Lecture 3 – Mining in Bitcoin overview summary – Tien Dat Le

Bitcoin miners has played one of the most important role in Bitcoin system that is to solve a difficult puzzle requiring a lot of computing resource to assist the whole networks to reach consensus about the distributed ledger. It also have the responsibility to validate correct block so that anyone can verify it just by sending a block to miner network. In general, miners will have to do 6 tasks:

1. Listen for transactions.
2. Maintain blockchain and listen for new blocks.
3. Assemble candidate block.
4. Find a nonce that makes block valid (Solving the puzzles)
5. Broadcast valid blocks and hope it will be accepted
6. Get profit from the rewards.

The difficulty of the puzzle and the computing resource of miners will both decide the time it is accomplished. The difficulty is often adjusted every 2 weeks or 2016 blocks to keep the average block time converge to 10 minutes as the computing resources may varied from time to time.

During the evolution of mining industry, there are 4 types of hardware has been used widely in Bitcoin mining: CPU, GPU, FPGA and ASIC.

Due to the probability distribution of mining reward, a miner alone will rarely get a reward within a year, they have to be gathering in a centralized entity called mining pool to mine together and sharing the rewards. All miners in the same pool will communicate using mining protocol has been standardized and used. To prove having a certain amount of mining power, miners requires to submit mining shares, i.e. a rare enough solution of the puzzle , to the pool manager. Pool manager will distribute the rewards proportional to the shares of miners.

As mining pool is a centralized entity, there is a phenomenon in 2014 in which there is a mining pool called GHash that has more than 50% of hash power. It leads to an attempt from mining pools to not attempt to avoid acquiring so much mining powers and miners to join different pools.

Since mining pools is the entity that have the power to create new blocks. They, in fact, also have the power to do many attacks to bitcoin protocol. They can do forking attack which allow them to do double spending by producing a longer chain than the main chain. However, it require to have more than 50% computing power to be effective. They can do sefl-fish mining, blacklisting and punitive forking and feather-forking.

As ASIC is much more superior in computing resources and then lead to the centralized mining farm in bitcoin which undermine its decentralization. Many attempt to propose alternative puzzles that is ASIC-resistent. One of the solution is memory-hard puzzled, which require to have a lot of memory to solve instead of cpu resource. A popular hash function of that kind is Scrypt which is used in Litecoin, a popular alt-coin. Another solution proposed is instead of Proof of work, miners will use Proof of Stake to do the consensus work. Node to join the consensus votes will have to deposit an amount of currency to a safe address. If it violate the correct result of consensus, the value of the currency will collapse and in turn it will lose the deposited money. This solution seems to be a good alternative to Proof of work as miners has consumed a lot of energy to do quite and useless work.