Name : Gihon Godwin Sillitonga

Casper the Friendly Finality Gadget

There are two major schools of thought in PoS design. The first, chain-based proof of stake, mimics proof of work mechanics and features a chain of blocks and simulates mining by pseudorandomly assigning the right to create new blocks to stakeholders. The other school, Byzantine fault tolerant (BFT) based proof of stake, is based on a thirty-year-old body of research into BFT consensus algorithms such as PBFT.

There is some The Casper Protocol :

- Proving Safety and Plausible Livenes
  We prove Casper's two fundamental properties: accountable safety and plausible liveness. Accountable safety means that two conflicting checkpoints cannot both be finalized unless ≥ 1\3 of validators violate a slashing condition (meaning at least one third of the total deposit is lost). Plausible liveness means that, regardless of any previous events (e.g., slashing events, delayed blocks, censorship attacks, etc.), if ≥ 2\3 of validators follow the protocol, then it's always possible to finalize a new checkpoint without any validator violating a slashing condition
- Casper's Fork Choice Rule
  There are pathological scenarios where Casper gets "stuck" and any blocks built atop the longest chain cannot be finalized (or even justified) without some validators altruistically sacrificing their deposit. To avoid this, we introduce a novel, correct by construction, fork choice rule.

There are two well-known attacks against proof-of-stake systems:

- Long Range Revisions
  In simple terms, long-range attacks are prevented by a fork choice rule to never revert a finalized block, as well as an expectation that each client will "log on" and gain a complete up-to-date view of the chain at some regular frequency (e.g., once per 1–2 months).
- Castastrophic Crashes
  The exact algorithm for recovering from these various attacks remains an open problem. For now, we assume validators can detect obviously malfeasant behavior (e.g., not including evidence) and manually create a "minority soft fork". This minority fork can be viewed as a blockchain in its own right that competes with the majority chain in the market, and if the majority chain truly is operated by colluding malicious attackers then we can assume that the market will favor the minority fork.

The exact algorithm for recovering from these various attacks remains an open problem. For now, we assume validators can detect obviously malfeasant behavior (e.g., not including evidence) and manually create a "minority soft fork". This minority fork can be viewed as a

blockchain in its own right that competes with the majority chain in the market, and if the majority chain truly is operated by colluding malicious attackers then we can assume that the market will favor the minority fork.