What is Consensus?

What is Consensus?

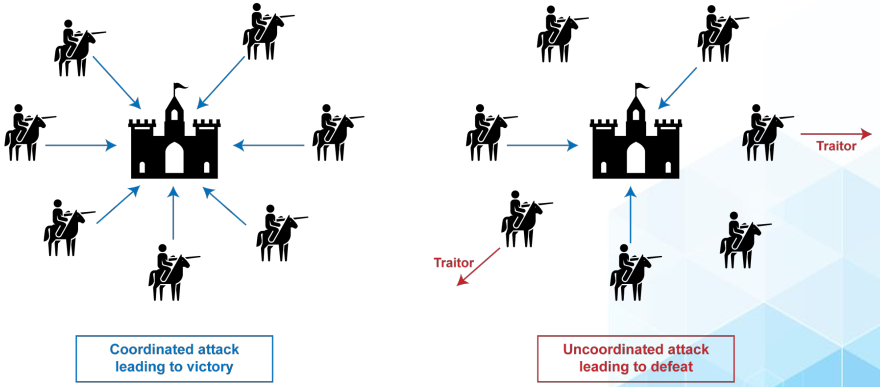
- Consensus mechanisms ensure all nodes are synchronized and agree on which transactions are legitimate and are added to the blockchain.
- A consensus algorithm may be defined as the mechanism through which a blockchain network reaches an agreement on the state of the blockchain.
- In a decentralized system without a central authority and a trustless foundation, consensus algorithm is important to achieve a common outcome between unknown nodes.
- Consensus mechanism assures that the protocol level rules are being followed and guarantees that all transactions occur in a trustless way.
- A resilient and efficient method to verify and validate transactions is required for a public network with variable numbers of active nodes.

Byzantine General Problem

Byzantine General's Problem was a logical dilemma that illustrates how a group of Byzantine generals may have communication problems when trying to agree on their next move.

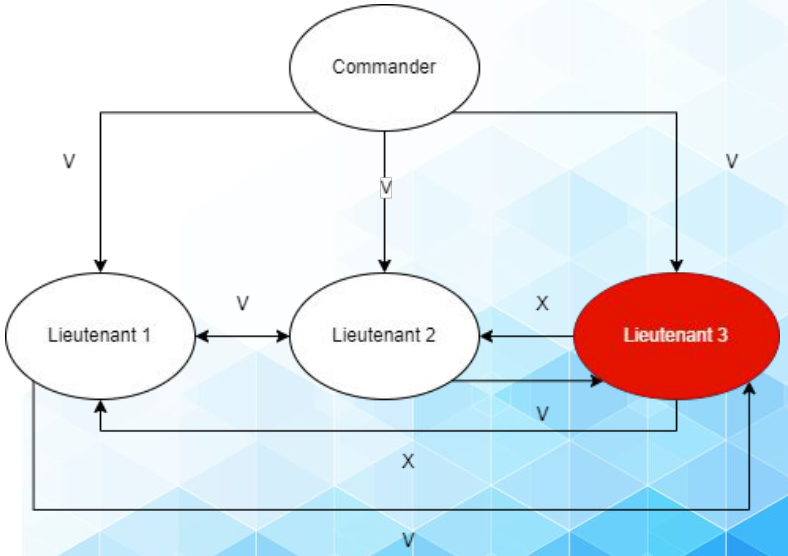
They are facing two very distinct problems:

- The generals and their armies are very far apart, so centralized authority is impossible, making coordinated attacks very tough.
- The city has a huge army, and the only way they can win is if they all attack at once.



Byzantine General Problem in Blockchain

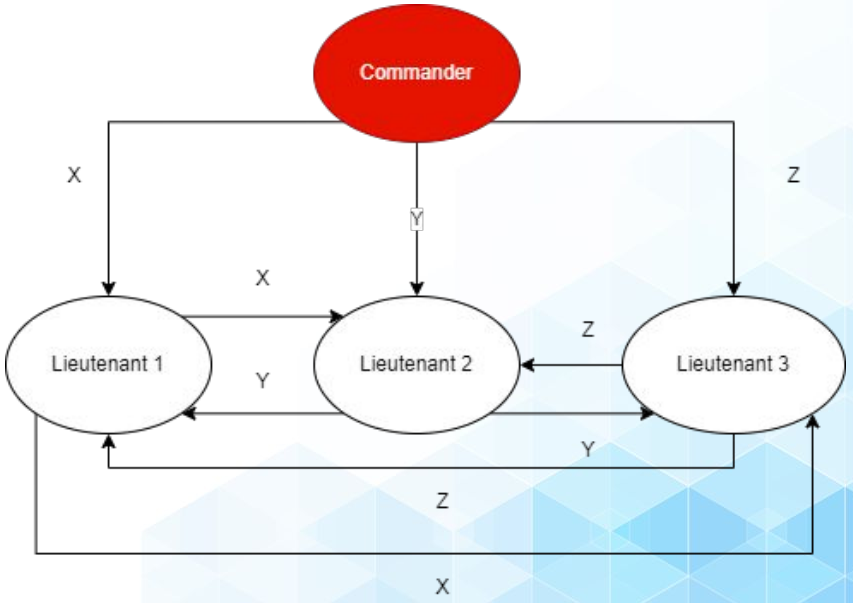
- As the blockchain is a distributed system trying to achieve a consensus about the state of the blockchain, it is also faced with Byzantine Generals problem.
- This problem in blockchain defined by consensus systems can be written as a commander lieutenant problem where the commander and lieutenant need to reach an agreement in the presence of dishonest nodes among them.
- The goal is to find the minimum number of dishonest nodes that a system can tolerate and still reach consensus.
- In case of a commander and 3 lieutenants, the commander sends messages to all lieutenants, and they share the massages among themselves.
    - If one lieutenant is malicious, he can send wrong messages to other lieutenants. But consensus can be achieved with a majority as 2 out of the 3 votes sent to lieutenants are the same.



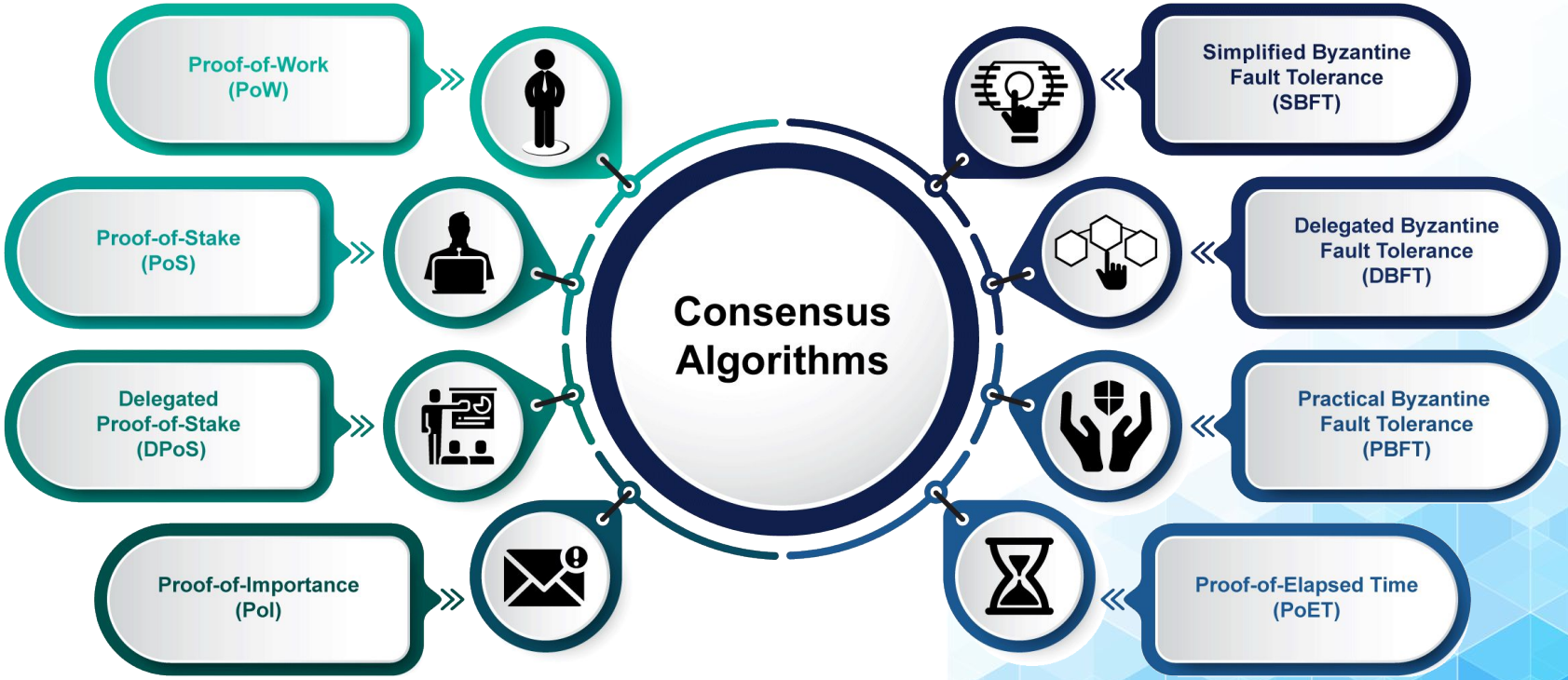
Byzantine General Problem in Blockchain

In the case of a malicious commander, the commander has sent three different commands to each lieutenant. When they share their information they find out that there is actually no majority with all different inputs. So each lieutenant chooses the consensus to retreat.

- Here the commander can be a node publishing the information, and lieutenants are network node participants. This shows that in order to reach a consensus, the network needs at least two-thirds or more reliable nodes.



Types of Consensus Algorithms



Blockchain Council

THANK YOU!

Any Questions?

Visit

community.blockchain-council.org

Mail Us

hello@blockchain-council.org