed as it does not worry about central points of failure in case of public block chain. These block chain are deployed where an individual or organization must always remain in control and information is to be kept private.
- Consortium chains involves some risks of private chain by removing centralized control. Consortium is suitable to organization that wants communication amongst one another,

4. CHALLENGES IN BLOCKCHAIN TECHNOLOGY

Even though block chain has great potential, it faces numerous different challenges, which limits the usage of block chain. Some of them are as follows.

4.1. Energy-Consumption Consensus Mechanisms:-

- Consensus protocol of Bitcoin as well as other block chain can create a great obstacle to widespread adoption
- In 2017, it was observed that bitcoin mining consumed energy equal to that of entire nation of Denmark. Thus, the problem.
- If Block chain technology is handled properly, the consensus protocol can be replaced with solution that are not power hungry server farms. what those solutions may be is yet to be discovered, but here lies the great opportunity for innovation to take DLT to the next level

4.2. Lack of Skilled Developers and Training program:-

- The number of Lack skilled developers is very surprising.
- It is ranked among top 20 fastest growing job skills, the number of block chain position increased by 200% in 2018 compared to 2017.
- 23% of large companies actively searching for distributed ledger technology, it can assumed that the market would flush with eager candidates, but on the contrary, the lack of training program has resulted in a talent glut.

4.3. Over Regulation & Under Regulation:-

- The question of whether to regulate or not to regulate Block chain depends on who you ask.
- If you ask Bitcoin market, rules and regulation imposed by government will halt the concept of adoption and innovation. If asked by some legal experts, these regulations are the only thing that will encourage and easy uncertainty.
- It all depends on perspective, but honest thinkers will agree that some of these regulations are necessary. It is only the matter of, how much disagreement ensues.
- Government around the world are exploring the block chain regulation needs.
- The challenge for every block chain stakeholders involved shaping government and other agency to make sure rules emerged makes sense for all concerned.
- Consortium of government and industries are forming address regulatory issues.

4.4. Scalability

- It is assumed that Block chain are slow, but that is not the case, small to medium sized network can boost transaction speeds that can exceed conventional databases.
- Transaction speed becomes an issues when thousands of nodes try to execute high volume transactions.
- For example, Visa Processing involved 2.000 transactions per seconds (TPS). Ethereum currently taps out around 15.
- So, if Visa like application is run on Ethereum, you won't get far.

- Thus, if block chain is to be scaled high, it needs some work around. While making it robust at high speeds as well as inherent advantages of DLT, this will be the greatest challenge block chain developers are facing today.

4.5. Integration

- Integration of legacy systems with DLT solutions poses hurdle for the industry. This is not because technical hurdler cannot be overcome, but there are few use cases where it has been done.
- Developers are targeting this end of the market.
- Greatest Reward will be reaped to those that specialize in interfacing block chain with finance platforms and healthcare.

5. POSSIBLE FUTURE TRENDS.

Block chain has shown great potential in academia as well as industry. Possible future Directions includes: Block chain testing, big data analytics and block chain application.

A. Block chain Testing

- Recently over 700 cryptocurrencies and different kinds of block chain are listed till now. However, some developers tends to lure investors by falsifying their block chain performance.
- Besides, when users wants to combine business with block chain, they have to know which block chain fits their requirements. So, there is a need for a block chain testing mechanism.
- Block chain testing is divided into 2 phases: standardization and testing phase. In the standardization phase, all criteria have to formed and agreed upon. When block chain is born, testing is done to check if block chain work well based on valid criteria defined as developers claim.
- As of testing phase, block chain is to be tested with different use cases.

B. Big data analytics

- Block chain can be combined with big data. Here we categorized the combination in to two types: data analytics and data management.
- As for Data analytics, Transactions on block chain can be used for analyzing big data. For Example, Pattern can be extracted for user trading. Users predict their potential partners trading behaviors.
- When it comes to data management, block chain stores important data as it being distributed and secure.

C. Block chain Applications

- As of now, Block chains are used in financial domain, but more and more applications are appearing in different fields. Traditional industries are taking block chain into consideration and using it in their field to enhance their system. For example: user reputation can be stored on block chain.
- A smart contract is computerized transaction protocol that executes terms of contract. This is the approach that can be implemented with block chain.
- In terms of block chain, smart contract is a fragment of code that are executed automatically by miners. Smart Contract has one such transformative potential in fields like IOT and financial services.

6. CONCLUSIONS

With its characteristics such as decentralization, immutability, peer to peer, Block chain has shown its potential for transforming the traditional industry. We first gave overview of block chain technologies including Architecture, characteristics. Then we listed Types, challenges and summarize future aspect of Block chain.

Nowadays, Block chain applications are emerging and we plan to conduct a detailed research on block chain based applications in the future

7. REFERENCES

- www.journals.elsevier.com
- technorely.com
- academy.binance.com
- medium.com
- www.ledgerjournal.org
- www.geeksforgeeks.org
- 101blockchains.com
- www.investopedia.com
- mlsdev.com
- www.pluralsight.com