SCDO Consensus Algorithm ZPoW Introduction

For the current mainnet, SCDO uses ZPoW algorithms which address sequential scientific computation and matrix properties. The main idea is to reduce parallel computation in the algorithm so that GPUs have less advantages over CPUs. We believe that by doing this we can make the network more decentralized. We have mathematicians working on the design of the PoW consensus. They are very experienced in algorithm design and optimization.

We are also working on a novel PoW framework that can combine multiple computational targets. Each miner can choose to compute one target or multiple targets. The framework uses an algorithm to dynamically adjust the difficulties of each target. Within a certain time range if too many blocks are mined with the same target, then the difficulty of this target will be larger than the difficulties of other targets. Then the miners computing other targets have a larger probability to mine the new block. The key idea of this framework is to balance the block distribution for different computational targets. Practically, to let this idea work, it's important to reward the miners' work even if they are not getting new blocks. We allow them to keep computing one target and use a computational proof to increase their chances of mining new blocks.

The current ZPoW algorithm can be merged into this mixed PoW framework. Other PoW algorithms can also be merged into this framework. With this framework, it is much harder for super miners to dominate the network. We know that 51% attack is dangerous and happens when a super miner can produce blocks continuously. Since the miners can always change their mining accounts, it doesn't work to set rules to restrict mining accounts. But under this mixed PoW framework, an attacker needs to compute several targets at the same time. If we have 10 computational targets in the framework, then it's 10 times harder for a 51% attack to succeed. Here is an analogy of this method: let's say John is super efficient, given the same task and time, he can do more work than any other person. Now we give him 10 tasks. Let another 10 people do the same tasks but each person just focuses on one task. Given one hour, John wins the game only when he does more work on each task. Because each of the other 10 people only focus on one task, and John needs to allocate his time on each task, it will be difficult for John to win the game. This illustrates the idea behind our mixed PoW framework. We believe this framework can provide decentralization for SCDO network.