Block Chain Technology (Byzantine Generals problem)

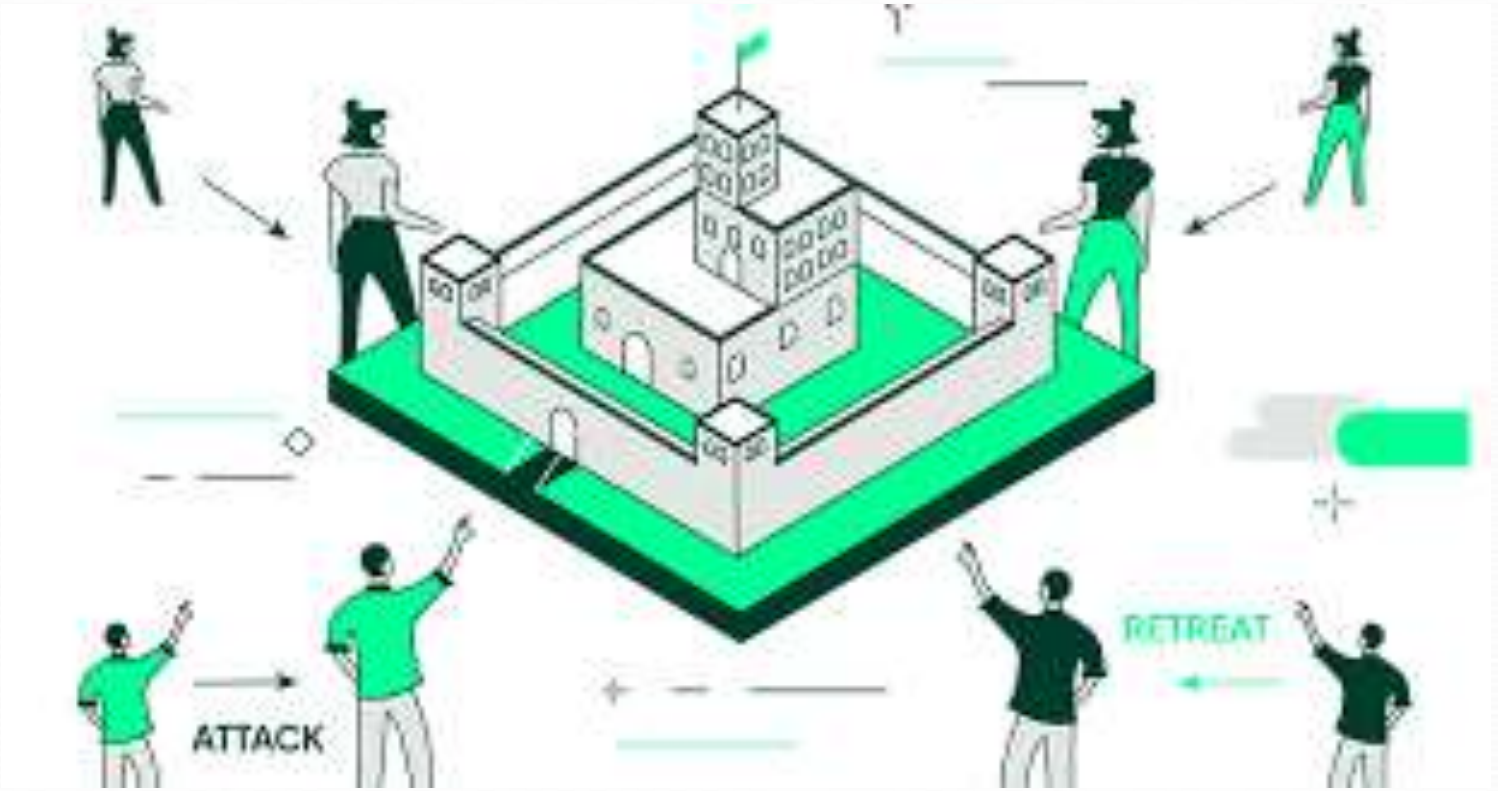
Dr. Siddhartha Roy

Byzantine Generals problem

- The Byzantine Generals' Problem is a classic problem in distributed computing that highlights the challenges of achieving consensus among a group of distributed and possibly faulty components. The problem is named after the hypothetical scenario it describes involving a group of Byzantine generals attempting to coordinate an attack on a common enemy. The generals must decide on a common plan of action, either to attack or retreat, and they need to reach a consensus for the operation to succeed.

- Scenario:
- A group of Byzantine generals surrounds an enemy city.
- Each general commands a portion of the army, and they need to agree on a common plan of action.
- Communication:

- The generals can communicate with each other only through messengers.
- Messengers may be unreliable, and their messages can be intercepted or altered by the enemy.



Source: https://www.bitstamp.net/learn/crypto-101/what-is-the-byzantine-generals-problem/

- Problem:

- Some generals may be traitors and provide conflicting orders to disrupt the decision-making process.
- The loyal generals must devise a strategy to reach consensus despite the potential presence of traitorous generals and unreliable communication.

- Objective:
- The goal is for the loyal generals to agree on a common plan of action (attack or retreat).
- The protocol must ensure that, if a general is loyal, the decision reached by the loyal generals is the decision of that general.
- The Byzantine Generals' Problem serves as a metaphor for the challenges in distributed systems where nodes (generals) need to reach an agreement in the presence of faulty or malicious components (traitorous generals). The problem becomes more complex as the number of generals and potential traitors increases.

- Solutions:
- Various solutions have been proposed to address the Byzantine Generals' Problem, including consensus algorithms that can tolerate Byzantine faults. Practical Byzantine Fault Tolerance (PBFT) is one such algorithm designed to achieve consensus in the presence of Byzantine faults. PBFT and other consensus mechanisms are employed in distributed systems like blockchain networks to ensure that all nodes can agree on the state of the system despite the possibility of some nodes behaving maliciously or experiencing faults.