**Week 1 Seminar Solutions**

1. What is Byzantine Generals’ Problem? Why the Byzantine Generals’ Problem could be your problem too?

Imagine divisions of a Byzantine army, attacking a completely encircled city. To proceed, the generals of each division, who are dispersed around the city’s periphery, must agree on a battle plan. However, while some generals want to attack, others may want to retreat.

In the official description of the Byzantine Generals’ Problem, there is a leader-follower set-up. In order to achieve consensus, the commanding general and every lieutenant must agree on the same decision.

The conditions are described as follows:

**Byzantine Generals Problem**. A commanding general must send an order to

his n - 1 lieutenant generals such that

IC1. All loyal lieutenants obey the same order.

IC2. If the commanding general is loyal, then every loyal lieutenant obeys the

order he sends.

Conditions IC1 and IC2 are called the *interactive consistency conditions*. Note

that if the commander is loyal, then IC1 follows from IC2. **However, the commander need not be loyal.**

To complicate matters, the generals are so far apart from each other that messengers are required in order for the generals to communicate. Also, one or more lieutenants may be a traitor, intending to sabotage the situation.

The Byzantine Generals’ Problem is the analogy most often used to illustrate the requirement for consensus for **distributed ledger technology (DLT)**.

The nodes in the distributed system must all agree on a certain set of rules and be able to move forward by agreeing on a particular assessment of a transaction before it is added to the database.

This is not easy, especially where thousands of nodes exist. In addition to that, each one must agree on the validity of new information to be added, thus preventing bad actors from sabotaging the ledger and rewriting history.

A specific type of consensus algorithm must be adopted to achieve this, enabling the nodes to work together to update the ledger securely.

2. What is Byzantine fault tolerance (BFT)?

Byzantine Fault Tolerance (BFT) is derived from Byzantine Generals’ Problem.

BFT is the feature of a distributed network to reach consensus (agreement on the same value) even when some of the nodes in the network fail to respond or respond with incorrect information. **The objective of a BFT mechanism is to safeguard against the system failures by employing collective decision making (both – correct and faulty nodes) which aims to reduce to influence of the faulty nodes.**

3. What is Centralised, Decentralised and Distributed networks?

**Centralised network:** In case of a centralised network, we have a central network owner. The central network owner is a single point of contact for information sharing. The biggest issue with a centralised network is with a single central owner it also becomes a single point of failure. Further, with a single copy stored with the owner, every instance of access to the resource leads to an access issue with time.

**Decentralised network:** As for the decentralised network, the we have multiple central owners that have the copy of the resources. This eliminates the biggest problem of single point of failure with centralised network. With multiple owners, if a particular central node fails, the information can still be accessed from the other nodes. Further, with multiple owners the speed of access to the information is also reduced.

**Distributed network:** The distributed network is the decentralised network taken to the extreme. It avoids the centralization completely. The main idea for the distributed network lies in the concept that everyone gets access, and everyone gets equal access.

4. Discuss the pros and cons of Centralised, Decentralised and Distributed systems.

**Points of Failure / Maintenance:** Centralised systems are easy to maintain as there is only a single point of failure. Decentralised have more but still finite. Distributed systems are the most difficult to maintain.

**Fault Tolerance / Stability:** Centralised can be highly unstable. Kill the leader and there will be chaos. Kill the leader for a decentralised system and you will have many decentralised systems. Distributed systems are very stable, and a single failure doesn’t do much harm.

**Scalability / Max Population:** Centralised — low scalability, decentralised — Moderate, Distributed — Infinite.

**Ease of development / Creation:** Centralised systems can be created really fast, you pick up a framework and apply it everywhere. For Decentralised and Distributed, you have to first work out the lower level details like resource sharing (trade) and communications (transport).

**Evolution / Diversity:** Since centralised systems follow a single framework, they don’t have diversity and evolve slowly. But for Decentralised and Distributed systems, once the basic infrastructure is in place, evolution is tremendous.

5. Is Bitcoin a permissioned or permissionless blockchain? How about Ripple? (XRP).

Bitcoin is a permissionless blockchain. Ripple is one of the largest cryptocurrencies, supports permission-based roles for participants. The Ripple network is something in between a public and private blockchain; a permissioned-on-permissionless blockchain, which is a permissible blockchain.

6. What is a 51% Attack? Any Real-World Examples?

A 51% attack refers to an attack on a blockchain—most commonly bitcoins, for which such an attack is still hypothetical—by a group of miners controlling more than 50% of the network's mining hash rate or computing power.

The attackers would be able to prevent new transactions from gaining confirmations, allowing them to halt payments between some or all users. They would also be able to reverse transactions that were completed while they were in control of the network, meaning they could double-spend coins.

They would almost certainly not be able to create new coins or alter old blocks. A 51% attack would probably not destroy bitcoin or another blockchain-based currency outright, even if it proved highly damaging.

Krypton and Shift, two blockchains based on Ethereum, suffered 51% attacks in August 2016.

In May of 2018, Bitcoin Gold, at the time the 26th-largest cryptocurrency, suffered a 51% attack. The malicious actor or actors controlled a vast amount of Bitcoin Gold's hash power, such that even with Bitcoin Gold repeatedly attempting to raise the exchange thresholds, the attackers were able to double-spend for several days, eventually stealing more than $18 million worth of Bitcoin Gold.

See more detail on:

<https://www.crypto51.app/>