Consensus Mechanism

Consensus Protocol

- The consensus protocol makes sure that every new block that is added to the Blockchain is the one and only version of the truth that is agreed upon by all the nodes in the Blockchain
- Consensus protocols form the backbone of blockchain by helping all the nodes in the network verify the transactions.
- Bitcoin uses proof of work (PoW) as its consensus protocol, which is energy and time-intensive.
- The rate of verification of transact cions in Bitcoin is relatively slow compared to Visa and MasterCard’s likes. Therefore, alternate consensus protocols were proposed.

Types of consensus protocols

- Proof of Work
- Proof-of-Stake
- Proof of Elapsed Time

Proof of Work

- Proof of Work consensus is the mechanism of choice for the majority of cryptocurrencies currently in circulation.

- The algorithm is used to verify the transaction and create a new block in the blockchain.

- Cryptocurrencies like Litecoin, and Bitcoin are currently using PoW. Ethereum was using PoW mechanism, but now shifted to Proof of Stake(PoS).

Purpose of PoW

The **purpose** of a consensus mechanism is to bring all the nodes in agreement, that is, trust one another, in an environment where the nodes don’t trust each other.

All the transactions in the new block are then validated and the new block is then added to the blockchain.

The block will get added to the chain which has the longest block height

❑ Miners(special computers on the network) perform computation work in solving a complex mathematical problem to add the block to the network, hence named, Proof-of-Work.

❑ With time, the mathematical problem becomes more complex.

PoW consensus algorithm

- **There are mainly two features that have contributed to the wide popularity of this consensus protocol and they are:**

❑ It is hard to find a solution to a mathematical problem.

❑ It is easy to verify the correctness of that solution.

The PoW consensus algorithm involves verifying a transaction through the mining process.

- **Mining:**

The Proof of Work consensus algorithm involves solving a computationally challenging puzzle in order to create new blocks in the Bitcoin blockchain. The process is known as 'mining', and the nodes in the network that engages in mining are known as 'miners'.

- The incentive for mining transactions lies in economic payoffs, where competing miners are rewarded with 6.25 bitcoins and a small transaction fee.
- This reward will get reduced by half its current value with time.

PoW consensus algorithm

Energy and Time consumption in Mining:

- The process of verifying the transactions in the block to be added, organizing these transactions in chronological order in the block, and announcing the newly mined block to the entire network does not take much energy and time.
- The energy-consuming part is solving the ‘hard mathematical problem’ to link the new block to the last block in the valid blockchain.
- When a miner finally finds the right solution, the node broadcasts it to the whole network at the same time, receiving a cryptocurrency prize (the reward) provided by the PoW protocol.

Mining reward:

- Currently, mining a block in the bitcoin network gives the winning miner 6.25 bitcoins.
- The amount of bitcoins won halves every four years. So, the next deduction in the amount of bitcoin is due at around 2024(with the current rate and growth).

PoW consensus algorithm

- The miners bundle up a group of transactions into a block and try to mine. To mine it, a hard mathematical problem has to be solved.
- This problem is called the proof of work problem which has to be solved to show that the miner has done some work in finding out the solution to the problem and hence the mined block must be valid.
- The answer to the problem needs to be a lower number than the hash of the block for it to be accepted, known as the ‘**target hash**’.
- A miner continues testing different unique values (known as a nonce(s)) until a suitable one is produced.
- The miner who manages to solve the problem gets the bitcoin reward and adds the block to the blockchain by broadcasting that the block has been mined.

Proof-of-Work consensus mechanism issues

- **The 51% risk**: If a controlling entity owns 51% or more than 51% of nodes in the network, the entity can corrupt the blockchain by gaining the majority of the network.

- **Time-consuming**: Miners have to check over many nonce values to find the right solution to the puzzle that must be solved to mine the block, which is a time-consuming process.

- **Resource consumption**: Miners consume high amounts of computing power in order to find the solution to the hard mathematical puzzle. It leads to a waste of precious resources(money, energy, space, hardware). It is expected that 0.3% of the world's electricity will be spent to verify transactions by the end of 2028.

- **Not instantaneous transaction:** Transaction confirmation takes about 10–60 minutes. So, it is not an instantaneous transaction; because it takes some time to mine the transaction and add it to the blockchain thus committing the transaction.

Proof of Stake

- **What is Proof-of-Stake:**

As understandable from the name, nodes on a network stake an amount of cryptocurrency to become candidates to validate the new block and earn the fee from it.

Then, an algorithm chooses from the pool of candidates the node which will validate the new block. This selection algorithm combines the quantity of stake (amount of cryptocurrency) with other factors (like coin-age based selection, randomization process) to make the selection fair to everyone on the network.

.Coin-age based selection:

The algorithm tracks the time every validator candidate node stays a validator. The older the node becomes, the higher the chances of it becoming the new validator.

- **Random Block selection:**
  The validator is chosen with a combination of ‘lowest hash value’ and ‘highest stake’. The node having the best weighted-combination of these becomes the new validator

A typical PoS based mechanism workflow:

1. Nodes make transactions. The PoS algorithm puts all these transactions in a pool.

2. All the nodes contending to become validator for the next block raise a stake. This stake is combined with other factors like ‘coin-age’ or ‘randomized block selection’ to select the validator.

3. The validator verifies all the transactions and publishes the block. His stake still remains locked and the forging reward is also not granted yet. This is so that the nodes on the network can ‘OK’ the new block.

4. If the block is ‘OK’-ed, the validator gets the stake back and the reward too. If the algorithm is using a coin-age based mechanism to select validators, the validator for the current block’s has its coin-age reset to 0. This puts him in a low-priority for the next validator election.

5. If the block is not verified by other nodes on the network, the validator loses its stake and is marked as ‘bad’ by the algorithm. The process again starts from step 1 to forge the new block.

Advantages of PoS:

- **Energy-efficient:**
  As all the nodes are not competing against each other to attach a new block to the blockchain, energy is saved. Also, no problem has to be solved(as in case of Proof-of-Work system) thus saving the energy.

- **Decentralization:**
  In blockchains like Bitcoin(Proof of Work system to achieve distributed consensus), an extra incentive of exponential rewards are in place to join a mining pool leading to a more centralized nature of blockchain. In the case of a Proof-of-Stake based system(like Peercoin), rewards are proportional(linear) to the amount of stake. So, it provides absolutely no extra edge to join a mining pool; thus promoting decentralization.

- **Security:**
  A person attempting to attack a network will have to own 51% of the stakes(pretty expensive). This leads to a secure network.

Weakness of a PoS mechanism:

- **Large stake validators:**
  If a group of validator candidates combine and own a significant share of total cryptocurrency, they will have more chances of becoming validators. Increased chances lead to increased selections, which lead to more and more forging reward earning, which lead to owning a huge currency share. This can cause the network to become centralized over time.

- **New technology:**
  PoS is still relatively new. Research is ongoing to find flaws, fix them and making it viable for a live network with actual currency transactions.

- **The ‘Nothing at Stake’ problem:**
  This problem describes the little to no disadvantage to the nodes in case they support multiple blockchains in the event of a blockchain split(blockchain forking). In the worst-case scenario, every fork will lead to multiple blockchains and validators will work and the nodes in the network will never achieve consensus.

Blockchains using Proof-of-Stake:

- Ethereum(Casper update)
- Peercoin
- Nxt

Proof of Elapsed time

- Proof of Elapsed time is a network consensus protocol developed by the Intel Corporation. The algorithm is predominantly used in permissioned blockchain ledgers. The hardware used in PoET is specially designed for this protocol. For example, Intel Software Guarded Extension (SGX) is used in networks using PoET.
- This consensus protocol is used to allocate blocks to miners on the network. In permissioned blockchain systems, the miners' identity is determined before allowing access into the network. Therefore, anonymity is not a feature in this protocol.
- Each node in the network is assigned a random waiting time. The first node to complete the randomly chosen period validates the new block. The specialized hardware puts the processor to sleep during the wait time—this repeats over all the blocks in the network.

Proof of Elapsed time

Disadvantages

- The major disadvantage of this algorithm is its dependency on specialized hardware. This exposes it to various security vulnerabilities due to the lack of standardized and tried and tested protocols.

Applications

- IBMs Hyperledger Sawtooth supports PoET mechanism for custom blockchain applications development.

Smart Contracts

- Introduction to Smart Contracts.
- Working of Smart Contracts.
- Decentralized Applications.
- Challenges in Decentralized Applications.

Introduction to Smart Contracts.

- Smart contracts are simply programs stored on a blockchain that run when predetermined conditions are met.
- They typically are used to automate the execution of an agreement so that all participants can be immediately certain of the outcome, without any intermediary’s involvement or time loss.
- They can also automate a workflow, triggering the next action when conditions are met.

Introduction to Smart Contracts..cont

Benefits of smart contracts

1.Speed, efficiency and accuracy

Once a condition is met, the contract is executed immediately. Because smart contracts are digital and automated, there's no paperwork to process and no time spent reconciling errors that often result from manually filling in documents.

2. Trust and transparency

Because there's no third party involved, and because encrypted records of transactions are shared across participants, there's no need to question whether information has been altered for personal benefit.

Introduction to Smart Contracts..cont

3. Security

Blockchain transaction records are encrypted, which makes them very hard to hack. Moreover, because each record is connected to the previous and subsequent records on a distributed ledger, hackers would have to alter the entire chain to change a single record.

4. Savings

Smart contracts remove the need for intermediaries to handle transactions and, by extension, their associated time delays and fees.

Working of Smart Contracts.

1. Parties agree to terms and conditions

- The creation of a smart contract starts with an agreement. The parties wishing to transact or exchange goods or services must agree on the terms and conditions of the arrangement. The parties involved must also decide how the smart contract will work, including what conditions must be met for the contract to execute and whether it will execute automatically.

2. The smart contract is created

- The transacting parties have multiple options to create a smart contract, ranging from coding it themselves to working with a smart contract developer. The terms of the agreement are translated into a programming language to create the smart contract, which specifies rules and consequences just as a traditional legal contract would.
- Creating a smart contract can be simple, but it’s important to note that a poorly designed smart contract is a major security risk. It’s critical to fully verify the smart contract’s security during this step.

Working of Smart Contracts..cont

3. The smart contract is deployed

- Once the securely designed smart contract is ready, the next step is to deploy it to a blockchain. The smart contract is broadcast to the blockchain just like any other crypto transaction, with the code of the smart contract included in the transaction's data field. The smart contract is live on the blockchain once the transaction is confirmed, and it cannot be revoked or changed
- That last part is important. Deploying a smart contract to a blockchain is like buying an item and intentionally throwing away the receipt. There are no returns, no refunds, and no exchanges—no exceptions.
- **4. Triggering conditions are met**
- A smart contract works by monitoring the blockchain or other credible information source for certain conditions or triggers. These triggers can include almost anything that can be verified digitally—a date reached, a payment completed, a monthly bill received, or any other verifiable event. Trigger conditions may also be met when one or more parties to the contract perform a specific action.

Working of Smart Contracts..cont

- **5. The smart contract is executed**
- When the trigger conditions are satisfied, the smart contract executes. A smart contract that executes automatically may perform one or several actions, such as transferring funds to a seller or registering a buyer’s ownership of an asset.
- **6. The contract result is recorded to the blockchain**
- The smart contract’s execution is immediately broadcast to the blockchain. The blockchain network verifies the actions performed by the smart contract, records its execution as a transaction, and stores the completed smart contract on the blockchain. The record of the smart contract is generally available for review by anyone at any time.

Decentralized Applications.

- A decentralised application is an application that can operate autonomously, typically through the use of smart contracts, that run on a decentralized computing, blockchain or other distributed ledger system.

- Like traditional applications, DApps provide some function or utility to its users. However, unlike traditional applications, DApps operate without human intervention and are not owned by any one entity, rather DApps distribute tokens that represent ownership.

- These tokens are distributed according to a programmed algorithm to the users of the system, diluting ownership and control of the DApp.

- Without any one entity controlling the system, the application is therefore decentralised.

Decentralized Applications..cont

- Smart contracts are used by developers to maintain data on the block chain and to execute operations. Multiple smart contracts can be developed for a single DApp to handle more complex operations