This post is opened for discussion re. the following fast confirmation rule for Ethereum proof-of-stake:

- Draft paper: confirmation-rule-draft.pdf (396.2 KB)
- Explainer blog post

This work was conducted together with Francesco D'Amato@fradamt, Roberto Saltini @saltiniroberto, Luca Zanolini @luca_zanolini, & Chenyi Zhang.

Confirmation Rule

Assumptions:

- From the current slot onwards, the votes cast by honest validators in a slot are received by all validators by the end of that slot, i.e., the network is synchronous with latency < 8 seconds

.

- This proposed change to the Ethereum protocol:
- If j

is the highest justified checkpoint block, and the current epoch is e

, then allow a branch with leaf block b

if the latest justified checkpoint in the post-state of b

is either j

, or from an epoch \ge e-2

- If j

is the highest justified checkpoint block, and the current epoch is e

, then allow a branch with leaf block b

if the latest justified checkpoint in the post-state of b

is either j

, or from an epoch \ge e-2

Notation:

- n

is the current slot, and e

is the current epoch.

- b

is a block from the current epoch e

.

- There are S

FFG votes from epoch e

in support of c

.

- W_f

is the weight of validators yet to vote in epoch e

, and W_t

is the total weight of all validators.

- The adversary controls \beta < \frac{1}{3}^{\textrm{rd}}

fraction of the validator set.

- The adversary is willing to bear a slashing of \alpha

(\leq \beta)

fraction of the validator set.

A short description of the rule (please seeconfirmation-rule-draft.pdf (396.2 KB) orblog post for explanation):

- p_{b}^n = \frac{\textrm{honest support for block } b}{\textrm{total honest weight}}

from validators in committees from b\textrm{.parent.slot} + 1

till n

.

- \textrm{isLMDConfirmed}(b, n)

is defined as p_{b'}^n > \frac{1}{2(1-\beta)}

for all b'

in the chain of b

.

- \textrm{isConfirmed}(b,n)

if: * the latest justified checkpoint in the post-state of b

is from epoch e-1

, and

- \textrm{isLMDConfirmed}(b,n)

, and

- [S - \textrm{min}(S, \alpha W_t, \beta (W_t - W_f))] + (1-\beta)W_f \ge \frac{2}{3}W_t

.

- the latest justified checkpoint in the post-state of b

is from epoch e-1

, and

- \textrm{isLMDConfirmed}(b,n)

, and

- [S - \textrm{min}(S, \alpha W_t, \beta (W_t - W_f))] + (1-\beta)W_f \ge \frac{2}{3}W_t

.

If \textrm{isConfirmed}(b,n)

, then b

is said to be confirmed

and will remain in the canonical chain.

Since p_b^n

cannot be observed, we define a practical safety indicator

q_b^n

to determine if p_b^n

is in the appropriate range:

- q_{b}^n = \frac{\textrm{support for block } b}{\textrm{total weight}}

from committees in slot b\textrm{.parent.slot} + 1

till slot n

- q_{b'}^n > \frac{1}{2} \left(1+\frac{\textrm{proposer boost weight}}{\textrm{total honest weight}}\right) + \beta

for all b'

in the chain of b

implies

\textrm{isLMDConfirmed}(b, n)

Performance

In ideal conditions, the rule would confirm a block immediately after the end of its slot.

Under typical mainnet conditions, we expect the rule to confirm most blocks within 3-4 slots (under 1 minute).

We observe the following values for q

(plot generated using this prototype):

[

q_plot

846×571 38.5 KB

](https://ethresear.ch/uploads/default/original/2X/1/133809368928eac36a12b930c866542202d23fc7.png)

The current slot is 6337565

, and the latest confirmed block is at slot 6337564

.

Previous Work

- Safe head with LMD – this post is an extension of the linked work.
- Safe block confirmation rule
- High confidence single block confirmations in Casper FFG