classmate
Date 30/6/21
Page

UNIT:-III

Distributed Consensus:-

* Nakamoto Consensus:-

The Nakamoto Consensus, as its name implies, was created by Satoshi Nakamoto, Bitcoin's pseudonymous founder in Bitcoin White Paper Nakamoto Consensus gave birth to Blockchain technology.

The Nakamoto Consensus is a set of rules that verify the authenticity of a blockchain network, using a combination of proof-of-work consensus algorithm on a Byzantine Fault tolerance peer-to-peer network

Prior to Satoshi's creation of Nakamoto Consensus, Byzantine fault tolerance was used in peer-to-peer network to maintain their authenticity. for a variety of cryptography-related projects and even some early form of digital currency

Scanned with CamScanner

However, there were problems in just BFT (Byzantine fault tolerance) system the voting system for Consensus requires a rotating election of leader. If leader act maliciously they can be removed by a vote from other nodes. In case of Bitcoin the Individual removal of leader will pose a huge problem when it comes to Scaling.

Satoshi's addition to using BFT on a P2P (peer-to-peer) network was to add idea of a PoW Consensus algorithm, where node had to mine to create fully trustless, decentralized network

PoW is the idea that miner support the network with literal "work". i.e Computing power. PoW is when full nodes competes to mine "blocks" faster than other nodes, the faster nodes will get reward, thus creating new bitcoin.

It creates an environment where honest node thrive & malicious nodes r discouraged

Scanned with CamScanner

How blockchain technology prevents double spending since the time-stamped blocks on blockchain makes it immutable.
The longest chain is the valid chain, since it is supported by majority of miner's computing power.

In Nakamoto Consensus, there is no block selection "voting" process like BFT. Instead the miners compete to solve a cryptographic puzzle.

Another aspect of Nakamoto Consensus comes from Satoshi putting a hard cap on amount of Bitcoin, there will only ever be a total of 21 million of cryptocurrency in circulation.
This creates artificial scarcity, which again add to the incentives for miners to participate in network

Nakamoto Consensus created the foundation for the large blockchain and cryptocurrency community. Satoshi created a consensus model that can be used for infinite no. of usecases besides bitcoin.

Scanned with CamScanner

* Proof - of - Work :-

The idea for proof-of-work was first published by Cynthia Dwork and Moni Naor in 1993, and was later applied by Satoshi Nakamoto in Bitcoin paper 2008.

PoW Consensus is the mechanisms of choice for majority of cryptocurrencies currently in circulation.

The purpose of Consensus algorithm is to bring all the nodes in an agreement that is, trust one another, in an environment where the nodes don't trust each other

All the transactions in new block is validated, miners perform computation work for adding a block to blockchain by solving a complex mathematical problem. Hence named proof-of-work. With time, mathematical problem becomes more complex.

Scanned with CamScanner

The process of verifying the transactions in the block to be added, organizing these transactions in a chronological order in the block and announcing the newly mined block to network doesn't take much energy & time. The energy consuming part is solving the hard mathematical problem to link new block to last block in valid blockchain

The First block in blockchain is called Genesis block and has no previous block hash value.

Changing the block requires regenerating all successors and redoing the work they contain which is practically impossible. This protects blockchain from tampering.

Bitcoin's PoW System:-

Bitcoin uses the Hashcash Proof of work system as the mining basis.

The hard mathematical problem can be written in abstract way like

Scanned with CamScanner

Given data A, find number 'x' such that hash of x appended to A results in a number lesser than B

The most widely used pow Consensus is based on SHA-256 and was introduced as part of Bitcoin.

→ Features of PoW system:-
There are mainly two features that have contributed to wide popularity of this Consensus protocol they are
1. It is hard to find a solution for mathematical problem
2. It is easy to verify the Correctness of the solution.

→ Main Issues with PoW:-

1. The 51% Risk:- If a Controlling Entity owns more than or equal to 51% of nodes in network, the entity can Corrupt the Blockchain by gaining majority of network.

Scanned with CamScanner

2. Time Consuming :- Miners have to check over many nonce values to find the right solution to puzzle that must be solved to mine the block. It is time consuming.

3. Resource Consumption :- Miners consume more computational power to solve hared mathematical problem. It leads to waste of precious resources.

Transactions are not instantenous as it takes 10-60 min for confirmation.

Cryptocurrencies Using PoW :-
litecoin, ethereum, Monero coin, Doge coin, Bitcoin.

Alternatives to PoW :-
Proof of Stake, Proof of Burn etc.

* Proof of Stake :-

The PoS Concept states that a person can mine or validate block transactions according to how many coins they hold. This means that the more coins owned by a miner, the more mining power they have.

Scanned with CamScanner

PoS is an alternative PoW Consenses. In PoW, mining requires a great deal of computation power to solve the hard mathematical puzzle. The computation power requires huge amount of electricity.

The PoS seeks to address these issue by attributing mining power to the proportion of coins held by a miner (virtual mining). This way the miner who own 3% of coins can theoretically mine 3% of blocks.

With PoS, the attacker would need to obtain 51% of the cryptocurrency to carry out 51% attack. Although it would be difficult & Expensive to accumulate 51% of a reputable digital coin. A miner with 51% share/stake in Coin would not have any interest to attack a network

In PoS no mining hardware is involved so there is no concern about ASIC Advantage.

Scanned with CamScanner

A virtual mining puzzle acheives all the goals of ASIC-Resistant puzzle.

NXT is an example of cryptocoin that uses PoS method.
Peercoin uses a mixed system (PoW + PoS)
Ethereum (ETH) is in process of switching to PoS system.

* Proof of Burn :-

The Concept of PoB idealized by Iain Stewart. It was proposed as a most sustainable alternative to PoW Consenses algorithm. PoB looks like PoW but with reduced rates of energy consumptions.

The block validation process of PoB based network does not require the use of powerful Computational resources like ASICs. Instead the cryptocurrencies are intentionally burned as a way to invest resource in blockchain. So miner do not invest in physical resource. Miners invest in virtual mining power.

Scanned with CamScanner

By performing coin burns, users are able to demonstrate their commitments to the network gaining the right to mine & validate the transactions.

The prpcess of burning coins represents virtual mining power, the more coins a user burns in favour of system the more mining power User gains. Thus higher chances to be choosen as next block validater.

The process of burning coins consists of sending these to public verifiable address where they become inaccessible & useless.
The address are randomly generated without having any private key associated with them!

The process of burning coins reduces the market availability and creates Economic Scarcity, causing a potential Increase in its value.
.. More than that, Coin burning is another way of Investing in Security of network.

Scanned with CamScanner

Similarly to PoW, PoB provides block rewards to miners within certain period of time, the reward are expected to cover initial investment of burned coins.

Advantages:-

1. Reduce power Consumption
2. No need for mining ~~HW~~ hardware
3. Encourages long-term Commitment
4. Coin tends to less Centralized

Disadvantages:-

1. The verification of work done by miners tends to be delayed.
2. The process of burning coin is not always transparent or easily verifiable by the average user
3. Some say PoB is not eco-friendly. More testing is needed to be done to confirm its efficiency & security.

Scanned with CamScanner

* Difficulty level :-

The difficulty target is the one that drives the POW in Bitcoin. The idea is that once a block is filled with valid transactions, the hash of the block is need to be calculated to be less than difficulty hash in same header.

The nonce in header starts from zero. The miner has to keep on incrementing this nonce and hashing the header till the hash value is less than target.

The difficulty bits of four bytes (32 bits) in header define what would be target hash value (256 bits) for that block to be mined. The nonce should be found in such a way that the hash of entire header should be less than target value.

Lower the target value, more difficult it would be to find header hash. Bitcoin uses SHA256, everytime you hash a block header that o/p is any no. b/w 0 to 2^{256}.

Scanned with CamScanner

If with your nonce the hash is less than target then the block will be accepted by entire network.

The target can be derived from 4-byte (8 hexadecimal numbers) difficulty bits in header using pre-defined formula that every node has by default.

Formula to Compute difficulty.

$$target = Coefficient * 2^{(8*(Exponent-3))}$$

If four byte difficulty bits in hex form are 0x1b0404cb

Exponent → 0x1b (first two hex digit)

Coefficient → 0x0404cb (rest of digits)

$$target = 0x0404cb * 2^{(8*(0x1b-0x03))}$$

$$target = 0x0000000000000404$$

Bitcoin is designed such that every 2016 blocks should take 2 weeks to be generated. It would take around 10min for each block.

Scanned with CamScanner

But there is possibility that block get generated within a minute or will take 15 mins to be generated. So difficulty is designed to increase or decrease

Assume T be amount of time taken for 2016 blocks.

So, difficulty target $\times \frac{T}{2 \text{ weeks}}$ ∴ will

be increased if T was less & decreased otherwise.

Now, it is evident that difficulty is adjustable.

After every 2016 blocks all blocks compute their new difficulty value. Using the formula.

$$\text{New Target} = \text{old target} * \left(\frac{T}{2 \text{ weeks}}\right)$$

$$\text{New target} = \text{old target} * \frac{(\text{time taken by 2016 block})}{12,09,600 \text{ sec}}$$

Scanned with CamScanner

The idea is to decrease the difficulty target when it requires to increase the complexity. So it takes more time.

* Sybil Attack:-

It is a type of attack seen in peer-to-peer networks in which a node in the network operates multiple identities actively at the same time and undermines the authority/power in reputation system.
The main aim of this attack to gain majority of influence in network to carry out illegal actions in the system.

A single entity has the capability to create and operate multiple identities

Types of Sybil Attack:-

1. In a direct attack, the honest nodes are influenced directly by sybil nodes
2. In an Indirect attack, the honest nodes are attacked ~~with~~ by sybil nodes which communicates directly with sybil nodes. This middle node is compromised as it's under malicious influence of sybil node.

Scanned with CamScanner

How Bitcoin network prevents Sybil Attack:-

Bitcoin network uses Pow Consensus to prove the authenticity of any block that is added to blockchain. A considerable amount of computing power is required to do work which provide Incentives to miners.

Currently 12.5 bitcoins are rewarded for every block mined, and no Incentives for faulty work.
A type of Sybil attack, called the 51% attack is also practically Impossible in bitcoin network because there are so many miners.

Ways to prevent Sybil attack:-

1. Giving different powers to different members:- This is on the basis of reputation system. Members with different power levels are given different reputation levels.

2. Cost to create an Identity:- To prevent multiple fake identities in the

Scanned with CamScanner

network, we can put cost for every identity that aims to join the network.

3. Validation of Identities before joining the network:

Direction validation :-
An already established member verifies new joiner of network.

Indirect validation :-
An established member verifies some other members who can in turn verify some other new comer in the network. As the new joiner are verified & validated by an established entity, the new joiner are trusted to be honest.

Energy utilization and alternate :-

Scanned with CamScanner