darkfi thunderbolt consensus

ertosns

31/12/2022

Contents

1 thunderbolt darkfi consensus

proposal for a consensus algorithms at least 3 times faster than alpha version implementation.

1.1 anonymous contiguous lottery

darkfi lottery $y < T$ isn't guranteed to be won once each slot, in fact, the best that can be done is having 1 single leader ≤ 33 of the time using discrete controller, that is an oscillating controller above and below the target value [1] this is the a proposal to fil the 66% gap for a faster tx processing.

1.1.1 thunderbolt darkfi consensus (beta)

the leadership maechanism is split into two parallel blockchains:

- leadership assignment blockchain: lottery using the same alpha mechanism for assigning the leadership to the winning stakeholder in the future time utilizing a smaller slot time $\delta^{lottery}$
- main blockchain: has larger slot time δ^{block} for evolving staked coin, rewaring minner, and validating transactions.

$$\delta^{lottery} = k\delta^{block} | k \in \mathbb{Z}, k \geq 3$$

2 leadership assignment blockchain:

using the same lead circuit only without the rewarding mechanism.

2.1 mechanism

- if competing stakeholder wins the lottery at slot i, the assigment circuit burn the old coin C_1, and mint a new coin C_2 with the same value.
- C_2 exits competition in lottery, and awaits it's turn to lead block at position $s = \phi(i)$[2] in the main blockchain.

[1] https://github.com/ertosns/lotterysim

[2] mapping function to the next available spot in the main blockchain.

3 main blockchain

exactly similar to the old circuit, with extra validation step, that validate that published proof in current slot s coorespond to the lottery winner in the leadership assignment blockchain at position i.

3.1 mechanism

- the stakeholder assigned a slot s publish a proof burning C_2, and minting new coin C_3 with value equal to previous value + reward value.
- C_3 enter the competition in the leadership assignment blockchain.

4 thunderblot limitations

- block slot time, and transaction processing time is limited by δ_{block} as a function of k, $\delta^{lottery}$.