COMP 4901W – Homework 3

A. K. Goharshady

Release Date: March 9, 2022
Deadline: March 24th, 2022 (23:59 HKT)

This homework accounts for 10% of your total grade. You should submit your solutions on Canvas as a single pdf file. Handwritten and scanned solutions will not be accepted since the TAs might be unable to read your handwriting. However, you can draw your figures, if any, by hand. You are also allowed to discuss the problems with your classmates but you have to write your solution on your own. All submissions will go through a plagiarism check. If you submit the same solutions as another student, you will both get a grade of F for the whole course. The deadline is firm and no extensions will be granted. You will receive feedback on your submission and normally be allowed to resubmit once. We reserve the right to disallow resubmissions if your original submission is of a very low quality or shows a lack of effort.

Exercise 1

This exercise accounts for 5% of your total grade.

At the time of writing, to successfully mine a single block in Bitcoin, you are expected to have to compute around 1.183×10^{23} hashes. Assuming that you use a gaming laptop that computes 10^8 hashes per second, it will take you more than 37 million years to successfully mine a single block. Of course, real-world miners use expensive dedicated hardware with much higher hash rates, but they still have to pay for their equipment and their electricity usage. It is not a great proposition to have to wait for a long time and do mining with no profits, just so that you get lucky after months, years or probably even decades and get paid a lot of money for successfully mining a single block. In other words, even though the expected reward of mining Bitcoins might be positive, the variance is so large that any typical miner would go bankrupt before getting their first rewards. The classical solution to this problem is called "pooled mining", where many miners join a "pool" and share both their computational power and their rewards. Most pools are centralized and have a single pool manager.

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?
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?
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?

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.]
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.]

Exercise 2

This exercise accounts for 5% of your total grade.

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.

Exercise 3

This is an extra-credit exercise. You are not required to submit a solution. However, any points you achieve here can be used to compensate potential lost points in other exercises or future homeworks. This exercise can compensate for up to 5% of your total grade.

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.
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.]