TLDR

: We present a single simplified Casper slashing condition to replace the two slashing conditions in the Casper FFG paper. The new slashing condition cannot be weakened, i.e. it is tight. It is also intuitive and makes the safety proof (even more) obvious.

Context

A year ago @vbuterin simplified the Casper slashing conditions, reducing the count from 4 to 2. Three months ago @dlubarov noticed the slashing conditions were not tight, i.e. that they could be weakened. Specifically, it was noticed that the second "no-surround" slashing condition can be specialised to finalisation votes, i.e. votes from a checkpoint to a direct child. It turns out the first "no-equivocation" slashing condition can also be weakened. By weakening both slashing conditions, a unified—and more natural—slashing condition emerges.

Construction

Notation:

Below s

and $\tilde{s}$

are sources, t

and $\tilde{t}$

are targets, and $h()$

is the height function.

Slashing condition:

A validator must not cast a vote (s, t)

that "hops over" one of his finalisation votes $(\tilde{s}, \tilde{t})$

, i.e. $h(s) \le h(\tilde{s})$

and $h(t) \ge h(\tilde{t})$

.

Visualisation:

It is natural to visualise votes as edges from source to target placed on a line according to their height. In that context a finalisation vote is a short edge of length 1, and vote hopping corresponds to edge hopping.

Safety proof:

Suppose two conflicting checkpoints finalise and consider their justification paths, each ending with a finalisation edge. One of the paths is no shorter (in height) than the other. Clearly, that path contains an edge that hops over the finalisation edge of the other path. This implies at least 1/3 of the validators cast a vote to hop over a finalisation vote.

Tightness:

The slashing condition is tight. Indeed, suppose it was possible to hop over one of your finalisation votes without getting slashed. If all validators vote, all vote the same way, and make a conflicting hop over one of their finalisation votes, then they can extend the conflicting hopping edge with a finalisation edge, thereby yielding two conflicting finalised checkpoints.