Blockchain Technology and Applications

CS 731

Other Consensus Algorithms

Dr. Ir. Angshuman Karmakar

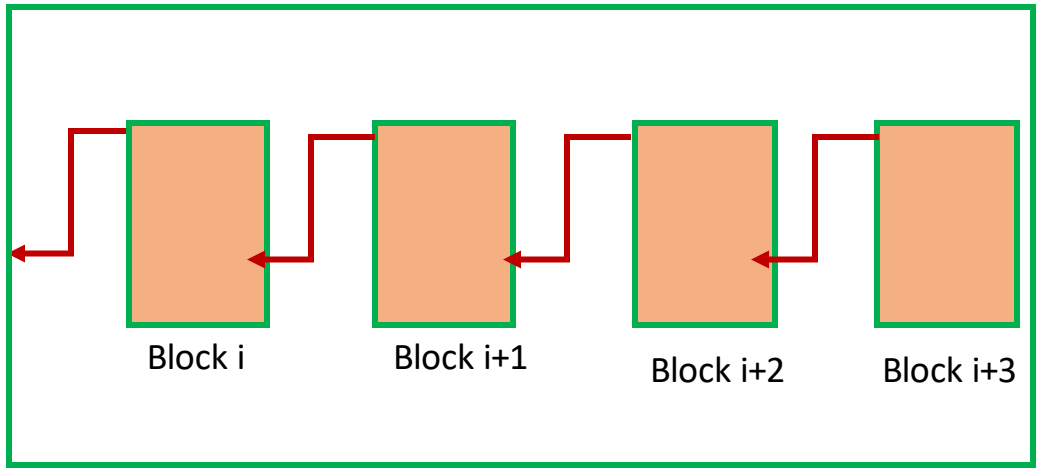
IIT Kanpur

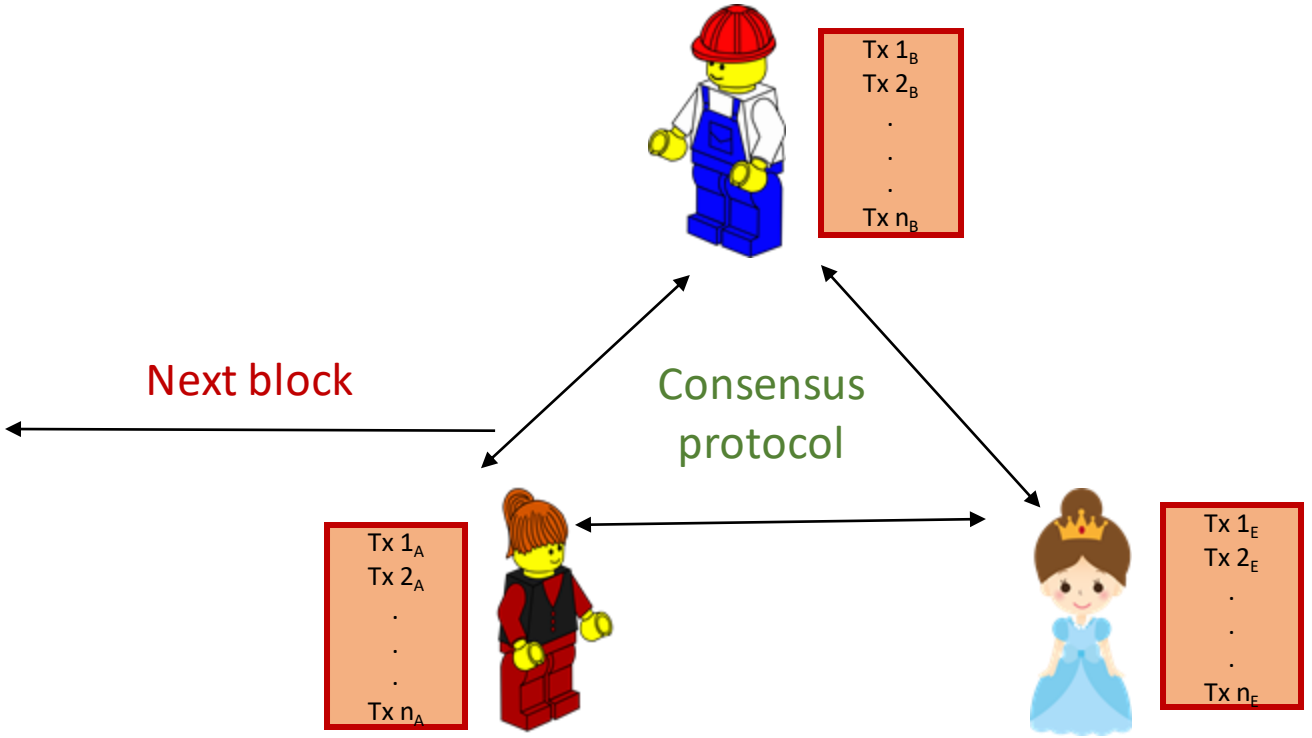
Teaching assistants

- **Sumit Lahiri (**sumitl@cse.iitk.ac.in**)**
- **Chavan Sujeet** (sujeetc@cse.iitk.ac.in)
- **Indranil Thakur** (indra@cse.iitk.ac.in)

Consensus

- At regular intervals nodes participate in a consensus protocol
- Decides the next block to be added to the blockchain
- If majority of the nodes are honest
- The blockchain is secure

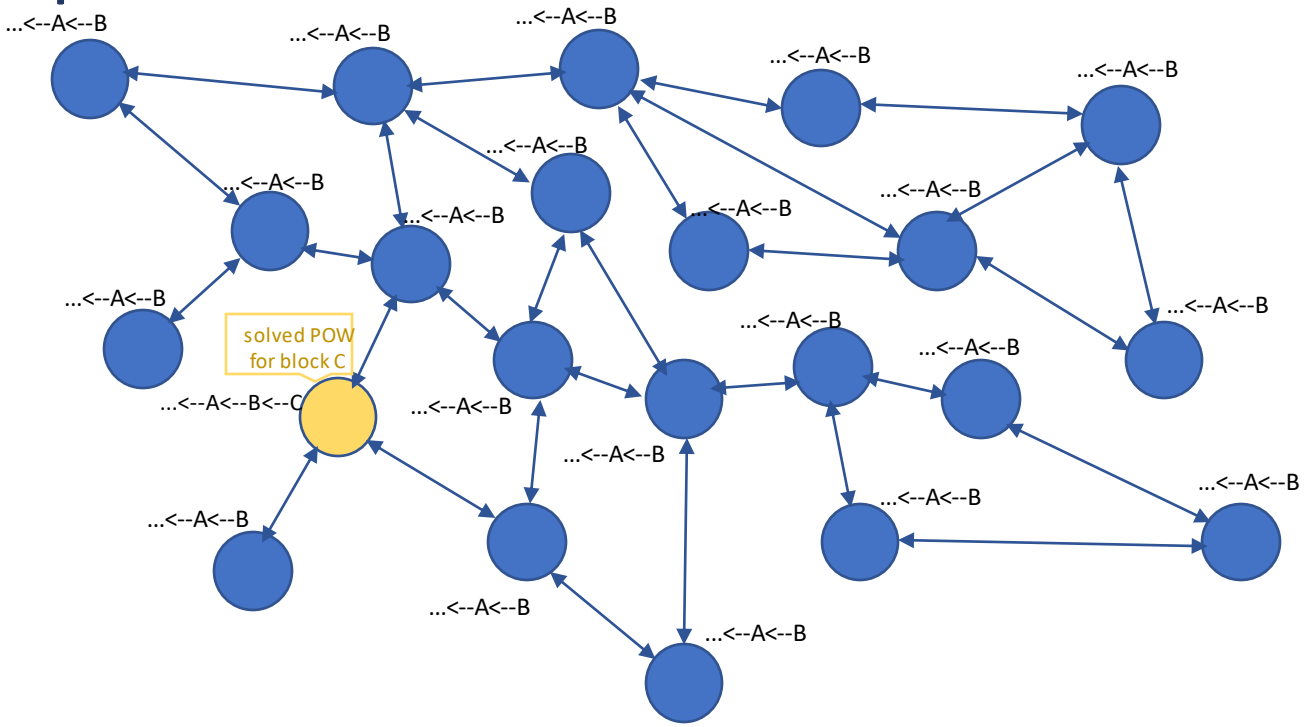




Consensus

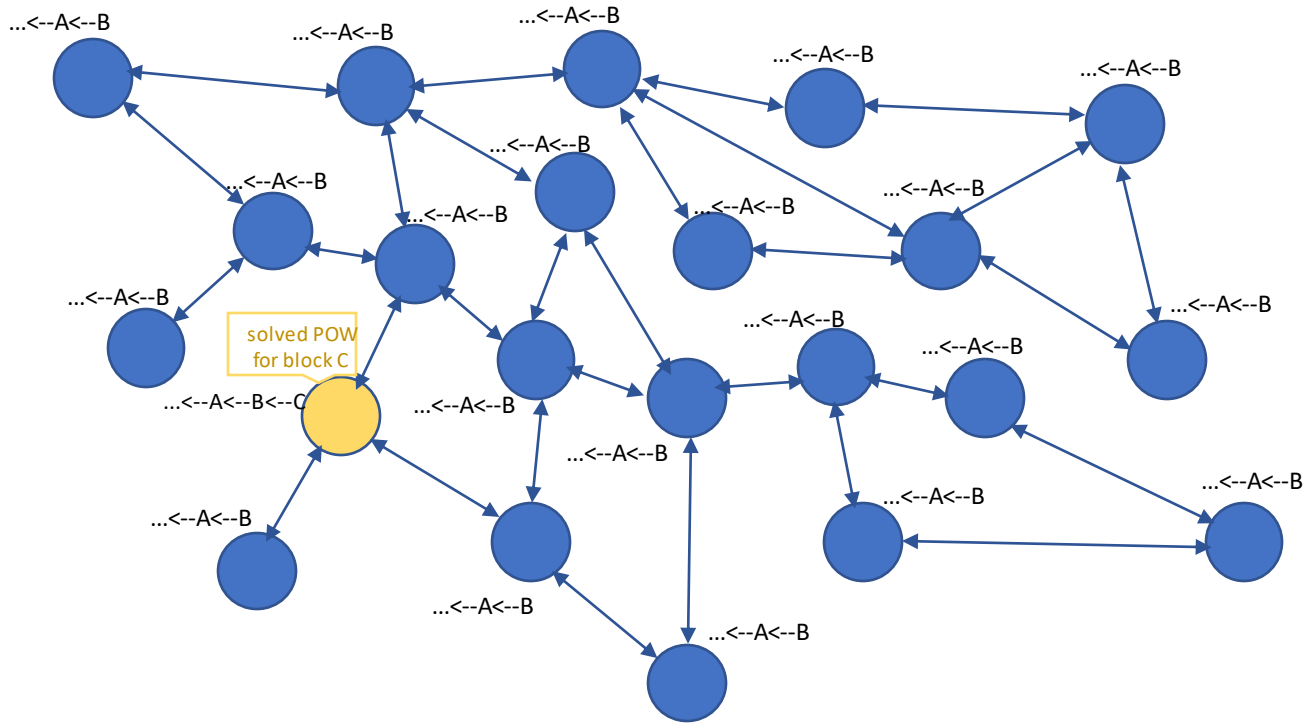
Proof-of-work

- Nodes must solve a hard mathematical problem
- Find H(x||k) such that H(x||k) < v
  - v is a difficulty parameter
  - It is adjusted at fixed time intervals
- Nodes compete to mine the next block



Proof-of-work

Drawbacks

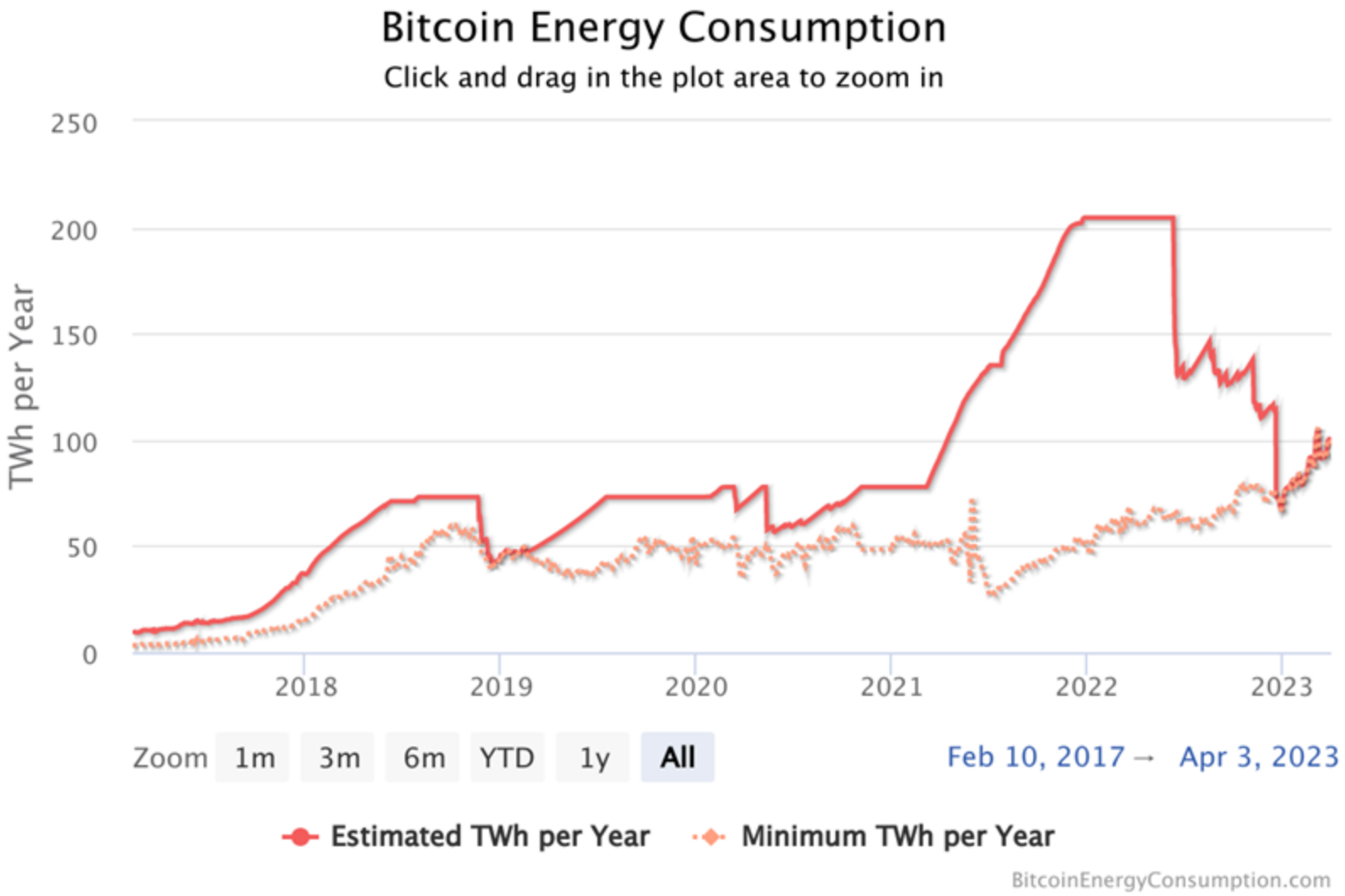


- All the nodes tries to solve the puzzle at the same time
- Miners usually employ expensive and energy intensive devices to solve the problem faster
- Once a winner is found all the work done by the other miners have to be discarded
- Significant loss of resources

Proof-of-work

Drawbacks

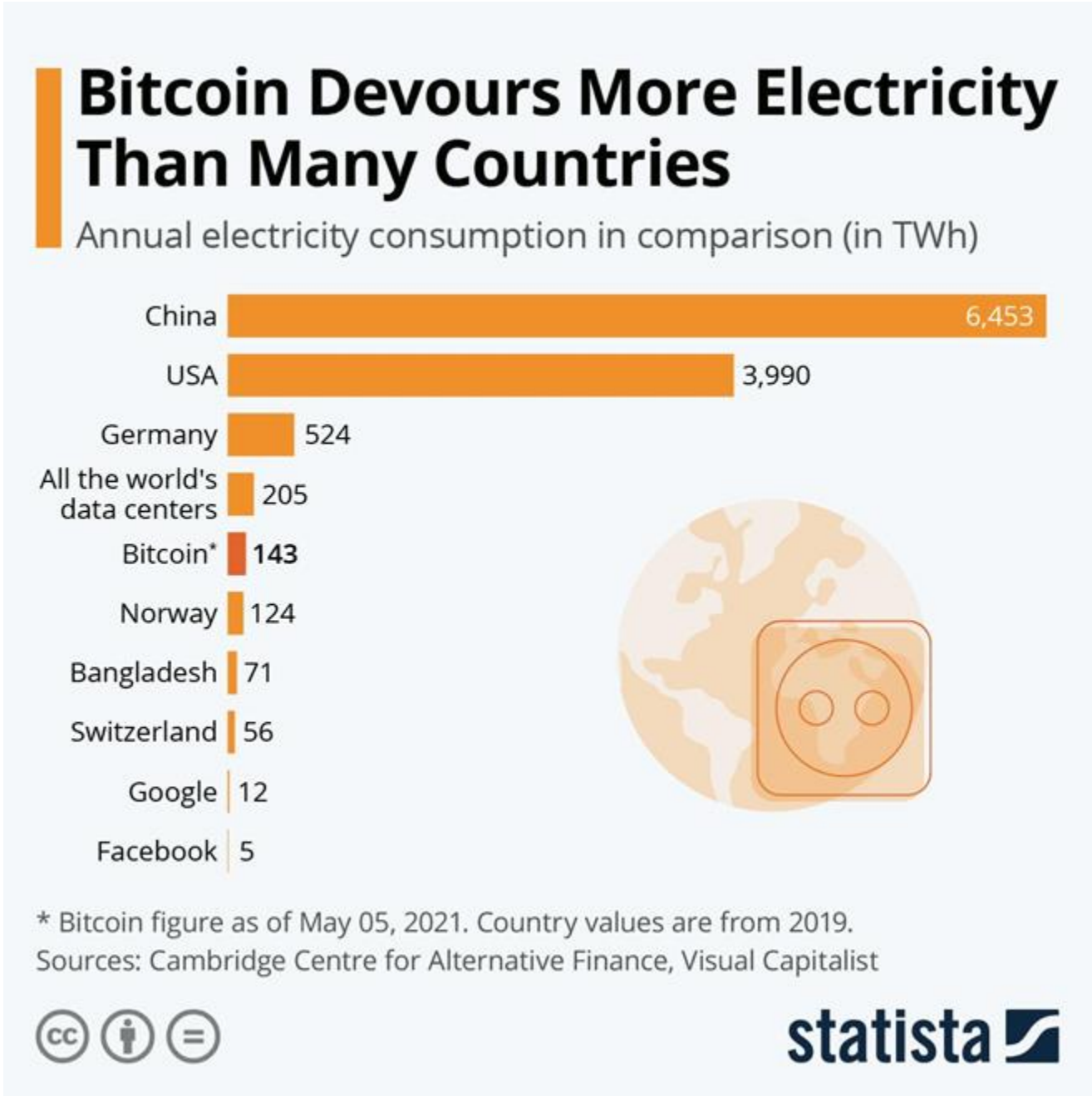
- Energy consumption



Proof-of-work

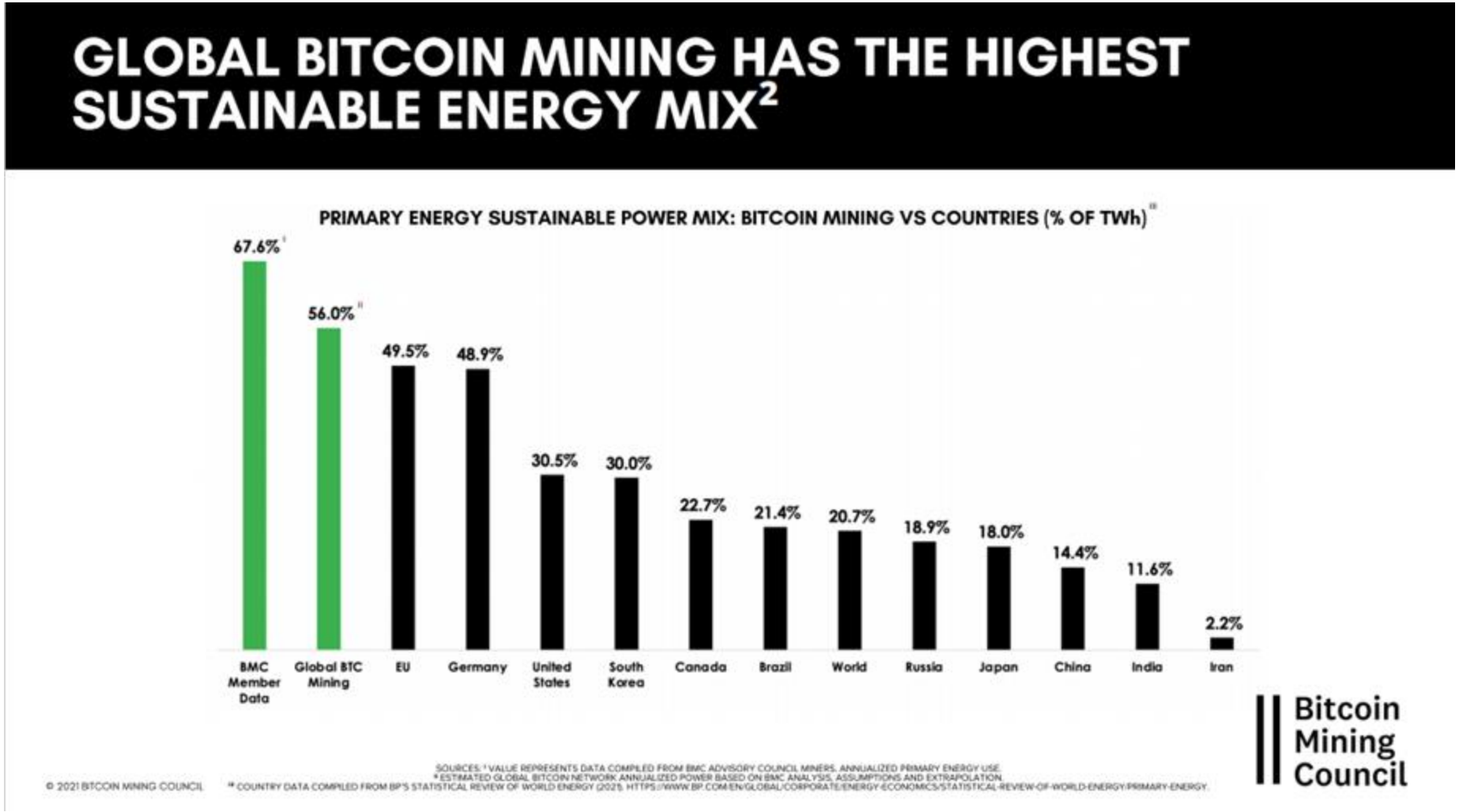
Drawbacks

- Energy consumption



Proof-of-work

Energy usage



Proof-of-work

Energy usage

CNET Your guide to a better future

Science

First Nuclear-Powered Bitcoin Mine in US Opening in 2023

Bitcoin miners are trying to make the notoriously polluting cryptocurrency a little more green.

Daniel Van Boom

Jan. 24, 2023 7:17 p.m. PT

2 min read

Proof-of-work

Energy usage

154,620 TWh[i]
TOTAL ENERGY GENERATED WORLDWIDE

50,000 TWh[ii]
ENERGY LOST DUE TO INEFFICIENCIES

188 TWh[iii]
ENERGY CONSUMED BY BITCOIN MINING ON THE WORLD'S ELECTRIC GRID

GLOBAL BITCOIN MINING CONSUMES 0.12%
OF THE WORLD'S ENERGY PRODUCTION

GLOBAL BITCOIN MINING CONSUMES 0.38%
OF THE WORLD'S ENERGY WASTED

SOURCES [i] BP STATISTICAL REVIEW OF WORLD ENERGY (2021), HTTPS://WWW.BP.COM/EN/GLOBAL/CORPORATE/ENERGY-ECONOMICS/STATISTICAL-REVIEW-OF-WORLD-ENERGY/PRIMARY-ENERGY.
[ii] INTERNATIONAL ENERGY AGENCY, HTTPS://WWW.IEA.ORG/DATA-AND-STATISTICS/DATA-PRODUCT/WORLD-ENERGY-STATISTICS-AND-BALANCES.
[iii] BMC ESTIMATED BITCOIN MINING ENERGY USE (SEPT 30, 2021).

Bitcoin Mining Council

Proof-of-work

Economies of scale

- Inequality and centralization

- Alice and Bob each opens a pizza shop
- Assume they have identical localities, ingredients, recipes, etc.
- Ideally, Bob and Alice should make profits proportional to their investments

Proof-of-work

Economies of scale

- Inequality and centralization

- Alice managed to find more investments
- She used the funds to open more pizza shops

Proof-of-work

Economies of scale

- Inequality and centralization

- Alice can do more things

1. Buy ingredients, fuel, etc in bulk at discount
2. Utilize her workforce efficiently
3. Optimize her distribution network,
4. Etc

- Alice can offer pizzas at lower price

Proof-of-work

Economies of scale

- Inequality and centralization

- Eventually Alice will start earning disproportionately more profit
- Bob will be out of business soon

- This is called economies of scale

Proof-of-work

Economies of scale

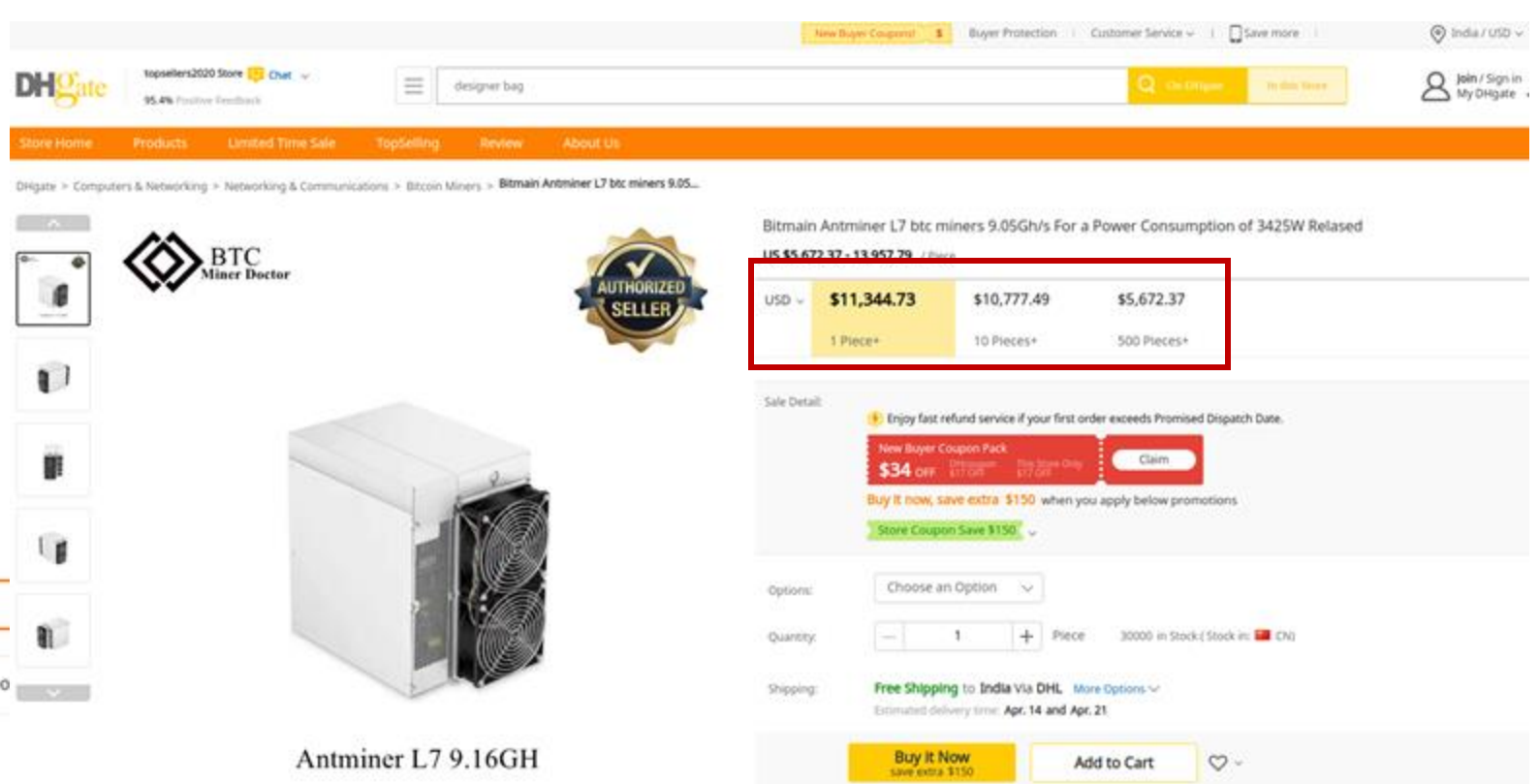
- Internal economies of scale
  - Happens within a company
  - Utilizing the resources
  - Reducing wastage
  - Better marketing, management, etc.
  - Case study: McDonald's*, Microsoft

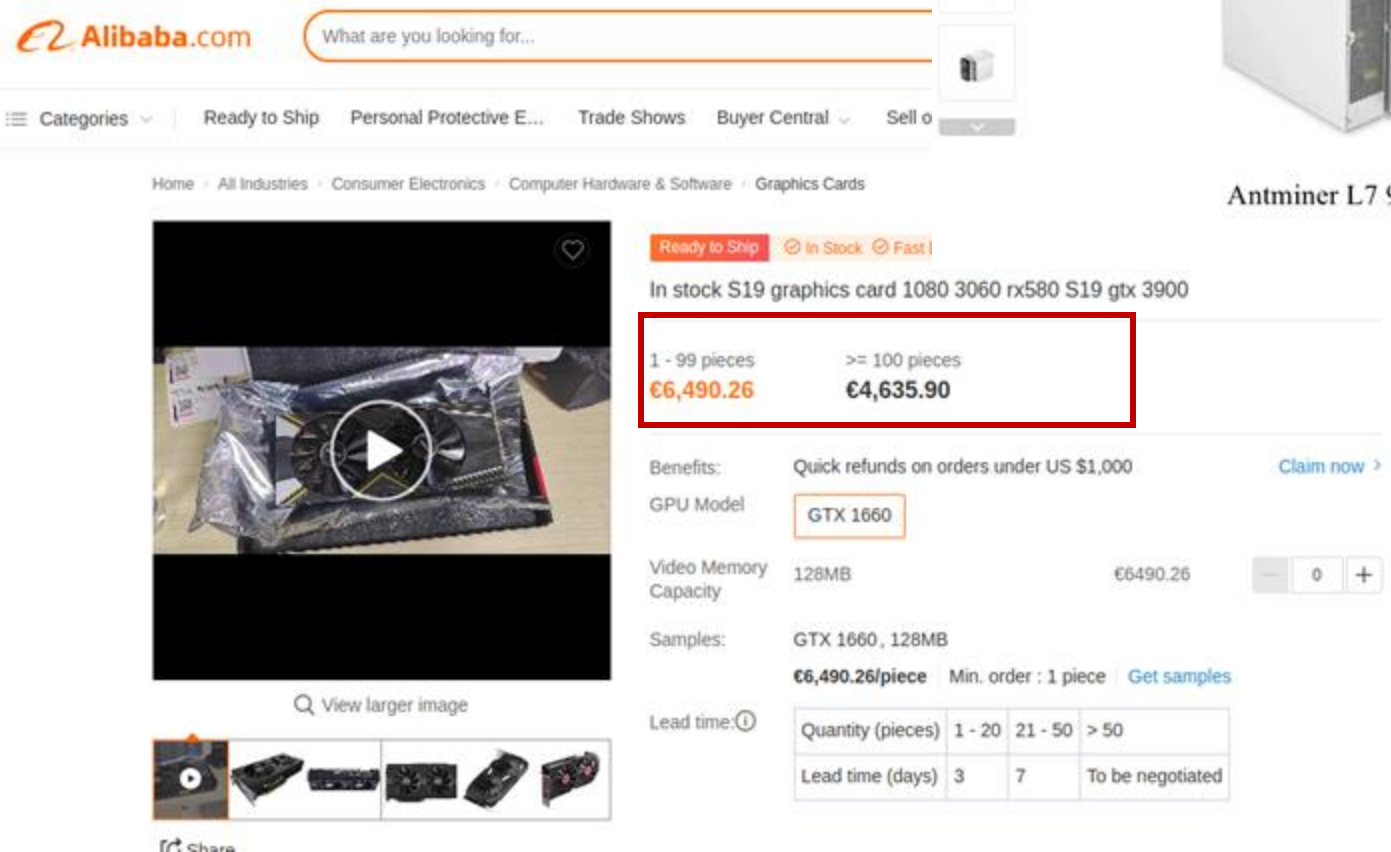
- External economies of scale
  - Factors that affect an entire industry
  - Better labour pool
  - Vicinity of resources
  - Tax cut, incentives, etc.
  - Case study: SEZs of India, China

*https://stanfordcomparativeadvantage.files.wordpress.com/2017/01/scharf-mcuniverse.pdf

Proof-of-work

Economies of scale



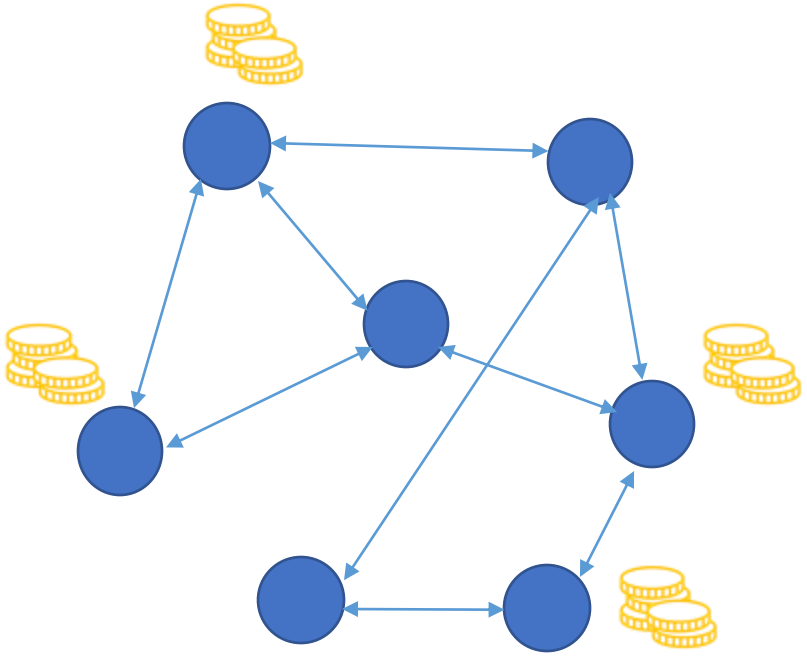


Proof-of-stake

- Recall in consensus protocol
  - A random node is chosen
  - This node proposes the next block
  - The probability of being chosen is proportional to some resources
  - The resources should be hard to monopolize

- Proof-of-work --> Hash power
- Proof-of-stake --> Stake in the network

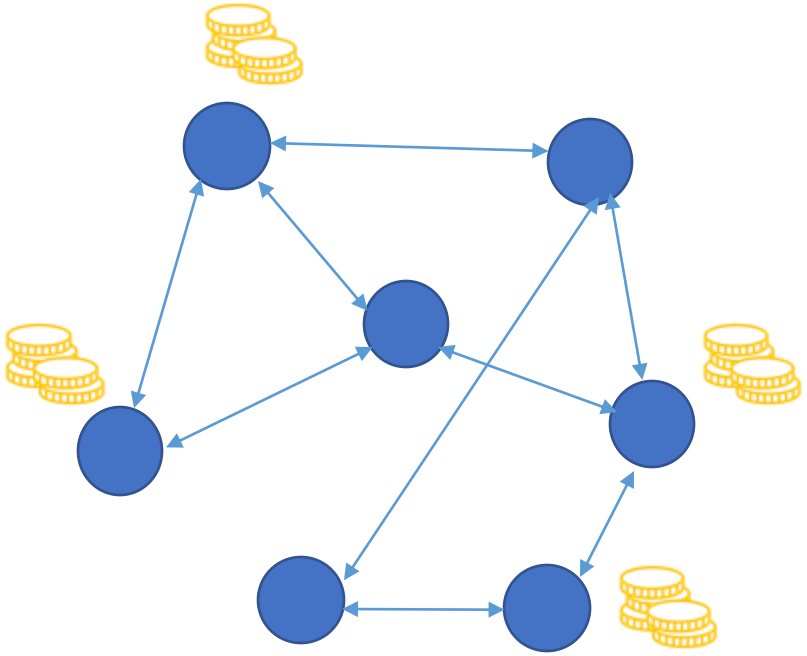
Proof-of-stake



- Nodes stake some number of coins or tokens to be part of the consensus mechanism

PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. Sunny King, Scott Nadal. https://decred.org/research/king2012.pdf

Proof-of-stake



- The probability of getting chosen is proportional to the staked amount
- There is a minimum amount to be staked

Proof-of-stake

- The probability of getting chosen is proportional to the staked amount
- There is a minimum amount to be staked
- Nodes are called validators instead of miners
- It might look like it favours wealthiest users in the network
- To combat this different solutions can be adapted
- Randomized block selection
  - Nodes with highest stakes and lowest hash values are selected
- Coin aging
  - Considers the time spent in waiting
  - The selection depends on the value (*time spent in waiting X coins staked)*
  - Once selected the waiting time resets to zero
  - Prevents nodes with larger stakes from dominating

Proof-of-stake

Rewards and penalties

- In Ethereum a node must stake at least 32 ethers to be a validator
- In proof-of-work, the time between the blocks is almost guaranteed by puzzle difficulty
- There is no puzzles in POS
- In Ethereum, there are slots of 12 seconds each
  - And epoch of 32 slots
- One validator is chosen as block proposed in each slot
- Also, in each slot a committee of validators are randomly chosen
- They are called attestors
- They vote for the validity of the proposed block
- Rewards are given for block proposition and attestation*

*see calculation here: https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/rewards-and-penalties/

Proof-of-stake

Rewards and penalties

- Similarly, coins are deducted for malicious activities
- Slashing
  - Ethers are deducted from malicious validators
  - For serious malpractices such as proposing or signing multiple blocks for the same time slot, voting for multiple blocks or trying to change the history
    - Ethers are gradually deducted from the balance effectively eliminating them from the validator network

Proof-of-stake

Rewards and penalties

- A block needs 2/3rd vote from attestors to achieve finality
- A group of validators with > 1/3rd stake might become inactive
- The rest of the validators have < 2/3rd majority
- The new blocks will not get enough votes for finality
- The inactivity leak protocol is activated
- Gradually slashes the stakes of inactive
- Until the shares of inactive validators become less than 1/3rd of the total stake
- The chain starts to move once the stake is reduced
- The POS can actively encourage nodes to follow the canonical behaviour by rewards and penalties

Proof-of-stake

Pros and cons

- Benefits
- Energy efficiency: No need to use special hardware like POW for mining
- Egalitarian
  - Low barriers for entry.
  - No large upfront investments or special equipment to be a validator
- Low risk of centralization: As more nodes can join and be validators or attestor there is less risk of centralization
- As there is low investment requirement the incentives can be lower
  - Making malicious activities even less lucrative
- Severe economic penalties make 51% type of attack even less attractive

Proof-of-stake

Pros and cons

- Disadvantages
- POS is younger and even less understood than POW
- Many different award and penalty mechanism
- More complex than POW

Proof-of-stake

Transition

- When a blockchain first starts
  - Mining is easy. Can be done even without specialized hardware
  - Coin prices are low so one can buy a large amount of coin in the beginning
- So, if POS is adapted from the beginning it will be prone to mount a 51% attack
- On the other hand, when a network grows large mining becomes hard and require more investments and specialized hardware
  - Prone to centralization, inequality, etc.

Proof-of-stake

Transition

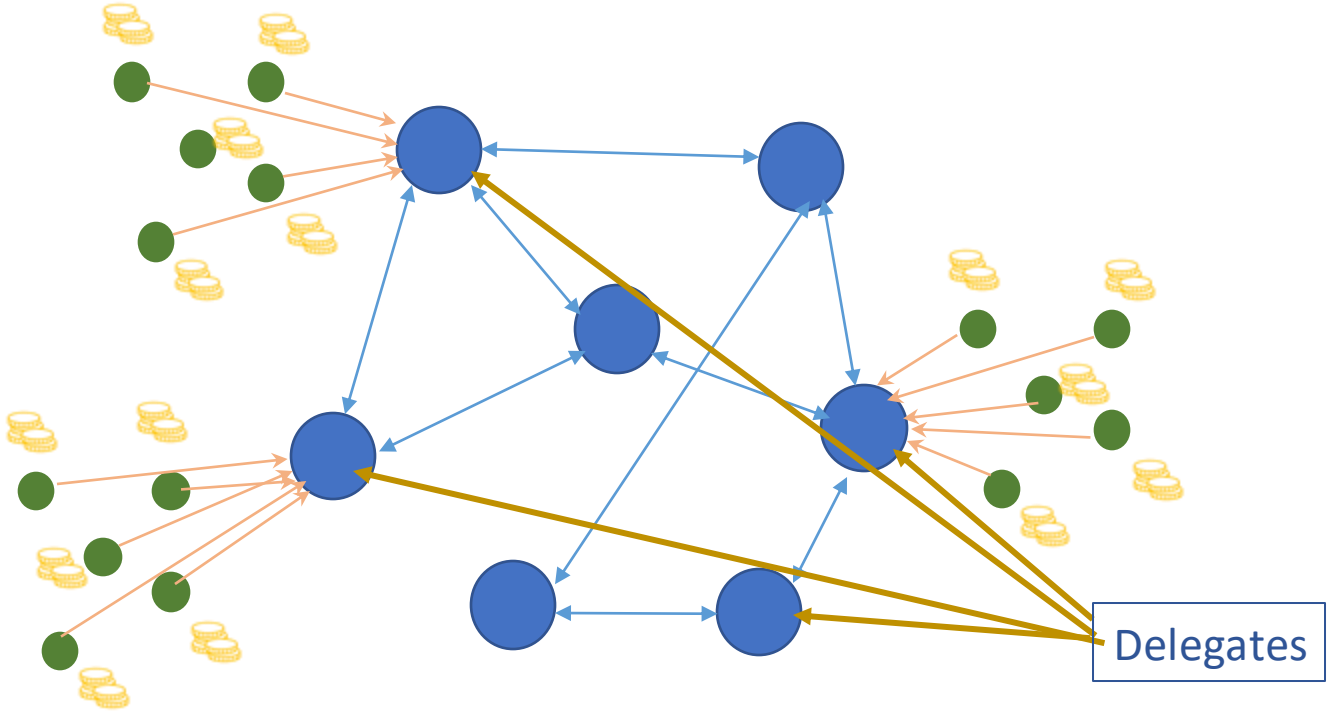
- The original POS (peercoin) proposal also started as POW to mine coins
- Later shifted to POS for overall security

- Ethereum transitioned from POW to POS in 2022
  - Ethereum 2.0

Other Consensus Mechanism

Delegated Proof-of-stake

Mechanism



- Like the POS here nodes also stakes coins
- But instead of voting themselves they vote for some delegates
- These delegates in turn choose the blocks which will be part of the blockchain

Delegated Proof-of-stake

Mechanism

- At each round a delegate is chosen
  - Based the amount of stake, age or some other criteria
- The delegates get a reward if they honestly propose a block
  - The reward are distributed to the nodes who voted for them in proportion to their stake
- Number of delegates much smaller than validators in a POS
  - 20-100
- Nodes vote for delegates who have an honest history of validation
  - Better odds for getting rewards
- If a node behave dishonestly nodes can effectively eliminate it from network

Delegated Proof-of-stake

Pros and cons

- All the benefits of POS
  - Less energy usage, egalitarian, rewards and penalties
- Faster
  - Small delegates--> Node selection and validation simpler
- As the nodes vote based on trustworthiness of delegates
  - More pressure to act honestly
- Nodes does not have to be online all the time
  - Recall inactive nodes lose stakes in POS
- Disadvantages
- Small number of delegates --> They can form a cartel and launch 51% attack
- More risk of centralization
- Even younger than POS

Proof-of-burn

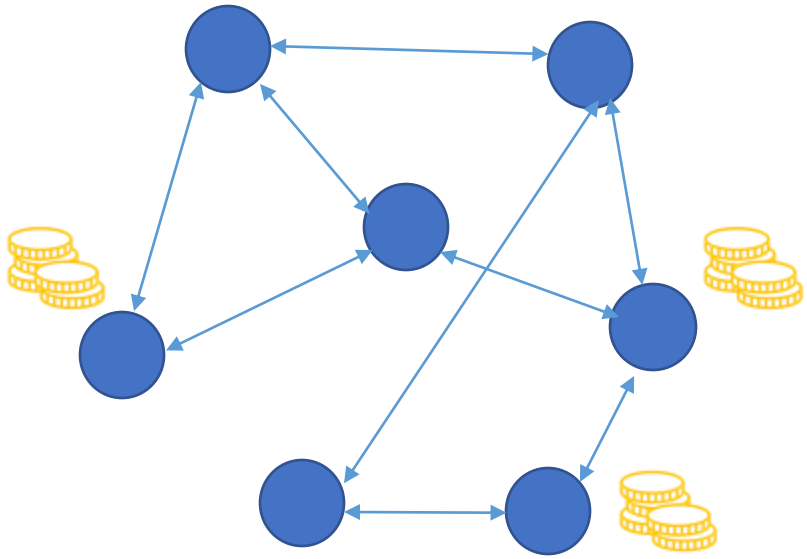
Burning of cryptocurrencies

- Burning of cryptocurrency
- Destroying the coins
  - Can be achieved by sending the coins to an irrecoverable address
  - For example, to a hash with 0x000..00
  - Eater address
- One must invert the hash to recover the coins
- Or the protocol dictate that no payment is possible from that address

- Creates scarcity of coins in circulation
  - Increases the coin price
- Analogous to stock buybacks

Proof-of-burn

Mechanism



- Nodes burn their coins to be a validator
- Probability of being chosen is proportional to the number of coins burned
- Nodes are rewarded if they propose a block

Proof-of-burn

Mechanism

- Consider this as a virtual mining
- The nodes need to spend initial investment through burning
  - Analogous to buying special hardware
- Since the nodes won't get their initial investment back
  - They are motivated to maintain the security of the network
- Nodes can recover their initial investment only after a long time
- Burned coin values are decayed periodically
  - Prevents early adopters to gain unfair advantage

Proof-of-burn

Pros and cons

- Fair coin distribution
- Only those are committed to network can mine
- Can be used to destroy old coins
  - Users can burn old coins to get new coins
- Initial coin offering: Burn coins from other network to get coins in the new network
- Less energy wastage than POW
  - No recurrence cost of electricity and real-estate
- Encourages long term commitment
- Coins are burned periodically --> Stability in prices, anti-inflationary measure
- Anyone can join like POS
- Example: Slimcoin, Facton, Counterparty

Proof-of-burn

Pros and cons

- Disadvantages
- Wasting resources by destroying already mined coins
- Dependent on other networks
- The validator selection require a lengthy process --> slower

- No guarantee of recovering the initial investment
- Coins are burned --> less liquidity
- Miner cannot leave the network without forsaking the initial investment
  - Unlike POS

Proof-of-Authority

- Like DPoS
- Validators must reveal their identity
- A node can be a validator based on many different criteria
  - History, credibility, rank in the organization, reputation, etc.
- Validators must completely conform to the rules of the blockchain
- A node must prove its trustworthiness
- A node prove long-term commitment to the network
- As evident from the name, the validators stake their reputation
- DPoS --> The validators are elected by community
- PoA --> The validators are *selected*
- Like DPoS the number of validators are small

Proof-of-Authority

- First, a leader is selected. The leader created a block and broadcasts to other validators
- In the second phase, validators distribute the block they received to one another
- If everyone accepts the block it is added to the blockchain. The process repeats with a new block leader
- If not, a vote is held to determine if the block leader is malicious
- If the node is found malicious it is removed from the network. Otherwise, the process restarts

Proof-of-Authority

Pros and cons

- Advantages
  - Fast
  - Scalable
  - Energy efficient

- Disadvantages
  - Centralized

Proof-of-Authority

Pros and cons

- Use cases
  - Mostly on private blockchains where the authority can be verified.
  - Privacy can be maintained while reaping the benefits of blockchain technology
- Supply chain logistics
  - Fast and actors are known
- Microsoft Azure*

*https://azure.microsoft.com/en-in/blog/ethereum-proof-of-authority-on-azure/

The End !!