Random pow and pos for blockchain

Wu ChengHe

brianwchh@gmail.com

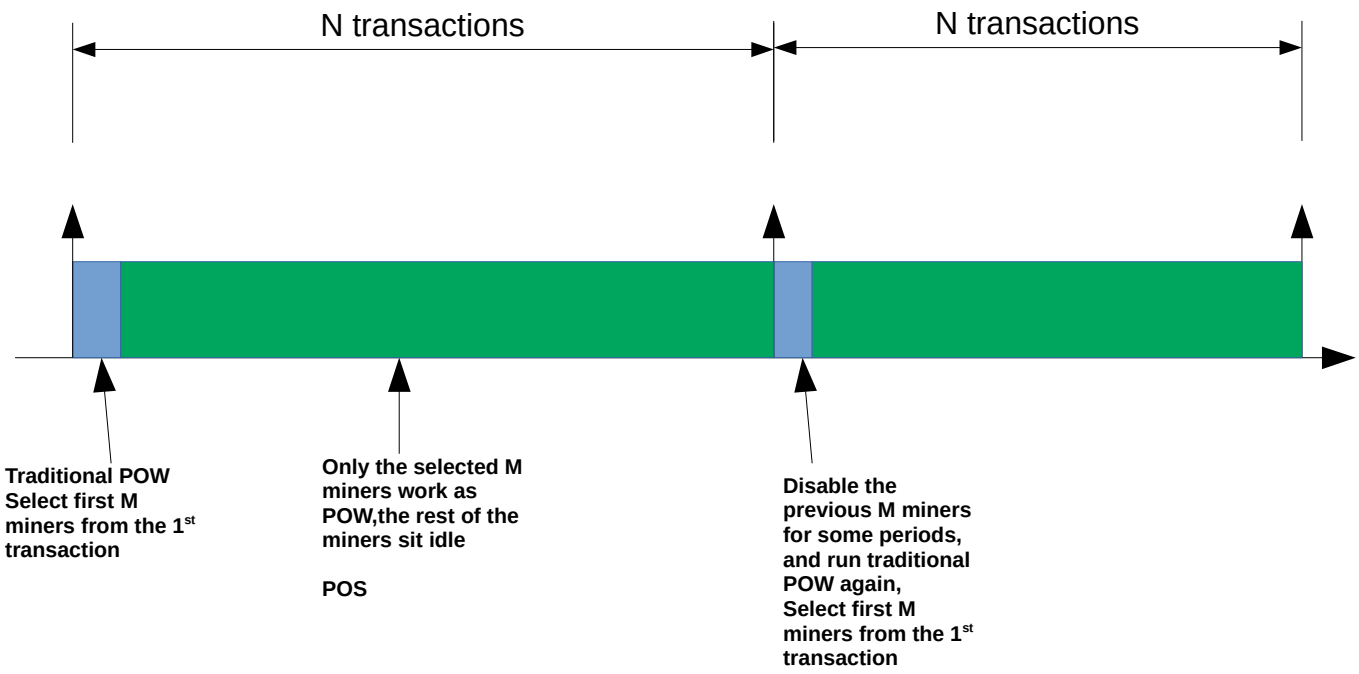
wuchenghe@vk.com

www.decensormedia.org

the problem of traditional proof of work is that it consumes a lot of power for every one to compute every transaction on the block-chain decision, and the first miner's decision is the final decision.

The problem of proof of state is that it is unfair and people will have doubt in the decentralization core value of the block-chain system, for it gives the richer guys more weights in a decision making.

To solve the power waste and maintain the trust from the public, we can come up with a solution which utilizes the randomness of the nature.



As shown above, we can divide the computation chain into cycles, each cycle contains N transactions, at the beginning of each cycle, all the miners on the network take part in the computation race, and the first M miners are selected for the decision makers in the rest of the

cycle, but in a proof of stake way, and the majority of the miners on the network sit idle, but randomly select another M miners as watchers who verify each decision, and and get great reward if he find any mistake, and replace the player in the decision maker team.

Why we use POS ? Because we believe people who invest more on the block-chain shows more long run responsibility,so that we encourage people to stay their money on the account,the amount of money stays on the account shows their trust and confidence in the block-chain system, it is similar to the political voting system, people trust and do some basic contribution to the community get the qualification to vote. How to compute the weight? Not just the instant amount of cropto-money, but should take the time into account, people willing to stay more money on the account gets higher weight.

In the proceeding n cycles, the previous M miners are disabled, this can prevent the computer monsters dominate the decision making, giving the majority an even chance to take part in the game.

Also we should provide the statistics to the public so that we can observe that whether the decision making power is biased. Those miners who are above a certain percentage level should get some punishment in which they are limited for some period of time from getting into the decision making team. Such that we discourage miners to invest a lot of money to develop ASIC for mining. Since these statistics are publically available, people will have more confidence in the system where they believe we truly decentralized and distribute opportunities among all players.

for the headache of storing one long long chain, we could find a way to break it into sever Genesis, everything evolutes, the blockchains between genesis may not be the same, this gives the opportunity to upgrade the system to fix the systematic bug or adapt to technology evolution.

2021.11.19