Unit - 2

Consensus

2.1 Consensus: Requirements for the consensus protocols, Proof of Work (PoW), Scalability aspects of Blockchain consensus protocols

2.1.1 Requirements for the consensus protocols

Blockchain is decentralized and distributed ledger technology. It is used to keep records of transaction over network. In blockchain there is no other third party exist who validate the information. The block chain is distributed over many nodes in the network.

The blockchain provides various properties such as follows:

- Security
- Transparency
- Decentralization
- Immutability
- Accountability

The consensus protocols play important role in blockchain. The consensus is called by the backbone of the blockchain which provides the validator to all the nodes present in the network. All the nodes in the network verify the transactions by using cryptographic hash function.

All the properties of blockchain can be applied based on consensus protocols that network is using. It is impossible to hack the blockchain network by hacker due to consensus protocol. There are various types of consensus used to solve the problem in blockchain.

Following are some consensus protocols:

- Proof of Work (Pow)
- Practical Byzantine Fault Tolerance (Pbft)
- Proof of Stake (Pos)
- Proof of Burn (Pob)
- Proof of Capacity

Proof of work

- This consensus algorithm is used to solve complex mathematical puzzles. The mathematical puzzles require lot of computational power and then node who solves the puzzle soon that gets the mine to the next block.
- The bitcoin uses the Proof of Work consensus algorithm. In this consensus the miner is selected for next block generation.

Practical byzantine fault tolerance (PBFT)

- The PBFT consensus algorithm is used in asynchronous system where no upper bound on when the response to the request will be received. This consensus algorithm is used on low overhead time.
- Practical byzantine fault tolerance selves the many problems regarding to byzantine fault tolerance solution which is available. BFT is the consensus used when some of the nodes in the network fail to respond or respond incorrect information. This algorithm is used in blockchain and distributed computing.

Proof of stake (PoS)

- It is alternative of proof of work (Pow). The PoS used by Ethereum which is shifted from PoW consensus. In this consensus algorithm the validators invest on the coin of the system by locking up some of their coins as stake.
- Instead of investing on expensive hardware to solve complex puzzles validators invest on locking up coins as stake. After that all the validators start validating the blocks. Validators placed bet on the block that they want to be added if the block is discovered the block is added into the chain.
- As the block gets added by validators, they win reward according to their bets and their stakes get increase respectively. At the end, a validator is chosen to generate a new block based on their economic stake in the network. Hence PoS encourages validators through an incentive mechanism to reach an agreement.

Proof of burn (PoB)

- The validators in the PoB invest on 'burn' coins by sending it to address from where the loss is irretrievable. The validators do not invest on expensive hardware equipment.
- The validators commit the coins to unreachable address to achieve privilege to mine on the system based on random selection process. Hence the burning means the validators committing the long-term investment on their short-term loss.
- The PoB implemented will cause the native currency to be burn by validators in bitcoins. The more coins the validator burn, better are their chances of being selected to mine the next block.

Proof of capacity (PoC)

- In the proof of capacity consensus algorithm, the validators invest on the hard drive space.
- The validators do not invest on the expensive hardware or burning coins.
- As validator gets more hard drive spaces, they can get chance to mine for next block and can earn block reward.

2.1.2 Proof of Work (PoW)

The proof of work is common consensus algorithm. It is a form of cryptographic zero knowledge proof. It used by popular crypto currencies as bitcoin and litecoin. It requires the proof of work done by the participant node and submitted by them which qualifies them to receive the right to add new transaction in blockchain.

The bitcoin takes the longer time to process mining mechanism and need higher energy consumption. This consensus mechanism prevents user double spending their coins and ensures that this chain is difficult to attack or overwrite.

The power of proof is developed by Cynthia Dwork with Moni Naor in 1993 than it is applied by Satoshi Nakamoto in bitcoin project at 2008. The 'proof of work' term is used by Markus Jakobsson with Ari Juels in 1999. It is the first consensus algorithm used in block chain technology. The PoW consensus algorithm is based on hash value and the validating transactions. The hash value is not considered until it gets number of trailing zeroes in the hash value.

The number with specified number of trailing zeroes in hash function over blockchain is called as Nonce. The PoW consensus algorithm is used by permission less public ledgers in blockchain. The protocol uses the computational resource to reach the consensus. The block in the blockchain are considered in the linear structure. In the PoW algorithm.

This consensus algorithm is used to solve complex mathematical puzzles. The mathematical puzzles require lot of computational power and then node who solves the puzzle soon that gets the mine to the next block. The bit coin uses the Proof of Work consensus algorithm.

The mining aspect of bit coins are decided by solving the cryptographic puzzle where random integer is found which is used to get specified number of leading zeroes in the hash function.

In this consensus the miner is selected for next block generation. The users can validate and signed every transaction by using public and private key assigned in blockchain network.

The PoW consensus is used by following crypto currencies;

- Litecoin
- Ethereum
- Monero coin
- Dogecoin

Classes Of Proof Of Work Consensus

There are two classes of proof of work consensus such as:

1. Challenge response protocols
2. Solution verification protocol

1. Challenge Response Protocols

In this protocol there is a direct link between the requester (client) and provider (server). The server chooses a challenge such as an item in a set with property then the client will search the relevant response in the set.

The response from client is sent back and checked by server. The challenge is chosen by server therefore the difficulty can be adapted to its current load.

If the solution of the challenge response protocol is known within bounded search space then the client works may be bounded. The following figure specifies the challenge response protocol.

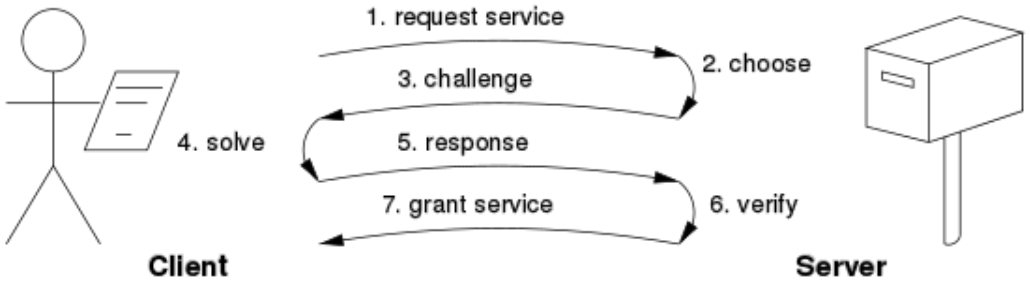

Fig. No. 1 Proof of Work challenge response.svg

2. Solution Verification Protocol

This protocol does not assume the link as result. The problem should be self-imposed before the solution sought by client. The server checks the problem and solution sent by client.

Some problems are unbounded probabilistic iterative procedures such as hashcash. The following figure shows the solution verification protocol.

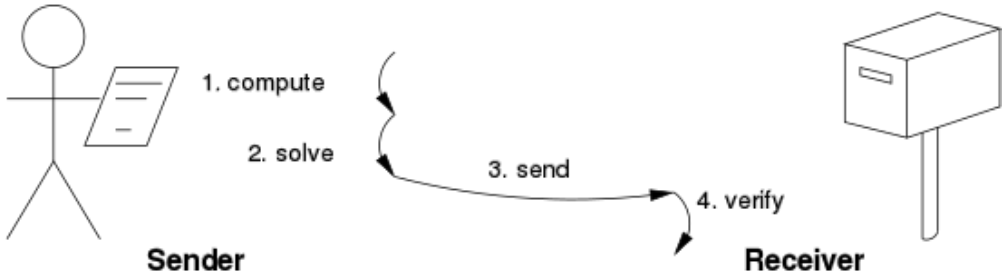

Fig. No. 2 Proof of Work solution verification.svg

Disadvantages of Proof of Work:

- ✓ The PoW consensus required more power consumption.
- ✓ It is resource intensive protocol as the miners waste more resource consumption in solving the harder mathematical puzzles.
- ✓ The risk of corrupting the network is 51% or more than that in PoW consensus.
- ✓ It is time consuming process. The PoW requires time to solve the mathematical puzzles.

Function of Proof of Work Consensus

Following list mentions the functions of proof of work protocol used in blockchain.

- Integer square root modulo a large prime
- Weaken flat shamir signature
- Hash sequence
- Puzzles
- Moderate
- Mbound
- Merkel tree
- Guided tour puzzle protocol
- Partial hash inversion

2.1.3 Scalability aspects of Blockchain consensus protocols

The blockchain is the record of transaction. The ability to keep support on increasing load of transaction as increasing in number of nodes is the scalability of blockchain.

The blockchain should be perform substantially in better scalability on the network. The permissioned blockchain uses the computationally inexpensive consensus mechanism.

Permissioned blockchain uses the consensus mechanism which is inexpensive computationally as compared to proof of work protocol. Therefore, the scalability and performance of permissioned blockchain is better as compared to permission-less blockchain.

Hyper-ledger fabric offers additional innovation with respect to roles of nodes including peers and orders.

2.2 Permissioned Blockchains: Design goals, Consensus protocols for Permissioned Blockchains

2.2.1 Permissioned Blockchains

The permissioned blockchain is the additional security system where only permissioned participant get access. The permissioned blockchain is different than public and private block chains.

The specific participant gets the access to do some actions which is maintained by access control layer. The permissioned blockchain is more secure than other blockchain over bit coins technology as it has access control layer. The participant who want identity, security and role definition in blockchain they will be favoured individually in the blockchain.

Yet permissioned blockchain is not so common as bitcoins and other crypto currencies like public blockchains. Permissioned blockchain have enabled new applications that depends on privacy and security such as:

- Supply chain provenance tracking

- Claims settlement
- Identity verification

Characteristic of Permissioned Blockchain

The permissioned blockchain is also known as private or permissioned sandboxes. It is closed network in which the designated parties, members of consortium, interact and participate in consensus and data validation are included.

Following are the key characteristics of permissioned blockchain.

- Controlled transparency based on goals of participating organization
- Development by private entities
- Lack of central authority
- Lack of anonymity

Permissioned blockchain working

The permissioned blockchain working can be done in multiple ways. The blockchains are defined as to read, write and access the information with permission in some blockchains. In permissioned blockchain some action to be performed by participants and their role in blockchain are control by intrinsic configuration of such blockchain.

The permissioned blockchain has control over participant's transactions and their role definition where the access and contribution of participant are seen. The maintaining of identity of each participant in blockchain on network is called as permissioned blockchain.

The permissioned blockchain is also referred as Consortium Blockchain. This blockchains are different than private where only known nodes can participate in the network.

The permissioned blockchain can be used by manufacturer producing a product industry where supply chain management is required. Permissioned blockchain is used in hyper ledger and chain.

Pros and Cons of Permissioned Blockchain:

Pros

- The decentralization is incremental
- Privacy is strong
- For specific use the customizability is available
- Performance and scalability

Cons

- Risk of corruption increases due to fewer participant
- Consensus can be easily overridden due to owners and operators can change the rules of consensus, immutability and mining
- Less transparency due to number of participants is limited

2.2.2 Design goals

The blockchain is decentralized for giving trust for each participant in the network. Therefore, the extent of decentralization is required for better design of blockchain.

Following are some of the design goals are defined in blockchain:

Peer to peer data distribution

- ✓ The peers are mostly privileged, equipotent participant in the network.
- ✓ The workload of network is distributed among the peers. Hence it is called as peer to peer network.
- ✓ Peers can be consumers of resources, suppliers, in contrast to the traditional client server model.

Decentralization

- ✓ How the members of consortium choose to structure their business relationships matters in permissioned blockchain to select the degree of decentralization.
- ✓ The no central control means it is not relevant here since the consortium manages entities in permissioned blockchain.
- ✓ The decentralization extension and quality are based on numbers of peers, the expected numbers of bad nodes in network and the type of consensus mechanism th members agree to.
- ✓ Permissioned blockchain always employ an algorithm such as Byzantine Fault Tolerance (BFT) which is differ from proof of work algorithm used in permission-less blockchain.
- ✓ The decentralization is the aspect of blockchain design it is having right governance model more important in blockchain.
- ✓ Power and control structure may not be evenly distributed in permissioned blockchain.
- ✓ The decentralization represents the network without central third party in the network.
- ✓ The network is strongly maintained by peer to peer network.
- ✓ The information is not passed by single point.

Immutability

- ✓ The object which state cannot be modified or changed after it is created is called as immutable object.
- ✓ The mutable files can be overwritten, or any changes can be made by participant on relational database.
- ✓ In the immutable files the data changes are recorded as separate time stamped file on immutable database.

Transparency

- ✓ The transparency in permissioned blockchain may not be important as compared to permission-less blockchain.
- ✓ It is depending on how business relationships are set up and how the blockchain is configured.

- ✓ The crypto currencies incentives are not built in into some of the permissioned blockchains.
- ✓ The primary incentive is to reduce the cost, time and ease of sharing in permissioned blockchain.

Trustless

- ✓ Power and trust are shared among all the participant to develop, mine and consume the network rather than concentrating on single individual or entity.
- ✓ The consensus mechanism is used to build trust in blockchain network.

2.2.3 Consensus protocols for Permissioned Blockchains

The consensus protocols are used to maintain common agreement in between all the nodes present in the blockchain network. There is various consensus model used to maintain fairness and transparency in blockchain network.

The consensus is chosen based on foundation of certain objectives as follows. The participants aim to collect all the agreement from the group of blockchain. Every participant of group needs to show the interest on that agreement.

Every participant will work as a team as they are putting their interest aside on blockchain network. Every participant gets equal rights to vote on network. The voting should be done by every participant of blockchain. Every participant should remain active on blockchain where every participant has equal responsibilities than others.

The permissioned blockchain uses the different consensus protocols than other permission less blockchain. There is various consensus are developed today for permissioned blockchain.

Following are the consensus algorithm that are used by permissioned block chain:

- Practical Byzantine Fault Tolerance (PBFT) consensus
- Federated Consensus
- Round robin consensus

Practical Byzantine Fault Tolerance (PBFT) consensus

Practical Byzantine Fault Tolerance (PBFT) consensus used mostly by permissioned blockchain. The permissioned blockchain need to facilitate consensus, each node exists in internal state of blockchain.

Each node receives message and then it is used to perform computation or operation on blockchain with respect to their internal state. The computation will be send to the other nodes to validate either transaction is valid or not.

After validating the transactions from all the nodes over network will be broadcasted by other nodes decision in the network. The consensus decision confirmed by total confirmation collected by all the nodes.

The PBFT consensus is used by low latency storage system like digital assets backed platform where are large number of transactions to carried out.

The PBFT is beneficial in digital assets backed platform.

Federated Consensus

The nodes in blockchain puts their trust on the set of signers from network which helps them to reach the consensus stage. The block signer uses the single block generator to receive, hold and filter all the transactions this process will be carried out in efficient manner.

The block validation process is done by signers on their generator signatures. Every block is validated with block generator sign and set of conditions which are fulfil by the network.

As the network get enough signatures to the block generator then block will get published to the network. The federated consensus is useful in security and transparency. This consensus is used by cross border remittance, real time KYC, etc. Stellar and Ripple blockchain uses the federated consensus.

Round robin consensus

The validators in round robin consensus take part by signing votes for blocks.

In round robin there are three main votes to be done by validators as:

- ✓ Prevote
- ✓ Precommit
- ✓ Commit

If the receiver got more than two third commit means to receive commits from two third majority of validators. When the two third majority of validators will be signed and broadcasted commits for that block then the block is considered as committed by the network.

The round-based protocol is used to determine the next blockchain at each height of the blockchain. Each round has three steps as propose, prevote and precommit with two special steps as commit and new Height. Every propose, prevote and precommit step take one third of total time allocated by that round.

Each round becomes longer than the previous round by small increase of time. This consensus s achieves in limited concurrent network. The round robin model is ideal for trade, finance and supply chain industries. The multichain and tender mint Blok chains uses the round robin consensus protocol.