COMP 4901W – Homework 7

A. K. Goharshady

Release Date: April 20, 2022
Deadline: May 4, 2022 (23:59 HKT)

This homework accounts for 10% of your total grade. You should submit your solution as a single `pdf` file. As usual, 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 entirely 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 10% of your total grade.

Alice owns 100 BTC on the Bitcoin Blockchain and Bob owns 1333 ETH on the Ethereum Blockchain. They would like to exchange their money so that Alice gets almost 1333 ETH and Bob gets almost 100 BTC[1]. However, this is complicated by two factors:

1. No party trusts the other, i.e. Bob is not willing to send his 1333 ETH unless he is assured that he will receive 100 BTC and Alice is not willing to send her 100 BTC unless she is assured that she will get 1333 ETH.
2. Alice and Bob are not willing to use the services of any third-party in any way. Specifically, they are not willing to exchange their cryptocurrencies for fiat or use any broker/exchange agent of any kind.

Design a secure protocol that solves this problem and allows Alice and Bob to exchange their money even though they have it on different Blockchains. Explain your protocol in detail and argue why it is secure.

[1] We say “almost” because they have to pay transaction/gas fees.