Summary of Bitcoin Mining

Xiaojie Zhu

February 5, 2018

Ming is a process to realise the transaction and block verification. In addition, it is the only procedure to generate new coins. Specifically, mining is a process to find a nonce making the hash result of concatenation of block and nonce smaller than the target value. As a bitcoin miner, the goal is to find a valid block and make profit. During the mining process, the miner needs to listen for transactions, maintain block chain, listen for new blocks, assemble a candidate block and find a valid nonce.

However, there are many factors influencing Bitcoin mining. The most important factor is the ability of hash rate. The first generation of mining hardware is CPU that is the design goal of basic Bitcoin network. Everyone can use their own PC to do mining. The second generation is GPU mining. Compared with CPU, GPU has obvious advantage in computing hash rate. However, as GPU is not designed for mining, some extra hardwares on the board are not necessary. The third generation is FPGA before the ASIC chip arrives. From the evolution of the hardware, the hash rate dramatically increases. In the other side, the energy consumption also increases. In total, more than 10 percent of a large power plant is consumed in the Bitcoin network.

Is it possible to make profit for miners with less computational power? The solution is the mining pool. The concept is miners cooperating to find a valid nonce. Based on the team work, many protocols are proposed to share the benefit. Mining share is a protocol for miners to prove their work by submitting the nonce that is most closely to the valid one. In the pay-per-share model, the payment is given based on the submitted share. There is no influence whether the pool finds a valid block or not. Another one is proportional model. In this model, only the reward are distributed to the miners based on their work.

With the invention of the mining pool, the 51 percent attack is more easy. In addition, the forking attack also becomes practical. However, due to economical consideration, miners tends to maintain their reputation by working honestly.

The mining puzzle should have property that it is hard to compute but easy to verify. In addition, the puzzle should be adjustable as the scale of the network changes. Following the ASIC-resistant concept, the memory-hard puzzle is proposed. For computing this puzzle,

large amount of memory is required. *Scrypt* is the representative. The weakness of *Scrypt* is the complex verification. The proof-of-Useful-work is proposed before Bitcoin appears. However, there are many challenges to adapting this puzzle to Bitcoin, e.g., equality for the nonce. Proof-of-storage is a puzzle that requires storing large amount of data. The proof-of-stake is a puzzle that only the miners having stake can propose new blocks. The alternative puzzle is proof-of-deposit. The miners will be rewarded if it hosts coins for long time. Obviously, no matter proof-of-stake or proof-of-storage can make rich miners more rich, which conflicts with the original design concept.

Although many puzzles have been proposed, the proof-of-work still dominates the cryptocurrency market and a puzzle for social welfare is desirable in the future.