SRI SIVASUBRAMANIYA NADAR COLLEGE OF ENGINEERING, KALAVAKKAM

(An Autonomous Institution, Affiliated to Anna University-Chennai)

SSN – RESEARCH INTERNSHIP

JUNE 2021

FINAL REVIEW REPORT

SUBMITTED BY

INTERN NAME : B RAGAVAN

COLLEGE : INDIAN INSTITUTE OF INFORMATION TECHNOLOGY, DHARWAD BATCH NO : 18BCS016

PROJECT TITLE : BLOCKCHAIN FOR IOT

FACULTY MENTOR : Dr .V.BALASUBRAMANIAN

DURATION : 17-JUNE-2021 TO 15-JULY-2021

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

SRI SIVASUBRAMANIYA NADAR COLLEGE OF ENGINEERING

RAJIV GANDHI SALAI, KALAVAKKAM – 603 110

TABLE OF CONTENTS

Problem Statement :

A primary challenge for IoT players is to protect the information in the entire IoT ecosystem. Security vulnerabilities make IoT devices an easy target for distributed-denial-of-service attacks, malicious attackers and data breaches.

A blockchain's distributed ledger is tamper-proof, eliminating the need for the involved parties to trust one another. As such, no single party has control over the massive amount of data the IoT devices generate. Blockchain encryption makes it virtually impossible for anyone to overwrite existing data records. Using blockchain to store IoT data adds another layer of security to prevent malicious attackers from gaining access to the network.

The integration of IoT and blockchain opens the door for new possibilities that inherently reduce the inefficiencies, enhance security and improve transparency for all involved parties while enabling secured machine-to-machine transactions. The coupling of these technologies allows a physical asset to be tracked from the moment raw materials are mined, for example, and among every step of the supply chain until it is with the end consumer.

In this project, I have simulated the exact method of transferring data from one machine to another by creating blocks(which may be composed of many transactions) and transferring them after the process of encryption(using secure hash algorithm or SHA512 for creating hash digest of the data in the block) and sending them to other machine using a peer to peer connection. As a process of demonstration I have just considered the file with the IP addresses of the destination nodes to be the body of the blocks. But this can also be

extended to embedding the user's secret data(such as love letters, Bank transactions,etc) into the body.

Objectives :

1. Develop a simple and effective python package having the functionalities of a typical Blockchain framework (like Hyperledger).
2. Publishing the developed package in PyPI site.
3. Demonstrate the actual working of Blockchain platforms like Hyperledger, etc.

Technologies Used :

- Python
- Visual Studio Code

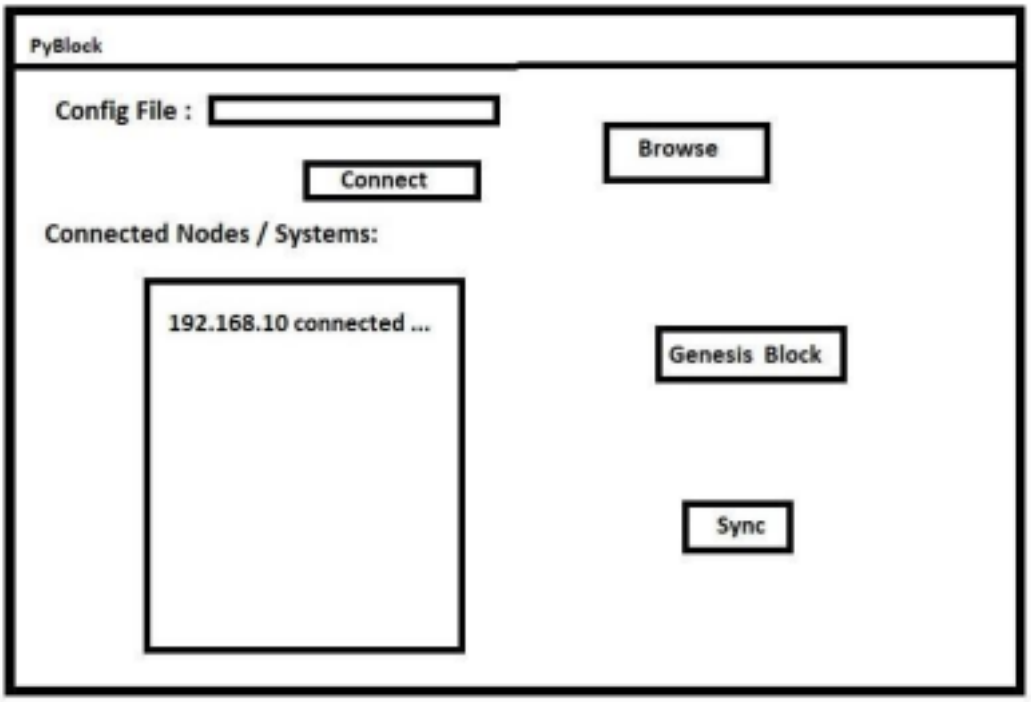
Methodology :

These are the features or methodologies implemented for the project:

1. Developing a Mesh like network (i.e. P2P) :

- This is the first part of our work which depicts a basic and simple peer-to-peer decentralized network class (framework) to build your own network. Basic functionality and Application specific functionality of the nodes and the connection to and from these nodes has been implemented. The intention of the module is to provide a good basis, without specific implementation, so everyone is really free to implement like they would like to do.

- The Nodes in the network are connected with each other. This means that each node provides a TCP/IP server on a specific port to provide inbound nodes to connect. The same node is able to connect to other nodes; called outbound nodes. When a node has a lot of connections with nodes in the network, the node will get most likely the required messages. You are able to send a message over the TCP/IP channel to the connected (inbound and outbound) nodes.



- As can be seen from the above diagram, we note that the system design should be in such a way that if we give a file(with the information about the respective IP addresses to establish a connection) in the Config File section and then click connect we get the output in the specified box once the peer to peer connection to the respective nodes have been established.

- Now when the Genesis Block button is clicked, the first block will be created by our python code and is broadcasted to all the nodes in the network. The nodes to establish communication can be decided by the user itself by modifying the sample1.txt file(file with all the destination IPs).

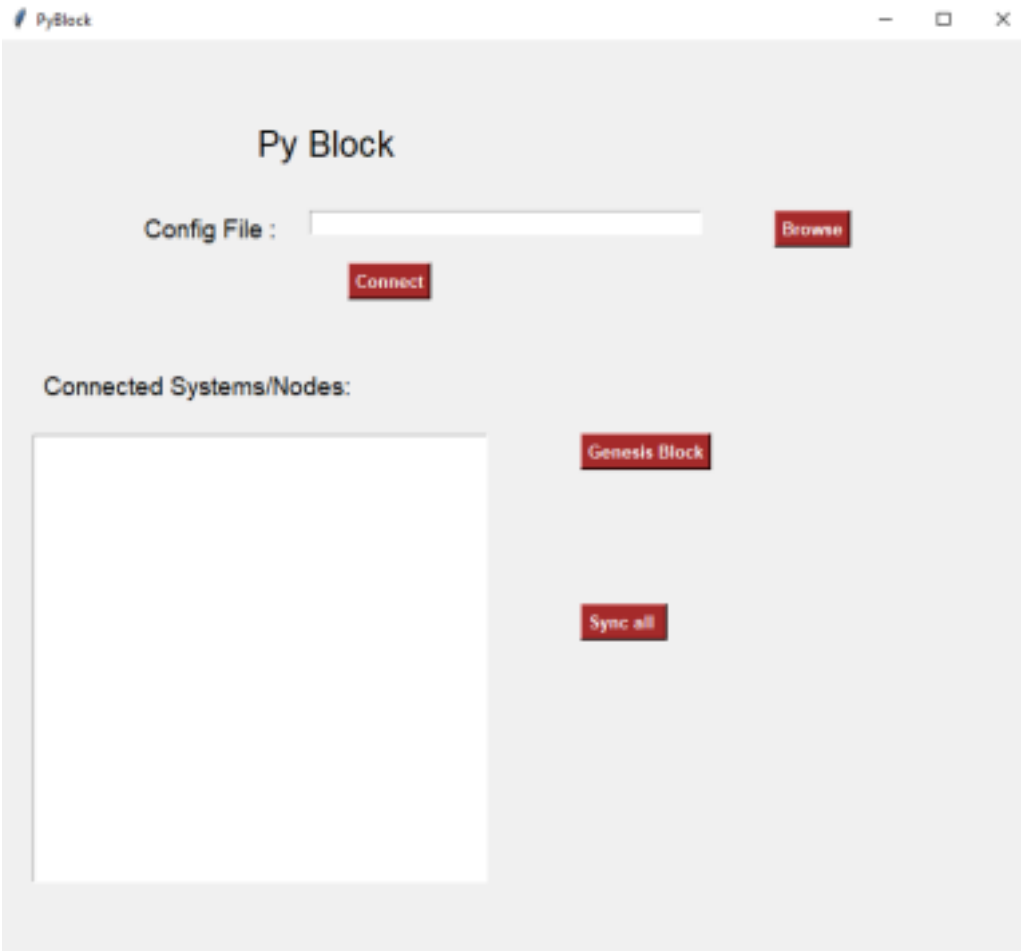
2. Initializing Genesis Block in all Peers / Nodes :

- The various blocks in the blockchain can be created as a list of dictionaries. The Genesis Block (also known as the first block in blockchain system) in our case has been created as a list [header ,body] to represent the two sections of the block in which the body is the **“** hash of the sample1.txt file **“** and the header is the “ dictionary composed of {BlockID,Timestamp,Previous Hash,Data Hash, Current hash(sha512(BlockID+timestamp+prevhash+datahash))} ”

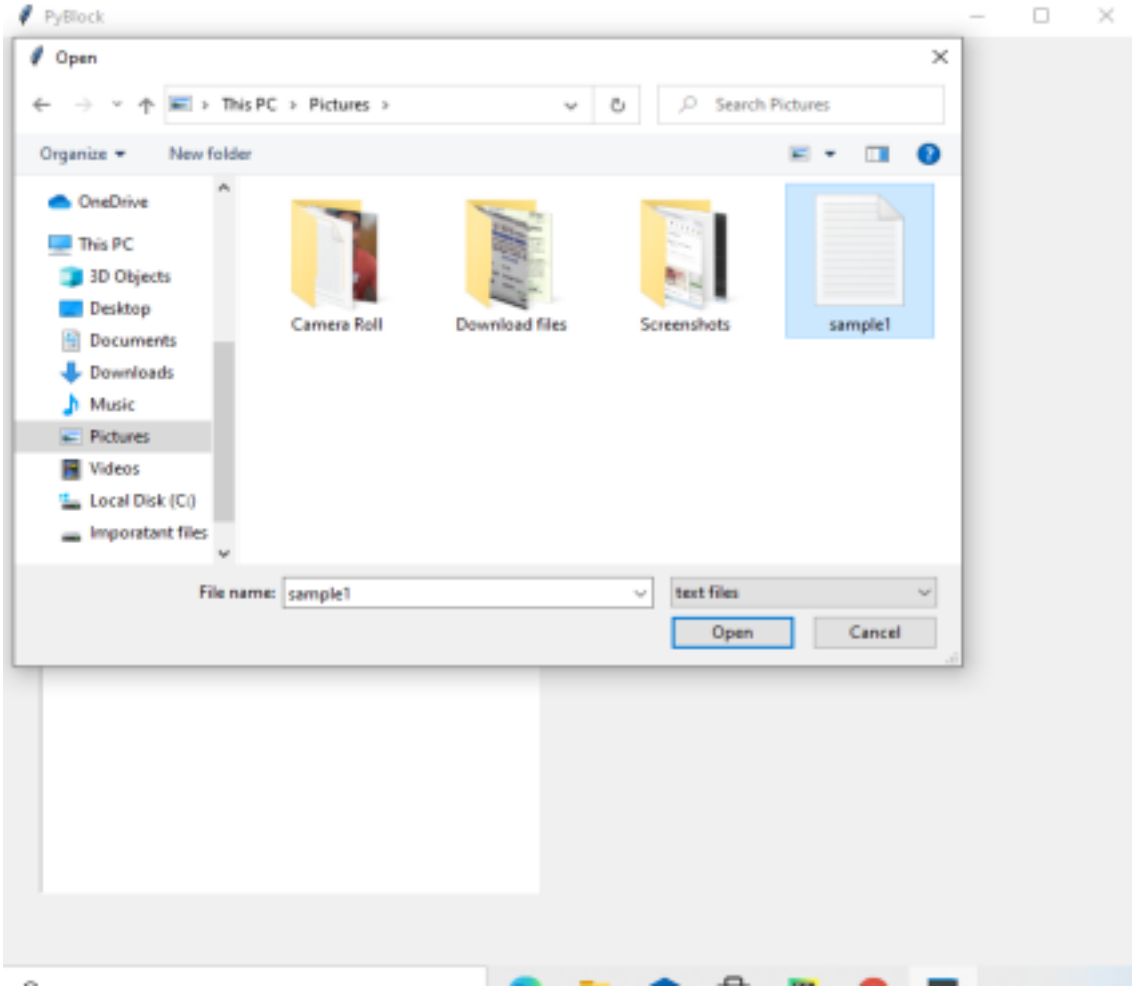
3. Performing Block creation and synchronizing with other Peers / Nodes.

- In this process more blocks are created after the creation of the first block and are linked to the hash of the previous block in a linked list fashion. Then these blocks are sent to the other nodes to which a peer to peer connection has been established.

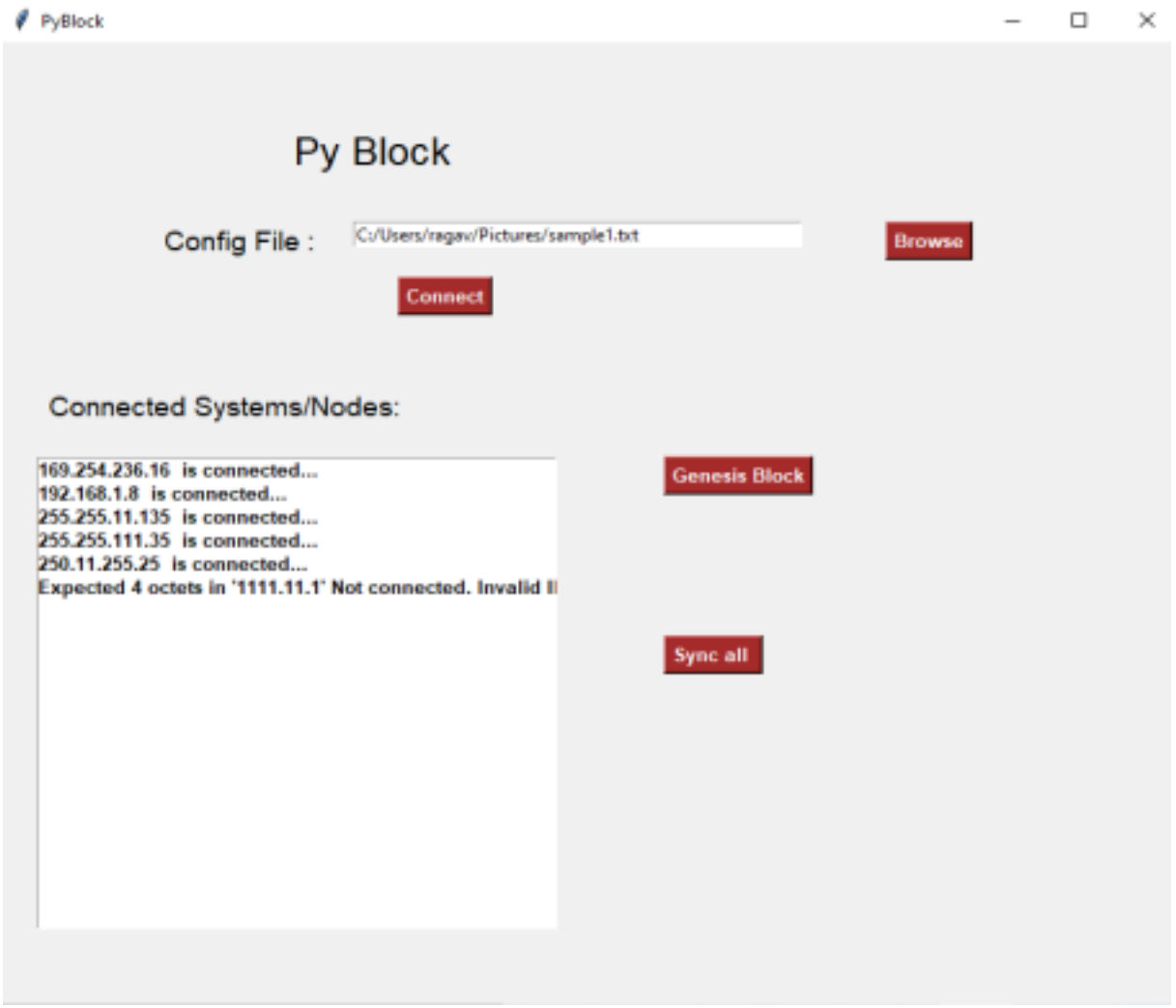
Screenshots :



Screenshot .1



Screenshot .2

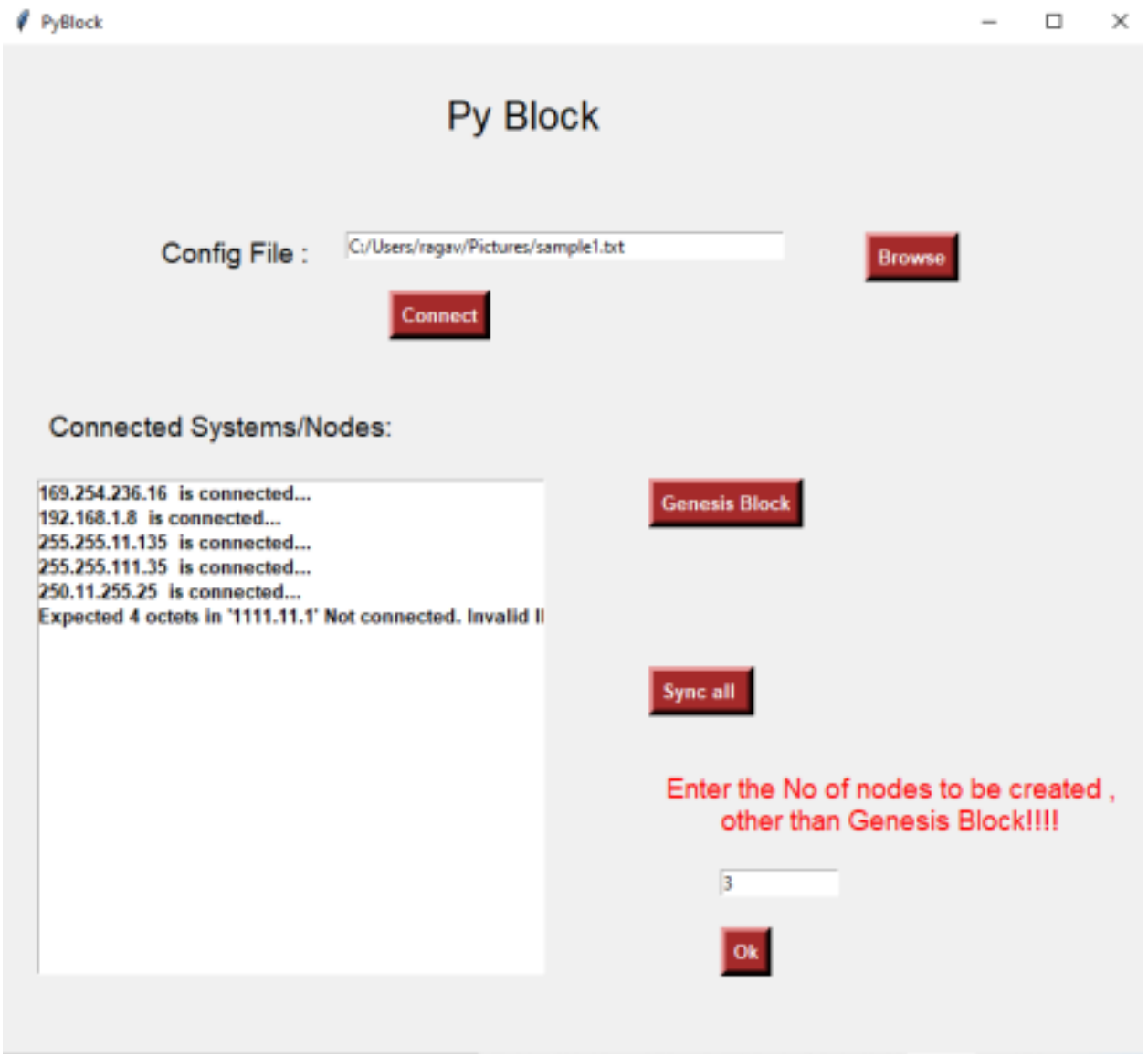


Screenshot .3

(We can see in screenshot.3 when you click the connect button it checks for all the valid Ip addresses and connects it to other Ip's .)

Screenshot.4

(These are the details of the Genesis block are displayed once the Genesis button is clicked.)



Screenshot.5

(In screenshot.5 when you click the button Sync all It requests the number of blocks other than the genesis block to be created and synced.)

Screenshot.6

Screenshot.7

Screenshot.8

References :

1. https://www.tutorialspoint.com/blockchain/index.htm
2. https://stackoverflow.com/questions/tagged/python

Result Analysis:

I found and explored how to connect peer to peer nodes and implement a small prototype of blockchain , its details and its functionalities in Iot devices.

Conclusion :

Blockchain technology has proven that it can assure the safety and security in Iot devices. And moreover this has paved a way for implementing blockchain principles in Iot devices. Further this will make a revolution in the future of Iot devices.