ECE 579: Blockchain and Cryptocurrencies 2020
Assignment 1 Part A - ScroogeCoin

In this assignment you need to write a Python code to create a blockchain based currency, i.e. ScroogeCoin. ScroogeCoin is discussed in section 1.5 of the book please read the section to understand the mechanisms of ScroogeCoin.

Design Overview:
The design has two main classes User and Scrooge. Scrooge will store the blockchain and will have the authority to create coins and accept transactions, put them into a block and add the block to the blockchain. Scrooge will contain a list to store the transaction requests and only process them to a block when Scrooge calls Mine function(you will implement this in part b). This should clear the transaction list and there is no limit on the number of transactions on a block. Each transaction will consume only a single coin but can output many. Users are only allowed to create transaction requests and forward them to Scrooge for processing.

A template for the Python functions is provided. You need to implement the necessary functions to finish the project.

A simple workflow (Part A + Part B) is as follows:

1. Scrooge and Users create public and private keys.
2. Scrooge create coins for the Users, meaning it creates transactions and add it to the transaction list.
3. Scrooge mines the list to put the transactions into the blockchain.
4. Users create transactions to send coins to each other. Transactions are forwarded to Scrooge for processing.
5. Once Scrooge receives a transaction, it will check if the transaction is valid (we explain the details under the function definitions). If it is valid, it adds the transaction to the transaction list. In case transaction is not valid, it should be discarded with displaying a message on the terminal.
6. Again, once Scrooge calls mine, it puts all the transactions into a block and adds it to the blockchain.

Required Libraries:

In order to run ScroogeCoin you need the following libraries:

- **Python3: to run the script**
- **GMP: required by fastecdsa**
- **fastecdsa : crypto library for Python**

In Part A of this assignment you only need to implement the following functions

Summary of the functions that Scrooge uses:

1. **KeyGen**: Create Public and Private Keys for Scrooge.
   Use curve=curve.secp256k1 for key generation.
2. **CreateCoins**: Only Scrooge can create coins to any user. The function takes a list of input addresses and amount of coins. It will create a transaction that creates coins and adds it to the transaction list which will be later mined. The transaction should be hashed and signed by Scrooge.
3. **Hash**: Hash can be computed for a string as
   hashlib.sha256(“1”).hexdigest()
4. **Sign**: Sign function that signs the input which is usually hash of a block or transaction.
5. **Add Transaction**: Add the submitted transaction by a user to your transaction list if the transaction is valid.

Summary of the functions Users uses:

1. **KeyGen**: Create Public and Private Keys for User.
   Use curve=curve.secp256k1 for key generation.
2. **Hash**: Take the hash of a block. Hash can be computed for a string as hashlib.sha256(“1”).hexdigest()
3. **Sign**: Sign the hash of a block and append it at the end of the block which creates a larger block that will be added to the blockchain.
4. **Send Transaction**: Prepare a transaction to pass it to Scrooge. The transaction should point to a block and a transaction ID which shows the coin balance that belongs to the user. The coins can be sent to multiple addresses. The total amount of input coins should match the total amount of output coins. Ex: User1 can point a location that holds 50 coins. User1 can spend all the coins between two other users (25 each, 10 User2 and 40 User3, etc.). Another option is that if User1 sends 10 coins to User2, he can send 40 coins back to his address. The transaction should be hashed and signed by the User and passed to Scrooge.

Student 1 Name:_____ ID:_____ Mailbox:_____
Student 2 Name:_____ ID:_____ Mailbox:_____

Function	Points	Sign
KeyGen	15	
CreateCoins	15	
Hash	15	
Sign	15	
Add Transaction	20	
Send Transaction	20	
Total	**100**	