BLOCKCHAIN

Unit3: Class 3

3. Consensus Algorithm – Proof of Stake (PoS)

- PoS is a Competitive consensus algorithm. It was created as an alternative to PoW because blockchains had difficulty meeting the transaction speed demands.
- Peercoin was the first currency to utilise the PoS

3.1 Stake

  - Must lock a certain amount of its currencies, called stake, into an escrow account in order to participate in the block creation process.
  - When a stakeholder escrows its stake, it implicitly becomes a member of an exclusive group. Only a member of this exclusive group can participate in the block creation process.
  - Stakeholder, leader, forger, minter, validators, retainer.
- Person can mine or validate block transactions according to how many cryptocurrency he holds.
- It is becoming popular in public blockchain networks as it is a lowcost alternative that supports greater decentralization.

3.2 Nothing at stake

  - Security hole in proof-of-stake systems. The problem can occur anytime there is a fork in the blockchain, either because of a malicious action or accidentally when two honest validators propose blocks simultaneously.
  - There are two or more competing blocks (Known as Fork) in the proof of Stake algorithm. You can stake your cryptocurrency on both blocks without consequence. This is called **nothing-at-stake** problem as in Fig. 1
  - PoW is not economically viable to mine on both chains

- But in PoS, there is a little cost involved in working on several chains and economic incentive to do so.

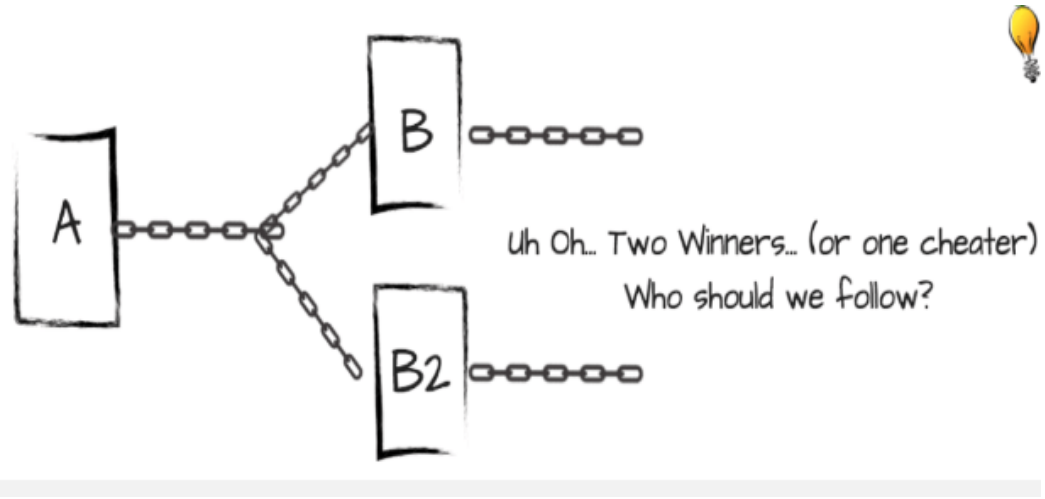

Fig.1

3.4 Pros

It is energy efficient and does not burn electricity when mining

It can be more expensive to attack than PoW- hackers need to purchase a large percentage of the native cryptocurrency

It scales easily to handle transaction load and size

3.5 Cons

- Rewards are weighted to those who stake their cryptocurrency the longest. The longer a miner stakes, the greater the reward. The network structure allows wealthy stakes to control more of the network and this may centralization and censorship.

PoS is used by Ethereum, Peercoin and Nxt

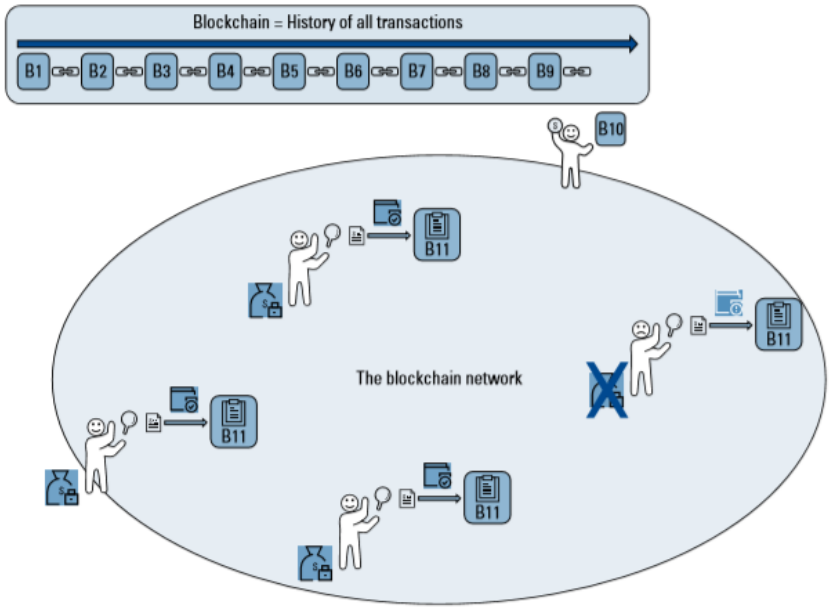

Fig. 2

Three different approaches

- Chained PoS
- BFT PoS
- Delegated PoS

3.6 CHAINED POS

The general idea of a chained PoS is to deploy a combination of PoW and PoS algorithms chained together to achieve any consensus. Because of this, there can be two types of blocks, PoW and PoS blocks, within the same blockchain system. To accomplish this, the corresponding algorithm relies on different approaches to select/assign a particular miner for creating a PoW block or select a set of validators for creating a PoS block in different epochs or after a certain number of blocks created.

In general, a chain based PoS can employ any of the following three different approaches to select the miner/stakeholder:

Randomised PoW Mining:

A miner who can solve the corresponding cryptographic PoW puzzle is selected in a random fashion.

Randomised Stakeholder Selection:

A randomised PoS utilises a probabilistic formula that takes into account the staked currencies and other parameters to select the next stakeholder. The other parameters ensure that a stakeholder is not selected only based on the number of their staked coins and act as a pseudo-random seed for the probabilistic formula.

Coin-age based selection.

A coin-age is defined as the holding period of a coin by its owner. For example, if an owner receives a coin from a sender and holds it for five days then the coin-age of the coin can be defined as five coin-days.

$$coin - age = coin * holdingperiod$$

Algorithms belonging to this class select the stakeholder using staked coins of the stakeholders and their corresponding coin-age.

3.7 BFT POS.

BFT PoS is a multi-round PoS algorithm. In the first step, a set of validators are pseudo-randomly selected to propose a block. However, the consensus regarding committing this block to the chain depends on the > 2/3 quorum of super-majority among the validators on several rounds. It inherits the properties of any BFT consensus, and as such, it tolerates upto 1/3 of byzantine behaviour among the nodes. In general, a BFT PoS algorithm favours towards consistency over availability when network partition occurs, within the setting of CAP theorem.

3.8 Delegated Proof of Stake(DPoS)

- The competition to be a validator happens outside of consensus. Those with better reputation scores, better website and social media accounts are selected.
- As a Stakeholder you elect “witnesses” who will validate transactions and create blocks for the network.
- EOS one of the most popular DPoS blockchains, only has 21 witnesses.
- Each of the EOS witnesses are paid fees for producing blocks and fee is set by the stakeholders.

- The witness nodes produce blocks one at a time in a round-robin fashion or by random selection.
- DPoS networks are used to build applications as they allow developers to scale up the size and increase the speed of their products.
- In DPoS, users of the network vote to select a group of delegates (or witnesses) who are responsible for creating blocks. Users utilise reputations scores or other mechanisms to choose their delegates. Delegates are the only entities who can propose new blocks. For each round, a leader is selected from the set of delegates who can propose a block. How such a leader is chosen depends on the respective system. The leader gets rewards for creating a new block, and is penalised and de-listed from the set of validators if it misbehaves. The delegates themselves compete with each other to get included in the validator list. In such, each validator might offer different levels of incentives for the voters who vote for it. For example, if a delegate is selected to propose a block, it might distribute a certain fraction of its reward among the users who have selected it. Since the number of validators is small, the consensus finality can be fast.

3.9 Pros:

- Like PoS, It is energy efficient
- It is fast- for example, EOS has a block time of 0.5 second.

3.10 Cons:

- It is a centralized system- this may make it prone to corruption

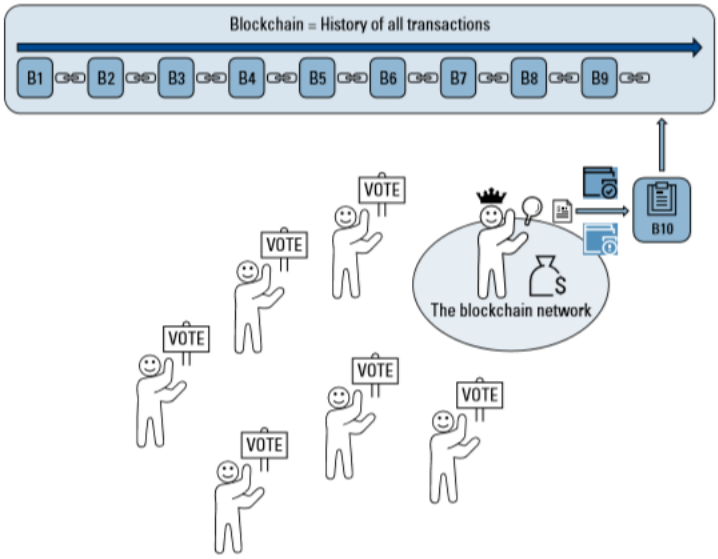

Fig. 3

3.11 Tendermint- BFT Proof of Stake

Tendermint is the first to showcase how the BFT consensus can be achieved within the PoS setting of blockchain systems.

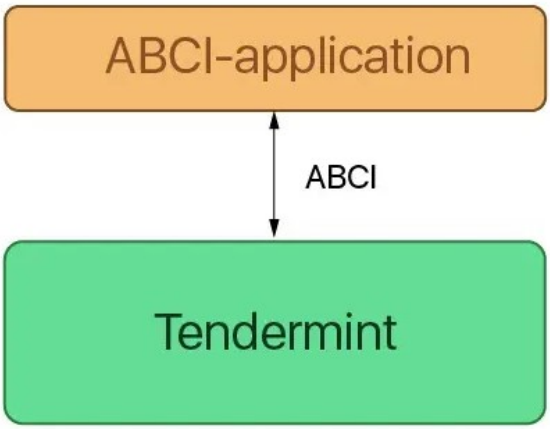

Fig: 4

It consists of two major components: a consensus engine known as Tendermint Core and its underlying application interface, called the Application BlockChain Interface (ABCI). The Tendermint core is responsible for deploying the consensus algorithm, whereas the ABCI can be utilised to deploy any blockchain application using any programming language.

The consensus algorithm relies on a set of validators. It is a round-based algorithm where a proposer is chosen from a set of validators. In each round, the proposer proposes a new block for the blockchain at the latest height. The proposer itself is selected using a deterministic round-robin algorithm, which ultimately relies on the voting power of the validators. The voting power, on the other hand, is proportional to the security deposit of the validators.

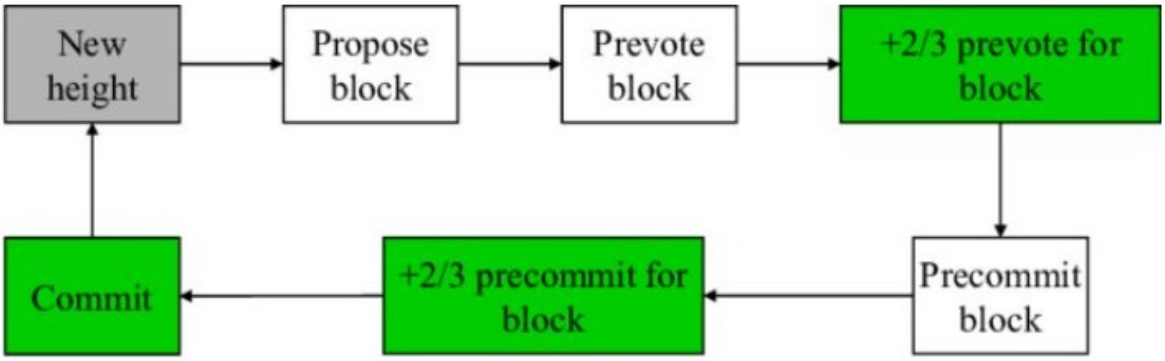

Fig: 5

The consensus algorithm consists of three steps (propose, pre-vote, and pre-commit) in each round bound by a timer equally divided among the three steps, thus making it a weakly synchronous protocol. These steps signify the transition of states in each validator. Fig. 6 illustrates the state transition diagram for each validator. At the beginning of each round, a new proposer is chosen to propose a new block. The proposed block needs to go through a two-stage voting mechanism before it is committed to the blockchain.

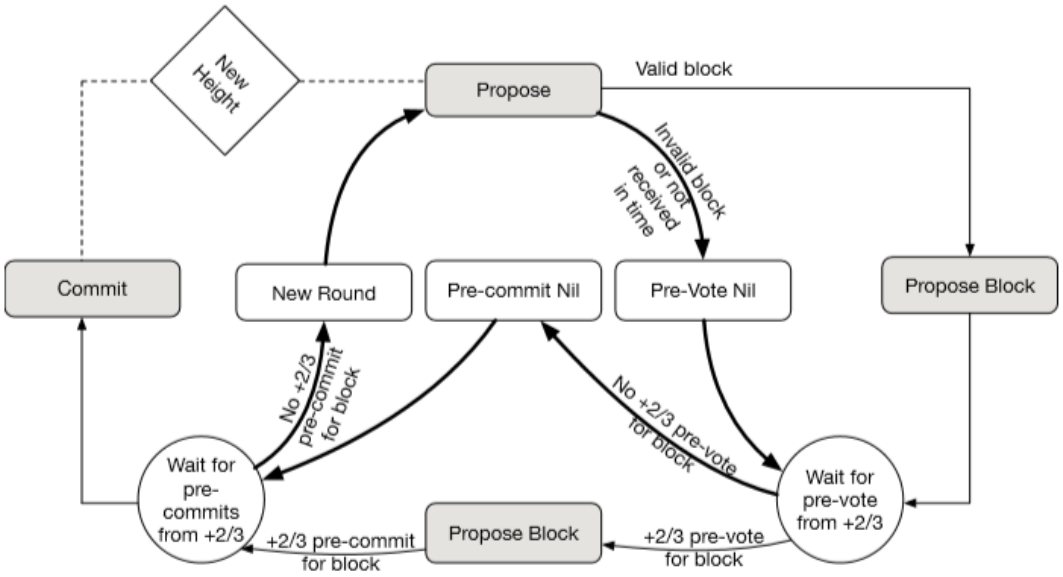

Fig: 6

When a validator receives the proposed block, it validates the block at first, and if okay, it pre-votes for the proposed block. If the block is not received within the propose timer or the block is invalid, the validator submits a special vote called Prevote nil. Then, the validator waits for the pre-vote interval to receive pre-votes from the supermajority (denoted as +2/3) of the validators. A +2/3 prevotes signifies that the super-majority validators have voted for the proposed block, implying their confidence on the proposed block and is denoted as a Polka in Tendermint terminology. At this stage, the validator pre-commits the block. If the validator does not receive enough pre-votes for the proposed block, it submits another special vote called Precommit nil. Then, the validator waits for the pre-commit time-period to receive +2/3 pre-commits from the supermajority of the validators. Once received, it commits the block to the blockchain. If +2/3 pre-commits not received with in the pre-commit time-period, the next round is initiated where a new proposer is selected, and the steps are repeated.

3.12 PoW Vs PoS