Overview of Blockchain Consensus Mechanisms

Cork Blockchain, 2018-08-14

Johannes Ahlmann,
johannes@fluquid.com

Image: https://cdn-images-1.medium.com/max/1600/1*DpVNUugFmEhGhblHmXxbVA.jpeg

Consensus Mechanism

"A **fault-tolerant** mechanism
that is used to achieve the necessary **agreement**
on a single **data** value or a single state of the network
among **distributed processes** or multi-agent systems."

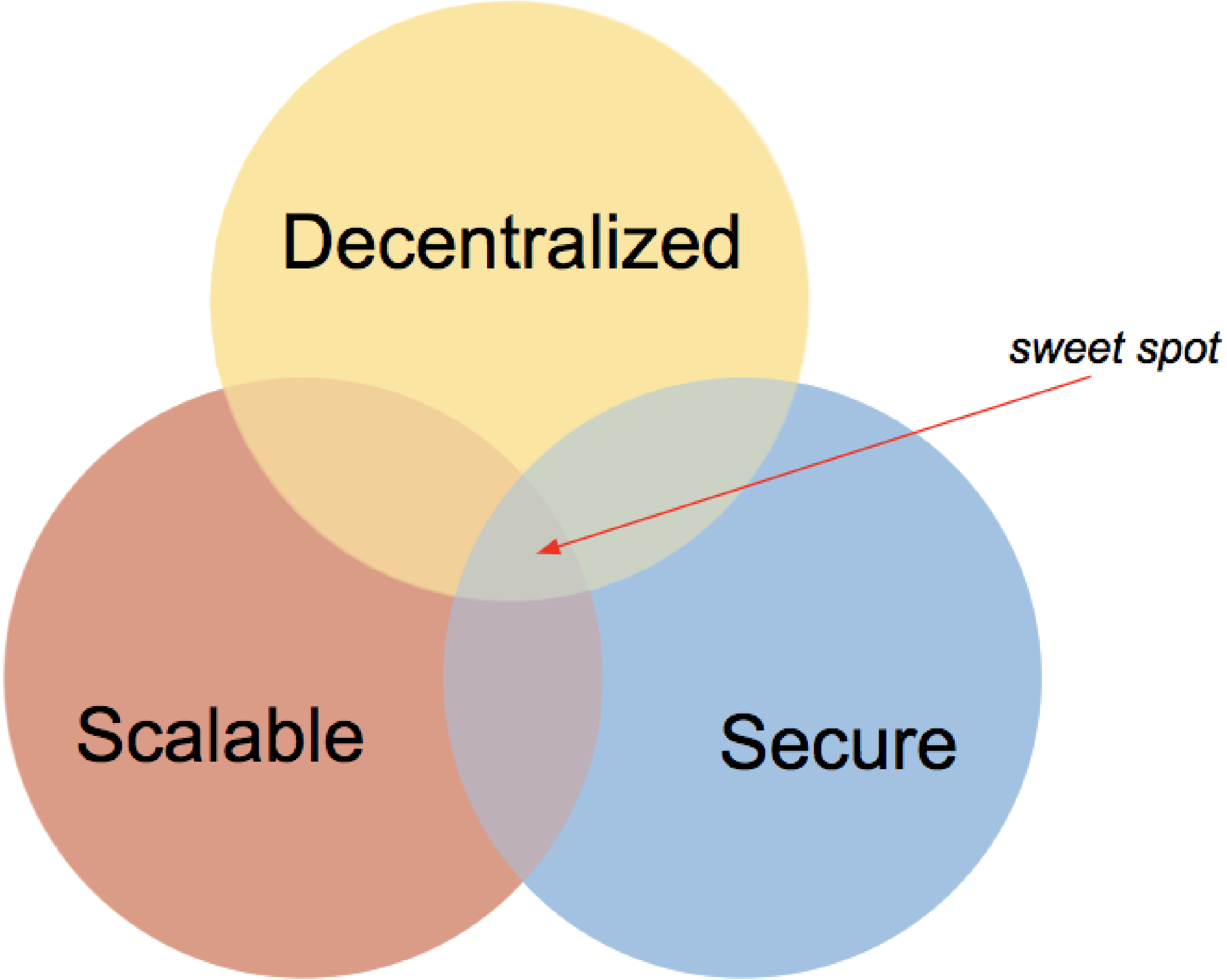
https://www.toolshero.com/wp-content/uploads/2017/09/consensus-oriented-decision-making-codm-toolshero-696x348.jpg

Byzantine Fault Tolerance

- "Crash Fault Tolerance" (CFT) aims to guarantee the functioning of a distributed system in the presence of machines crashing or disconnecting and reconnecting at random
- "Byzantine Fault Tolerance" (BFT) aims to guarantee the ability of a group of nodes to achieve consensus in the presence of malicious actors who are trying to subvert the consensus process in their favour, or prevent consensus from being achieved.
- BFT is a much harder goal than CFT, and hasn't been solved mathematically at scale; BFT generally makes use of cryptographic signatures, etc.
- Approximations of BFT exist, but they all come with significant constraints and limitations attached
  (i.e. Practical BFT achieve consensus in the presence of up to 1/3 malicious actors and <20 total nodes)

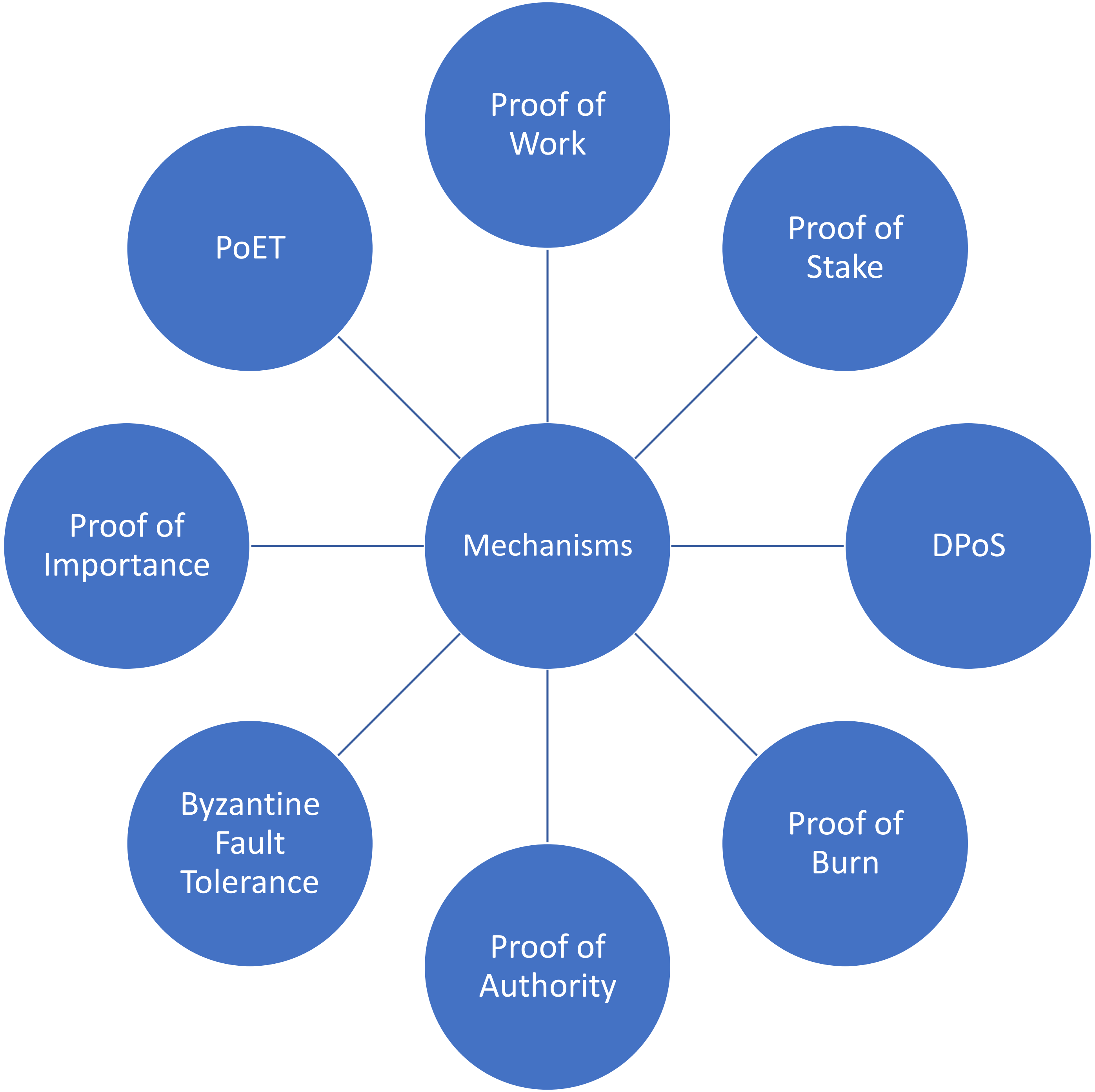
The Scalability Trilemma

- Each of the three goals by itself is "easy" to achieve
- But you have to sacrifice one of Decentralization, Scalability or Security to achieve a high level in the other two
- Bitcoin sacrifices scale (to some degree) for decentralization and security
- Ripple, Stellar, EOS sacrifice decentralization (to some degree) for scale and security
- Related to CAP Theorem for Distributed Data Stores:
  - Consistency
  - Availability
  - Partition Tolerance



https://cdn-images-1.medium.com/max/1600/1*wB2_druDLJECNI9NGEcrqQ.png

Consensus Mechanisms



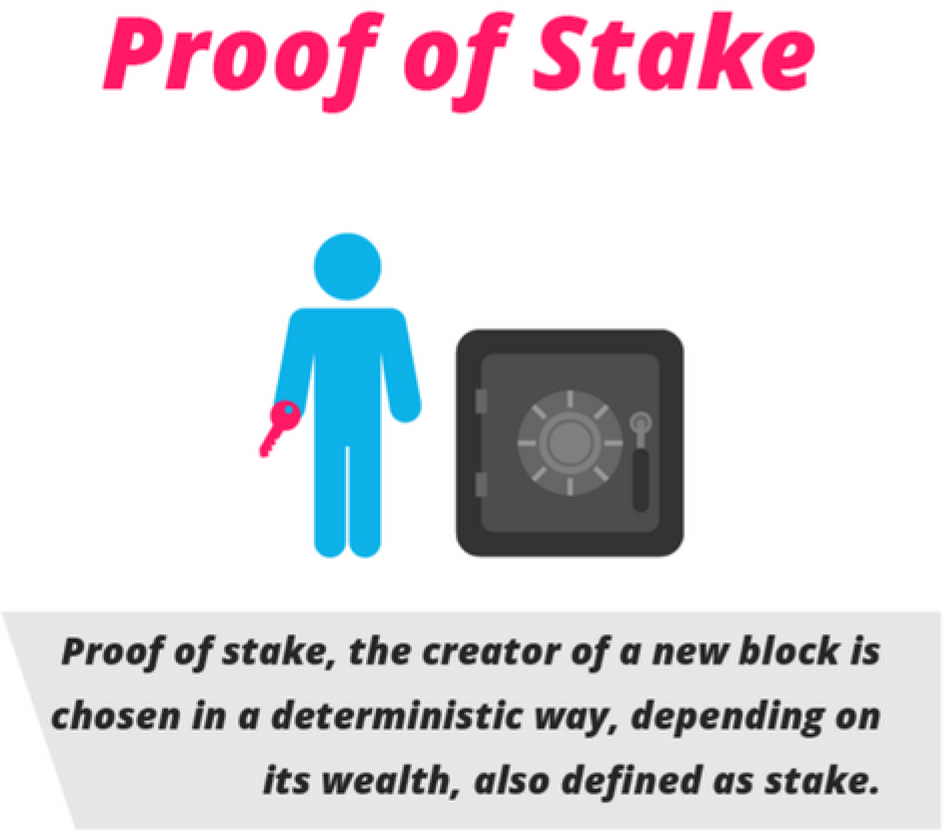
Proof of Work

- Uses scarce resource, i.e. electricity to perform a fair lottery for block creation and chain selection
- Probability of receiving block reward is roughly proportional to "work performed" / "energy burnt"
- Performs:
  - chain selection
  - coin distribution
  - who produces blocks
  - when blocks are produced
- Not a mathematical solution, but a game theoretical mechanism that leverages monetary and other incentives to "keep people honest"
- Bitcoin would not work if coins did not have a financial value
- Examples: Bitcoin, most cryptocurrencies

https://en.bitcoinwiki.org/upload/en/images/thumb/5/55/Ea5b21f014547b4b44cf2dafcd76aad2.jpg/400px-Ea5b21f014547b4b44cf2dafcd76aad2.jpg

Proof of Stake

- Staked amount is locked away and can't be accessed for a time period, and can be forfeit if the created block is invalid
- Probability of receiving "minting fee" is proportional to the amount staked
- <u>Pros</u>
  - less electricity usage
  - stronger alignment of incentives (miners vs. coin holders)
  - mining centralization, ASIC
- <u>Cons</u>
  - Naive PoS only addresses chain selection
  - The rich are getting richer
  - Risk of Loss of Funds (stakes need to be in hot wallet)
- BFT-based
  - Tendermint, Ethermint
- Chain-based
  - Ethereum Casper, NXT, PeerCoin, Decred (hybrid), Dash, NEO, Stratis, Lisk, PIVX



Proof of Stake

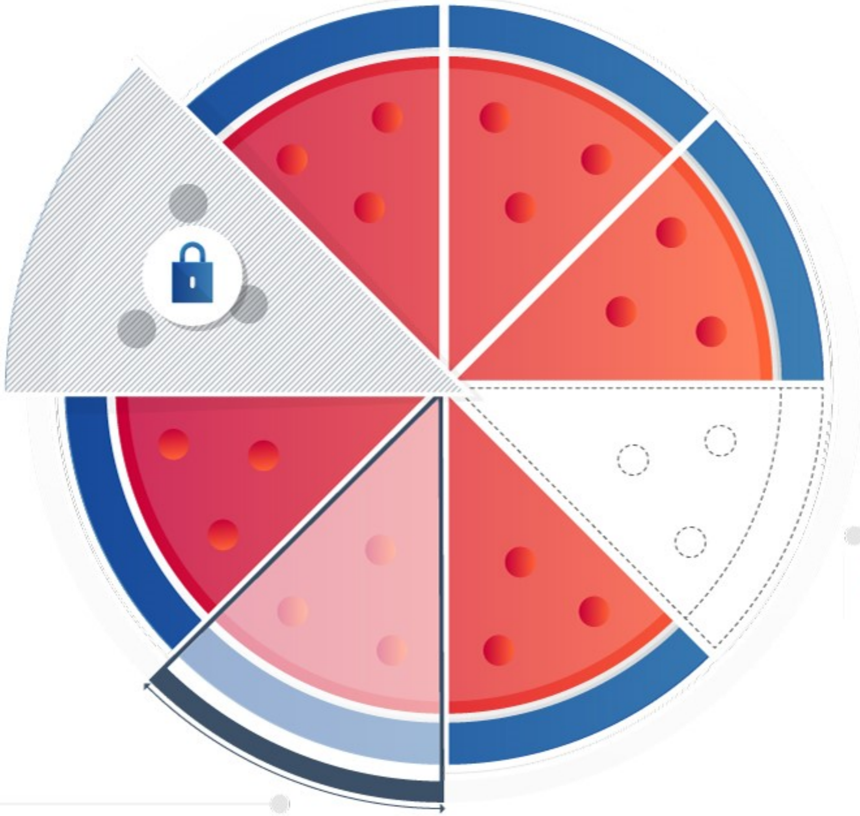
Proof of stake, the creator of a new block is chosen in a deterministic way, depending on its wealth, also defined as stake.

https://cdn-images-1.medium.com/max/1600/0*IVoaV2-p8z3mWsST.png

Proof of Stake

*In **Proof of Stake**, each validator owns some stake in the network, and has to lock it in order to be selected.*

1 **Anyone who holds the base cryptocurrency can become a validator,** although sometimes a locked up deposit is required.



2 A validators chance of mining a block is based **on how much of a stake (or cryptocurrency) they have.**

For example, if you owned 1% of the cryptocurrency, you would be able to mine 1% of all its transactions.

3 The PoS protocol will randomly assign the right to create a block in between selected validators, based upon the value of their stakes.

The chosen validator is rewarded by a part or the whole of the transaction fee.

Lisk ACADEMY

https://lisk.io/content/5-academy/2-blockchain-basics/4-how-does-blockchain-work/8-proof-of-stake/8-pos-infographic.jpg

Delegated Proof of Stake

- Nodes vote for Witnesses (top 100 are paid, top 20 earn a regular salary), nodes can withdraw their vote in case of improper conduct by a Witness
- Relies upon a group of delegates to validate blocks on behalf of all nodes in the network
- Pros: Scalable, energy efficient, cheap transactions.
- Cons: Partially centralized
- Examples: Bitshares, EOS, Steemit

Proof of Burn

- Generate a random target address;
  it is infeasible to find the private key for a given public address
- Send existing coins to this unspendable address as "proof of burn". The tokens cannot never be recovered
- Selected block mining probability proportional to burnt coins, or use "proof of burn" to bootstrap/ seed new coins
- Examples: SlimCoin,
  CounterParty (for seeding)

https://cointelegraph.com/news/the-full-story-of-cannabiscoins-premine-burn

Proof of Elapsed Time (PoET)

- Nodes need to be identifiable and accepted into the network (permissioned blockchain)
- Uses Trusted Hardware for "fair lottery". Every node generates a random number for how long it has to wait, and the random number utilitizes Trusted Computing hardware.
- Requires "Intel Software Guard Extensions (SGX)" on node CPUs
- Examples: Hyperledger Sawtooth

https://www.hyperledger.org/wp-content/uploads/2018/01/Hyperledger_Sawtooth_Logo_Color.png
http://www.stickpng.com/assets/images/58568d224f6ae202fedf2720.png

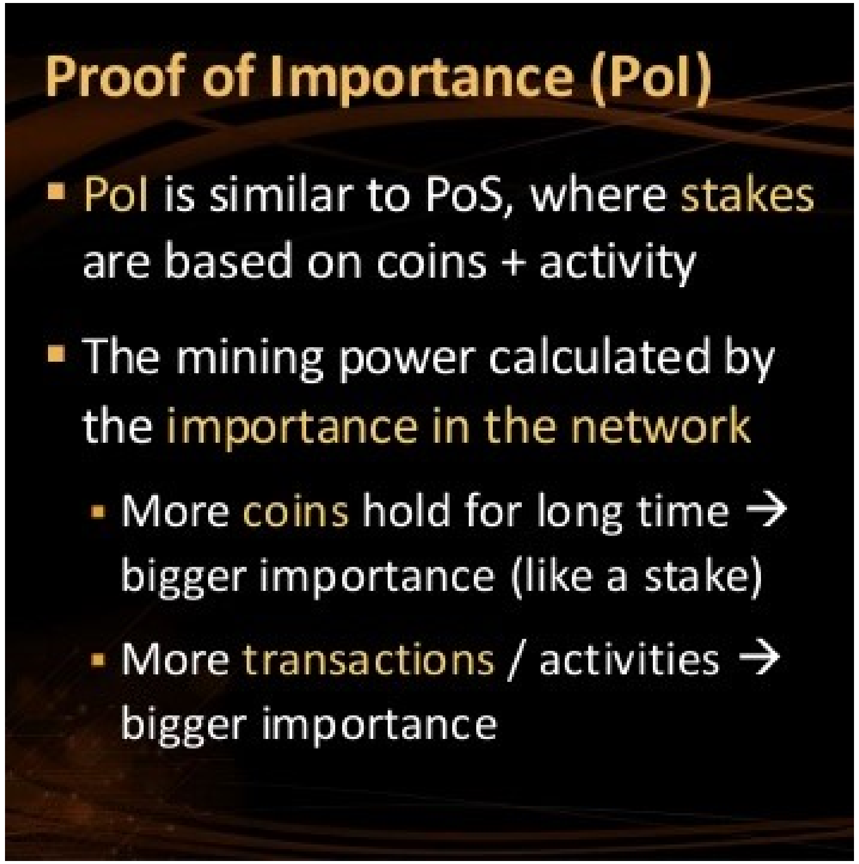
Proof of Authority

- Stakes social capital, rather than financial capital
- By identifying validators, PoA consensus becomes inherently centralized. Therefore, it’s best suited for private blockchains and consortiums
- Validators should be scarce, so there is a desire to hold the title.
- Nodes "stake their reputation"
- Inherently centralized
- Examples: Parity/ Kovan, Rinkeby, VeChain

https://cdn-images-1.medium.com/max/1500/1*vQ3fRvhuKa1gt1KYscIsrg.png

Proof of Importance

- Proof of Importance recognizes that other factors (than staked amount and coin hold time) can be taken into account when determining what nodes provide the most value to a network
- <u>Key factors:</u>
  - Net transfers, or total spent in the last 30 days.
  - Vested amount of currency to create blocks.
  - Nodes that are clustered, aka more intermingled, are more heavily weighted.
- Examples: XEM



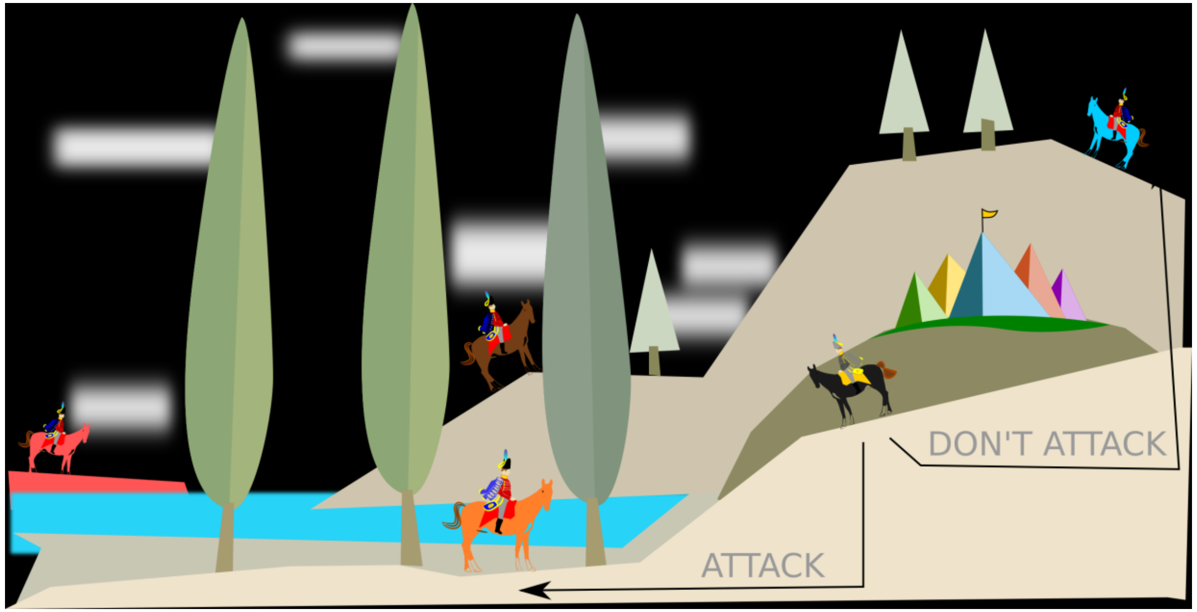
Proof of Importance (PoI)

- PoI is similar to PoS, where stakes are based on coins + activity
- The mining power calculated by the importance in the network
  - More coins hold for long time → bigger importance (like a stake)
  - More transactions / activities → bigger importance

Image: https://www.slideshare.net/nakov/consensus-algorithms-nakov-jprofessionals-jan-2018

Byzantine Fault Tolerance

- Centralized, Permissioned
- Can tolerate 1/3 malicious nodes
- Variants, Applications
  - Practical BFT (PBFT), Istanbul - don't scale beyond 20 nodes
  - Redundant BFT (RBFT)
  - Federated Byzantine Agreement (Stellar, Ripple)
  - Honeybadger



https://www.iconspng.com/image/40058/byzantine-generals-problem

Attacks on Proof of Stake

- **Nothing at Stake**
  - Staker can stake on all candidate chains; and will be seen as having staked on whichever chain ultimate "wins"
  - This can in principle be detected, but changing stakes is necessary for convergence.
    Explicit multiple staking rounds addresses this to some degree
  - Stake does not add to the convergence of the system;
    In contrast for PoW energy is a real-world finite resource
- **Long Range Attack**
  - Attacker could buy a key to an address that is now empty but had a large token balance in the past, and generate alternative history from that point
  - Solution: checkpointing
    Problem: checkpointing introduces centralization/"ask a friend" security model

Thank You!

Resources

- https://medium.com/the-daily-bit/9-types-of-consensus-mechanisms-that-you-didnt-know-about-49ec365179da
- https://cointelegraph.com/news/why-blockchain-needs-proof-of-authority-instead-of-proof-of-stake
- https://blog.cosmos.network/consensus-compare-casper-vs-tendermint-6df154ad56ae
- https://blog.bitmex.com/complete-guide-to-proof-of-stake-ethereums-latest-proposal-vitalik-buterin-interview/