COMP 4901W – Homework 2

Name: SON Hangyul

SID:20537267

Email: hson@connect.ust.hk

Exercise 1

1. Who forms the block in a centralized pool? In other words, who chooses which transactions will be included in a block mined by the pool?

The pool manager decides the transaction to be included to the block. The pool manager will most likely include his/her public key as a part of the block in order to receive the block reward when the block has been mined.

2. As a pool manager, how can you ensure that the miners in your pool are not mining with their own identity (instead of the pool's) and any rewards they obtain will be paid to the pool? What happens if a miner does not announce the block they found to you, but instead publishes it on the network?

The pool manager will have to give out the pool-participating miners a block with a nonce information missing. The individual miners will mine nonce according to the block given, a block with pool manager's public key. Therefore, even if a miner has found a nonce to the block, the miner cannot mine with their own identity, because this will result in a hash entirely different from the solution. The miner might not announce the block they have found, but this would mean the loss of the entire pool which leads to the loss of the miner that has hidden the solution.

3. As a pool manager, how can you compute/approximate the amount of hash power that each participating miner is contributing? As a miner who joins a pool, how can you be sure that you are being rewarded in proportion to your contribution to the computational power of the pool?

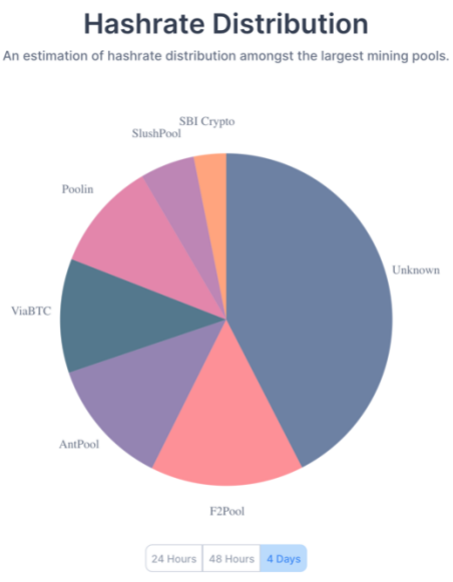
1) Solving the puzzle for the current bitcoin protocol is very hard.
2) However, the pool manager can design easier puzzles which are even solvable to smaller miners. For example, if the current difficulty of the puzzle is to find a nonce that results in 10 leading zeros, the pool manager can design the difficulty to find a nonce that results in a hash with 3 leading zeros.
3) The individual miners can check two different occasions. The occasion in which the real bitcoin puzzle is solved, and when the solution to the puzzle designed by the pool manager has been solved. Since there can be more than one cases in which hash result with 3 leading zeros, report the pool manager of the nonce whenever such solution is found.

4) When the block is finally added with a block reward, the pool manager can distribute reward proportional to the number solutions to the easier puzzle each miners have solved. Since the easier puzzle can be solved even by a small scale miners, they can also receive a portion of the reward for their contribution.
5) The more easier puzzle solved, this implies that the particular miner has had higher computation power(hash rate) and therefore is a fair mechanism to distribute block reward.

4. What happens if a pool has more than 50% of the total hash power? Which security guarantees of the blockchain can be violated? [Note: This has happened in the past.]

Then the entire blockchain is vulnerable to the 51% attack. Controlling more than 50% of the hash power means that eventually the pool can choose the longest chain. This implies that the pool has the power to add or ignore blocks from other participating miners. Even if other participating miners might have found the nonce and added to the chain, if the monopoly-pool decides to ignore such block and continue mining from the previous block, forked version that the pool choose will eventually become the longest chain. As a result the pool with majority hash power has the power to block certain transactions or make a transaction and overturn it, also known as double spend attack. This violates the security guarantee of the blockchain which states: The majority of the network is honest. There is chance for a pool with more than 50% of the total hash power to not be honest.

5. Based on the current distribution of hash power on the Bitcoin network, how many pool managers have to collude in order to be able to blacklist a particular coin and not allow it to be spent? [Please include the data you used at the time of your solution so that we can verify you solved this problem correctly.]



Given the current hash rate distribution, only if a mere 4-5 pool manager collaborate, they can blacklist a particular coin.

Exercise 2

Suppose that you are a malicious miner in one of the big pools. Assume that your pool controls 20% of the total hash power on the Bitcoin network and you control 0.1% of the total hash power. Devise an attack in which you successfully obtain shares from the pool's rewards but do not contribute to the pool's total revenue. It is fine if you personally lose money in this attack, e.g. due to shrinking shares as a result of lower overall revenue of the pool, as long as the losses incurred by the pool are significantly more than your personal losses,

I am malicious miner hoping to damage the revenue of a particular pool. And therefore, I hope the miners in the pool to move to my friend mining pool instead.

Pool manager gives me a block without a nonce to solve. And will distribute the reward according to the proportion of how many nonces to the easier puzzle designed by pool manager has been solved. Even with 0.1% total hash power, I still have the probability of finding the nonce the actual blockchain puzzle. If the nonce is found, instead of submitting the solution to the blockchain network which will reward the pool manager, I can simply hide the solution. However, I can continue to submit the puzzle of the pool to prove my contribution to solving the puzzle. When the puzzle to the block is finally solved by an other miner in the pool, the pool miner will distribute the reward according to each miners contribution. Therefore, I can receive a proportion of the block reward which could have been found earlier by me. Even though I don't submit the solution to a block for a long time, the pool cannot blame me as I can be simply be considered unlucky. As a result, I can receive rewards which other miners have contributed, but not submit any myself. The pool will be spending a portion of block rewards for a miner with practically no participation.

Exercise 3

1. Suppose that you are one of the big pools and control 10% of the total hash rate. You are competing with another pool that also controls 10% of the total hash rate. You know that miners generally favor pools that provide better average rewards in proportion to the contributed computational power. Devise an attack that decreases the average rewards in the competing pool in comparison with your pool and incentivizes the miners to migrate to your pool.

This attack is similar to the one in Exercise 2.

1. Use 5% of the total hash rate to enter the competing pool.
2. Hide whenever the block is found. However, receive all the contribution rewards for a block.
3. Now the total hash power of the competing pool is 15% but the total reward will be the same as 10% hash power. Therefore the average reward will be reduced.
4. On the other hand my pool now only control 5% of the total hash rate. But the average reward would have remained the same given that no attacks have been made to my pool. The decrease of total reward will decrease proportionally with hash power, thus no loss of average rewards per miner.
5. Miners from the competing pool will likely find other pools for higher average rewards which includes my pool. As a result, if I now return back to my pool I can have $10 + \alpha$ % of the total hash rate.

2. Suppose that you are the biggest pool on the network and control 45% of the total hash power. Devise an attack that lets you get more than 45% of the total block rewards on average. [Hint: When you find a valid block, it might be beneficial not to announce it but to try to find another block.]

1. Since I control 45% of the total hash power, I have 45% chance of finding the block.
2. If I find a block, instead immediately revealing the block to the public as any honest miner would do, I hide the block information and continue mining on from the newly found block.
3. Other miners are still working on the block that I have found.
4. Luckily, I find an another block and lead other miners by 2 blocks.
5. This continues on until the public blockchain length has only one block difference from my secrete blockchain in which I have added several blocks.
6. Then due to the blockchain protocol the longest chain is accepted as the main blockchain. As my the blockchain that I have been secretly is longer than the public blockchain that other miners have been working on, the public blockchain gets replaced with mine.
7. Therefore the work of other miners are erased. This implies for at least the past few blocks the contribution to the entire blockchain has been entirely made by my pool.

8. As a result, on average more than 45% of the total block rewards can be owned by my pool. This is not because the number of registered block increased, but because my pool removed the contribution proportion of other miners due to the luck that followed my pool for few blocks.