Random pow and pos for blockchain

Wu ChengHe

brianwchh@gmail.com

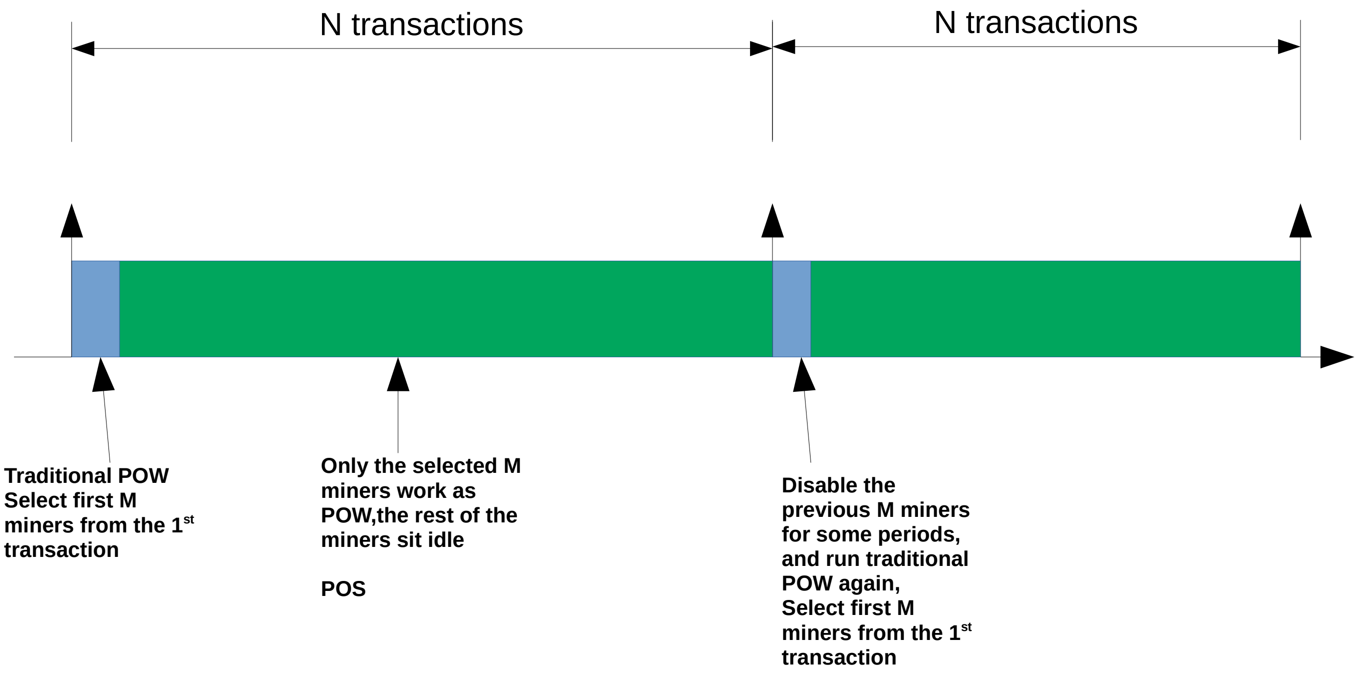
wuchenghe@vk.com

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.


N transactions
N transactions
Traditional POW Select first M miners from the 1st transaction
Only the selected M miners work as POW,the rest of the miners sit idle
POS
Disable the previous M miners for some periods, and run traditional POW again, Select first M miners from the 1st transaction

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.

Update : the purpose of having miners is to witness the transaction, the more the better, how to attract more people to become miner ? To cut the share of the transaction fee, or lucky draw.

But the purpose of proof of work is kind of off the road ! Misleading people to compete the computation power so that they can be the first one to come up with the correct answer. And centralized the opportunity to the hands of big companies who are able to provide super computers that consume a lot of electricity power, and thus the majority gets fewer and fewer opportunities, and then they finally quite the game, leaving the blockchain system depending on a handful companies to make the decision of each transaction, so it is dangerous for any blockchain system.

So in all the outcome of the original proof of work has the following 2 main drawbacks:

1. electricity power waste

2. centralize the opportunities on the hands of powerful miners and drives the majority of miner away.

So in order to guarantee the randomness of the system, attract more people to become the miner and witness the transactions, and save more electricity power, we can redesign the rules which will eventually forbidden miner to use server grade computer or GPU / ASIC, or even destop or laptop computer, ideally people can buy embedded miner board from the market and plug-and-play.

For each POW algorithm puzzle, we can set a time limit, if the time for a miner to solve the puzzle is less than the limit, their answer is invalid. two reasons that might lead their answer to be invalid, first, they may use powerful computer, second the randomness in the algorithm in the puzzle itself, so everyone is kindly like playing lucky draw, they want their mining machine to be fast, but don't expect them to be that fast otherwise the outcome is invalid, so too fast to make the right guess is not always good.

Under such rule, the miner has to use power saving embedded device! And thus we decentralize the opportunities from the hands of the big companies to the majority, having a hundred embedded device miners is always better than just counting your block-chain system on just on gain computer miner! And since embedded mining device is cheap, and it further encourage more and more people to join the mining game, it is just like they can make money on the way home, sometimes get super gift, from time to time the system make some lucky draw, high expectation attracts more people want to become the lucky guy! Even he does not become the lucky guy through out the whole year, he still gets the real opportunity to get the mining fee from some transactions.

Under the same principle, we can also set some limits on the weight, so that the opportunity does not centralize on the hands of rich miner, but do give fair opportunities to the miners who are willing to stay their money in the block-chain system, because they trust the future of the system.

In this way, it is much easier for people to understand how block-chain works under the hook, we tend to trust something we understand it is truly good! And then we will have enough motivation to become the block-chain end users and miners as well at the same time.

https://github.com/brianwchh/random-pow-and-pos-for-blockchain

2021.11.19