Blockchain Project Report

Cryptocurrency Using Python

April 21, 2022

Submitted By

Group Number: 16

Shivam- 1906070

Aman Kumar - 19060673

Raushan Kumar- 1906078

Shubham Shandilya- 1906069

Abhishek Jaiswal- 1906072

Under the Project Guidance of

Project Mentor

Dr. Ditipriya Sinha

Asst. Professor CSE Dept , NIT PATNA

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERINGNATIONAL INSTITUTE OF TECHNOLOGY PATNA

(An Institute of National Importance)

MAHENDRU, PATNA, BIHAR - 800005

Project Report

April 21, 2022

Table of Contents

1.Crytocurrency

A cryptocurrency is a digital or virtual currency that is secured by cryptography, which makes it nearly impossible to counterfeit or double-spend. Many cryptocurrencies are decentralized networks based on blockchain technology—a distributed ledger enforced by a disparate network of computers. A defining feature of cryptocurrencies is that they are generally not issued by any central authority, rendering them theoretically immune to government interference or manipulation.

1a- Key Features:

- DIGITAL OR VIRTUAL CURRENCY
- BASED ON BLOCKCHAIN TECHNOLOGY
- USES DECENTRALIZED NETWORK
- USES CRYPTOGRAPHY TO SECURE TRANSACTIONS
- DON'T HAVE AN CENTRAL ISSUING OR REGULATING AUTHORITY
- IT'S AN PEER TO PEER SYSTEM

1.b Crytocurrency Examples

- BITCOIN
- ETHEREUM
- LITECOIN
- RIPPLE

1.c Why Cryptocurrency

PARAMETERS	CRYPTOCURRENCY	FIAT CURRENCY
Generated	Cryptocurrency is generated over computers	Fiat currency is generated by means of government
Medium of Trade	Crypto is exchanged digitally	Fiat currency is exchanged physically
Presented	Crypto currencies are pieces of existing codes over the internet.	Fiat currencies are found in coins and notes
Supply	The delivery of crypto currency is restrained	The delivery of fiat currency is limitless
Controlled by	These currencies are not controlled by	These currencies are controlled by using

2.Blockchain Technology in Crytocurrency

A blockchain, originally block chain, is a growing list of records, called blocks that are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. Only blockchain can solve the challenges because of the characteristics of blockchain. The major characterizes of blockchain are:-

- **Immutability**: the creation of data records that are permanent (cannot be changed or deleted);
- **Traceability**: Using blockchain an item can be easily tracked to find the provenance in the transaction history.
- **Security**: Blockchain is considered to be a highly secure system due to its digital signature and encryption. The system is specially designed to be secure, convenient, and tamper-proof.
- **No Single point of failure**: The ledger is distributed across every single node in the blockchain who are the participants. So, it is distributed.
- **Fraud prevention**: Since various consensus protocols are needed to validate the entry, it removes the risk of duplicate entry or fraud
- **Transparency**: The transactions that take place are transparent. The individuals who are provided authority can view the transaction.
- **Smart Contracts(Chaincode)**: With the smart contracts, the businesses can pre-set conditions on the blockchain. The automatic transactions are triggered only when the conditions are met.
- **Time-stamping:** Every entry created in the blockchain is securely tracked with a time-stamp (Permanency makes backlogging impossible).

3. Implementation

3.a How to run it

First, install requirements.txt.

pip install -r requirements.txt
Then you have 2 options:

Run miner.py to become a node and start mining
Run wallet.py to become a user and send transactions (to send transactions you must run a node, in other words, you must run miner.py too)
Important: DO NOT run it in the python IDLE, run it in your console. The miner.py uses parallel processing that doesn't work in the python IDLE.

3.b How this code works

There are 2 main scripts:

miner.py
wallet.py
Miner.py
This file is probably the most important. Running it will create a node (like a server). From here you can connect to the blockchain and process transactions (that other users send) by mining. As a reward for this work, you recieve some coins. The more nodes exist, the more secure the blockchain gets.

miner.py has 2 processes running in parallel:

The first process takes care of mining, updating new blockchains and finding the proof of work.

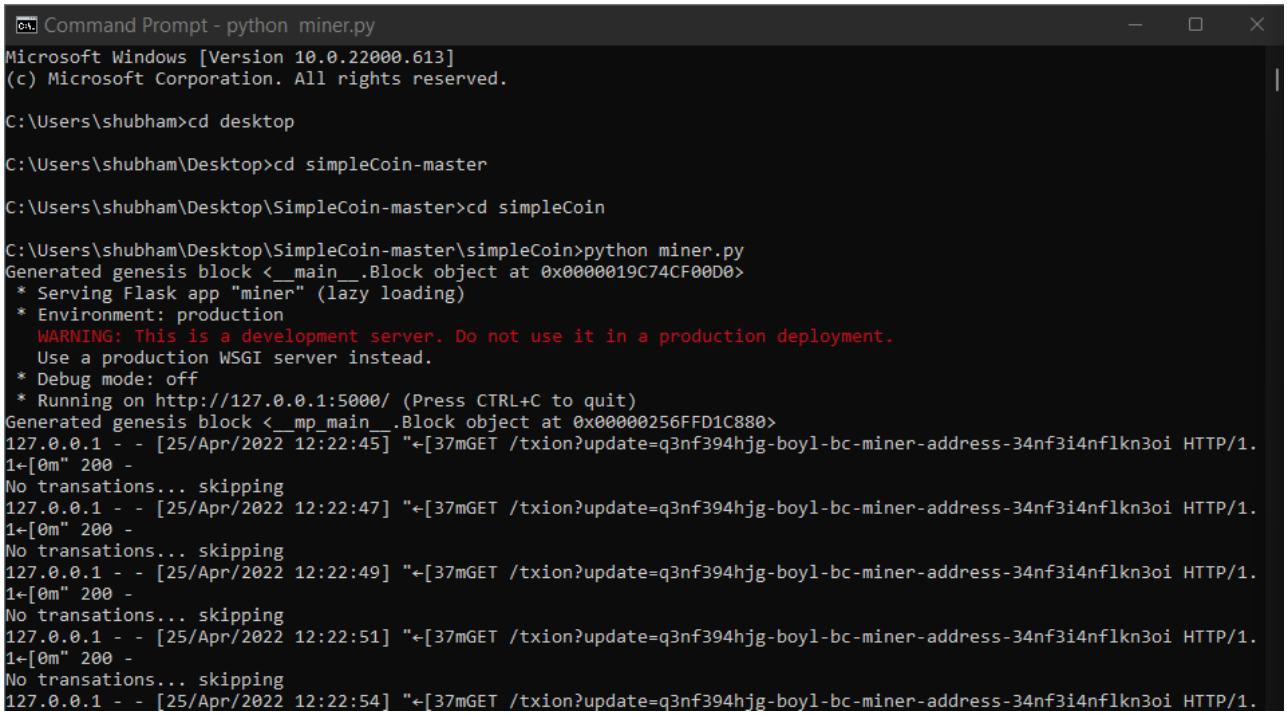
The second process runs the flask server where peer nodes and users can connect to ask for the entire blockchain or submit new transactions.

Wallet.py
This file is for those who don't want to be nodes but simple users. Running this file allows you to generate a new address, send coins and check your transaction history (keep in mind that if you are running this in a local server, you will need a "miner" to process your transaction). When creating a wallet address, a new file will be generated with all your security credentials. You are supposed to keep it safe.

3.c Working

3.c.a Running miner.py

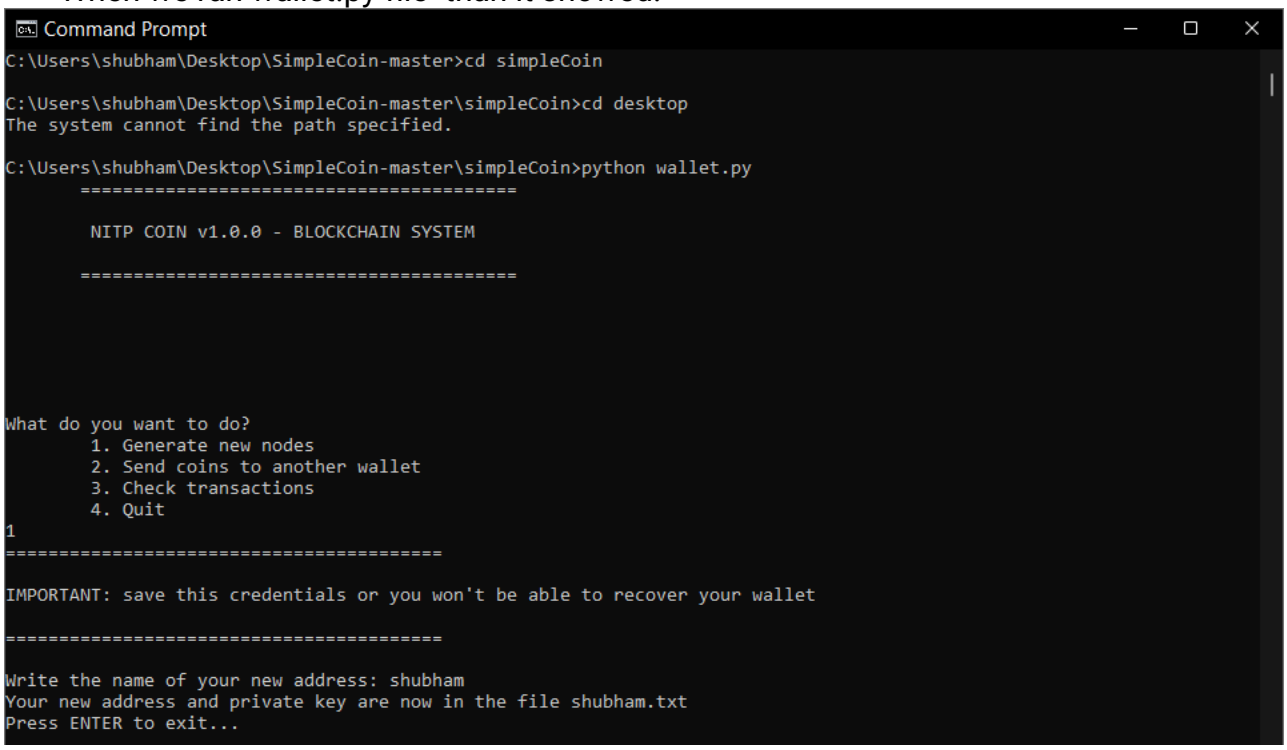
When we ran miner file using command “python miner.py” than it showed



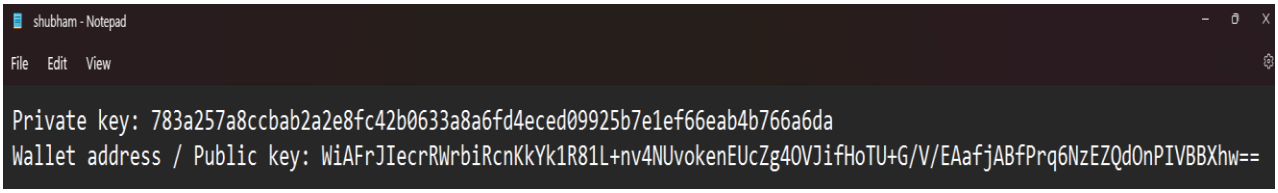
Initially when there was no any transaction in mempool than minor did not get any transaction to mine.so our program has showed “NO transaction… skipping”.

3.c.b Running wallet.py

When we ran wallet.py file than it showed:



when we entered "1" as input than it asked the name of the user after that we entered name "Shubham" then it created a file named Shubham.txt which contained public key and private key of the user.

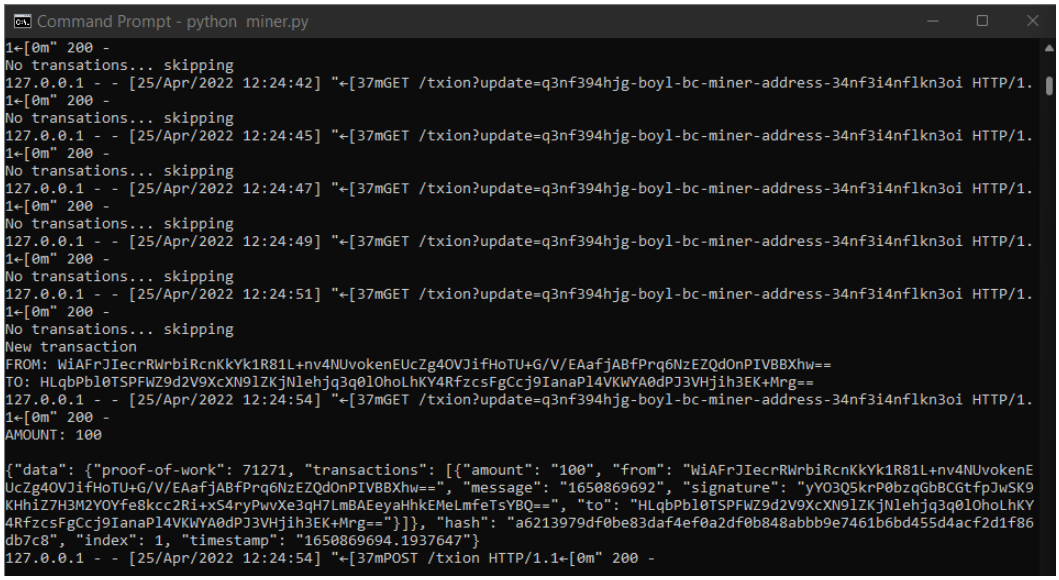


3.c.c Doing transaction:

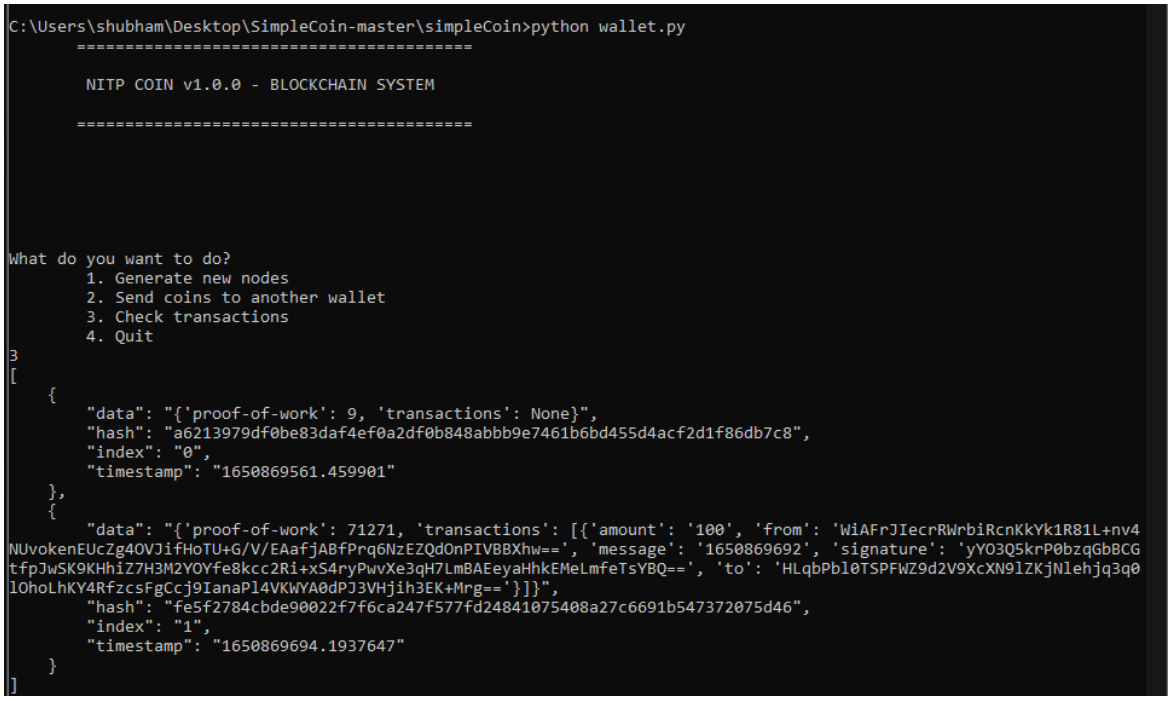
While doing transaction our program demanded public key and private key of the sender and also public key of the receiver wallet. It checked all the keys and did one transaction.

```
C:\Users\shubham\Desktop\SimpleCoin-master\simpleCoin>python wallet.py
       ========================================

        NITP COIN v1.0.0 - BLOCKCHAIN SYSTEM

       ========================================




What do you want to do?
        1. Generate new nodes
        2. Send coins to another wallet
        3. Check transactions
        4. Quit
2
From: introduce your wallet address (public key)
WiAFrJIecrRWrbiRcnKkYk1R81L+nv4NUvokenEUcZg4OVJifHoTU+G/V/EAafjABfPrq6NzEZQdOnPIVBBXhw==
Introduce your private key
783a257a8ccbab2a2e8fc42b0633a8a6fd4eced09925b7e1ef66eab4b766a6da
To: introduce destination wallet address
HLqbPbl0TSPFWZ9d2V9XcXN9lZKjNlehjq3q0lOhoLhKY4RfzcsFgCcj9IanaPl4VKWYA0dPJ3VHjih3EK+Mrg==
Amount: number stating how much do you want to send
100
========================================


Is everything correct?

From: WiAFrJIecrRWrbiRcnKkYk1R81L+nv4NUvokenEUcZg4OVJifHoTU+G/V/EAafjABfPrq6NzEZQdOnPIVBBXhw==
Private Key: 783a257a8ccbab2a2e8fc42b0633a8a6fd4eced09925b7e1ef66eab4b766a6da
To: HLqbPbl0TSPFWZ9d2V9XcXN9lZKjNlehjq3q0lOhoLhKY4RfzcsFgCcj9IanaPl4VKWYA0dPJ3VHjih3EK+Mrg==
Amount: 100

y/n
y
Transaction submission successful

Press ENTER to exit...
```

This transaction arrived in the mempool and miner mined it and added a block to the blockchain.



We can also see in the user transaction:



Results and Discussion

Blockchain provide transparency in the transaction. It is very disruptive technology.in this project ,we have created a cryptocurrency named NITP coin which is working based on blockchain technology implement in python high level programming language. We can also make this project more interactive using user interface.

Conclusion

Blockchain technology has many characteristics which may provide for further certainty over the contents which are to be stored in the land registry. Having a complete record is amust, as otherwise doubts and uncertainties will always be present. Thus, it is of utmost importance that a country's legislation requires that anything affecting property rights be recorded within the registry (regardless of the system used). This includes *inter alia* the recordation of property transfers, lease agreements, overriding interests, usufruct rights, etc. It is only after this is ensured that a blockchain-based land registration system would be able to provide us, with certainty, a true picture of what rights are held by a person (legal ornatural) over a specific property.

References:

1. https://github.com/cosme12/SimpleCoin
2. https://www.investopedia.com/terms/c/cryptocurrency.asp
3. https://en.wikipedia.org/wiki/Cryptocurrency
4. https://en.wikipedia.org/wiki/Blockchain
5. https://www.coinbase.com/learn/crypto-basics/what-is-a-crypto-wallet

Team Members : Group - 16

Shivam- 1906070

Aman Kumar- 1906073

Raushan Kumar- 1906078

Abhishek Jaiswal- 1906072

Shubham Shandilya- 1906069