

Sodiq Baruwa 8688155

MINER ID: sbaru060

-Transaction.java

This class is used to record the key details of the transaction that takes place; the sender , the receiver and the amount of bitcoin being transferred. The constructor takes in three parameters (bitcoinExcahnged-> amount, from -> sender, to ->receiver). The class also has getter methods for the sender, receiver and the amount. Finally the class implements a toString() method where the transaction information is printed to the console .

-Block.java

This class is used to record the key details of every block that gets added to the blockchain. In addition to storing information from the transaction class, it also stores the timestamp, the index, the nonce, the previous hash and the hash along with their respective getter methods.

The myNonce() function generates the nonce-> this is explained further below in the proof of work description section

The class also has a toString representation.

-Blockchain.java

This class contains the main() function. It uses a scanner to prompt the user to make transactions and if it's a valid transaction that gets added to a block chain; It will save the it into a new text file.

This class has fromFile{this basically uses a buffered reader to get the individual values from the text file and put it into a block} and toFile methods which reads and write to the file;

This class has a validate method which checks all the hashes by making sure they correspond to the values in the corresponding block. It makes sure the index and previousHash attributes are consistent. Finally it makes sure each sender can only transfer bitcoins if they have enough bitcoins to make the transaction

This class has a getBalance() method that returns how much bitcoins is leftover after each transaction

This class has an add() method which adds a block to the blockchain created in the constructor.

-Proof of work description

The poof of work is essentially the mechanism used to create the nonce, it uses a random generator along with a for loop to generate a hash (this hash needs the first 5 values to be zero). The hash() method from theSha1 class takes in the toString() method from the Block class as an input parameter.

Below is a table that shows for each transaction (these are the transactions after the original three transactions that was given to us initially), and the second column is it's corresponding number of trials before the nonce is found.

Instance of transaction	Number of trials
3	1280784

4	702705
5	3267677
6	1985229
7	34492256
8	54694
9	12919
10	931608
11	4536992
12	6456825
Average	5372168.9