title: Gasper description: An explanation of the Gasper proof-of-stake mechanism. lang: en

Gasper is a combination of Casper the Friendly Finality Gadget (Casper-FFG) and the LMD-GHOST fork choice algorithm. Together these components form the consensus mechanism securing proof-of-stake Ethereum. Casper is the mechanism that upgrades certain blocks to "finalized" so that new entrants into the network can be confident that they are syncing the canonical chain. The fork choice algorithm uses accumulated votes to ensure that nodes can easily select the correct one when forks arise in the blockchain.

Note that the original definition of Casper-FFG was updated slightly for inclusion in Gasper. On this page we consider the updated version.

Prerequisites

To understand this material it is necessary to read the introductory page onproof-of-stake.

The role of Gasper {#role-of-gasper}

Gasper sits on top of a proof-of-stake blockchain where nodes provide ether as a security deposit that can be destroyed if they are lazy or dishonest in proposing or validating blocks. Gasper is the mechanism defining how validators get rewarded and punished, decide which blocks to accept and reject, and which fork of the blockchain to build on.

What is finality? {#what-is-finality}

Finality is a property of certain blocks that means they cannot be reverted unless there has been a critical consensus failure and an attacker has destroyed at least 1/3 of the total staked ether. Finalized blocks can be thought of as information the blockchain is certain about. A block must pass through a two-step upgrade procedure for a block to be finalized:

1. Two-thirds of the total staked ether must have voted in favor of that block's inclusion in the canonical chain. This condition upgrades the block to "justified". Justified blocks are unlikely to be reverted, but they can be under certain conditions.
2. When another block is justified on top of a justified block, it is upgraded to "finalized". Finalizing a block is a commitment to include the block in the canonical chain. It cannot be reverted unless an attacker destroys millions of ether (billions of $USD).

These block upgrades do not happen in every slot. Instead, only epoch-boundary blocks can be justified and finalized. These blocks are known as "checkpoints". Upgrading considers pairs of checkpoints. A "supermajority link" must exist between two successive checkpoints (i.e. two-thirds of the total staked ether voting that checkpoint B is the correct descendant of checkpoint A) to upgrade the less recent checkpoint to finalized and the more recent block to justified.

Because finality requires a two-thirds agreement that a block is canonical, an attacker cannot possibly create an alternative finalized chain without:

1. Owning or manipulating two-thirds of the total staked ether.
2. Destroying at least one-third of the total staked ether.

The first condition arises because two-thirds of the staked ether is required to finalize a chain. The second condition arises because if two-thirds of the total stake has voted in favor of both forks, then one-third must have voted on both. Double-voting is a slashing condition that would be maximally punished, and one-third of the total stake would be destroyed. As of May 2022, this requires an attacker to burn around $10 billion worth of ether. The algorithm that justifies and finalizes blocks in Gasper is a slightly modified form of Casper the Friendly Finality Gadget (Casper-FFG).

Incentives and Slashing {#incentives-and-slashing}

Validators get rewarded for honestly proposing and validating blocks. Ether is rewarded and added to their stake. On the other hand, validators that are absent and fail to act when called upon miss out on these rewards and sometimes lose a small portion of their existing stake. However, the penalties for being offline are small and, in most cases, amount to opportunity costs of missing rewards. However, some validator actions are very difficult to do accidentally and signify some malicious intent, such as proposing multiple blocks for the same slot, attesting to multiple blocks for the same slot, or contradicting previous checkpoint votes. These are "slashable" behaviors that are penalized more harshly—slashing results in some portion of the validator's stake being destroyed and the validator being removed from the network of validators. This process takes 36 days. On Day 1, there is an initial penalty of up to 1 ETH. Then the slashed validator's ether slowly drains away across the exit period, but on Day 18, they receive a "correlation penalty", which is larger when more validators are slashed around the same time. The maximum penalty is the entire stake. These rewards and penalties are designed to incentivize honest validators and disincentivize attacks on the network.

Inactivity Leak {#inactivity-leak}

As well as security, Gasper also provides "plausible liveness". This is the condition that as long as two-thirds of the total staked ether is voting honestly and following the protocol, the chain will be able to finalize irrespective of any other activity (such as attacks, latency issues, or slashings). Put another way, one-third of the total staked ether must be somehow compromised to prevent the chain from finalizing. In Gasper, there is an additional line of defense against a liveness failure, known as the "inactivity leak". This mechanism activates when the chain has failed to finalize for more than four epochs. The validators that are not actively attesting to the majority chain have their stake gradually drained away until the majority regains two-thirds of the total stake, ensuring that liveness failures are only temporary.

Fork choice {#fork-choice}

The original definition of Casper-FFG included a fork choice algorithm that imposed the rule:`follow the chain containing the justified checkpoint that has the greatest height` where height is defined as the greatest distance from the genesis block. In Gasper, the original fork choice rule is deprecated in favor of a more sophisticated algorithm called LMD-GHOST. It is important to realize that under normal conditions, a fork choice rule is unnecessary - there is a single block proposer for every slot, and honest validators attest to it. It is only in cases of large network asynchronicity or when a dishonest block proposer has equivocated that a fork choice algorithm is required. However, when those cases do arise, the fork choice algorithm is a critical defense that secures the correct chain.

LMD-GHOST stands for "latest message-driven greedy heaviest observed sub-tree". This is a jargon-heavy way to define an algorithm that selects the fork with the greatest accumulated weight of attestations as the canonical one (greedy heaviest subtree) and that if multiple messages are received from a validator, only the latest one is considered (latest-message driven). Before adding the heaviest block to its canonical chain, every validator assesses each block using this rule.

Further Reading {#further-reading}

- Gasper: Combining GHOST and Casper
- Casper the Friendly Finality Gadget