Casper Slashing Conditions

Christian Reitwießner
chris@ethereum.org

Basic Definitions

Let $\mathcal{V}$ be the (finite) set of *validators*, where each $v \in \mathcal{V}$ has a positive deposit $\mathrm{w}(v)$ ("weight"). We assume neither those deposits nor the validator set itself to change. 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* $\mathrm{parent}(H)$.

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

$$\mathrm{prepratio}_{\mathcal{M}}(H, n, n_0) = \frac{\sum\{w(v) \mid (v, H, n, n_0) \in \mathcal{M}\}}{\sum_{v \in \mathcal{V}} \mathrm{w}(v)}$$

and the prepare ratio of H at the view n is

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

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.

Defined $\text{slashed}_{\mathcal{M}}(v_0)$ to be true if and only if at least one of these conditions are met for v_0.

Properties

Conjecture 0.1 (Accountable Safety)**.** *If $(v_1, X, n_1), (v_2, Y, n_2) \in \mathcal{M}$, $X \neq Y$ and there is no $k \in \mathbb{N}$ such that $X = \text{parent}^k(Y)$ or $Y = \text{parent}^k(X)$, then*

$$\sum\{\text{w}(v) \mid v \in \mathcal{V}, \text{slashed}_{\mathcal{M}}(v)\} \geq \frac{1}{3} \sum\{\text{w}(v) \mid v \in \mathcal{V}\}.$$

Conjecture 0.2 (Plausible Liveness)**.** *Let $\mathcal{M} \subseteq \mathcal{C} \cup \mathcal{P}$ be finite such that less than a third of the validators are slashed, i.e.*

$$\sum\{\text{w}(v) \mid v \in \mathcal{V}, \text{slashed}_{\mathcal{M}}(v)\} < \frac{1}{3} \sum\{\text{w}(v) \mid v \in \mathcal{V}\}.$$

Then there is a set of messages $\mathcal{M}' \supseteq \mathcal{M}$ and a hash $H \in \mathcal{H}$ such that

1. $(v, X, n) \in \mathcal{M}' \setminus \mathcal{M} \Rightarrow \neg\text{slashed}_{\mathcal{M}}(v)$ *(only contains new messages from unslashed validators)*
2. *there is no $(v, H, n) \in \mathcal{M}$ (H has not been commited previously)*
3. *there is some $(v, H, n) \in \mathcal{M}'$ (H is commited now)*
4. *for all $v \in \mathcal{V}$ if $\text{slashed}_{\mathcal{M}'}(v)$ then $\text{slashed}_{\mathcal{M}}(v)$ (no newly slashed validator)*