Professional Blockchain Course

Consensus Mechanisms

What is Consensus?

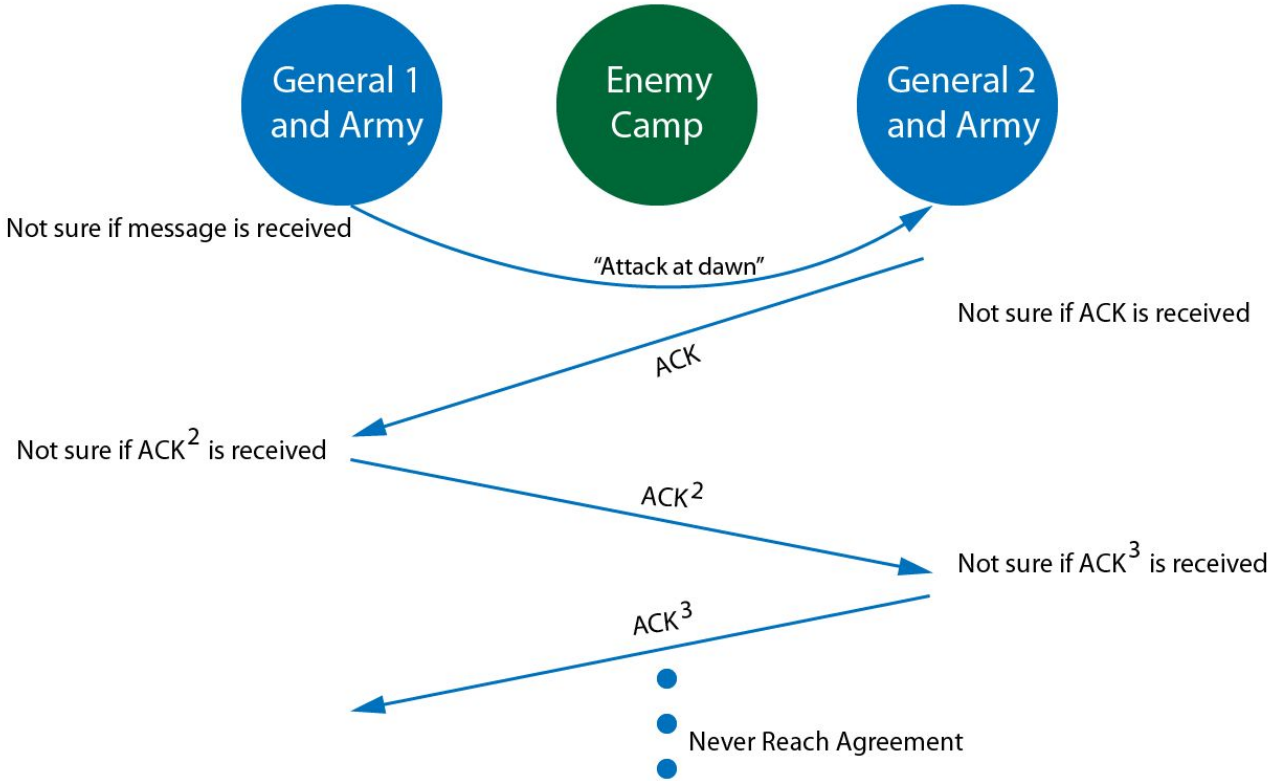
- Blockchains are decentralized systems which consist of different participants who act depending on incentives they receive and the information that is available to them.
- When a new transaction gets broadcasted on the network, nodes connected to the network have the option to either include that transaction 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

- This problem describes a scheme where two generals are attacking a prevalent enemy. General 1 is considered the leader and the other general is regarded as the follower.
- Each general's army on its own does not have the strength to defeat the enemy army; thus they need to collaborate and attack at the same time.
- For them to collaborate and agree on a time, General 1 needs to send a messenger across the enemy's territory that will provide the time of the attack to the other General. However, there is a probability that the messenger will get captured by the enemies, and thus the message won't be delivered. This will result in General 1 attacking while General 2 and his army hold their ground.
- Even if the first transmission goes through, General 2 has to acknowledge that he has received the news, so he sends a messenger back, thus repeating the previous scenario where the messenger can get caught. This extends to infinite message exchange, and therefore, the generals are unable to reach an agreement.

Two Generals Problem



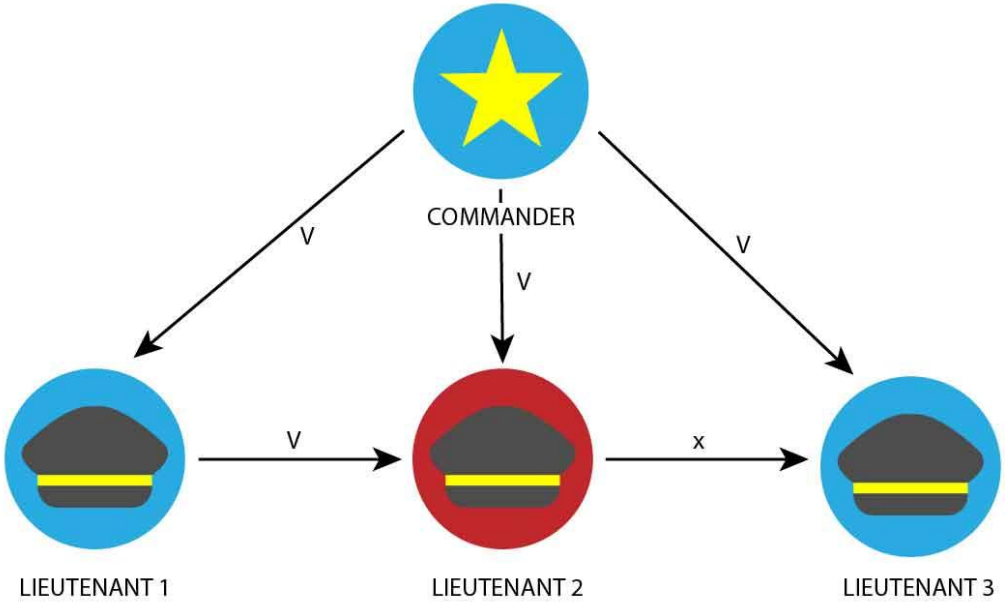
Byzantine Generals Problem

- A more generalized version of the Two Generals Problem describes more than two generals agreeing on the time of the attack. Additionally, 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 5 am, but instead they do not attack).
- To reach a consensus here, the commander and all the lieutenants must agree on the same decision.
- Let's change the scenario to a Commanding General and Lieutenants based approach. So when General issues an order, every loyal Lieutenant will follow the same to attack.
- If the commander 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.

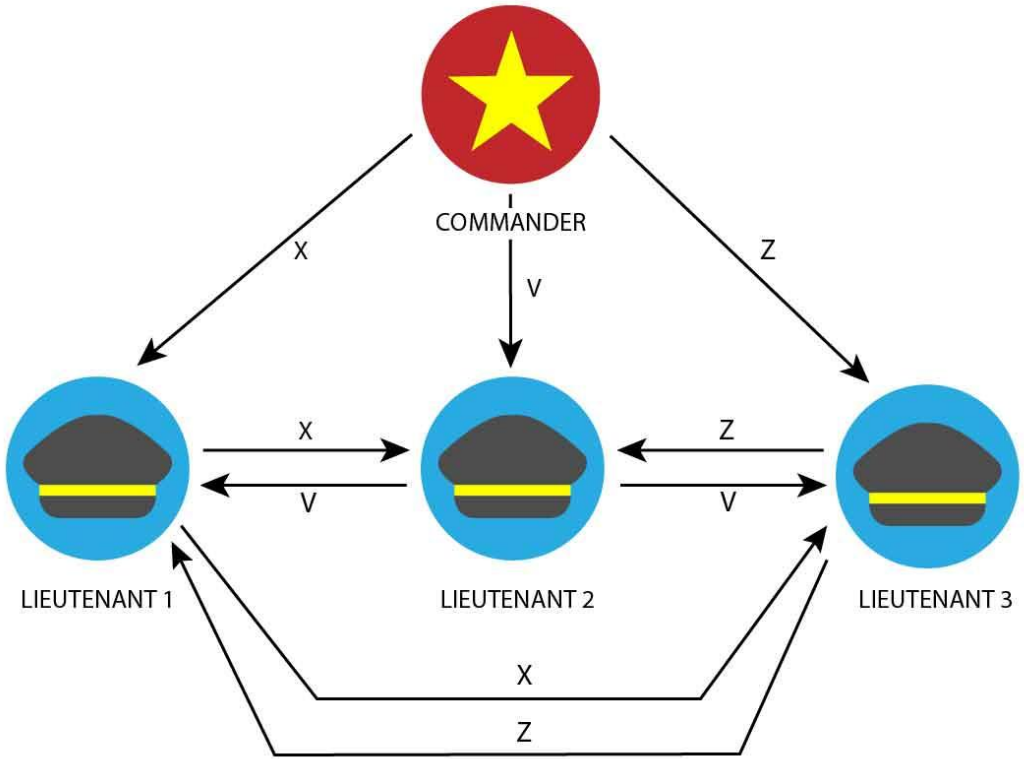
Explanation with Example

- Take an example; every Lieutenant needs to convey orders within 10 minutes. In other words, 10 minutes are required for communicating a message for an attack.
- Moreover, the passing of messages is related to appending the message and then sending them to the next Lieutenant.
- Example:
- General - Attack at 3 am
- Lieutenant 1 - Attack at 3 am, Attack at 3 am
- Lieutenant 2 - Attack at 3 am, Attack at 3 am, Attack at 5 am
- As you can see 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.

When Lieutenant is a Traitor



When Commander is a Traitor



How does it relate to Blockchain?

- Blockchains are decentralized ledgers which are not controlled by a central authority. Due to the value stored in these ledgers, bad actors have substantial economic incentives to try and cause faults.
- Proof-of-Work is a probabilistic solution to the Byzantine Generals Problem as described in depth by Satoshi Nakamoto.
- It follows the longest chain rule where miners shift to the chain which is being more worked upon.
- When a miner solves the puzzle and confirms the block, all the nodes in the network will verify if the block is valid and add it to their copy of the chain. The nodes first need to reach a consensus on the validity, only then the network will synchronize, and the state of the blockchain will update.

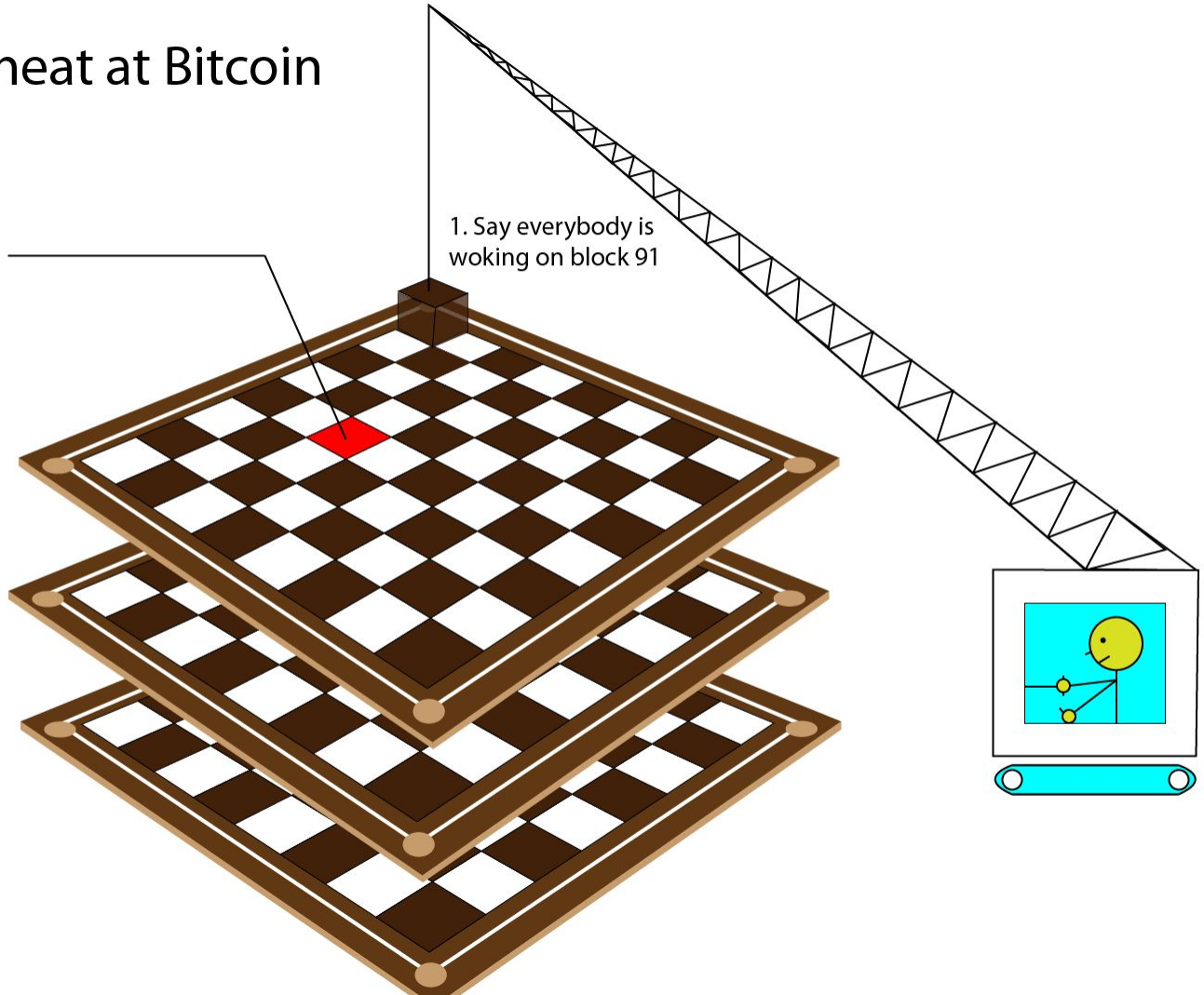
Why you can't cheat at Bitcoin

1. Say everybody is woking on block 91

2. But one miner wants to alter a transaction in block 74

3. He'd have to make his changes and redo all the computations for blocks 74-90 and do block 91. That's 18 blocks of expensive computing

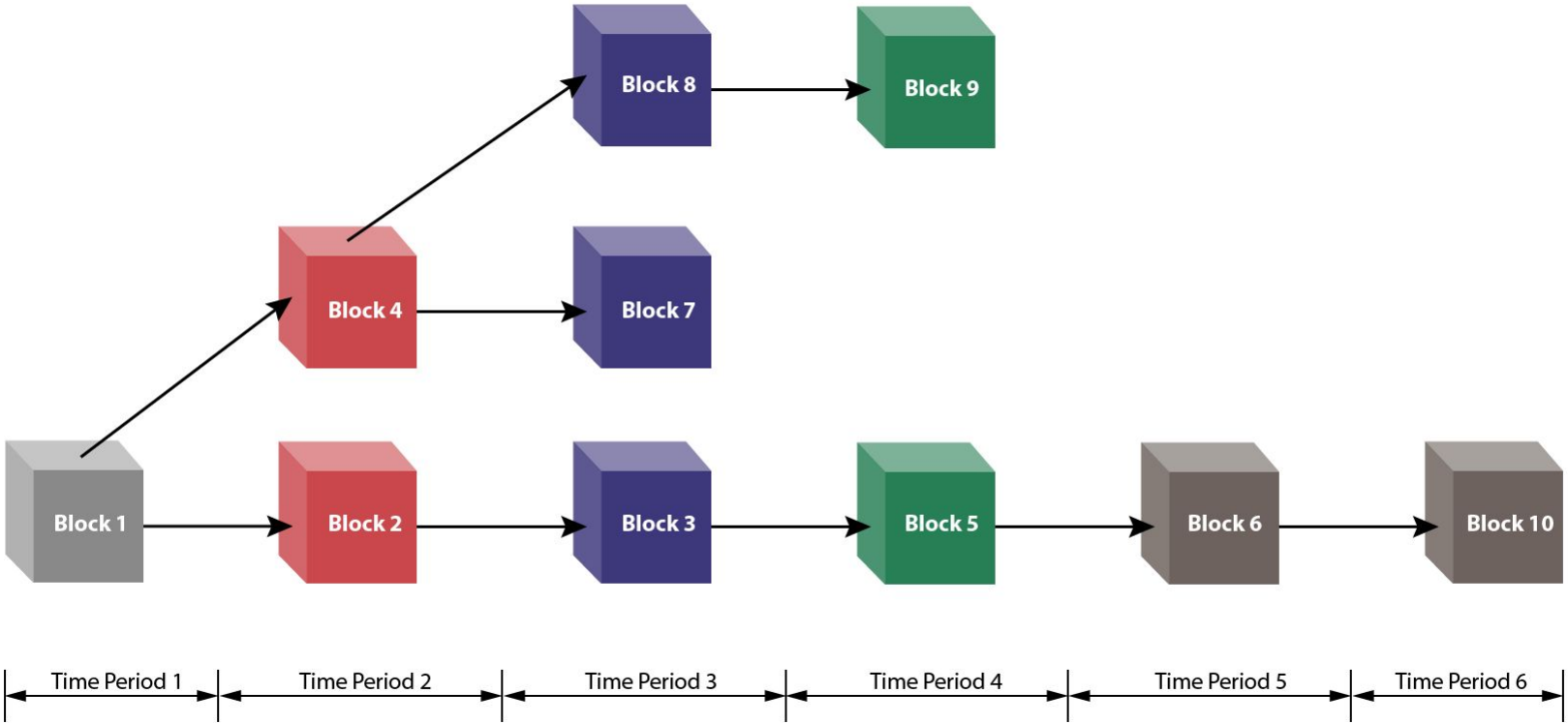
4. What's worse, he'd have to do it all before everybody else in the Bitcoin network finished just the one block (number 91) that they're working on



Conflict Example in Mining

- Multiple miners work on mining the Blocks.
- Suppose two miners can confirm a block within a fraction of seconds
- Other miners start working in for the next blocks.
- Bitcoin and Ethereum identify the longest chain based on total work is done/difficulty.
- Node prefers the first-seen valid chain with the most work measured in terms equivalent to the sum of the difficulty of all the blocks.

Conflict Example in Mining



Longest Chain Rule

- In Public Blockchains like Bitcoin, conflicts are being resolved by the longest chain rule.
- Let’s say a miner received the first Block 4 then he will start building the next Block on top of that Block 4.
- Now, in a few seconds that miners see another Block 2, so that miner will keep an eye on that new Block.
- If the next Block 3 is being detected from other nodes in Blockchain then that miner will disregard the 4 and will accept the new longest chain which is 1-> 3-> 5 and so on.
- Conventional wisdom states that it is therefore wise to wait for six blocks to confirm a transaction.

THANK YOU

For more information contact
info@we2blocks.com