**Vid 74 – Assignment 4: Blockchain branching**

Clean up tasks 🡪 joining to a non-head node, which is necessary because we have miners that are receiving new blocks at different places

The wallet is storing a Blockchain. Let’s say then a wallet receives (from a miner) the block on top, which doesn’t fit on the end of the head node. Need to be able to add these because it could be that this will soon become the longest



Stopping the miner and then create a brand-new block that will attach NOT to this head node but to a block further back in the chain (0:00 – 1:10)

1:50 - 6:00 🡪 Failing to Add Sister Block

Graphical user interface, text, application

Description automatically generated

7:48 🡪 Creating Genesis.dat making a copy of WalletBlocks.dat and renaming that copy to Genesis.dat

supposed to ensure that the wallet and miner can always get back in sync

**Vid 75 – Assignment 4: Solution**

Reviewing walletServer function 🡪 and how the new block added to the longest chain becomes the new head block and the previousBlock is removed as the head block (0:00 - 1:45)

A screenshot of a computer

Description automatically generated with low confidence

This code just adds sister blocks over and over

Text

Description automatically generated

Correct output for the wallet 🡪 last time I had correct balances was before started adding to a branch chain!!

Text

Description automatically generated

**Vid 76 – Assignment 5: Replay Attacks**

Avoiding Duplicate Transactions (separates ETH from BTC)

We’re playing the role of the hacker, one of the ways to do this is by creating duplicate txs

Miner opens the server connection, received txs from wallets, If it finds an actual tx it appends it to the tx list

Text, application

Description automatically generated

10:50 🡪 when this is true (when its my own address) then not this is gonna be false. When this is NOT true (if its not me) then send it to the port.

15:10 🡪 Output

Text

Description automatically generated

Professors Output

Graphical user interface, text, application

Description automatically generated

**Vid 77 – Assignment 5: Solution**

Ethereum calls this the tx nonce, which is just the index of the tx

Text, letter

Description automatically generated

Our wallet should be keeping track of these tx\_inx

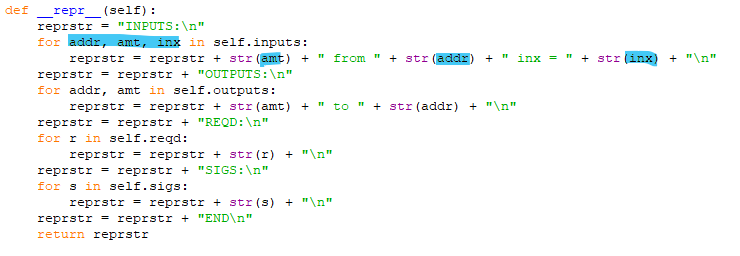
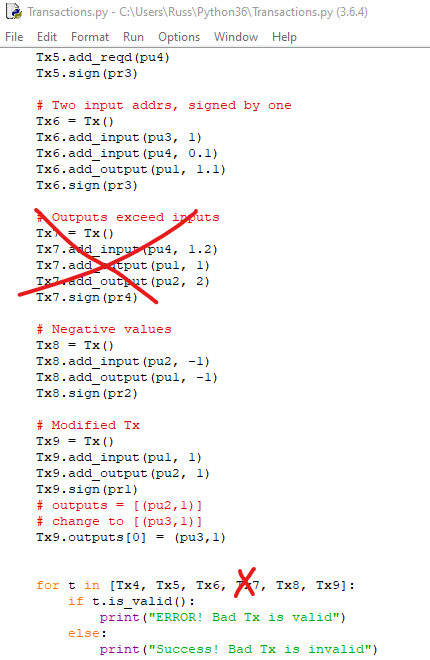
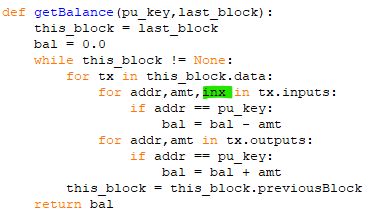
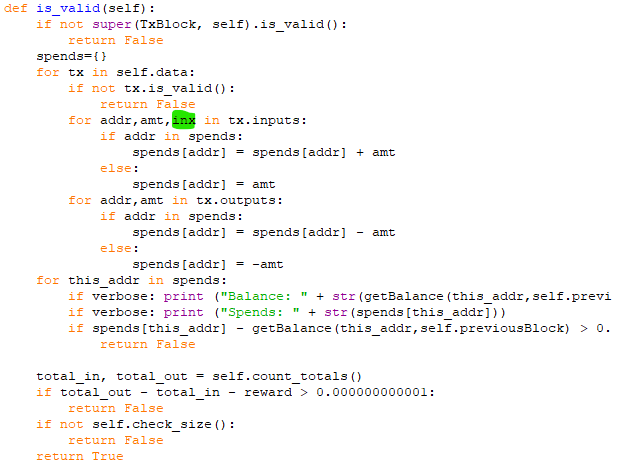
Graphical user interface, text

Description automatically generated

Correct Output for Transactions

Graphical user interface, text

Description automatically generated



Getting rid of Tx7 B/c the outputs can exceed inputs, this is actually the responsibility of the miner (before 8:13)

Only TxBlock needs to worry about these indices actually being passes in the right order

9:05 – 9:45 🡪 adding to is\_valid in TxBlock

getLastTxIndex 🡪 function that looks back thru the blockchain and finds the last tx that includes this addr as one of the inputs

A picture containing graphical user interface

Description automatically generated

10:30 🡪 Creating function getLastTxIndex under balance

**Vid 78 – Approaches to Replay Attacks**

How do Blockchains avoid these duplicate transactions?

* Account Balance method (ETH)
  + Involves additional transaction index



* UTXO – Unspent Transaction Output method (BTC)
  + Rather than keeping track of the balances of specific addresses it keeps track of unspent transaction outputs (which means they know the amt in them and know what public key that controls them)

1:00 – 3:30 🡪 explanation of the UTXO method

A screenshot of a computer

Description automatically generated with low confidence

3:30 – 4:20 🡪 UTXO w/ 3 transactions

Graphical user interface

Description automatically generated

4:29 – End 🡪 Advantages and Disadvantages

Graphical user interface, text

Description automatically generated

**Vid 79 – Assignment 6: Multiple Miners**

* Task: keep the miner blockchain up to date
* Must consider the blocks that are mined by other miners
  + Need to have a way for those blocks to also get into the blockchain that is maintained inside our miner

Diagram

Description automatically generated

Many miners can send blocks to our miner and we need to take those blocks and add them to our internal blockchain

* Remove from the tx\_list 🡪 any txs that were included in this miner
* Remove duplicate indices that I see are already in other txs

Diagram

Description automatically generated

Task 1 🡪 we’re going to receive some blocks from another miner and were going to have to remove the transactions in this block from our transaction list so we don’t duplicate

1:30 🡪 Starting Assignment creating the test case