Block Chain Technology (Consensus Mechanism)

Dr. Siddhartha Roy

- Evolution of cryptocurrency
- Bit coin Mining
- Role of miners
- Consensus Mechanism in block chain
  - **Proof of Work (PoW)**
  - **Proof of Stake (PoS)**
  - **Practical Byzantine Fault Tolerance (PBFT)**

Evolution of Crypto currency

- 1983: eCash by David Chaum
- •Money is stored in the computer digitally signed by the bank
- 1989: DigiCash Inc. founded by David Chaum
- •ECash could not provide much additional benefit
- •Not very popular among people currency management
- overhead is more than bank notes
- •1998: The company got bankrupted

- 1998: Wei Dai publishes another anonymous, distributed
- electronic cash system called b money
- •Nick Szabo describes "bit gold"
- •Participants solve a cryptographic puzzle that depends on
- the previous puzzle
- Some central control still needs to verify that the puzzle
- has been solved correctly
- Can we verify the proof of the puzzle solving in a
- distributed way?

- 2011: Litecoin got introduced
- 2015: Ethereum network went live
- Sometime around 2016: Term "Blockchain" got popular
- 3rd January 2009: Nakamoto mined the first block of the Bitcoin network(called the genesis block)
- 2013: Coinbase reported selling US$1 Million worth of Bitcoin
- But, why should someone solve the puzzle?

Mining a block in bitcoin network

- Consider an open network where all nodes are connected and don’t trust each other.
- There are special nodes, called the Miners
- Miners propose new blocks –solve the puzzle (find the nonce corresponding to a target block hash), and add the solution as a proof of solving the challenge to be the leader
- Why someone would want to be the leader?
- Earn money (bitcoin) by solving the puzzle!
- Mining a Block: The Reward

- Encourage the community to participate in the mining through incentives
- Produces new Bitcoins in the System
- The Bitcoin network works like a Reserve Bank to regulate the flow of Money (Bitcoin) in the market, but without governance intervention or monitoring
- The miner who is able to solve the puzzle becomes the leader
- The block from the leader is appended in the blockchain

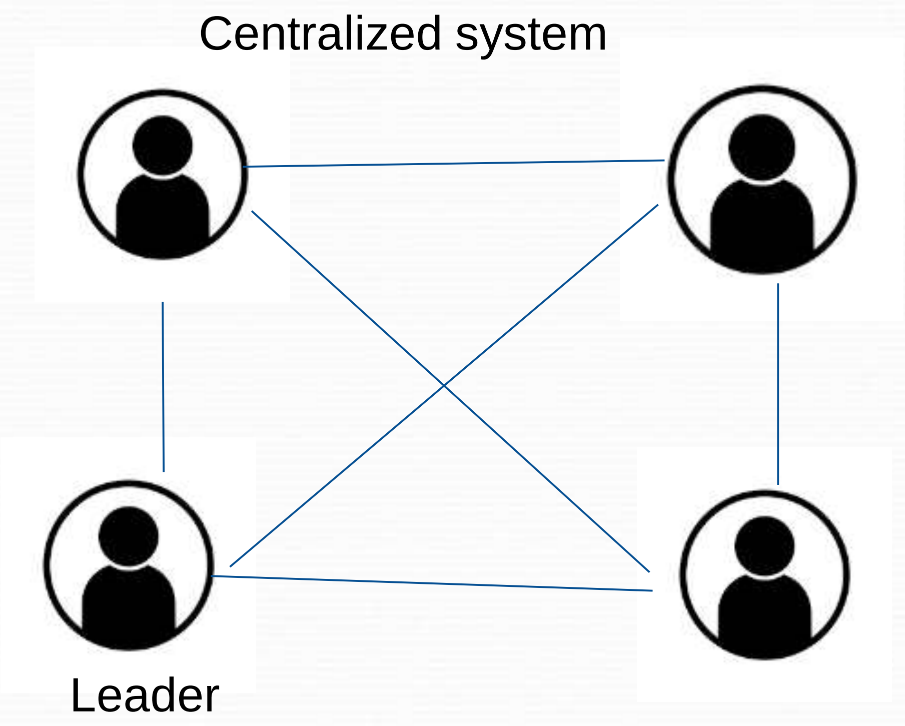
Role of miners

- The network is open
- But nobody knows each other
- A Puzzle will be generated from the system
- Everyone tries to solve it
- One who gives the solution first becomes the leader
- Whatever the leader says, everyone agrees to that

Consensus mechanism in block chain

- Consensus mechanisms are protocols or algorithms used in blockchain networks to achieve agreement on the validity of transactions and maintain the integrity of the distributed ledger. They ensure that all participants in the network agree on the state of the blockchain. Different consensus mechanisms have been developed, and each has its own set of advantages and trade-offs.

Consensus mechanism in block chain



All the decisions are taken by the leader or a board of decision makers.

This isn’t possible in a block chain because a block chain has no “leader”. For the block chain to make decisions, they need to come to a consensus using “consensus mechanisms”.

- *Consensus decision-making is a group decision-making process in which group members develop, and agree to support a decision in the best interest of the whole. Consensus may be defined professionally as an acceptable resolution, one that can be supported, even if not the "favourite" of each individual. Consensus is defined by Merriam-Webster as, first, general agreement, and second, group solidarity of belief or sentiment."*
- *Source:Wikipedia*

- Proof of Work (PoW):

- Process: Participants (miners) compete to solve complex mathematical problems. The first one to solve it gets the right to add a new block to the blockchain and is rewarded with newly created cryptocurrency (e.g., Bitcoin).
- Security: Provides a high level of security but requires significant computational power, making it energy-intensive.

- Proof of Stake (PoS):

- Proof of Work (PoW) is a consensus algorithm used in blockchain networks to achieve agreement on the state of the distributed ledger. It was introduced as a solution to the Byzantine Generals' Problem, ensuring that a decentralized network of nodes can agree on the validity of transactions and maintain a secure and tamper-resistant blockchain.

- **Practical Byzantine Fault Tolerance (PBFT):**
- **Process:** A set of nodes (replicas) agree on the validity of transactions through a series of rounds of communication and voting. Requires a two-thirds majority for consensus.
- **Performance:** Offers low latency and high throughput, making it suitable for permissioned blockchains.