**Blockchain Assignment 1**

**Ajjarapu Jyothi**

**m22cs007**

**Process of execution:**

1. We require postman and spyder and mongodb to execute these files.

2. Firstly, I have created an account in mongodb and set the ip address in the network access tab to 0.0.0.0/0, then proceed to database connect option, set the platform to python, as I am using python and version as 3.6 or later. We get a URL from here.

My URL is: mongodb+srv://Jyothi:jyothi123@cluster0.t5qddp4.mongodb.net/?retryWrites=true&w=majority

3. I have created the mongodb.py file, where I used this URL and wrote the code to store my block chain data.

4. Created a privpubkey.py file, which generates the public, private keys using rsa techniques.

5. Now created the 1stnode.py and 2nd node.py files. When we run them, we get a link in the output.

6. copy the link and open the postman app.

7. Paste this link with a forward slash in the bar, and start to give the function names there. Use get method. Since we need the output in the postman.

8. This will give us the output based on the code used.

9. If we need to send some data to the console, we use post method there.

10. Thus we can mine the block chain based on the nodes created. It displays if there are any errors in the function being used.

**Brief about the assignment:**

I am using Spyder interface and postman to execute the assignment. Initially, we have to import all the libraries. We require pymongo, since I am using mongodb to store the blockchain data. And we need other libraries like datetime, hashlib, json, flask,uuid etc. Hashlib is used to generate the hash, here we are using sha 256.

I am generating public and private keys using the rsa encryption technique. This is a separate file. And I am using mongodb to store the data. So I created a separate file, which stores the database information. I have posted the url of my mongodb database. In this file, I have created four functions, which are used to insert the data into the block chain, mongodb database, print the block chain and deleting the chain.

Now, I have imported both these files along with the libraries to create another file, which is used to create the node in the chain. This file has all the functions that are required to create the block chain, mine and decentralize the chain. A block contains: index, timestamp, proof, merkelroot, previous hash and transactions. And the hash to the transactions is also added , that hash is generated from the sha256 algorithm. Here I am using “proof of work” consensus algorithm. It sets the hash operation to be:

hash\_operation = hashlib.sha256(str(new\_proof\*\*2 - previous\_proof\*\*2).encode()).hexdigest()

Later, It checks if the hash operation has four zeroes at the beginning of the hash, if yes, it sets the proof to be true.

Validating the block chain: It checks for the previous block hash and sees if its matching wih the current block previous hash field. And hash having four zeroes at the beginning of the block.

Adding a transaction: It adds the sender, receiver and amount information, and appends to the previous transaction.

Like this all the required functions are defined. And mining of the nodes is executed.