Part 1: Mining Bitcoin

Winning Nonce: 12452

Corresponding Hash: 0009e766bc42829a78b16ea6fc5bf924c38284c487515a188d404648770046b2

Part 2: Bitcoin Mining Strategy

In this last part you will think about a strategy of mining BitCoins. A BitCoin miner tries to find some strings attached to original message such that the new message after Hash calculation starts with k zeros. Only the first miner who solves the cryptographic puzzle receives the mining reward and the transaction fees.

* (a)  Suppose you have several opponents who have similar computational ability to you, and they all start with x = 0 and then try different numbers according to the ordering rule (0,1,2,3,...). In order to compete against them, what might be you strategy?
* Answer: My strategy would be to start with a number greater than 0, because the chances of the correct nonce being = 0 are very small, and being a step ahead of the competition is extremely valuable since only the fastest miner claims a reward. If it doesn’t matter how much time I beat them by, then I would choose x = 1, because I would always beat other miners starting at x =0. Otherwise, I may choose a higher number like x = 100. (I am thinking about the orphan branches that we talked about today in class. You mentioned if I beat another miner by only 1 second, it is possible that we could create two segments of the chain, resulting in one of our chains becoming an orphan chain.)
* (b)  Suppose you happen to find that there is another smart guy who uses your strategy in a), what should you do? Suppose again that, each time you get a new strategy, some new smart guy enters the game and uses your newly-developed strategy, what will you do?
* Answer: I would have to get more computing power. I cannot think of another way to guarantee that I win every time if other miners keep adopting my latest strategy. At first I would start with x = 1, then 2, then 100, etc., but then there would be no way to consistently beat other miners if they choose the same starting point (or a better one) than me.
* (c)  What might be miners’ strategies of choosing numbers for trials in equilibrium?
* In equilibrium, you’re going to hit limits on computing power, as well as get stuck in a rat race of always trying to pick a more optimal strategy than all other miners. In equilibrium, miners may try to form groups to combine strategies and split profits. In this case, each miner may not make as much money, but he/she is trying to ensure that his team wins every time so that his computing power/money spent on electricity is not wasted.