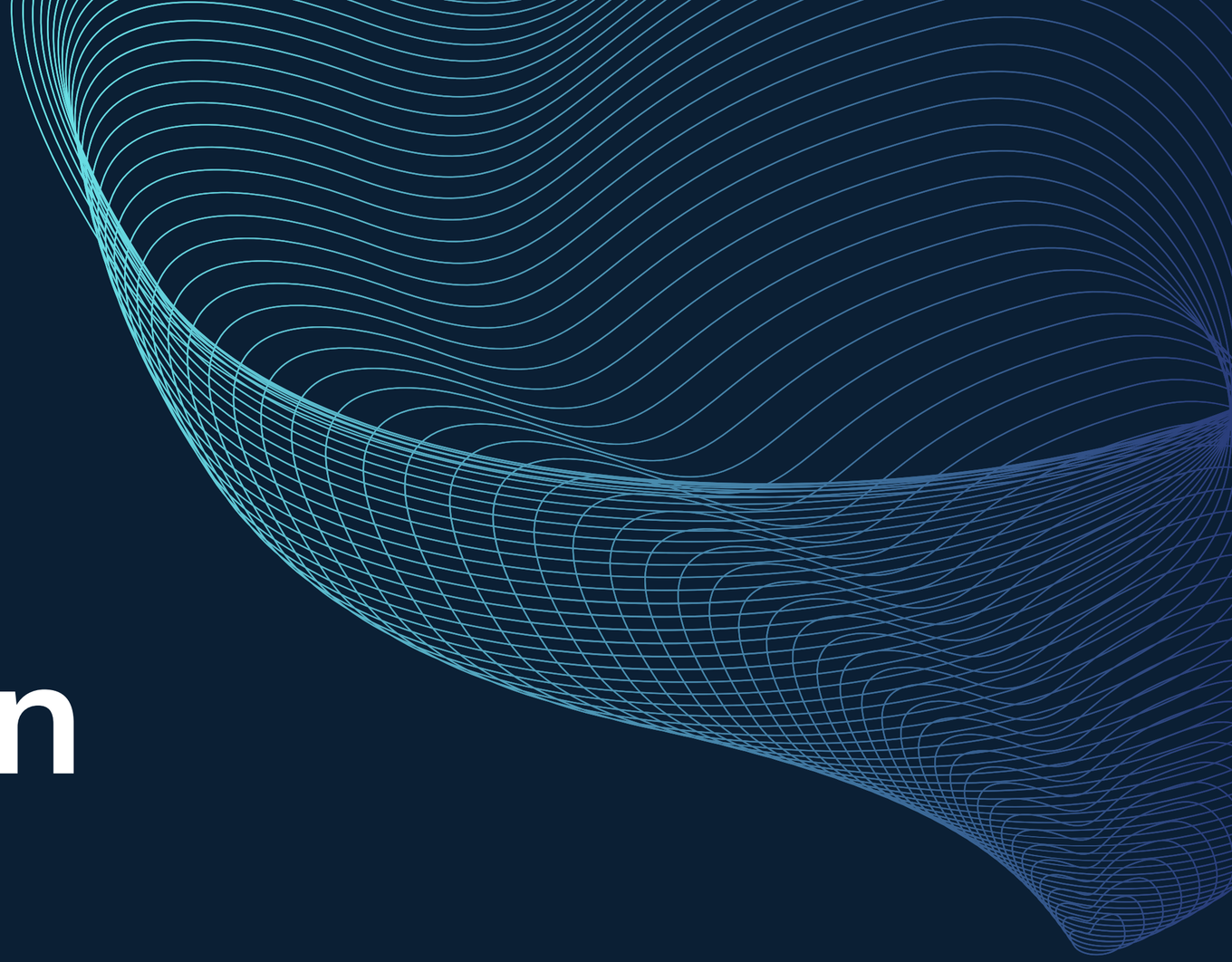
Florian Rascoussier



PhD Track 4 Year project

Consensus in blockchain applications

June 7th 2022

Table of content

Basics of consensus

Creating Consensus

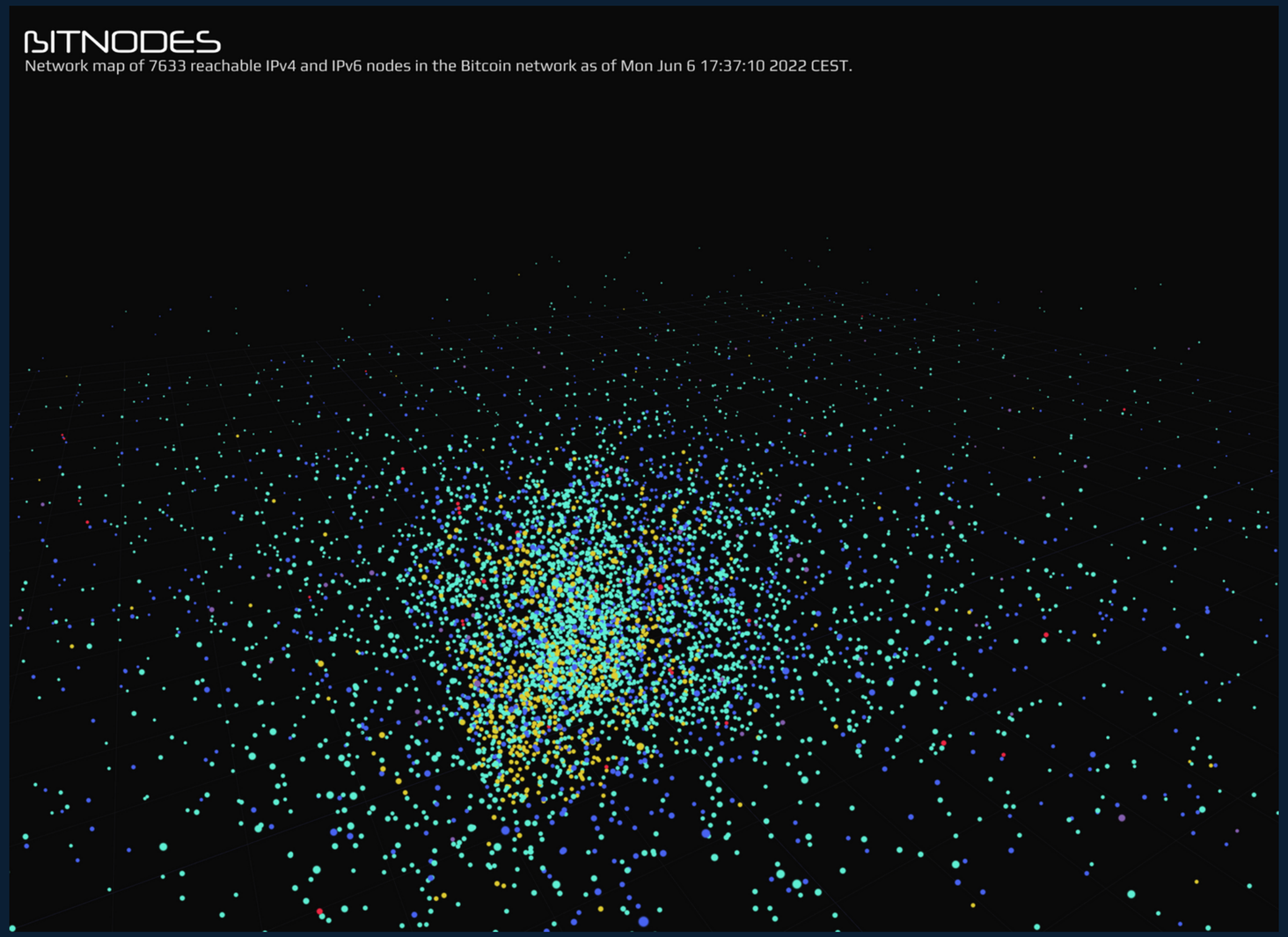
Proofs of Something

Questions & Answers

What is consensus

By definition, and in practice

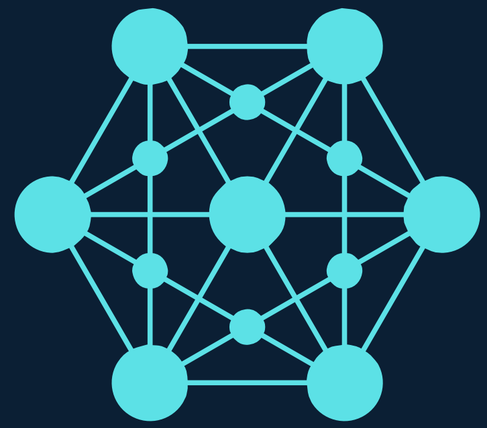
What is consensus



Consensus:

1 - general agreement : UNANIMITY	2 - The judgment arrived at by most of those concerned	3 - group solidarity in sentiment and belief

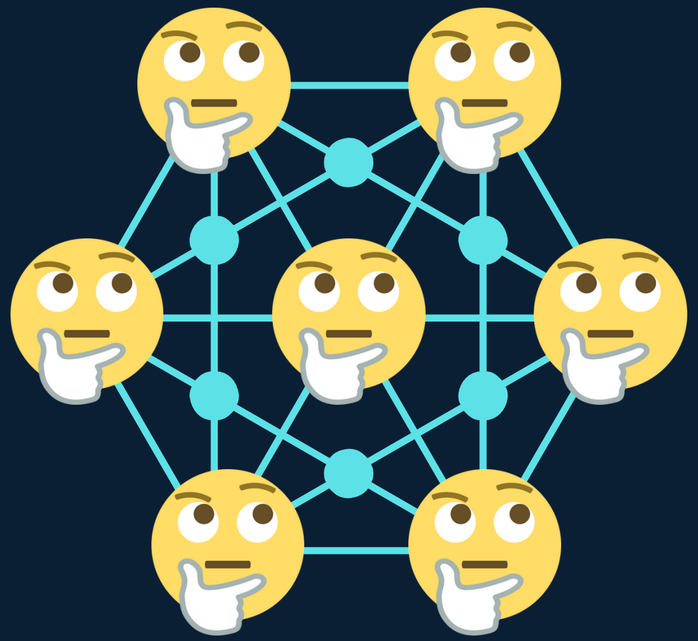
Overall reliability vs **fault tolerance**

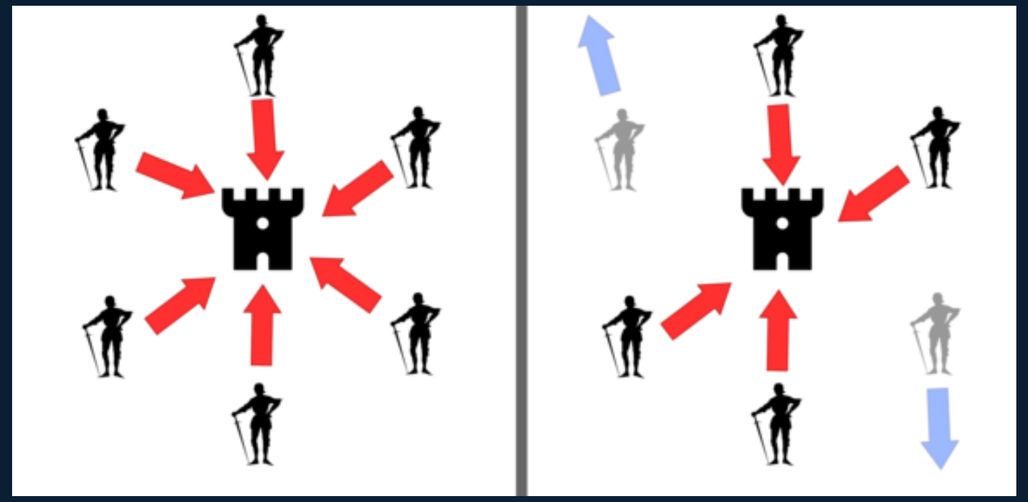


- Oyinloye, D.P.; Teh, J.S..; Alawida, M.; Jamil, N. Blockchain Consensus: An Overview of Alternative Protocols. Symmetry 2021, 13, 1363.
- https://en.wikipedia.org/wiki/Consensus_(computer_science)
- https://www.merriam-webster.com/dictionary/consensus
- https://www.larousse.fr/dictionnaires/francais/consensus/18357

Byzantine Generals

Byzantine fault tolerance (BFT)



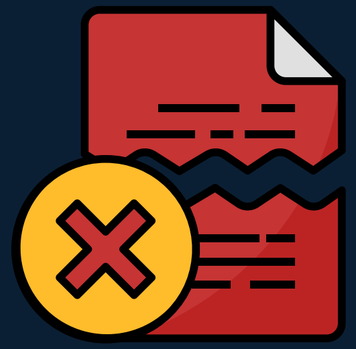


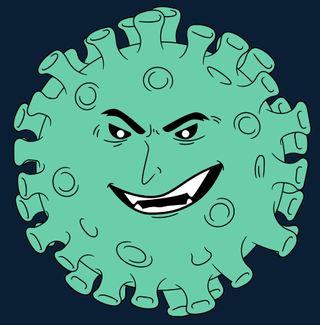
- Lamport, L.; Shostak, R.; Pease, M. (1982). "The Byzantine Generals Problem" (PDF). ACM Transactions on Programming Languages and Systems. 4 (3): 387–389.
- Matthias Fitzi (2002). "Generalized Communication and Security Models in Byzantine Agreement" (PDF). ETH Zurich
- https://en.wikipedia.org/wiki/Byzantine_fault.

Creating Consensus

How to ensure consensus

Consensus ?





First Past the Post

First Past the Post is the name for the electoral system used to elect Members of Parliament (MPs) to Westminster.

Read More →

WHERE IT'S USED
- Westminster
- United States
- India

PROPORTIONALITY	★★☆☆☆
VOTER CHOICE	★★☆☆☆
LOCAL REPRESENTATION	★★★☆☆

Single Transferable Vote

With the Single Transferable Vote, the strength of the parties matches the strength of their support in the country, and representatives - for example, Members of Parliament - have a strong connection to their local area.

Read More →

WHERE IT'S USED
- Ireland
- Scottish Local Elections
- Northern Ireland Assembly
- Malta

PROPORTIONALITY	★★★★☆
VOTER CHOICE	★★★★★
LOCAL REPRESENTATION	★★★★★

Additional Member System

The Additional Member System uses a mix of first past the post constituencies and party lists.

Read More →

WHERE IT'S USED
- Scottish Parliament
- Senedd Cymru / Welsh Parliament
- Germany
- New Zealand

PROPORTIONALITY	★★★★☆
VOTER CHOICE	★★★☆☆
LOCAL REPRESENTATION	★★★☆☆

Alternative Vote Plus

Recommended by the Jenkins Commission in 1998, the Alternative Vote Plus (AV+) system has not been used anywhere in the world.

Read More →

WHERE IT'S USED
- Nowhere

PROPORTIONALITY	★★★☆☆
VOTER CHOICE	★★★★☆
LOCAL REPRESENTATION	★★★★☆

Two-Round System

The top two candidates go through to a second election and voters choose their favourite.

Read More →

WHERE IT'S USED
- Presidents of many countries
- France

PROPORTIONALITY	★★☆☆☆
VOTER CHOICE	★★★☆☆
LOCAL REPRESENTATION	★★★☆☆

Alternative Vote

With the Alternative Vote (AV) your constituency gets a Member of Parliament (MP) the majority support.

Read More →

WHERE IT'S USED
- Australia
- Irish President

PROPORTIONALITY	★★☆☆☆
VOTER CHOICE	★★★☆☆
LOCAL REPRESENTATION	★★★★☆

Supplementary Vote

With the Supplementary Vote, candidates have to campaign to get a broader base of support.

Read More →

WHERE IT'S USED
- UK Mayors
- Police and Crime Commissioners
- Mayor of London

PROPORTIONALITY	★★☆☆☆
VOTER CHOICE	★★★☆☆
LOCAL REPRESENTATION	★★★☆☆

Borda Count

A rarely used points based electoral system.

Read More →

WHERE IT'S USED
- Nauru
- Kiribati
- Eurovision

PROPORTIONALITY	★★★☆☆
VOTER CHOICE	★★☆☆☆
LOCAL REPRESENTATION	★★★☆☆

Party List Proportional Representation

In Party List systems, seats in parliament closely match how many votes each party receives, but there is often a weaker constituency link.

Read More →

WHERE IT'S USED
- Israel
- Brazil
- South Africa

PROPORTIONALITY	★★★★★
VOTER CHOICE	★★★☆☆
LOCAL REPRESENTATION	★★☆☆☆

BFT protocols

public-key cryptography

$n > 3t$

pBFT

PRACTICAL BYZANTINE
FAULT TOLERANCE

pBFT consensus rounds (views):

1. **client** request to **leader** node
2. **leader** broadcasts the request
3. **nodes** reply to **client**.
4. **client** awaits f+1 similar replies

f -> maximum number of potentially faulty nodes.

pBFT

Hyperledger:
blockchain consortium under The Linux Foundation

Implementations:
Hyperledger Fabric
Zilliqa

Transaction finality

Energy Efficiency

Low reward variance

Scaling

Sybil attacks

Advances Solutions

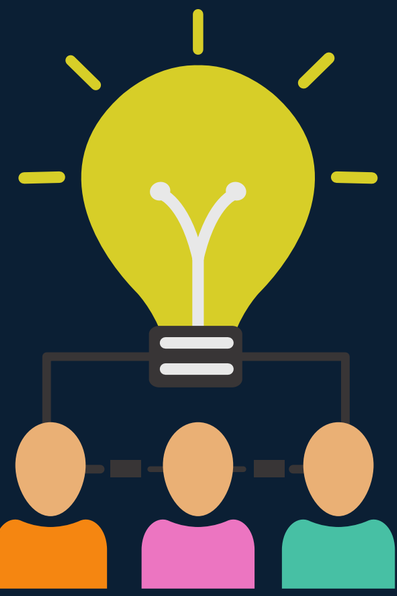
performance and cost: **Q/U**, **HQ**, **Zyzzyva**, **ABsTRACTs**

robustness: **Aardvark** and **RBFT**

Multiple: Adapt

reduce replicas: **A2M-PBFT-EA** and **MinBFT**

PoS: **endermint BFT**



Proofs of Something

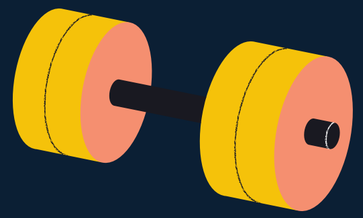
cryptographic proof

What ?

Blockchain: distributed ledger technology

- Security
- Accountability
- Decentralization
- Transparency
- Immutability

Proof of Work (PoW)



Well known: solve a simple random puzzle

1. Only one miner can write a block at a given time
2. All miners try to solve problem (hard and random)
3. First to win writes block
4. Other nodes check and validate (simple verif)
5. Longest chain is true chain
6. difficulty adjusts itself

Simplicity

High Energy Costs

Low reward variance

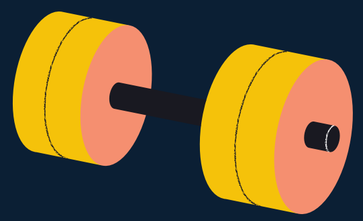
resource biased

51% attack

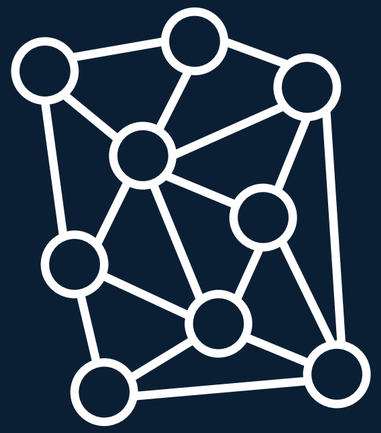
High Energy Costs

high entry cost

Proof of Space (PoSpace)



Shabal’s algorithm



based on **hard-to-pebble** graphs

Proving you have devoted space instead of computation time.

Efficient Pebbling: A Space/Time Tradeoff

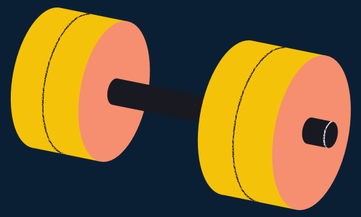
1. You can pebble a vertex only if all of its parents have been pebbled
2. This means that the sources can be pebbled at any time
3. Pebbling a vertex is storing the hash of its parents
4. Removing a pebble is freeing that memory
5. Compare Shabal's algo solutions and keep best space/time value

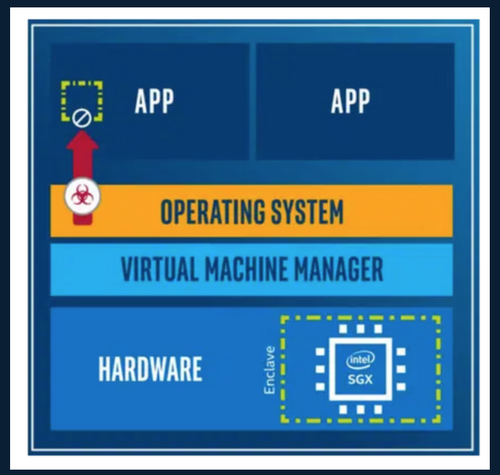
Real Useful resource

resource biased

High entry cost

Proof of Elapsed Time (PoET)





<u>Using specialized software and hardware:</u>

PoET follows a lottery system, giving every node the same chance:

1. Each node in the network is assigned a random waiting time.
2. The first node to complete the randomly chosen period validates the new block

Hyperledger Sawtooth

dependency on specialized hardware

Lack of standardization

Proof of Stake (PoS)

Validation via Staking:

1. Use coins as collateral and lock it
2. Get a chance to mine (validate block)
3. selection: amount staked + other

Other: stake age, random, lowest hash and highest stake...

Stakeholder incentives

Low 51% attack probability

Energy Efficiency

Low barrier to entry

Easy Multiple Forks

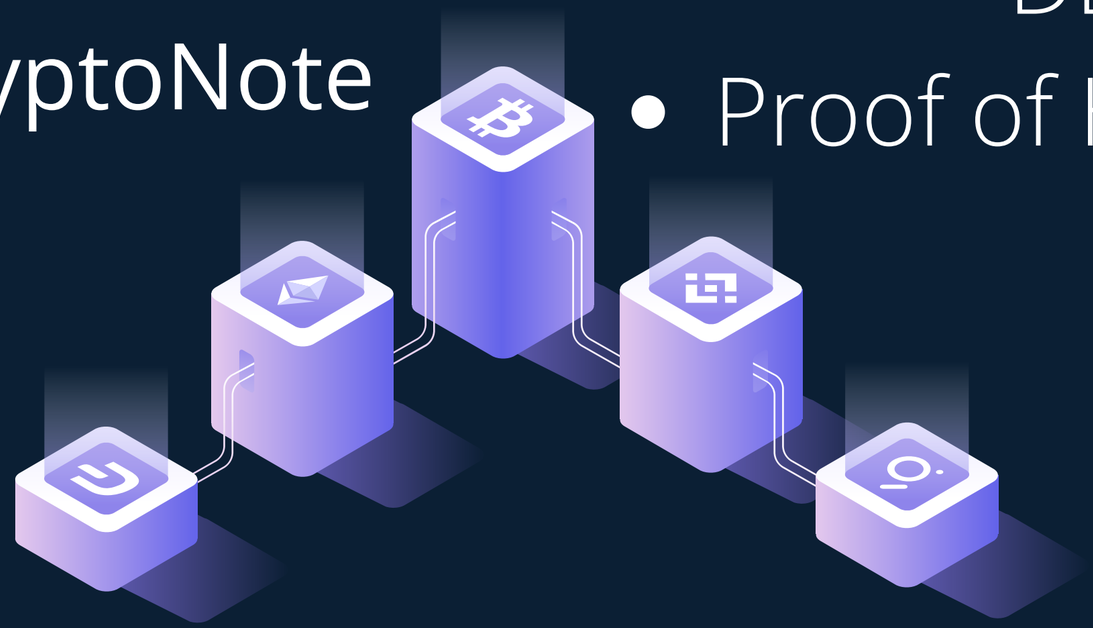
Validators with large stakes

Nothing-at-stake

long-range attacks

And many many other...

- DPoS
- DPoR
- Hybrid PoW + PoS
- CryptoNight/CryptoNote
- Quark
- Scrypt
- Equihash
- NeoScrypt
- DBft
- Proof of Humanity



Questions

And other additional elements

Sources

- Oyinloye, D.P.; Teh, J.S..; Alawida, M.; Jamil, N. Blockchain Consensus: An Overview of Alternative Protocols. Symmetry 2021, 13, 1363.
- https://en.wikipedia.org/wiki/Consensus_(computer_science)
- https://www.merriam-webster.com/dictionary/consensus
- https://www.larousse.fr/dictionnaires/francais/consensus/18357
- https://en.wikipedia.org/wiki/Byzantine_fault
- Matthias Fitzi (2002). "Generalized Communication and Security Models in Byzantine Agreement" (PDF). ETH Zurich.
- Lamport, L.; Shostak, R.; Pease, M. (1982). "The Byzantine Generals Problem" (PDF). ACM Transactions on Programming Languages and Systems. 4 (3): 387–389.
- https://www.section.io/engineering-education/blockchain-consensus-protocols/
- https://en.wikipedia.org/wiki/Proof_of_work
- Jakobsson, Markus; Juels, Ari (1999). "Proofs of Work and Bread Pudding Protocols". Secure Information Networks: Communications and Multimedia Security. Kluwer Academic Publishers: 258–272

- https://golden.com/wiki/SpaceMint_(cryptocurrency)
- https://www.blockchain-council.org/blockchain/what-are-the-alternative-strategies-for-proof-of-work/
- Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. Tech.
- rep. Jan. 2009.
- https://en.wikipedia.org/wiki/Proof_of_work#cite_note-JaJue1999-1
- Saleh, Fahad (2021-03-01). "Blockchain without Waste: Proof-of-Stake". The Review of Financial Studies. 34 (3): 1156–1190.
- Li, Wenting; Andreina, Sébastien; Bohli, Jens-Matthias; Karame, Ghassan (2017). "Securing Proof-of-Stake Blockchain Protocols". In Garcia-Alfaro, Joaquin; Navarro-Arribas, Guillermo; Hartenstein, Hannes; Herrera-Joancomartí, Jordi (eds.). Data Privacy Management, Cryptocurrencies and Blockchain Technology. Lecture Notes in Computer Science. Cham: Springer International Publishing. pp. 297–315.
- https://journalducoin.com/defi/consensus-blockchain-proof-of-elapsed-time/