How to realize validator rotation in CBC Casper is an open question.

In this post, I present a modification of CBC Casper for validator rotation.

The more formal version of this proposal is[here](#).

Prerequisite

The latest CBC Casper paper with [the draft of Section7 by Nate Rush](#) (The compiled version is [here](#).)

I reuse definitions and lemmas in the original paper.

Overview

- Replace weight

in CBC parameters with weights

$\mathcal{W}$

, which is a set of all possible weight.

- Define a function to calculate a weight from a consensus value (block)

- E.g. Calculate a weight from the information (e.g. entry/exit transactions, slashing transactions, etc.) included in the chain until its parent block

- E.g. Calculate a weight from the information (e.g. entry/exit transactions, slashing transactions, etc.) included in the chain until its parent block

$\mathrm{Weight}: \mathcal{C} \rightarrow \mathcal{W}$

- Modify the fork choice rule (estimator

) to use Weight

so that the result is deterministic regardless of validator rotation. * E.g. Modify LMD GHOST to score a block b

by $\mathrm{Weight}(b)$

in the “best children selection”.

- This is originally proposed in the previous draft of[Casper TFG paper](#).

- E.g. Modify LMD GHOST to score a block b

by $\mathrm{Weight}(b)$

in the “best children selection”.

- This is originally proposed in the previous draft of[Casper TFG paper](#).

- Validators make a decision on a chain if all blocks in the chain are decided to win best children selection in GHOST at its height for any future states where there are t

equivocations or less by $\mathrm{Weight}(b)$

. * To detect this finality, we use clique oracle for the best children properties

. * Validators decide on a chain if there are cliques for any blocks in the chain.

- We weight a clique agreeing on a block b

by $\mathrm{Weight}(b)$

.

- Validators decide on a chain if there are cliques for any blocks in the chain.

- We weight a clique agreeing on a block b

by $\mathrm{Weight}(b)$

.

- To detect this finality, we use clique oracle for the best children properties

. * Validators decide on a chain if there are cliques for any blocks in the chain.

- We weight a clique agreeing on a block b

by $\mathrm{Weight}(b)$

.

- Validators decide on a chain if there are cliques for any blocks in the chain.

- We weight a clique agreeing on a block b

by $\mathrm{Weight}(b)$

.

- From these, the protocol has safety i.e. validators do not decide on conflicting blocks if there are t

equivocations or less by $\mathrm{Weight}(b)$

for any b

they decided on.

- For liveness, we allow validators to exit by a bounded ratio every time a block is supported by a certain size of a clique (on-chain finalized

). * Any exited validator's weight is set to 0

. They can not create a valid message by his public key.

- For any block b

, validators who have a non-zero weight in $\mathrm{Weight}(b)$

can exit up to α

by weight. * Hence the $1 - \alpha$

weight (by ratio) can contribute to the clique agreeing on the block

- For plausible liveness, fault tolerance is $< (1 - 2\alpha)/3$

(by ratio)

- Hence the $1 - \alpha$

weight (by ratio) can contribute to the clique agreeing on the block

- For plausible liveness, fault tolerance is $< (1 - 2\alpha)/3$

(by ratio)

- An on-chain finalized block

is defined as a block which is supported by a clique larger than or equal to $(2 - \alpha)/3$

(by ratio). * This is the maximal threshold which does not break plausible liveness.

- Strictly speaking, we need to subtract 1 unit from this threshold.

- This is the maximal threshold which does not break plausible liveness.

- Strictly speaking, we need to subtract 1 unit from this threshold.

- The blockchain can include an exit transaction if and only if it does not make the exiting weight exceed α

for the oldest non-on-chain-finalized block.

- Any exited validator's weight is set to 0

. They can not create a valid message by his public key.

- For any block b

, validators who have a non-zero weight in $\mathrm{Weight}(b)$

can exit up to α

by weight. * Hence the $1 - \alpha$

weight (by ratio) can contribute to the clique agreeing on the block

- For plausible liveness, fault tolerance is $< (1 - 2\alpha)/3$

(by ratio)

- Hence the $1 - \alpha$

weight (by ratio) can contribute to the clique agreeing on the block

- For plausible liveness, fault tolerance is $< (1 - 2\alpha)/3$

(by ratio)

- An on-chain finalized block

is defined as a block which is supported by a clique larger than or equal to $(2 - \alpha)/3$

(by ratio). * This is the maximal threshold which does not break plausible liveness.

- Strictly speaking, we need to subtract 1 unit from this threshold.

- This is the maximal threshold which does not break plausible liveness.

- Strictly speaking, we need to subtract 1 unit from this threshold.

- The blockchain can include an exit transaction if and only if it does not make the exiting weight exceed α

for the oldest non-on-chain-finalized block.

- Any validator can go offline when her exit transaction is included in a block and the block gets finalized subjectively by t

such that $t < (1 - 2\alpha)/3$

.

N.B. Proofs of these claims are WIP.