Distributed Systems Seminar

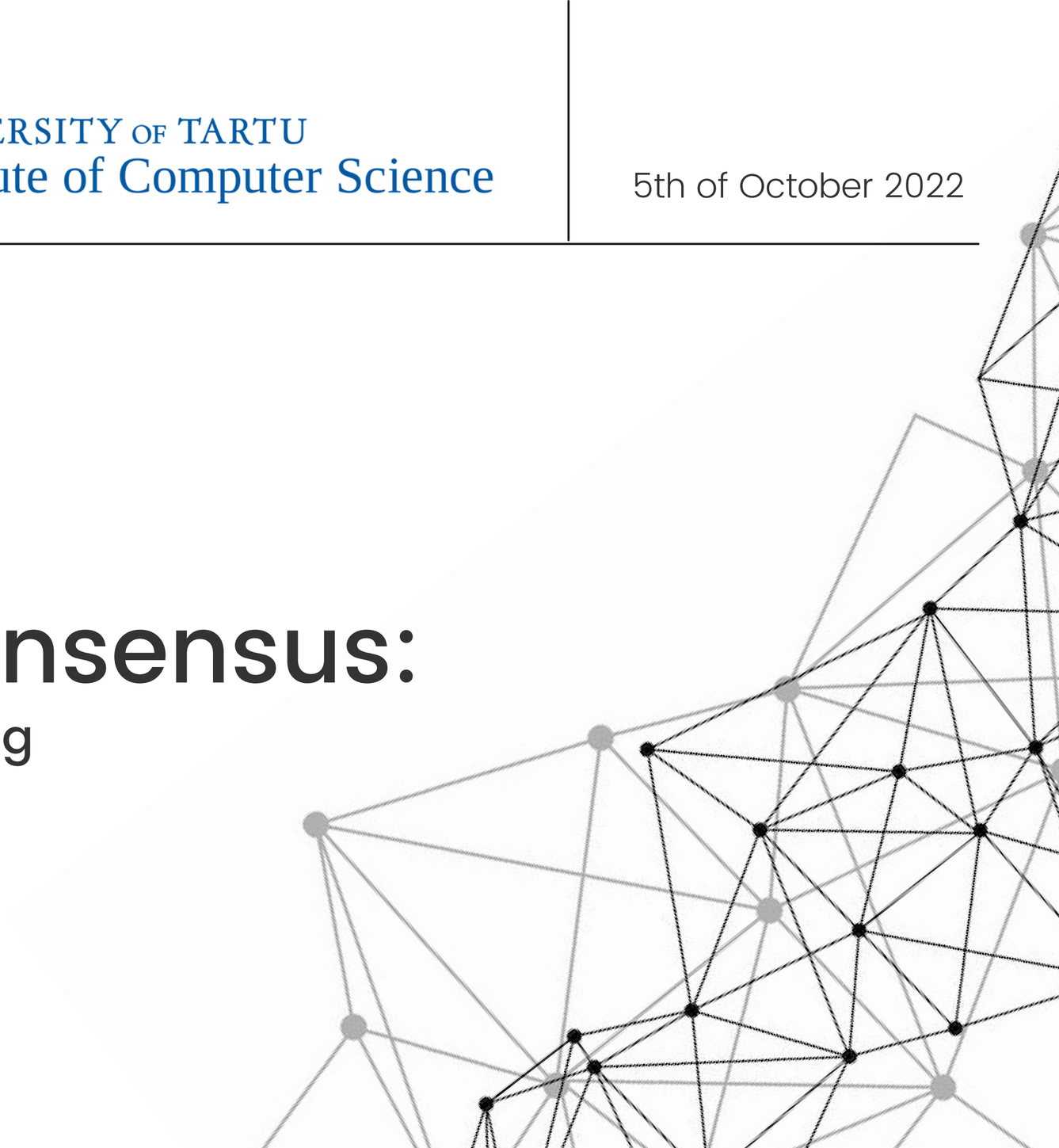
UNIVERSITY OF TARTU
Institute of Computer Science

5th of October 2022

The Units of Permissionless Consensus:

Towards Mobile and Edge Computing

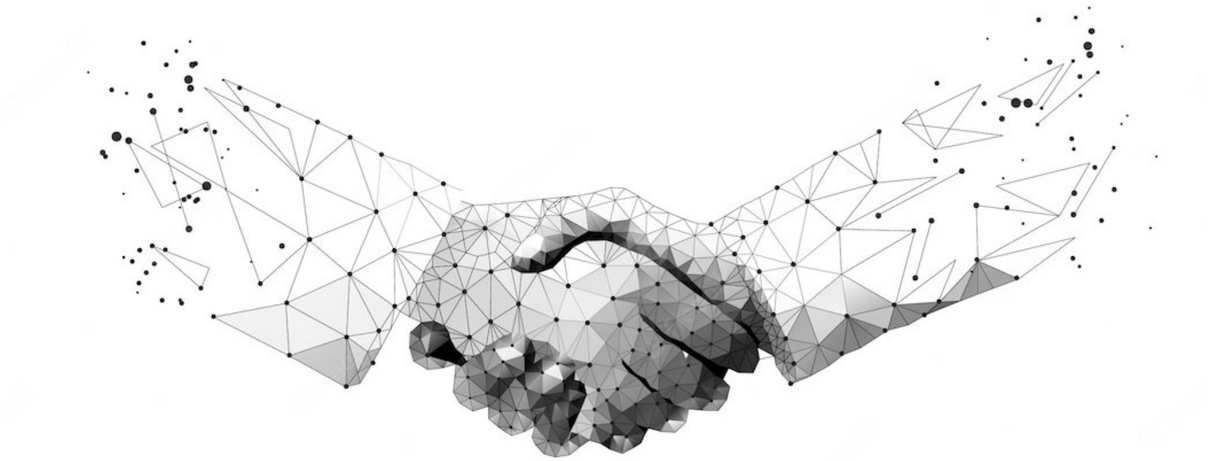
Eduardo Ribas Brito



[1] Reaching Agreement in the Presence of Faults
M. Pease, R, Shostak, and L. Lamport, 1980

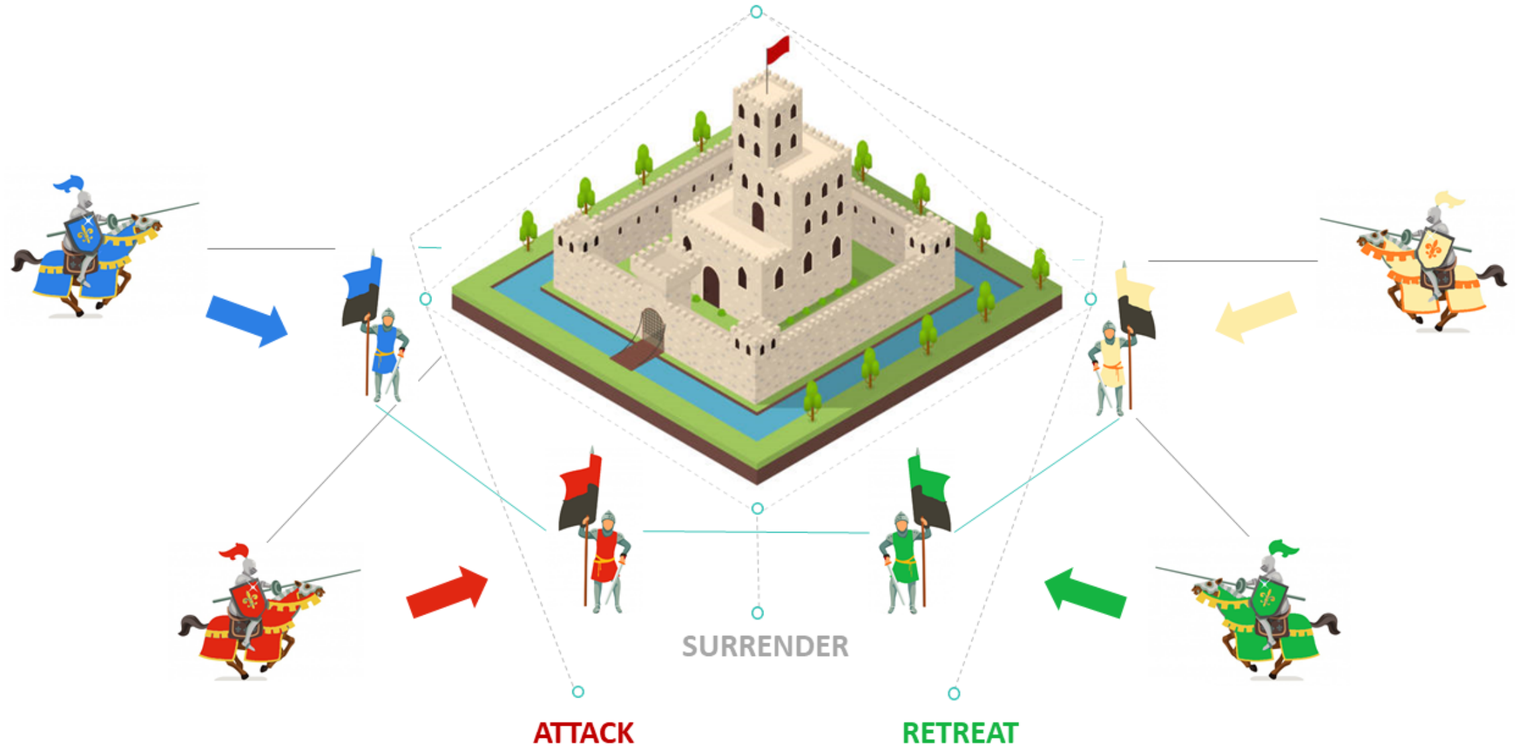
Consensus is...

Reaching an agreement between multiple parties in the potential presence of faulty individuals.



[2] The Byzantine Generals Problem
M. Pease, R, Shostak, and L. Lamport, 1982.

The Byzantine Generals Problem

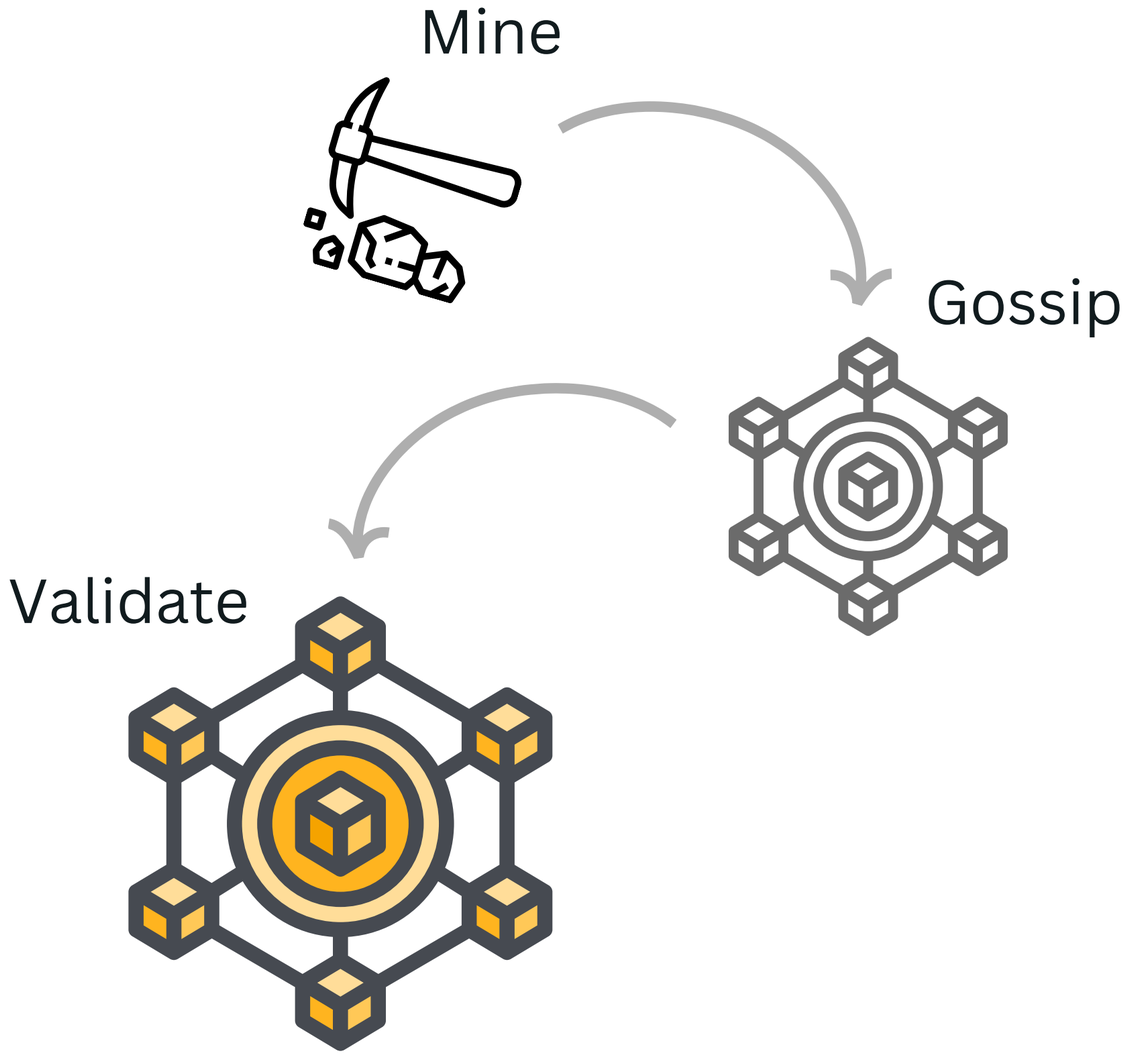


[3] Bitcoin: A peer-to-peer electronic cash system.
Satoshi Nakamoto, 2008.

Permissioned vs Permissionless

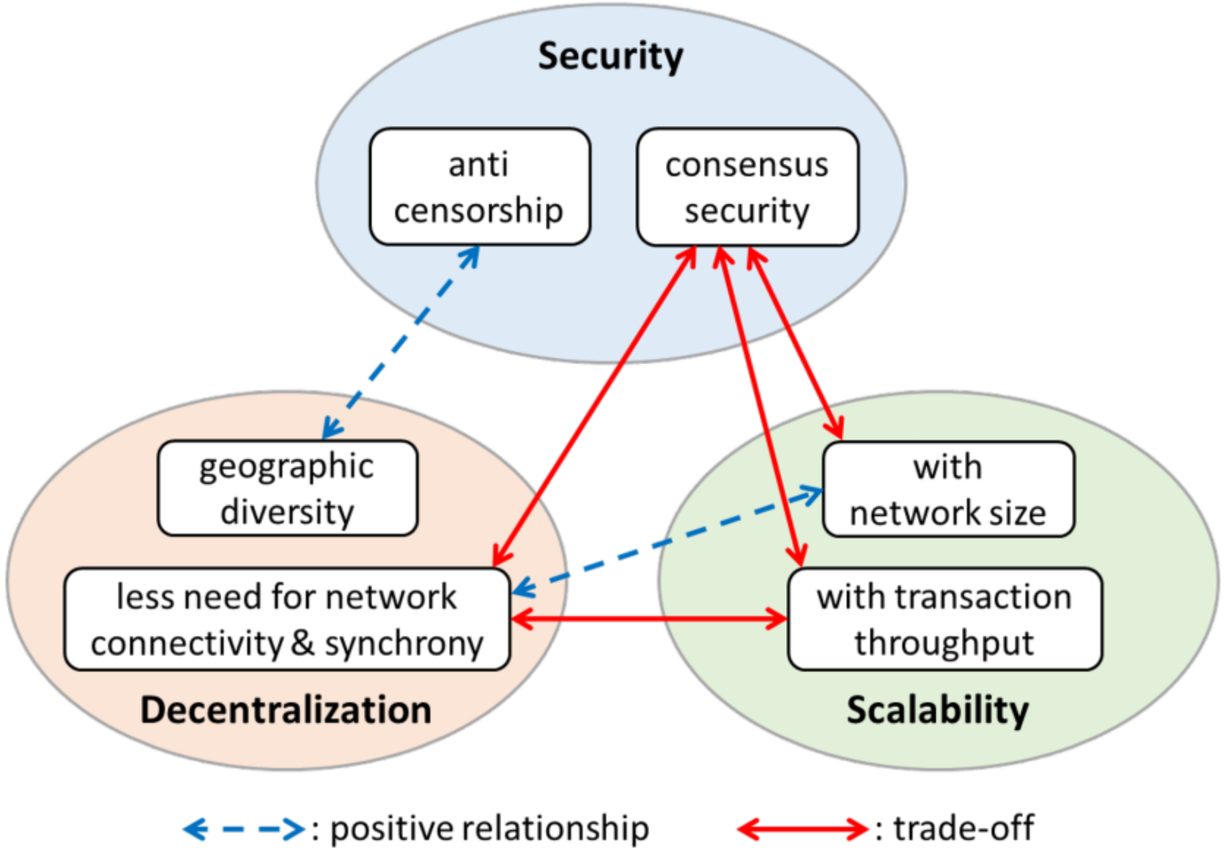
[4] A survey of distributed consensus protocols for blockchain networks.
Yang Xiao, Ning Zhang, Wenjing Lou, and Y. Thomas Hou. 2020.

The Building Blocks of Permissionless Consensus



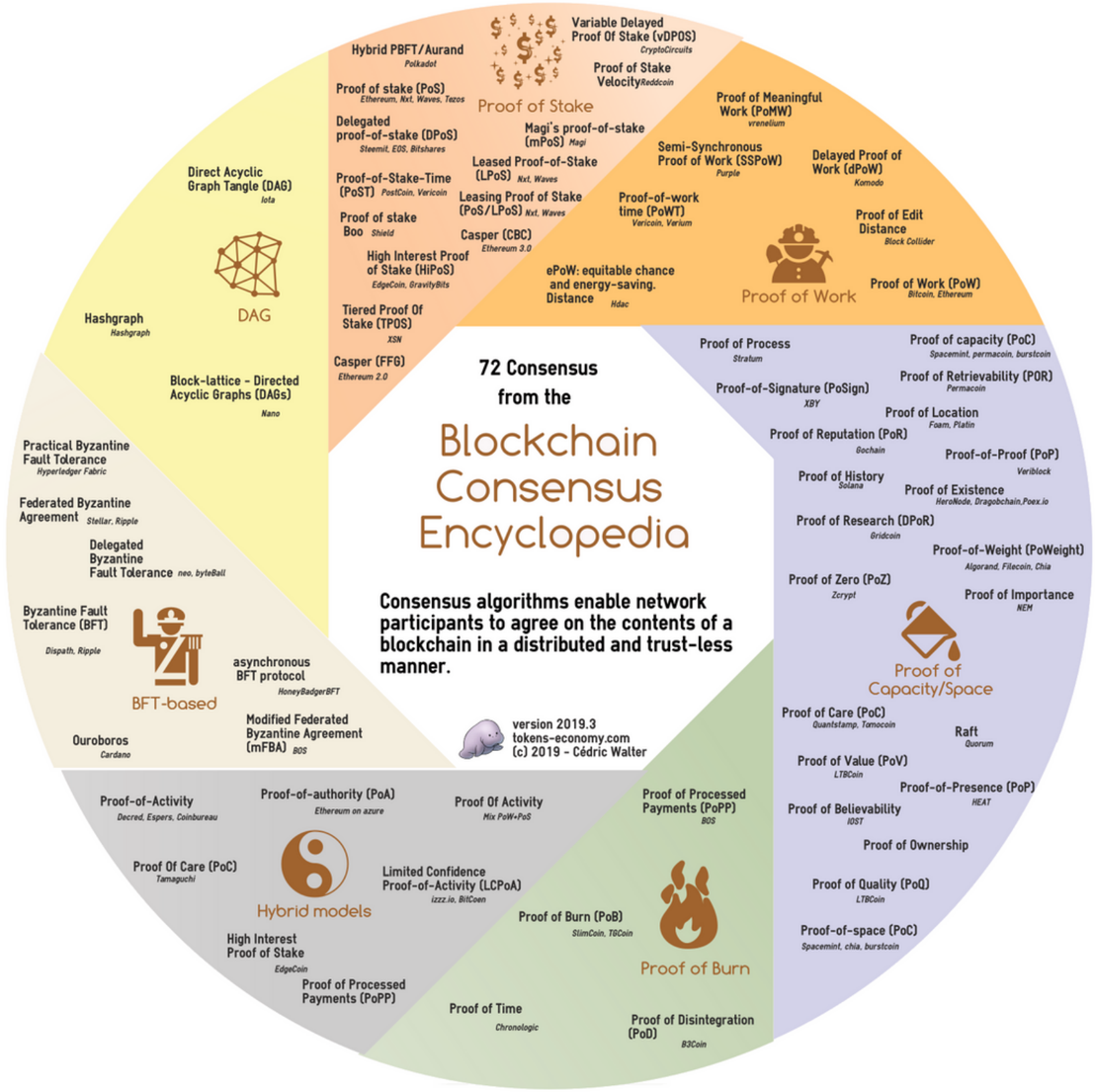
[5] A survey on consensus mechanisms and mining strategy management in blockchain networks. Wenbo Wang, Dinh Thai Hoang, Peizhao Hu, Zehui Xiong, Dusit Niyato, Ping Wang, Yonggang Wen, and Dong In Kim.

Trade-offs and Trilemma



[6] A comprehensive review of blockchain consensus mechanisms.
Bahareh Lashkari and Petr Musilek.

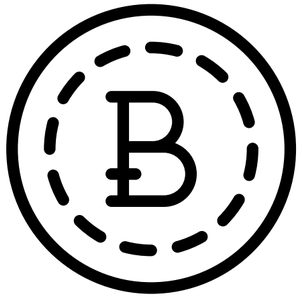
The Chaotic Diversity of Consensus Algorithms



[7] Deconstructing blockchains: A comprehensive survey on consensus, membership and structure
Christopher Natoli, Jiangshan Yu, Vincent Gramoli, and Paulo Esteves-Verissimo.

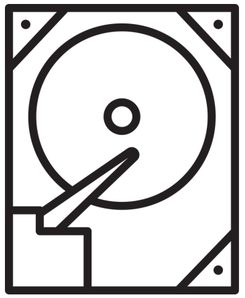
Alternatives to Proof-of-Work

Proof-of-Stake



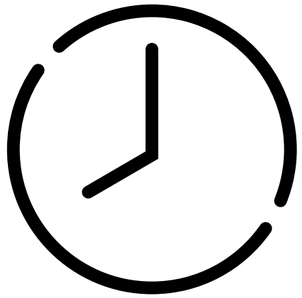
Chain-based
Committee-based
BFT-based
Delegated PoS
Proof-of-Authority

Proof-of-Space



Proof-of-Capacity
Proof-of-Retrievability

Proof-of-Elapsed-Time



Trusted Execution Environments
Proof-of-Stake

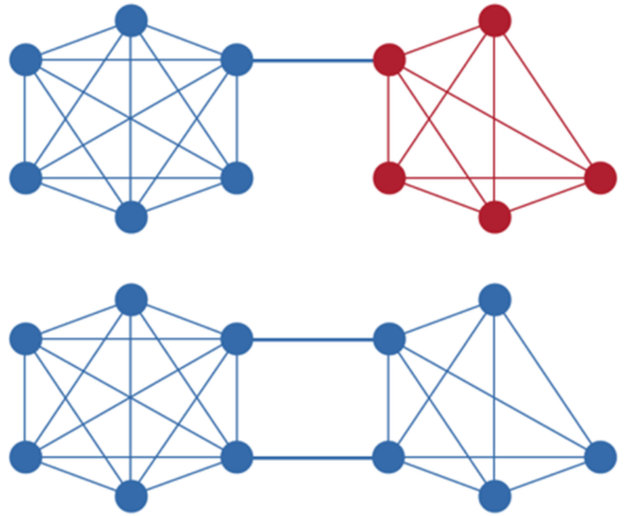
Proof-of-Location

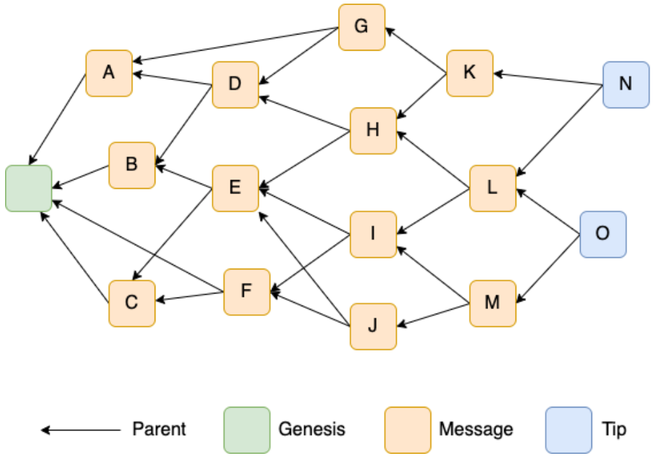
Location Validation
Close Proximity

[8] Analysis of the XRP ledger consensus protocol.
Brad Chase and Ethan MacBrough.

Different Approaches

XRP Ledger Consensus Protocol





DAGs
blockDAG
vs
txDAG

[9] A survey on consensus methods in blockchain for resource-constrained IoT networks. Mehrdad Salimitari, Mainak Chatterjee, and Yaser P. Fallah.

Permissionless Consensus in Resource-Constrained Networks

Distributed Systems Seminar

UNIVERSITY OF TARTU
Institute of Computer Science

5th of October 2022

The Units of Permissionless Consensus:

Towards Mobile and Edge Computing

Eduardo Ribas Brito