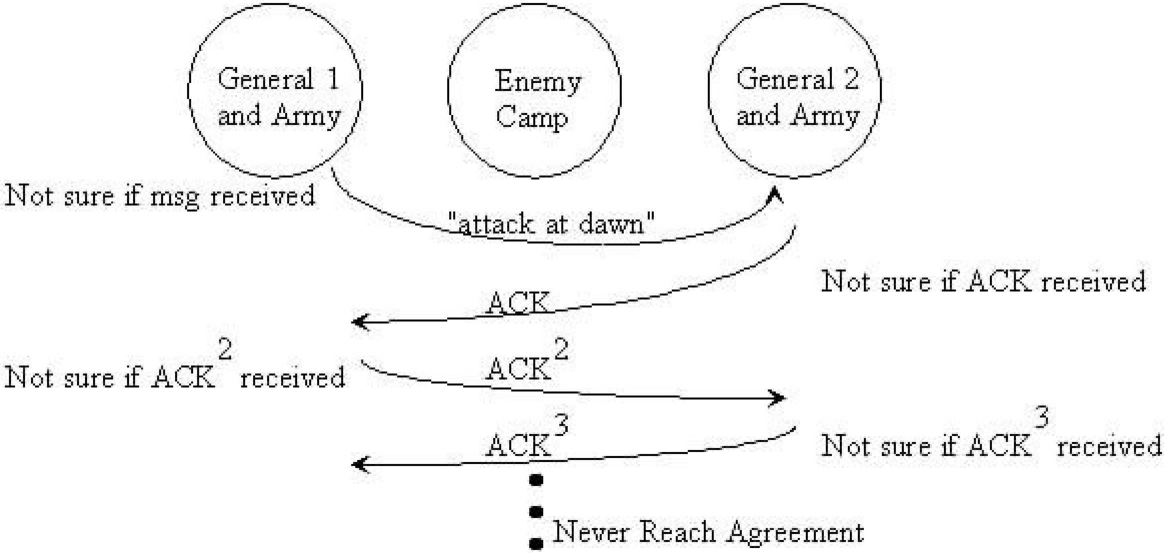
Consensus Mechanism

What is Consensus?

- Blockchains are decentralized systems which consist of different participants who act depending on incentives they receive and the information that is available to them.
- When a new transaction gets broadcasted on the network, nodes connected to the network have the option to either include that transaction to their copy of ledger or to ignore it. When the majority of the nodes which comprise the network decide on a single state, the **consensus** is achieved.

Let’s dive into 2 Generals Problem and understand the consensus better.

Two Generals Problem

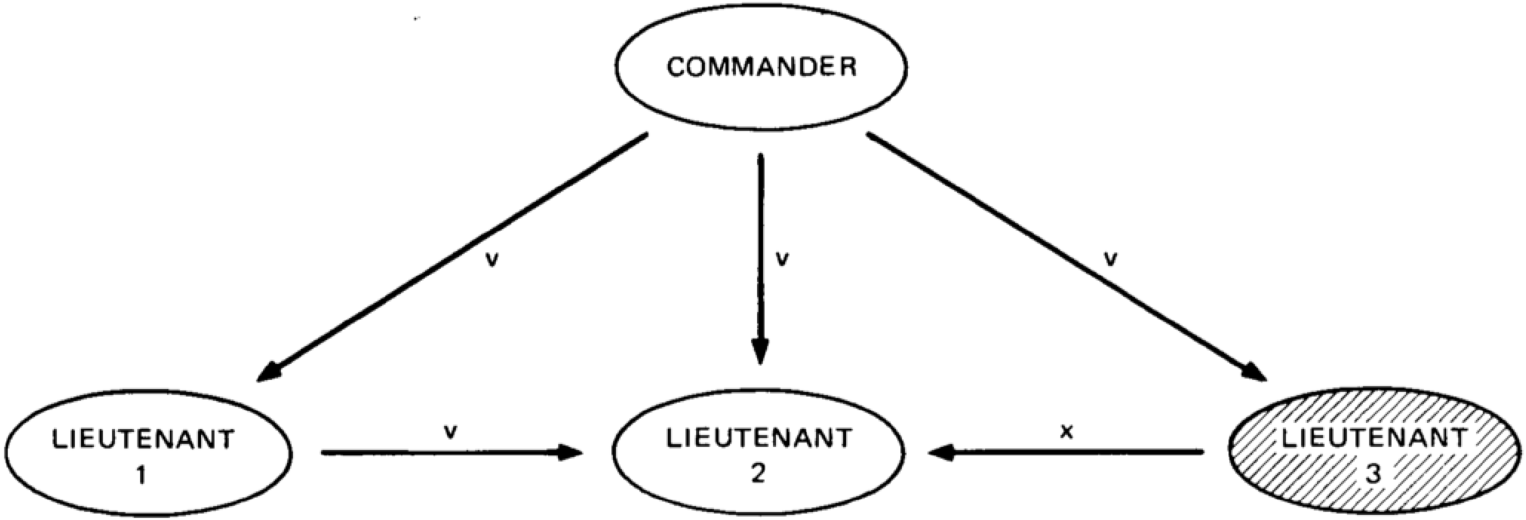


Source: https://medium.com/loom-network/understanding-blockchain-fundamentals-part-1-byzantine-fault-tolerance-245f46fe8419

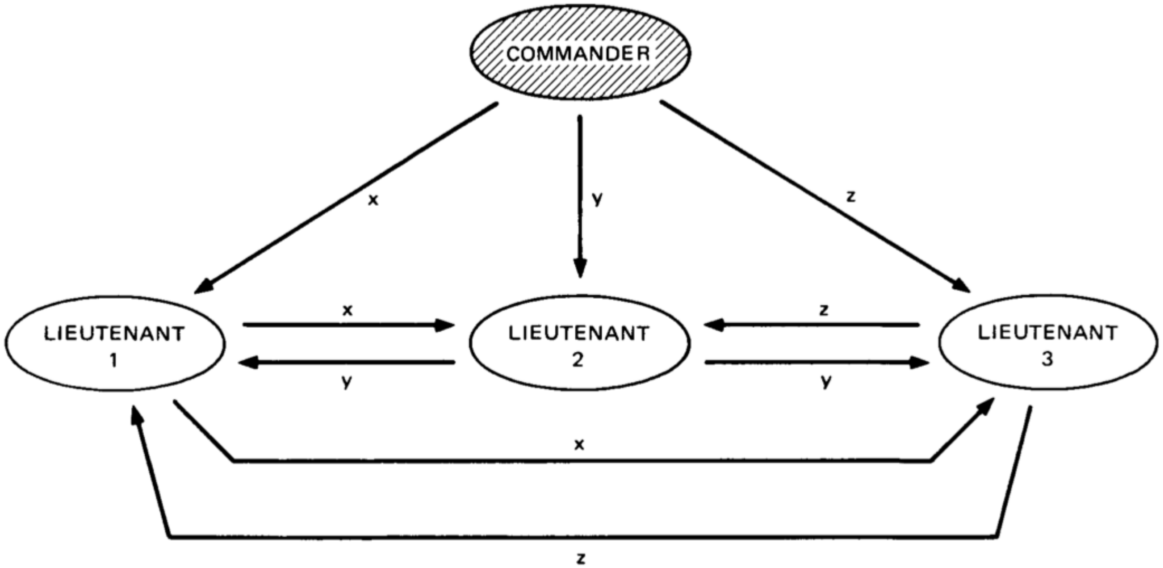
Byzantine Generals Problem

- A more generalized version of the Two Generals Problem describes a group of generals agreeing on the time of the attack. Apart from that, one or more generals can be the traitors, meaning that they can lie about their attack choice (e.g., they say that they agree to attack at 9 am, but instead they do not attack).
- To reach a consensus here, all the generals must agree on the same decision.
- Let’s change the scenario to a Commanding General who issues the attack and all others as who will follow the same to attack.
- If the Commanding General is a traitor, the consensus is still achieved. As a result, all lieutenants take the majority vote over the Default value.
- This implies that the algorithm can reach a consensus as long as 2/3 of the actors are honest. If the traitors are more than 1/3, the consensus is not reached, the armies do not coordinate their attack, and the enemy wins.

Lieutenant is the Traitor



Commander is the Traitor



Solution

- Take an example; every Lieutenant take 10 mins to convey orders. In other words, 10 minutes are required for communicating a message for an attack.
- Moreover, the passing of messages is in a way where each message is appended to the last message before sending it to the next Lieutenant.
- Example:
  - General - Attack at 9 am
  - Lieutenant 1 - Attack at 9 am, Attack at 9 am
  - Lieutenant 2 - Attack at 9 am, Attack at 9 am, Attack at 4 am
- If the Lieutenant 2 is a traitor, then the 3rd Lieutenant can verify that the incoming message is not in synchronization.
- Moreover, if Lieutenant 2 decides to change all the previous messages too, then each message would take 10 minutes thus Lieutenant 2 will be working for 30 mins.
- But Lieutenant 3 expects the message to come in 10 minutes, thus again giving in that Lieutenant 2 is a traitor.
- If the commander is a traitor, then he might send different orders to different Lieutenants, which will come into consensus but since the messages don’t follow the structure of providing in the same attack time, the default option of retreat will come to action.

How does it relate to Blockchain?

- This is solution which is described with Proof of Work for Bitcoin Blockchain.
- Each block has to follow the formulation guidelines of 10 mins in Bitcoin.
- Each block is appended to the last one by incorporating the Block hash.
- Consensus is achieved once ⅔ of the actors agree on a block.
- Verification of the Blocks is done by the miners.

Thank You