COMP 4541 – Homework 2

A. K. Goharshady

Release Date: March 29, 2024
Deadline: April 8, 2024 (23:59 HKT)

This homework accounts for 10% of your total grade. You should submit your solutions on Canvas as one pdf file and one sol 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. Your solutions must be 100% your own work. All submissions will go through a plagiarism check. 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 4% of your total grade.

Alice wants to prove to Bob that she has 100 BTC.

1. Design a protocol by which Alice can prove her ownership of 100 BTC to Bob by doing exactly one transaction on the blockchain but keeping her ownership (except for transaction fees).
2. Design a protocol by which Alice can prove her ownership of 100 BTC to Bob without performing any transactions.
3. Design a protocol by which Alice can burn the 100 BTC, making sure that they will never be accessible to herself or anyone else, and prove this to Bob.
4. In your protocols above, can Bob obtain any information about Alice's past or future transactions, i.e. transactions that were either performed before your protocol or after it? If so, how can Alice defend against this and preserve her privacy?

In all of your protocols, you should make sure that Alice cannot replay someone else's proof. For example, if Carol is proving to Alice that she has 100 BTC, Alice should not be able to reuse Carol's proof to convince Bob that she herself has 100 BTC.

Exercise 2

This exercise accounts for 3% 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.

Explain your attack in detail. You should find out about the mechanisms used by the largest mining pools and reference them in your solution.

Exercise 3

This exercise accounts for 3% of your total grade.

Bob owns 1 BTC on the Bitcoin Blockchain and Alice owns 20 ETH on the Ethereum Blockchain. They would like to exchange their money. Unfortunately, neither side trusts the other. Thus, Bob is not willing to transfer the BTC to Alice unless he is assured of receiving the ETH. Similarly, Alice would not transfer the ETH to Bob first unless she is guaranteed to receive her BTC.

1. Design a trustless protocol that allows Alice and Bob to exchange their money with each other. Prove that your protocol is secure and no side can steal the other's money.
2. Implement your protocol by providing a Solidity contract that performs the ETH side of the deal and Bitcoin scripts for the BTC side. Put your Bitcoin script in the pdf file of your solution. Submit your Solidity contract as `exchange.sol`. Make sure you explain both implementations in your writeup.