Blockchain Terms

Blockchain: it's a shared database that contains transaction!

Trusted 3rd Party: Entity that facilitates interactions between 2 parties.

Ledger: List of Transaction records.

Blockchain Framework: Transaction, Wallet, Signature, Mempool, Network, Consensus, Hashing, Block,
Blockchain.

Bitcoin: A digital currency that utiliezes the blockchain to facilitate financial transactions.

Hashing: Hashing is an idea you may already be familiar with. It's a way to create a digital fingerprint for a piece of data. It's a fundamental idea behind what makes the blockchain work.

Bitcoin uses SHA256 as hash function.

Block: a container that holds a list of transactions to be added to the blockchain.

*Blockchain: Shared digital ledger that records a list of transactions.

For us, the blockchain is specifically the place where data is stored. Every other component is the system around the blockchain that helps make it all work.

*Blockchain: Digital ledger that contains the entire history of transactions made on the network.

First block on blockchain called genusis block.

Peer-to-Peer Network: A network of computers that allows information to be shared across users.

Distributed Network: A network that allows information to spread out across many users.

The memory pool (also known as the mempool) is the waiting place for transactions before they enter the blockchain. The blockchain can only handle so much information at once, and the backlog of information goes here. In this section, we'll go over many more details about what a memory pool is and why it's important.

Consensus is how the blockchain makes decisions. Basically consensus is an idea, but the idea is implemented through many different algorithms. These algorithms are all different ways to try and achieve consensus more effectively. Things like proof of work, proof of stake, and DBFT are all consensus algorithms.

*Consensus: How the network reaches agreement about which transactions are most trustworthy.

Proof of work algorithm: system where information can be costly to produce, but easy to verify

Block Data + Nounce (number with the block header) = Hash value

Proof of stake is another algorithm used to help achieve consensus on a blockchain. The key idea behind proof of stake is that it focuses on giving votes to members, depending on how much stake they have in the success of the chain.
This is different than proof of work and results in some interesting new ideas

*Proof of state: seeks to achieve consensus by giving votes to those with stake in the system

** Proof of Stake**: Algorithm that seeks to achieve consensus by giving votes to those with stake in the system.

** Delegated Byzantine Fault Tolerance** or DBFT for short, is yet another important consensus algorithm. Unlike proof of work or proof of stake, DBFT tries to achieve consensus by assigning roles to nodes to help coordinate consensus.

Delegated Byzantine Fault Tolerance: Consensus algorithm based on assigning roles to nodes to help coordinate consensus.

recap!

Proof of Work (PoW)

Bitcoin figured out how to use the Proof of Work algorithm to solve this issue.

The main innovation that Satoshi Nakamoto introduced in Bitcoin's white paper is using proof of work (POW) to achieve consensus without a central authority and solve the double-spend problem.

How Does It Work?

PoW involves miner nodes, or miners, to solve a math puzzle that requires a lot of computation power. Whichever miner is able to solve the puzzle the fastest is able to add a block of transactions to the blockchain, and in return, they are paid the transaction fees from all the transactions included in the block as well as paid by the network with bitcoins that were newly created upon the "mining" of the block.

Potential Issues

2 Commonly discussed issues with Proof of Work are:

Extremely High-Energy Consumption
A Monopoloy of Miners which Leads to a Concern for System Centralizations

Proof of Stake

In the Proof-of-Stake Consensus Protocol, there are no more miners; instead, there are Validators. These validators, or stakeholders, determine which block makes it onto the blockchain. In order to validate transactions and create blocks, validators put up their own coins as "stake". Think of it as placing a bet - if they validate a fraudulent transaction, they lose their holdings as well as their rights to participate as a validator in the future. In theory, this check incentivizes the system to validate only truthful transactions.

Potential Issues

We discussed the "Nothing At Stake" problem in which a bad acting Validator places bets on multiple forks so they theoretically always win out in the end.

Proposed Solutions

Slasher Strategy which entails penalizing validators if they simultaneously create blocks on multiple chains.

Delegated Byzantine Fault Tolerance (dBFT)

dBFT uses a system similar to a democracy where Ordinary Nodes the system vote on representative Delegate Nodes to decide which blocks should be added to the blockchain. When it’s time to add a block, a Speaker is randomly assigned from the group of Delegates to create a new block and propose the new block. 66.66% of delegates need to approve on the block for it to pass.

Potential Issues

Two issues we explored were the case of the Dishonest Speaker and the Dishonest Delegate.

Dishonest Speaker

There is always a chance the Speaker, who is randomly selected from the Delegates, could be dishonest or malfunction. In this situation, the network needs to rely on honest delegates to vote the proposed block down so it doesn’t reach 66% approval. It is up to users of protocol who vote on Delegates, to find out which delegates are not trustworthy and vote on other delegates that are truthful.

Dishonest Delegate

In this case, the chosen Speaker is honest but there are Dishonest Delegates in the system meaning even if they receive a proposal for new block that is faulty, they can say it is valid. If it is a minority of delegates that are dishonest, the block will not make it and new speaker is elected.