COMP4901W Homework 3

KIM, Jaehyeok (20550178)

The Hong Kong University of Science and Technology

Exercise 1

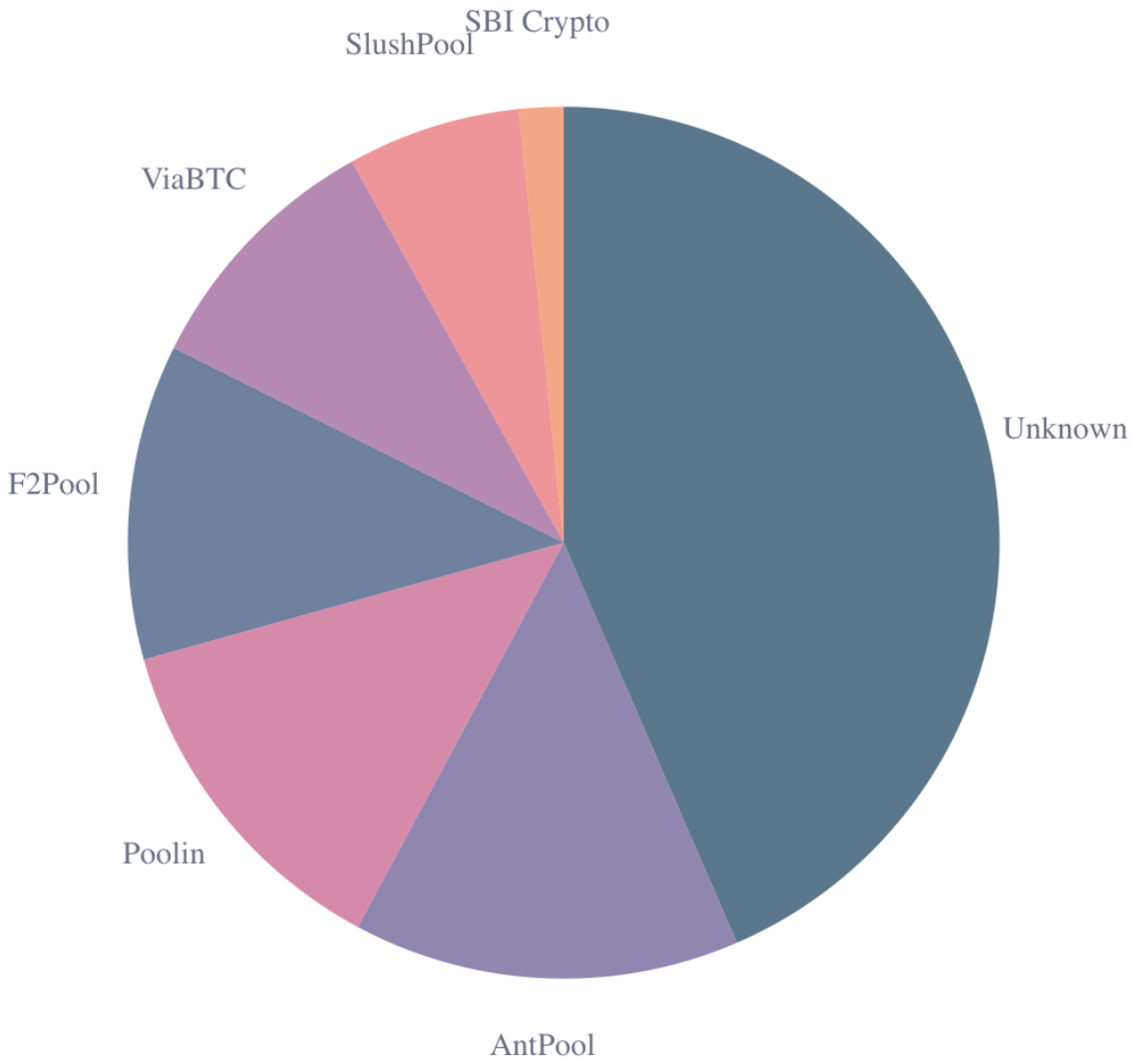
1. The blocks in a centralized pool are formed by the pool managers. The pool manager will choose which transactions to be included in each block mined by the pool.

2. When creating a block, it contains the address of the miner which would be the address of the pool manager. When the miner finds the correct nonce, he cannot change the address of miner to his one since the nonce will then not hold. If the miner wants to mine with his address, he has to include his address and this is just equivalent to mining the block personally on his own.

3. The pool manager can asks the participating miners to send their partial Proof-of-Work (PoW) called a share that is close to the complete PoW. For example, the pool manager can set another difficulty that is a bit easier than the actually PoW difficulty. The shares sent by the miners will be accepted if it meets the minimal contributing difficulty or rejected otherwise. When the block is successfully mined, the reward can then be distributed proportionally based on the number of accepted shares.

4. If a pool has more than 50% of the total hash power, the pool can rewrite the whole history as mentioned in the lecture. They can possibly start from any points they want and make another branch longer than the current consensus chain. This will easily violate the Bitcoin's core security assumption once the pool (majority) decides to do something bad. For example, this will possibly lead to a double-spending problem as the processed transactions could be cancelled due to the majority's history rewriting.

5. As shown in the figure on the next page, the top-4 pools (AntPool, Poolin, F2Pool, ViaBTC) has about 50% of the total hash rate. Thus, by having at least 4 pool managers colluding or 5 (with SlushPool) to be sure, they will be able to blacklist a particular coin by not including the transaction using the particular coin to the new block. Even if it has been processed by another pool, the colluding pools can change the history and vanish the block including the transaction using the particular coin.


SBI Crypto
SlushPool
ViaBTC
Unknown
F2Pool
Poolin
AntPool

Exercise 2

Since the rewards are given based on the number of accepted shares (partial PoW) mentioned in Exercise 2, I can simply use 0.1% computing power to only share partial PoW and discards the valid/complete PoW. In this way, I will successfully obtain part of the pool's rewards while not contributing to the pool's total revenue. Since the pool's total revenue will be reduced from this attack, the amount of rewards I get from the shares will also reduce. However, as mentioned in the question, the losses incurred by the pool are significant more than that.

Exercise 3

1. I can let part of my 10% (e.g. 50% of my computing resources) to sabotage the other pool such that they participate but never share the correct PoW just like in exercise 2. By doing so, the hash rate of the other pool will increase from 10% but the rewards per hash rate will be decreased since the my computing resources will never share the correct PoW and takes the rewards. Therefore, the average rewards that the other miners get will be reduced while it stays the same in my pool. Accordingly, the miners in the other pools will be attracted to my pool since they can obtain higher share rewards.

2. By being the biggest pool, we can choose to delay the announcement of the blocks and secretly mines the next block in advance. If the original consensus chain seems to be catching up the chain length of ours, our pool can simply announce the blocks we have not announced yet. Until to be almost caught up by the public consensus chain, we can keep mining our own chain privately. Later, when we announce our longer chain to the public, the part of the original consensus chain will be discarded (similar to fork). Accordingly, the other 55% of the hash power are wasted. This attack will increase our total block rewards on average from 45% as the proportion of the blocks mined by our pool on the chain will be increased while other pools are wasted.