Mohammad H. Tabatabaei

Mining

Mining plays an integral role in validating transactions, making blocks and maintaining the blockchain, and even minting coin in cryptocurrency applications. In order to become a miner in the network, one have to join the bitcoin network and connect to other nodes. Once joining the network, all the historical blocks will be downloaded by the node in order to have all previous transactions for the future validations. After bootstrapping, a miner has to compile a set of valid transactions that he has from his pending transaction pool into a Merkle tree. Then, it has to be putted in a block, which is pointing to the previous block, But the process of storing transactions into the block is not such simple and need a lot of computation work. Miners have to try various nonces in order to reach a block hash that is below a specific target. This process is taking about 10 minutes for each block, and as more miners join the network and mining hardware advances, blocks are found faster and the difficulty is increased so that this average time will remain constant.

Mining hardware has developed through the time. It was first done by CPU and general-purpose computers but as passing the time this kind of mining became less profitable with the current difficulty. GPU mining was the alternative that could perform more detailed computing of hash but this also was replaced by FPGAs and ASICs because of the electricity consuming and lack of profitability compare to the new solutions. Today, individuals mine rarely and most of the work is done by professional mining centers because of the expenses.

A better solution for individuals who are interested in mining is to join a mining pool. Each pool has a manager that run a bitcoin node, collecting transactions into a block and send it to all of its members in the pool. Then, all of the members work on the block to find a hash below the target and receive reward according to the amount of their working in the network. The mechanism of rewarding in pool mining can be pay-per-share or proportional. Proportional paying has lower risk for the manager as they only pay to the members if a valid block is found.

As the basis of bitcoin mining is on the concept of hashing and in this method participants with smaller power of computation has no benefits in joining the network, some solutions are proposed to replace the current proof of work in bitcoin or at least in other use cases. Memory-hard puzzles was one of the attempts that tried to be ASIC-resistant and required a large amount of memory instead of CPU time. Scrypt is one of those memory-hard hash function for this purpose and used in some other cryptocurrencies and use cases instead of proof of work. However, all of the proposed alternatives could not be completely resilient to ASIC hardware and a lot more works on new solutions is required for defining ASIC-resistant mining puzzles.