BlockChain Report

Miner ID: xzhou086

Descriptions:
Sha1 is a given Class that calculates hash.

Transaction Class has information of sender, receiver and amount.
The methods in side the class are its constructor and getter methods.

Block Class has index, timestamp, transaction, nonce, previousHash and hash.
The methods are 2 constructor, getter methods and reneNonce(). It needs 2 constructors because one is to initialize all variable and the other one has no nonce. The one with no nonce is used to be called from main and create a block without knowing the nonce.and then after generating a new nonce, the first constructor will be called. The use of reneNonce will be in description under how to generate nonce.

BlockChain uses an arraylist (blocks) to store the blocks.
-It has contractor and getter method.
Method:
- fromFile(String filename) read information from a file with given file name
- toFile(String filename) write the information into a file with a given file name
- validateBlockchain() checks if the blocks in a blockchain is valid. Index should be in order. Previous hash should be the same as the hash of previous block.
-There are 2 getBalance() method, but with different parameters. The one with (String username) is to get balance of after transaction. The method with (String username, int size) is to get the balance right up to the size needed.(right up to whatever number transaction)
- add method adds the given block into blockchain
- The main method asks the user to input data and adds into blockchain or if the user choose to only validate without adding any data(this is used to validate other miner's work).

How to generate a new nonce:
The method is called reneNonce() in Block class.
The variable "select" includes all the keyboard input and a random character is choose from there. Use java.util.Random and generates a random character each time the loop runs. The loop also runs random time so that the length of nonce is random(between 1 to 15).It will keep regenerating until hash starts with 00000. The if statement checks if hash starts with 5 zeros by using substring and compare it to first 5 characters of hash.

Name: Amy Zhou
Student ID: 300018781
CSI2110 (A)

Statics Table

# of transaction	#of trials for hash	nonce	hash
1	2483009	8uEs	00000e0ddd7a53ea38a0e197df10e5a7ca3fee3c
2	322464	MMZREJs,sUR	000004dfffc4bc18ea4070c94ce5106a08232e29
3	813563	.3UIwGku	000009ba008513760f39a635c8b05881326bc602
4	951798	T@Yf0+cN3	000008b37c05146c5346a32a4f2b65b436b70c7e
5	1794003	1b_Q5*.!3&	00000c8d3f0860470b0fc4e9a6f3f09453ac558d
6	177968	bu?3dPw+x-0m43@	000000c0aff4435c02c9ebb87e1f53d97660f058
7	2127295	KT1	00000e3c4ccbfc15ef57b8a1d12af7c5e50e487a
8	638745	Kd3L%J	00000cb9fff3ff326ee7840faa0b4a3187bec99d
9	299224	fVLB	0000030a2325343b98934fbed67da34d0ccb427b
10	2254065	YIjS4GrQ0ycUHO	00000ee75426570612c815820ed3ee83b182a47f

Average trials: 1024753.4