Proposal of a new cryptocurrency

Intro

This new cryptocurrency (based on bitcoin lite) will use coin-age Proof of Stake like PeerCoin as part of the Sybil resistance. Each user will have a coin-age for each UTXO that is calculated by multiplying the age of the UTXO with the number of coins it holds. This coin-age will help you find a proof faster based on the value of your coin-age. This means that the more old coins you have, the easier the Proof of Work will be [1]. There will be some formula for determining the handicap added to your proof requirement based on your coin-age. As the author of PeerCoin discusses, this protocol leaves itself vulnerable to attackers taking over 51% of the coin-age of the market.

A proposed solution to this was to have checkpoints that the community agrees has a clean history with no evidence of attacks. If an attack was to occur, the block will be forced to revert to this checkpoint, discarding any activity that happened during the attack. This is mostly a counter-measure for this attack in the early stages of the currency, where it is most vulnerable to the attack. The plan is to remove this feature in later changes of PeerCoin. I have come up with a different type of defense against this type of attack that will be discussed below.

Eligibility to Mint

The novelty I have come up with for my cryptocurrency is to have a way to select who is eligible to mint new blocks. This allows less powerful entities to have a chance of reaping the rewards without being overshadowed by the bigger entities in the network every time. The idea being that only 2^{-x} of the minters are eligible to mint a new block each block. The eligibility is determined by having to matching your public key with the first x bits of the previous block hash.

This x value can then be adjusted so that the threats of attacks are lessened. This novelty is similar to the way NXT determines eligibility of a miner to mine a new block [2]. The algorithm behind it is a bit different, but has the same idea (This fact was unknown to be at the time of coming up with my novelty).

The pros of this protocol compared to Bitcoin is that this selective minting combined with the coin-age gives individual users a bigger chance of successful minting, thus making the whole network more decentralized [3].

Determining Consensus

If no proof is found within a certain number of time (or a minting stage), the minting restriction is lowered by one bit to allow more minters to try finding their proof. This just makes sure that a block will be minted in a reasonable time. For example, if an initial restriction only allows for one laptop to submit proof, it could take weeks for a block to be minted, which is not ideal. Once a minter finds a proof, the process of verifying the proof has a few steps:

- Verify the minter is allowed to provide a proof at this time. This could be based on timestamp the message received by the network has and comparing it to a local timestamp.
- Verify the coin-age of the minter, and that the minter has reset his coin-age in the block.
- Verify the proof provided agrees with the coin-age handicap.

If there is a tie, the proof with the highest coin-age handicap wins. This is to avoid big mining pools with little coin-age to control the network just because they have enough power to overpower any handicap provided by a coin-age.

References:

[1] PeerCoin, Proof of Stake consensus. https://university.peercoin.net/#/9-peercoin-proof-of-stake-consensus

[2] Whitepaper:Nxt https://nxtwiki.org/wiki/Whitepaper:Nxt

[3] What is Proof of Stake? https://hackernoon.com/what-is-proof-of-stake-8e0433018256