Course II:

DeFi Primitives

4. Joining the World of DeFi

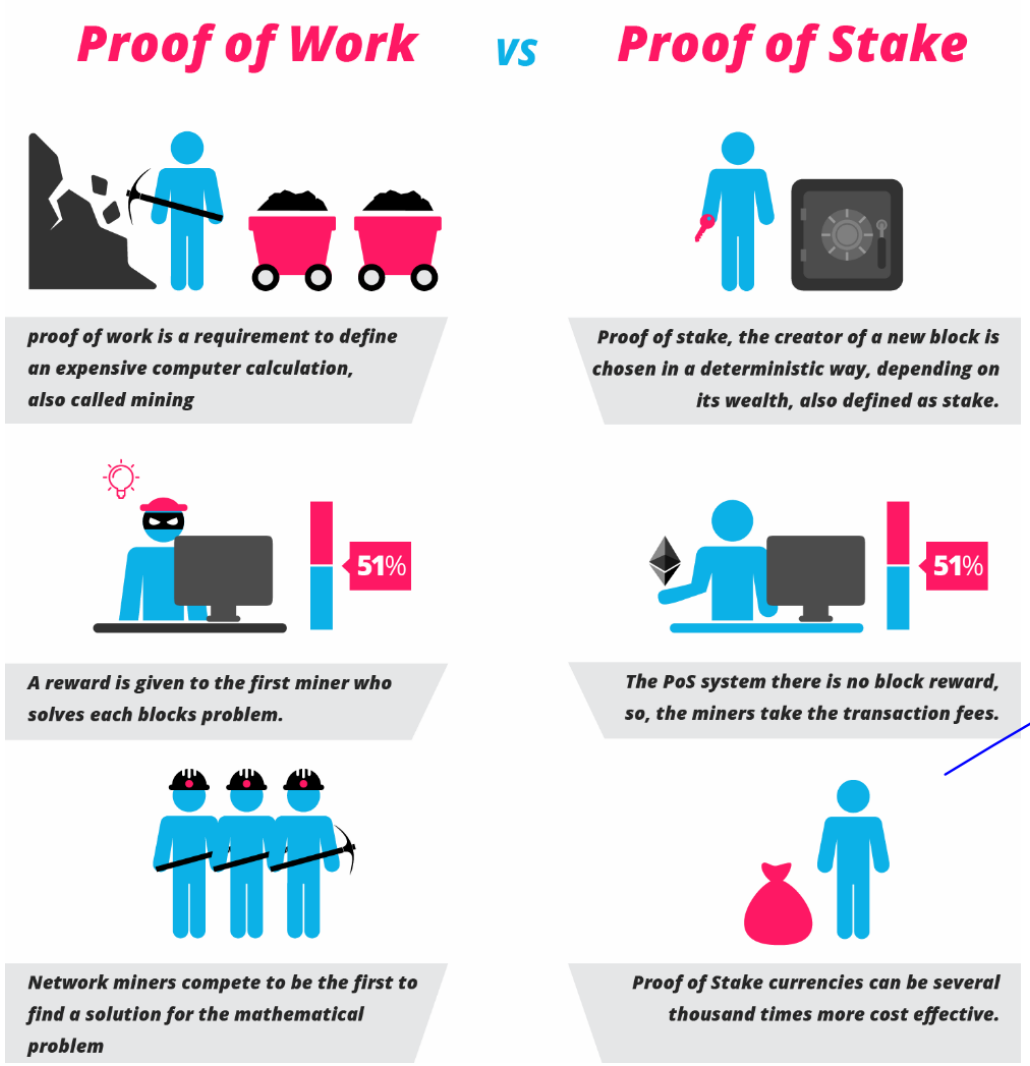
(ii) Blockchain Tech Big Picture

d) Consensus

Tech Big Picture

Key ingredients

- **Consensus Mechanisms**: Consensus is the mechanism by which nodes agree on both the historical blockchain as well as the new additions to the historical blockchain.



Tech Big Picture

Consensus is an agreement among a group of people on an idea, statement, or plan of action

- Majority: 51%
- Supermajority: 66% (sometimes higher)
- Unanimous: 100%
- Weighted: not all votes weighed equally

Tech Big Picture

- Consensus is typically only relevant when there is no centralized leader
  - A jury must reach a consensus on a court verdict (unanimous)
  - The senate must reach a consensus on new bills being passed (majority or supermajority)
- Particularly important when there is significant disagreement or potential for untrustworthy parties in the discussions around the decision

Tech Big Picture

The agreement of system components (nodes) on the [next] state of the system, or the transition between the current state and the next state

- The nodes must agree on a set of valid transactions representing the change from the current state of the system to the next state of the system
- Consensus must be achieved automatically (without human oversight)

Tech Big Picture

- Consensus is irreversible: posted transactions are final
- Blockchain consensus is a subset of distributed system consensus
  - Distributed System: A number of independent computers linked by a network
- Must be resistant to malicious or false actors

"Consensus is the process by which all nodes agree on the same ledger"

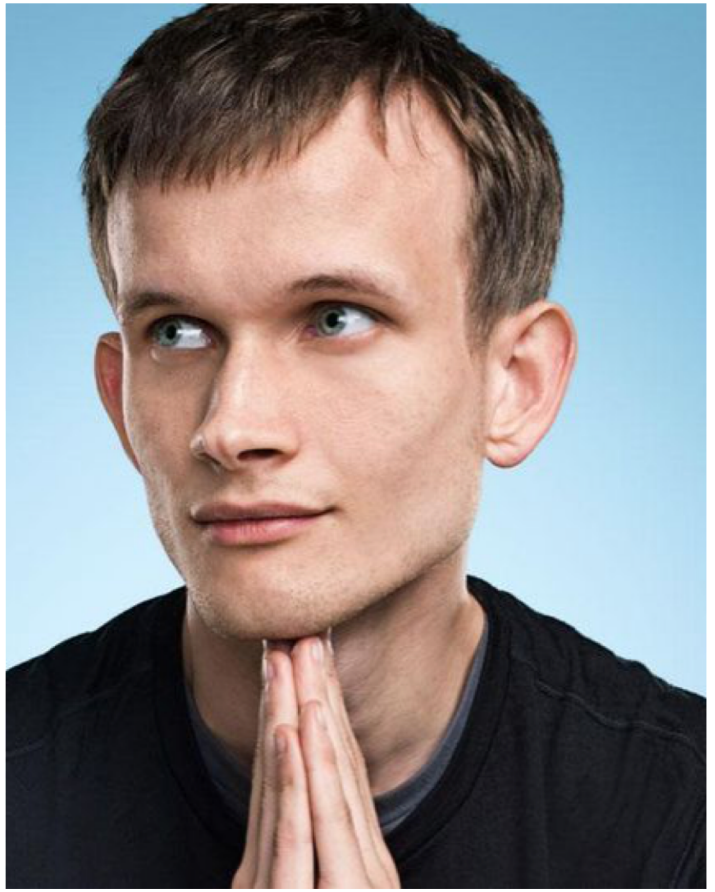
Tech Big Picture

- Consensus is a very difficult problem when parties are not trusted
- The network must maintain integrity in order to maintain value
- Past transactions must be trusted for the network to function
- Thus, the ability to verify transactions without trust is needed
- This problem is solved with various forms of consensus
- The consensus problem can often be rephrased as the ability to trust the result of a transaction or block, without trusting the parties involved in the transaction, or the party that verified it

Tech Big Picture

"The purpose of a consensus algorithm, in general, is to allow for the secure updating of a state according to some specific state transition rules, where the right to perform the state transitions is distributed among some economic set."

- Vitalik Buterin (Co-Founder of Ethereum)



https://bcfocus.com/wp-content/uploads/2018/05/2018051515042388.jpg

Tech Big Picture: Proof-of-Work (PoW)

- A given node collects transactions that are broadcast to the entire network and stores them in a block
  - Before including transactions in the block, the node verifies that the transactions are valid
    - Invalid transactions result in a block being rejected by the other nodes)
  - The transactions are typically assembled in a type of Merkle tree
  - The transactions pay a fee to the mining node to be included the transaction, higher fees are included first

Tech Big Picture: Proof-of-Work (PoW)

- The mining node begins solving an extremely difficult cryptographic hashing problem, with the transactions being part of the input to the problem
  - This is essentially a guessing game with a very low chance of guessing correctly
  - Once the correct answer is known, it is very easy for other people to check that it works
  - Part of the motivation for solving the problem is that the miner can give themselves a reward

Tech Big Picture: Proof-of-Work (PoW)

- The mining node that has found the correct solution broadcasts it to the rest of the network, and begins the next block with another complex cryptographic hashing problem
  - The longest blockchain (weighted by work) is always taken to be the correct chain, and thus the other miners will also begin the new problem: the length of each block is determined by how much work it took to create
  - The other nodes can quickly check that the transactions included in the block are valid, and that the broadcast solution is actually a solution to the problem
- Repeat

Tech Big Picture: PoW Strengths

- Proven reliability/Predictable block times/Robust
- Does not rely on any other node being trustworthy
- Only known vulnerability is the so-called ‘51% attack’
  - One miner or group of miners is able to take over the resources driving the chain forward
  - However, expenditure of large computing and energy cost to take 51% would be lost if crypto collapsed
- Uncensorable and publicly broadcast
  - Public transactions can be seen as a drawback in some cases

Tech Big Picture: PoW Drawbacks

- Enormous waste of resources
  - Bitcoin mining uses much energy as Argentina
- ASIC hardware give advanced miners and pools a substantial advantage over the average miner
  - Massive start up costs can result in centralization of pools and resources
  - A regular computer has essentially no hope of ever mining a block

Tech Big Picture: PoW Drawbacks

- Scalability issues
  - Lower transaction throughput
  - Lowering the block time (problem difficulty) is potentially less secure
- Miners often sell the coins immediately, removing any loyalty to the chain they are mining

Tech Big Picture: Current PoW S[illegible]

- Bitcoin
- Ethereum (2.0)
- Litecoin
- Bitcoin Cash
- Many, many more

Many systems launch with a Proof-of-Work-like consensus mechanism, but later transition to a different, less resource intensive approach, often with proprietary features

Tech Big Picture: Proof-of-Stake (PoS)

- The right to mine blocks is given out randomly, but proportionally, based on ‘stake’
- Stake is defined as some form their share or involvement in the network
  - Often the amount of the currency owned
  - Example: If you stake 10%, you could expect to win the right to mine 10% of all blocks

https://crypviz.io/wp-content/uploads/2017/11/proof-of-stake.png

Tech Big Picture: Proof-of-Stake (PoS)

- The chosen miners still do some form of guess-and-check to create the block:
  - They try various combinations of features of their address and wallet, and previous block variables
  - The number of combinations possible is based on their stake, hence why larger stakeholders have higher chances of successfully mining the block
  - These combinations are quickly exhausted, making PoS significantly less computationally intensive

Tech Big Picture: Proof-of-Stake (PoS)

- The miners are incentivized to only provide valid blocks, as they have great incentive to keep the network functioning correctly (their stake or holdings will be worthless if the network fails to function)
  - Some implementations demand that miners put their coins into escrow that is lost if they break the rules

Tech Big Picture: Proof-of-Stake (PoS)

- The block is validated as usual by the rest of the network before they continue to the next block
- There are many variations on Proof of Stake (often named something slightly different), and the mechanisms by which rewards are distributed, validators are selected, and stake is determined

Tech Big Picture: PoS Strengths

- No useless mining: there is no unnecessary use of resources to further power the blockchain
- Little to no hardware advantage
  - ASIC mining pools do not have a significant advantage over a powerful home computer
- Those ‘guarding’ the value of the coins have the most to lose if the network is compromised
  - The incentives to be honest are aligned with individuals motives

Tech Big Picture: PoS Strengths

- The 51% attacks becomes essentially infeasible
  - An attacked would need to accumulate 51% of all the coins on the network to accomplish this
  - Currently for Ethereum this is $6 Billion, which would be lost if the attack were successful
- Proof of Stake has the potentially to be magnitudes more efficient than PoW, making it significantly more scalable
  - Very high transaction throughput is possible with PoS (transactions per second)

Tech Big Picture: PoS Drawbacks

- Theoretically encourages centralization:
  - Higher stake means higher rewards, keeping the ‘rich’ richer

Campbell R. Harvey

https://www.youtube.com/watch?v=pzIl3vmEytY

Tech Big Picture: PoS Drawbacks

- Proof of Stake is often claimed to be not as secure as Proof of Work
  - There are many implementations of various ‘claimed’ security, and most of these just need to stand the test of time to be considered more secure

Tech Big Picture: Other Consensus Mechanisms

- Many systems including
  - Delegated Proof of Stake
  - Delegated Byzantine Fault Tolerance
  - Proof of Capacity
  - Proof of Elapsed Time
  - Proof of Identity
  - Proof of Authority
  - Proof of Activity

https://www.allerin.com/blog/8-blockchain-consensus-mechanisms-you-should-know-about https://blockgeeks.com/guides/blockchain-consensus/