Kabeer Ahmed SE-19028

Byzantine Generals Problem

The Byzantine Generals Problem is a game theory issue that highlights how difficult it is for dispersed parties to reach consensus without the aid of a reliable central authority. How can members of a network agree on a certain truth when no member has access to other members' identities?

The Byzantine Generals analogue in game theory the issue is that Byzantium is under siege by multiple generals. They have encircled the city, but they must determine when to launch an assault as a group. They will succeed if every general launches an attack at once, but they will fail if each general launches an attack independently. The generals are unable to communicate securely with one another since Byzantium's defenders might intercept or deceptively broadcast any signals they send or receive. How do the generals coordinate simultaneous attacks?

A good illustration of the Byzantine Generals Problem is money. How can a community create a kind of payment that all members can rely on and accept? For a significant portion of history, cultures have chosen to use uncommon items like shells or glass beads or precious metals as currency. The Byzantine Generals Problem was partially resolved by gold since it was respected and acknowledged in decentralized systems like international trade. Its weight and purity, however, continued to be suspect, and they still are. Gold's partial inability to resolve the Byzantine Generals Problem led to the formation and issue of money being taken over by dependable central actors, typically governments. Governments monopolized mints to promote confidence in the value and purity of currency. The Byzantine Generals Problem was plainly not resolved by centralized systems. Governments, the supposedly reliable central authorities for money, routinely betrayed that confidence by stealing, devaluing, or altering the currency.

How Bitcoin Solves the Byzantine Generals Problem

Bitcoin was the first realized solution to the Byzantine Generals Problem with respect to money. Many proposals and projects preceding Bitcoin had attempted to create money separate from the government, but all had failed in one way or another.

Blockchain Solves the Double Spend Problem

As a monetary system, Bitcoin needed a way to manage ownership and prevent double spends. To achieve this in a trustless manner, Bitcoin uses a blockchain, a public, distributed ledger which stores a history of all transactions. In the Byzantine Generals analogy, the truth that all parties must agree to is the blockchain.

If all members of the Bitcoin network, called nodes, could agree on which transactions occurred and in what order, they could verify ownership of bitcoin and establish a functioning, trustless money without a centralized authority

Proof-of-Work Solves the Byzantine Generals Problem

By employing a Proof-of-Work method to provide a clear, objective set of rules for the blockchain, Bitcoin was able to resolve the Byzantine Generals Problem. A network participant who wants to contribute data—known as blocks—to the blockchain must disclose evidence that they put a lot of effort into making the block. The developer of this work incurs high expenditures as a result, which encourages them to disclose accurate information.

There can be no dispute or tampering with the information on the Bitcoin network since the rules are impartial. The method for deciding who may create new bitcoins is also objective, as are the rulesets dictating which transactions are acceptable and which are invalid. The past of Bitcoin is unchangeable because it is very difficult to erase a block after it has been committed to the network.

Members of the Bitcoin network may therefore always agree on the blockchain's current status and all of its transactions. Each node independently confirms the validity of blocks based on the Proof-of-Work requirement and transactions depending on additional criteria.

All nodes on the network will instantly identify false information as objectively invalid and ignore it if any member of the network tries to broadcast it. Bitcoin is a trustless system because each node can independently verify all data on the network, eliminating the need to rely on other users.

Proof-of-stake (PoS) and Delegated proof-of-stake (DPoS)

PoS is another blockchain consensus mechanism that seeks to address the Byzantine general’s problem. It was first deployed in 2012. PoS-based networks, unlike PoW-based networks, are not reliant on cryptocurrency mining. Instead, a technique called staking is performed.

Users (called validators) stake funds in this system. Validators who own more coins on a blockchain can validate more blocks and earn greater rewards. Users that attempt to validate incorrect transactions risk losing their staked cash.

In a PoW-based network, users may stake coins using standard home PCs as opposed to sophisticated equipment. Many PoS-based networks have developed defenses against double-spending assaults and other possible security flaws brought on by Byzantine failures. For instance, Ethereum 2.0 (Serenity) will employ the Casper PoS algorithm, which necessitates the consent of two-thirds of nodes in order to construct a block.

Developed for the first time in 2014, delegated proof-of-stake is a blockchain consensus method that functions similarly to proof-of-stake. Both call on people to risk their money. In DPoS-based networks, only a select group of users—referred to as delegates—can validate transactions and create blocks.

Generally speaking, every user of a blockchain can stake bitcoin to support a delegate candidate. Block rewards are often given out in proportion to the money staked by elected nodes to their voters during delegate elections.With DPoS, nodes can reach consensus much more quickly than they can with PoW or PoS. This implies that transactions can be processed much more quickly at scale. Due to the tradeoff, maintaining a high level of Byzantine fault tolerance using DPoS could become challenging in some circumstances.

It may be simpler for nodes to conspire against the interests of the majority because fewer nodes are responsible for maintaining the network's security. On the other side, DPoS-based networks attempt to prevent this situation by having delegate elections often to make sure that delegates are held responsible for their choices.