Proof Of Transaction v2

Key Improvements:

- Increased frequency of proof-of-transaction rewards
- Lower proof-of-transaction reward, but large increase in PoT rewards overall
- Increased blockchain security through increased PoT “checkpoints” via PoT rewards
- Reduced minimum transaction size for PoT consideration from 500 to 1 FLT.
- Addition of variable PoT difficulties depending on the number of transactions occurring per block

Frequency vs Reward Percentage

In looking at the current state of proof-of-transaction rewards specifically, we found that based on the difficulty, they occurred roughly every 200 blocks on average, with the payout being 50% of the proof-of-work reward.

While the frequency of PoT cannot be predicted, it is my estimate that they will occur on 80% of blocks, so again considering 1000 blocks, 800 blocks would pay PoT rewards.

For example, if you take into consideration 1000 blocks, with a block reward of 20 FLT.

Current algo PoT payout per 1000 blocks = 100 FLT
Proposed algo PoT payout per 1000 blocks = 800 FLT

Security

The increase in frequency of proof-of-transaction flagged blocks leads to an increase in bockchain security, using PoT as another system of block checkpointing. As a result of additional proof-of-transaction flagging, a 51% attack employed in an attempt to change transaction order or double spends should effectively be thwarted, resulting in a complete fork of the attackers blockchain from the mainnet blockchain.

Automation Protection

Since the inception of proof-of-transaction, one of the hot topics is always “can I send coins back and forth constantly to generate rewards”.

There has always been protections for this sort of thing, but with v2 of proof-of-transaction, the reward system is now mostly geared 99% towards small outputs (person to person, person to store, etc). Large outputs to many addresses are now given a higher PoT difficulty, effectively greatly decreasing ones chances of gaming the system.

In addition, as was always the case, sending a large number of transactions will effectively disqualify these transaction from PoT consideration, incurring a loss of transaction fees for the attacker.