Contents

1. Introduction

This project is aimed to create Scroogecoin, a blockchain based cryptocurrency, in Python.

2. Design Overview

The design has two main classes User and ScroogeCoin which will be described below.

3. Implementation

Used Modules:

- fastecdsa - https://pypi.org/project/fastecdsa/
- hashlib - https://docs.python.org/3/library/hashlib.html
- json - https://docs.python.org/3/library/json.html

Used Data structures:

- dict - defined using {key:value, key:value, ...} or dict[key] = value. They are used in this code for blocks, transactions, and receivers. Can be interated through using dict.items() - https://docs.python.org/3/tutorial/datastructures.html#dictionaries
- lists -defined using [item, item, item] or list.append(item) as well as other ways. They are used to hold lists of blocks aka the blockchain - https://docs.python.org/3/tutorial/datastructures.html#more-on-lists

ScroogeCoin Class:

- 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 (that will be implemented 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.

User Class:

Users are only allowed to create transaction requests and forward them to Scrooge for processing.

A simple workflow 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:
    - 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.

4. Test Results

```
Initial balances of the users:
User 0 : 0
User 1 : 0
User 2 : 0
User 3 : 0
User 4 : 0
User 5 : 0
User 6 : 0
User 7 : 0
User 8 : 0
User 9 : 0

Scrooge added coins to Users 0, 1, 3, 5, 8, and 9:
User 0 : 10
User 1 : 20
User 2 : 0
User 3 : 50
User 4 : 0
User 5 : 15
User 6 : 0
User 7 : 0
User 8 : 5
```

```
User 9 : 5

block:0
previous hash:1bad6b8cf97131fceab8543e81f7757195fbb1d36b376ee994ad1cf17699c464
signature:
 ↪(1545870050154275534307329562500372419492400423575030420731011178886518442825 2,␣
 ↪1174175855598960989124466231125129695202992524019094535400961623008572204716 9)

tx:0
sender: 806ba6f70fa289db5bf544164e382365ca3b0269fd4167aec1c63ccf4942622d
hash: 3e80f596a933250489ec5658cc5ea8f0dd01009c1281a9e4a39a886573840ad6
consumed coins: block - -1, tx - -1, amount - -1
receivers:
account: 678d55980c498a8aa31c454ce52605dc100a6def6876b441e2b3b898b742318e, ammount: 10
account: 7e30cf2eb7324bff87755b9974b265002e39cd141f52d1a249001774e9349d58, ammount: 20
account: 1d04594bea692de2f3525fe26389104e7ca8072069a6f0e9026d3f83bf89a87b, ammount: 50
account: 65cc76f042ff9535e1af9e92e947f7d05ebf04dbc9fc84a381fb4da9055c2dc7, ammount: 15
account: 3e759a1b505ccd98bfd20e406e42e150785056e8007bc60d6c0a48f3c90721cc, ammount: 5
account: 74b4965518d7f9e631bf9fe160d6f926356bec2bcbe9c0c95997befbb494f2ce, ammount: 5
signature:␣
 ↪(2729312928871126493518091354272412769747260658969696361329392890743970340655 3,␣
 ↪1040839676476499324163568495417719925355270085193573399818428753586350748802 13)

* Test 0: mine a valid transaction that consumes coins from a previous block.

User 0 sent 8 coins to himself and 2 coins to User 1.

The balances of the users after transaction:
User 0 : 8
User 1 : 22
User 2 : 0
User 3 : 50
User 4 : 0
User 5 : 15
```

```
User 6 : 0
User 7 : 0
User 8 : 5
User 9 : 5

Display block 1.

block:1
previous hash:4488435b3dcc7022c3c8cc8dab34029ab352e1a811522a200d962d672b978a3f
signature:(57409616635561522975143149803983986978430248303414019154595283289399114450146,
609008276534075395721761110508841746902196837040973601437224495432754776047 34)

tx:0
sender: 2820d68f508799694927b1f6daced46fa26305b6e6303b96bfa23f3a0a728c21
hash: 834efb5e985a066411145678715d70d5896350c6249d7f5a49933d40d0a95267
consumed coins: block - 0, tx - 0, amount - 10
receivers:
account: 83248698bc66591784eefea75a13aa39f7808ea906b56df56e9d5fd7e93c9d5f,
ammount: 2
account: 2820d68f508799694927b1f6daced46fa26305b6e6303b96bfa23f3a0a728c21,
ammount: 8
signature:
(865083949483606979266536751524541444384171482119894812663292032095656774117 92,
595033256844938856900616157844007363432205003277466529210148374237873971269 04)

* Test 1: mine an invalid transaction where the consumed coins are invalid.

User 0 sent 14 coins to User 3.

The transaction was discarded: the coins were not created before!

The balances of the users after transaction:
User 0 : 10
```

```
User 1 : 20
User 2 : 0
User 3 : 50
User 4 : 0
User 5 : 15
User 6 : 0
User 7 : 0
User 8 : 5
User 9 : 5

Display block 1.

The requested block does not exist on the chain.

* Test 2: mine an invalid transaction where the consumed coins were already spent.

User 3 sent 25 coins to himself and 25 coins to User 2, User 5 sent 15 coins to User 1.

The balances of the users after transaction:
User 0 : 10
User 1 : 35
User 2 : 25
User 3 : 25
User 4 : 0
User 5 : 0
User 6 : 0
User 7 : 0
User 8 : 5
User 9 : 5

block:1
previous hash:2db0fcbfe0a94e326826fb6cb09b7223152beb9896731f799d0af0424ce19208
```

```
signature:
 ↪(319872411875032877473078750938317819546390305699948447354794333667337386740 61,␣
 ↪105243610268469471027690773662487077685817088877514768713424717995027981033 31)

tx:0
sender: c3652c4cfa03e61850b8c82e95af9154b712593033aba8df31d73a4820ccb5f3
hash: a39c0c421a96a9b12c1ba5fb0f051448699c1d8c82fc07a643404ab1432e81b7
consumed coins: block - 0, tx - 0, amount - 50
receivers:
account: c3652c4cfa03e61850b8c82e95af9154b712593033aba8df31d73a4820ccb5f3, ammount: 25
account: 98afaad83ef0b515acf928acf1c6e872a81b4b9df6c47d617991d7923d59ef29, ammount: 25
signature:␣
 ↪(332317604805146238872636848439026671677842201913372686295652865759162799532 54,␣
 ↪681831695414564931196287396659794328964465698752923913656854786391324643506 46)

tx:1
sender: 1af3ce0358a2ea22b22eeee4a8fc6b5d5486c34f4a49c32735097c13695a5475
hash: c329e79c7f62948537e816221bc8ae9a7e650a30b13c36aaf6fd5443324482d1
consumed coins: block - 0, tx - 0, amount - 15
receivers:
account: 9e32ec30b364b982652b3591eba952bf8eb54f25188e62880c8c2256e4d503e6, ammount: 15
signature:␣
 ↪(761824282572317469714378873408881022265542648147360796726076168330504645260 94,␣
 ↪172095887096112703309446574448800117354297565547424777525424664060517785360 82)

User 5 made an attempt to send already spent 15 coins to User 2.

The transaction was discarded: double spending!

The balances of the users after transaction:
User 0 : 10
User 1 : 35
User 2 : 25
User 3 : 25
```

```
User 4 : 0
User 5 : 0
User 6 : 0
User 7 : 0
User 8 : 5
User 9 : 5

Display block 1.

block:1
previous hash:2db0fcbfe0a94e326826fb6cb09b7223152beb9896731f799d0af0424ce19208
signature:
 ↪(319872411875032877473078750938317819546390305699948447354794333667337386740 61,␣
 ↪105243610268469471027690773662487077685817088877514768713424717995027981033 31)

tx:0
sender: c3652c4cfa03e61850b8c82e95af9154b712593033aba8df31d73a4820ccb5f3
hash: a39c0c421a96a9b12c1ba5fb0f051448699c1d8c82fc07a643404ab1432e81b7
consumed coins: block - 0, tx - 0, amount - 50
receivers:
account: c3652c4cfa03e61850b8c82e95af9154b712593033aba8df31d73a4820ccb5f3, ammount: 25
account: 98afaad83ef0b515acf928acf1c6e872a81b4b9df6c47d617991d7923d59ef29, ammount: 25
signature:␣
 ↪(332317604805146238872636848439026671677842201913372686295652865759162799532 54,␣
 ↪681831695414564931196287396659794328964465698752923913656854786391324643506 46)

tx:1
sender: 1af3ce0358a2ea22b22eeee4a8fc6b5d5486c34f4a49c32735097c13695a5475
hash: c329e79c7f62948537e816221bc8ae9a7e650a30b13c36aaf6fd5443324482d1
consumed coins: block - 0, tx - 0, amount - 15
receivers:
account: 9e32ec30b364b982652b3591eba952bf8eb54f25188e62880c8c2256e4d503e6, ammount: 15
```

```
signature:␣
↪(76182428257231746971437887340888102226554264814736079672607616833050464526094,␣
↪17209588709611270330944657444880011735429756554742477752542466406051778536082)

* Test 3: mine an invalid transaction where the total amounts of the in and out coins do␣
↪not match.

User 0 sent 8 coins to User 1 (while the input amount was 10 coins).

The transaction was discarded: the amounts of input and output coins do not match!

The balances of the users after transaction:
User 0 : 10
User 1 : 20
User 2 : 0
User 3 : 50
User 4 : 0
User 5 : 15
User 6 : 0
User 7 : 0
User 8 : 5
User 9 : 5

Display block 1.

The requested block does not exist on the chain.

* Test 4: mine an invalid transaction where the signature is forged.

Somebody sent 10 coins to himself, pretending to be User 0, but the signature was␣
↪incorrect.

The transaction was discarded: signature is invalid!
```

```
The balances of the users after transaction:
User 0 : 10
User 1 : 20
User 2 : 0
User 3 : 50
User 4 : 0
User 5 : 15
User 6 : 0
User 7 : 0
User 8 : 5
User 9 : 5

Display block 1.

The requested block does not exist on the chain.
```

5. References

1. Y. Doroz. ECE 579B: Blockchain and Cryptocurrencies: Assignment 1. Worcester Polytechnic Institute, 2020.

2. S. Goldfeder, J. Bonneau, A. Miller, A. Narayanan, E. Felten. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. United States: Princeton University Press, 2016.