Casper Slashing Conditions

Christian Reitwießner
chris@ethereum.org

0.1 Basic Definitions

Let $\mathcal{V}$ be the (finite) set of *validators*. We assume it to be fixed for now. Let $\mathcal{H}$ be the (finite) set of *hash values*, usually the set of bitstrings of 256 bits. Finally, $\mathbb{N} := \{0, 1, \dots\}$ is the set of natural numbers.

Since hashes in $\mathcal{H}$ correspond to blocks in a blockchain, we assume every hash has a *parent* $\operatorname{parent}(H)$.

Valid Messages

Every validator can broadcast messages, which can be either *prepare* messages from the set

$$\mathcal{P} := \{(v, H, n, n_0) \mid v \in \mathcal{V}, H \in \mathcal{H}, n, n_0 \in \mathbb{N}, n > n_0\}$$

or *commit* messages

$$\mathcal{C} := \{(v, H, n) \mid v \in \mathcal{V}, H \in \mathcal{H}, n \in \mathbb{N}, n > 0\}.$$

Signatures ensure that only the validator v can send messages (v, H, n, n_0) and (v, H, n).

Slashing Conditions

Let $\mathcal{M} \subseteq \mathcal{P} \cup \mathcal{C}$ be the set of messages visible to the Casper contract at a certain point in time. Depending on this set, the contract will slash the deposit of validators. To ease notation, let us define some notions:

The *prepare ratio* of a hash $H \in \mathcal{H}$ at a view $n \in \mathbb{N}$ depending on the view $n_0 \in \mathbb{N}$ is

$$\operatorname{prepratio}_{\mathcal{M}}(H, n, n_0) = \frac{\#\{v \in \mathcal{V} \mid (v, H, n, n_0) \in \mathcal{M}\}}{\#\mathcal{V}}$$

and the prepare ration of H at the view n is

$$\operatorname{prepratio}_{\mathcal{M}}(H, n) = \max_{n_0 \in \mathbb{N}} \operatorname{prepratio}_{\mathcal{M}}(H, n, n_0)$$

Note: If the validator set can change, the above definitions will get more complicated.

The Casper contract slashes the deposit of a validator v_0 if any of the following conditions are met:

1. $(v_0, H, n) \in \mathcal{M}$ for some $H \in \mathcal{H}$, $n \in \mathbb{N}$, and $\text{prepratio}_{\mathcal{M}}(H, n) < \frac{2}{3}$.
   – A hash was commited that was not properly prepared.

2. $(v_0, H, n, n_0) \in \mathcal{M}$ for some $H \in \mathcal{H}$, $n \in \mathbb{N}$, $n_0 > 0$ and $\text{prepratio}_{\mathcal{M}}(\text{parent}^{n-n_0}(H), n_0) < \frac{2}{3}$.
   – A hash was prepared based on an ancestor that was not properly prepared.

3. $(v_0, H, n), (v_0, H', n', n_0') \in \mathcal{M}$ for some $H, H' \in \mathcal{H}$, $n, n', n_0' \in \mathbb{N}$ and $n_0' < n < n'$.
   – A hash was prepared ignoring an already committed hash.

4. $(v_0, H, n, n_0), (v_0, H', n, n_0') \in \mathcal{M}$ for some $H, H' \in \mathcal{H}$, $n, n_0, n_0' \in \mathbb{N}$ and $(H, n_0) \neq (H', n_0')$.
   – Two different prepare messages were sent for the same view.

Note that both $\text{prepratio}_{\mathcal{M}}$ functions are monotonous in $\mathcal{M}$ and thus also the conditions are monotonous in $\mathcal{M}$.