Homework 6 – CSCI 181
52 points

For this homework, I am not expecting your program to run/execute properly. Please use any programming language you prefer, but some parts of your functions may look like pseudocodes and that is okay.

Consider the SimpleCoin2 approach discussed in the lecture. Suppose you want to implement the logic used by entity G to process transactions and produce the ledger.

The entity G receives a PayCoin transaction and needs to check if this transaction is valid before adding it to the ledger. You will need to write functions for this scenario.

1) (10 points) Create a PayCoin transaction data structure or class with all the fields it requires.
2) (10 points) Create the blockchain (ledger), (assume the data part of each block contains only one transaction of type PayCoin). You do not need to compute the hashes,
3) (32 points) Write a function that checks whether a given new transaction is valid or not. If valid then add it to the blockchain. The definition of "valid" transaction is in the lecture notes. **Make sure to add enough comments to explain what you are doing.**

Assumptions:

Assume you have access to everyone's correct public key. Public keys are also included in the *recipient* field of the transaction. Also assume there is a function already implemented that verifies signatures and returns True or False: `boolean verifySignature(pubKey, message, signature)`