

# **Blockchain Project-1**

**Authors: Hemanth Vasireddy, AAKASH MALEPATI**

**Platform Used: Python 3**

## **Requirements**

1. Python
2. Pip

Pip installation:

Pre-requisites: Python should be present on the system and added to path

1. Open cmd
2. Type the command `curl https://bootstrap.pypa.io/get-pip.py -o get-pip.py`
3. Now type `python get-pip.py`
4. A message will be displayed as Successfully Installed pip.

## **Steps for execution**

Give the below commands in the cmd

1. Go to the location of the file.
2. `pip install ecdsa`
3. `python3 application.py`

## **Contents of the file**

`__init__.py`

`application.py`

`Block.py`

`Blockchian.py`

`Pool.py`

`scratch.py`

`Transaction.py`

`User.py`

## **Code Flow:**

1. Creating an initial transaction for genesis block.
2. Adding multiple transactions to genesis block.
3. Creating a genesis block.

#### 4. Mining genesis block.

```
Mining Genesis Block
=====
Transactions:
[<Transaction.Transaction object at 0x0000013CC4311750>, <Transaction.Transaction object at 0x0000013CC4311750>,
<Transaction.Transaction object at 0x0000013CC4311750>, <Transaction.Transaction object at 0x0000013CC4311750>,
<Transaction.Transaction object at 0x0000013CC4311750>, <Transaction.Transaction object at 0x0000013CC4311750>,
<Transaction.Transaction object at 0x0000013CC4311750>, <Transaction.Transaction object at 0x0000013CC4311750>,
<Transaction.Transaction object at 0x0000013CC4311750>, <Transaction.Transaction object at 0x0000013CC4311750>]
Previous Block Hash:
0
Merkle Root:
c686bdf823609102853c411c11ae57594f38b9bc83b433c66a7f7e394bbdd0c
Nonce:
74548
Hash:
000095465bc7d5348320e900a1333e79f7f4b7d76661c56c2906a7070e829170
```

#### 5. Creating a blockchain with the genesis block.

```
Displaying the Blockchain
=====
Block Hash: 000095465bc7d5348320e900a1333e79f7f4b7d76661c56c2906a7070e829170

Printing the balance
=====
100000000
```

#### 6. Creating the users.

#### 7. Using dictionaries to create user objects.

```
Creating user object
=====
<User.User object at 0x0000013CC4311C90>

Adding user to the dictionary (Structure created in User.py file
=====
Making transfers from user0 to all users
The transfers won't be immediately reflected in the receipt's wallet as the block is not yet mined
=====
Inside pay function
Collected the required transactions from wallet...
[[VerifyingKey.from_string(b'\x02\xc5\xbd\x1e\xea\x81(\x17\xbd\xc6\xa1\xd9\x14r\x84&g\xb7\xe2\xe0\x86R\x89\x1c\xfb\x0b\x8f\xac\xef\x8e\xfbvG', SECP256k1, sha1), 1000], [VerifyingKey.from_string(b'\x02u\xfa;\xba\xb2\x0c\xa7\x00(\x1a\x9f\xfd\xa9s\xfb\x16\x02\x0fS\xc1\xe2\x08/\xb7\x96<\xc4\x93c&\x95', SECP256k1, sha1), 49999000]]
Adding transaction to the pool.....
Added Transaction to the pool
```

8. Making initial transfers.
9. Making transfers between users.
10. Displaying wallets every time a transfer happens.

```

payment 1 successful
=====
user1's wallet:
-----WALLET-----
Total available balance is : 0
Change that will be recieved after mining the next block : 0
PENDING Transactions-----
Total Processing balance is : 0

user0's (Genesis) wallet:
-----WALLET-----
9ee5ae256275a30da18e5e3a19f9836946ed7133dc5c443d734c40cd1c1813f755bc8ae62f2f377a98f86111c70210aa2cc72bd2ced546e
ec54cb26f978e9424 10000000
9ee5ae256275a30da18e5e3a19f9836946ed7133dc5c443d734c40cd1c1813f755bc8ae62f2f377a98f86111c70210aa2cc72bd2ced546e
ec54cb26f978e9424 10000000
9ee5ae256275a30da18e5e3a19f9836946ed7133dc5c443d734c40cd1c1813f755bc8ae62f2f377a98f86111c70210aa2cc72bd2ced546e
ec54cb26f978e9424 10000000
9ee5ae256275a30da18e5e3a19f9836946ed7133dc5c443d734c40cd1c1813f755bc8ae62f2f377a98f86111c70210aa2cc72bd2ced546e
ec54cb26f978e9424 10000000
9ee5ae256275a30da18e5e3a19f9836946ed7133dc5c443d734c40cd1c1813f755bc8ae62f2f377a98f86111c70210aa2cc72bd2ced546e
ec54cb26f978e9424 10000000
Total available balance is : 50000000
Change that will be recieved after mining the next block : 49999000
PENDING Transactions-----
9ee5ae256275a30da18e5e3a19f9836946ed7133dc5c443d734c40cd1c1813f755bc8ae62f2f377a98f86111c70210aa2cc72bd2ced546e
ec54cb26f978e9424 10000000
9ee5ae256275a30da18e5e3a19f9836946ed7133dc5c443d734c40cd1c1813f755bc8ae62f2f377a98f86111c70210aa2cc72bd2ced546e
ec54cb26f978e9424 10000000
9ee5ae256275a30da18e5e3a19f9836946ed7133dc5c443d734c40cd1c1813f755bc8ae62f2f377a98f86111c70210aa2cc72bd2ced546e
ec54cb26f978e9424 10000000
9ee5ae256275a30da18e5e3a19f9836946ed7133dc5c443d734c40cd1c1813f755bc8ae62f2f377a98f86111c70210aa2cc72bd2ced546e
ec54cb26f978e9424 10000000
9ee5ae256275a30da18e5e3a19f9836946ed7133dc5c443d734c40cd1c1813f755bc8ae62f2f377a98f86111c70210aa2cc72bd2ced546e
ec54cb26f978e9424 10000000
Total Processing balance is : 50000000

```

11. Each block is mined after 4 transactions are happened

## 12. Printing all blocks

```
Printing Blockchain
=====
Block Hash: 000095465bc7d5348320e900a1333e79f7f4b7d76661c56c2906a7070e829170
Block Hash: 0000c6a7bcf3cfb0934728e400d63e1b085c4953a8c8cb8d5f44713348448f8a
Block Hash: 00000ce756824dc9ef763351be7864ed390fb79a4a1fa99dee3ac932f3d86058
Block Hash: 0000e7650aad709950cf16964eb86799dbdca663a877b60dbfeaafa67c04b777

Printing all Blocks...
=====
Transactions:
[<Transaction.Transaction object at 0x0000013CC4311750>, <Transaction.Transaction object at 0x0000013CC4311750>, <Transaction.Transaction object at 0x0000013CC4311750>, <Transaction.Transaction object at 0x0000013CC4311750>, <Transaction.Transaction object at 0x0000013CC4311750>, <Transaction.Transaction object at 0x0000013CC4311750>, <Transaction.Transaction object at 0x0000013CC4311750>, <Transaction.Transaction object at 0x0000013CC4311750>]
Previous Block Hash:
0
Merkle Root:
c686bdbf823609102853c411c11ae57594f38b9bc83b433c66a7f7e394bbdd0c
Nonce:
74548
Hash:
000095465bc7d5348320e900a1333e79f7f4b7d76661c56c2906a7070e829170
```

## 13. Wallets are updated once a block is mined.

```
user0 Balance : 9994000 Processing Balance : 0 change due : 0
user1 Balance : 1000 Processing Balance : 0 change due : 0
user2 Balance : 1000 Processing Balance : 0 change due : 0
user3 Balance : 1000 Processing Balance : 0 change due : 0
user4 Balance : 1000 Processing Balance : 0 change due : 0
user5 Balance : 1000 Processing Balance : 0 change due : 0
user6 Balance : 900 Processing Balance : 100 change due : 0
```