Nama : Muh Nardika

NIM : 1103184124

Kelas : TK-42-PIL

**SUMMARY**
**CASPER POS PAPERS**

**Casper Protocol**

In casper's simplified version, there is a set of validators and proposal mechanisms that still generate child blocks from blocks existing to form a block that continues to grow. Under normal circumstances, it is expected the proposal mechanism will propose the blocks one by one in the linked list. But in cases of network latency or intentional attacks, the proposal mechanism will sometimes produce multiple children from the same parent.

Casper's task is to choose one child from each parent, thus selecting a canonical chain from the beam tree. Casper considers only the subtrees of the checkpoints forming a post tree inspection. The genesis block is a checkpoint, and any block that is high in the tree block (or block number) is an exact multiple of 100 is also a checkpoint. The "checkpoint height" of a block with a block height of 100 * k is simply k; equivalent, the height h(c) of the checkpoint c is the number of elements in the checkpoint chain that extends from c (non-inclusive) to the root along the parent link.

And the validator can broadcast a voice message containing four pieces of information, two checkpoints s and t together with their heights h(s) and h(t). We require s to be grandma t ancestors in the checkpoint tree, otherwise the vote is considered invalid. If the validator's public key is not in the validator set, the vote is considered invalid. Together with the signature of the validator.

**Casper**

Casper is a partial consensus mechanism that incorporates proof of stake algorithm research and Byzantine fault tolerant consensus theory. In a PoS system, blockchain adds and approves new blocks through a process in which anyone who holding coins in the system can participate, and the influence the agent has proportional to the number of coins it has. This is a much more efficient alternative for proof of work (PoW) mining and enabling blockchain to operate without the high cost of mining hardware and electricity

**Casper Fork Rules**

Casper is more complicated than standard PoW designs. Thus, the choice of fork must be customized. Modified fork selection rules should be followed by all users, validators, and even the underlying block proposal mechanism. If the user, validator, or the block proposer instead follows the standard PoW fork choice rule "always builds on over the longest chain", there is a pathological scenario where Casper is "stuck" and blocks anything which is built on the longest chain cannot be completed (or even justified) without some validators altruistically sacrificing their deposits.

**Attacks on POS System .**

***Long Range Revisions,*** After the validator coalition withdrew their deposits, if the coalition had more than 23 from the old stash in the past, they can use their historical majority to complete checkpoints that contradict each other without fear of being slashed (because the money has already been withdrawn). Here called Long Range Revisions. In simple terms, ranged attacks is much prevented by the fork selection rule to never return a block that have been completed, as well as the expectation that each client will "log in" and get the latest complete view of the chain on multiple regular frequencies

***The Exact Algorithm,*** for recovering from these attacks remains open problem. For now, we assume the validator can detect behavior that is clearly inappropriate (e.g., lacks evidence) and manually create a "minority soft fork". This minority fork can seen as a blockchain in its own right that competes with chains majority in the market,

.