PROJECT 4.1
README
DISTRIBUTED OPERATING SYSTEMS PRINCIPLES
COP 5615

Group Info:

	Name	UFID
1.	Manishkumar Chopra	17967121
2.	Nimish Kochhar	61394423

What is working:

From the bitcoin protocol, we have implemented the following:

1. Creating a blockchain with a Genesis block - A blockchain with just the starting block
2. Calculating the block's hash - Block's hash need to be calculated to verify the integrity of the block
3. Adding pending transactions - Blockchains have pending transactions that are added every time a new block is mined
4. Mining the block - Miners need to show the proof-of-work to mine a block
5. Mining rewards - The reward a Miner gets to mine a block
6. Allowing to pay a fee with the transaction - This fee is received by the miner in addition to Mining rewards, making it more lucrative to include a particular transaction for mining
7. Mining difficulty - Kept the difficulty low so that the coins can be mined very fast
8. Creating transactions - Single input, single output transactions
9. Transacting bitcoins - Transfer of bitcoins from one wallet to another
10. Signing transactions - Making sure that the client signs for its own wallet and nobody tampers with a transaction
11. Calculating the balance in a client's wallet - Making sure the amount sent, amount received, mining rewards and fee received are taken into account
12. Checking the validity of the transaction - Check if it's not tampered with and is properly signed
13. Checking the validity of the blocks - Check if the block's untampered and all the transactions in it are valid
14. Checking the validity of the blockchain - Make sure all the blocks are valid in the blockchain and all the blocks are in the correct order. Also make sure that the hash of the current block is the previousHash of the next block
15. Calculating the Merkle tree root - It which will be sent later in the block header to other peers to ensure that the transactions list has not been tampered with

We have also implemented unit and functional tests to check the validity of our coin. They are named as:

1. Creates a blockchain - Verifies if the blockchain is properly created with the right parameters and the Genesis block.
2. Creates a block - Checks if the new block's parameters are correct
3. Creates a transaction - Checks if the new Transaction has all the right parameters
4. Invalid Transactions check - Checks if all the different ways an invalid transaction can exist are identified. They can be transactions without from and to address, there can be transactions without signature, there can be transactions with false signature or there can be transactions where the sender doesn't have enough balance
5. Invalid Block check - Verifies that the block's new hash is not the same as its currentHash if the block is tampered with
6. Invalid Blockchain check - Verifies that any change in a block or a transaction invalidates the blockchain. This check will be used in the distributed system by the nodes to reject an attacker's attempt to tamper with the chain
7. Hashing check - Makes sure that the hashes stored in the blocks and the hashes calculated for the transactions are valid and are calculated properly
8. Basic functionality test with wallet - A dummy scenario in which client1 mines a block to receive mining reward. Client1 then sends 10 coins to client2 with 10 coins as fee. Client1 then tries to send another 100 coins to client2 but receives a response saying there isn't enough balance to perform this transaction. Client1 then sends 50 coins to client2. Client3 mines these transactions and receives the reward with the fee. In the end, we make sure that every wallet has the right amount of balance. Client1's wallet has 30, Client2's wallet has 60 and Client3's wallet has 110 coins

How to run the program tests:

Unzip bitcoin.zip, cd into bitcoin folder
then run the project tests by typing on the terminal:
mix test

NOTE: This project is still a work in progress so only the unit and functional tests can be performed using the above mentioned directions

Bonus Part:

We have implemented more features than required to perform the basic operations like mine bitcoins, implement wallets (enough to get the other goals) and transact bitcoins. Explanations for all these features are mentioned in the "What is working" section above. They are:

1. Signing transactions
2. Calculating the balance in a client's wallet
3. Checking the validity of the transaction

4. Checking the validity of the blocks
5. Checking the validity of the blockchain
6. Calculating the Merkle tree root
7. Allowing to pay a fee with the transaction