COMP 4901W – Homework 2

A. K. Goharshady

Release Date: February 28, 2022
Deadline: March 15th, 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. 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.

Consider the Centralized Ledger (CL) discussed in the lectures, in which a central bank keeps track of the ledger but anyone can create accounts and transact. Can the central bank perform the following actions? If yes, explain how. If no, explain why.

1. Freeze a specific coin (output) so that it cannot be spent.
2. Confiscate or change the ownership of a coin (output).
3. Reverse a transaction that was already on the chain.
4. Spend a coin that does not belong to the central bank.
5. Identify every transaction's payer and payee (in the sense of obtaining their real-world identity).
6. Allow transactions only if both the payer and the payee are fully identified in the real world.
7. Blacklist a certain individual and disallow their transactions.
8. Whitelist certain individuals and only allow transactions from them.

Exercise 2

This exercise accounts for 5% of your total grade.

Alice wants to prove to Bob that she has 10 BTC.

1. Design a protocol by which Alice can prove her ownership of 10 BTC to Bob by performing 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 10 BTC to Bob without performing any transactions.
3. Design a protocol by which Alice can burn the 10 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?