



BLOCKCHAIN PROJECT

Submitted By:

Bhavesh Toshniwal (CS18MTECH11029)

And

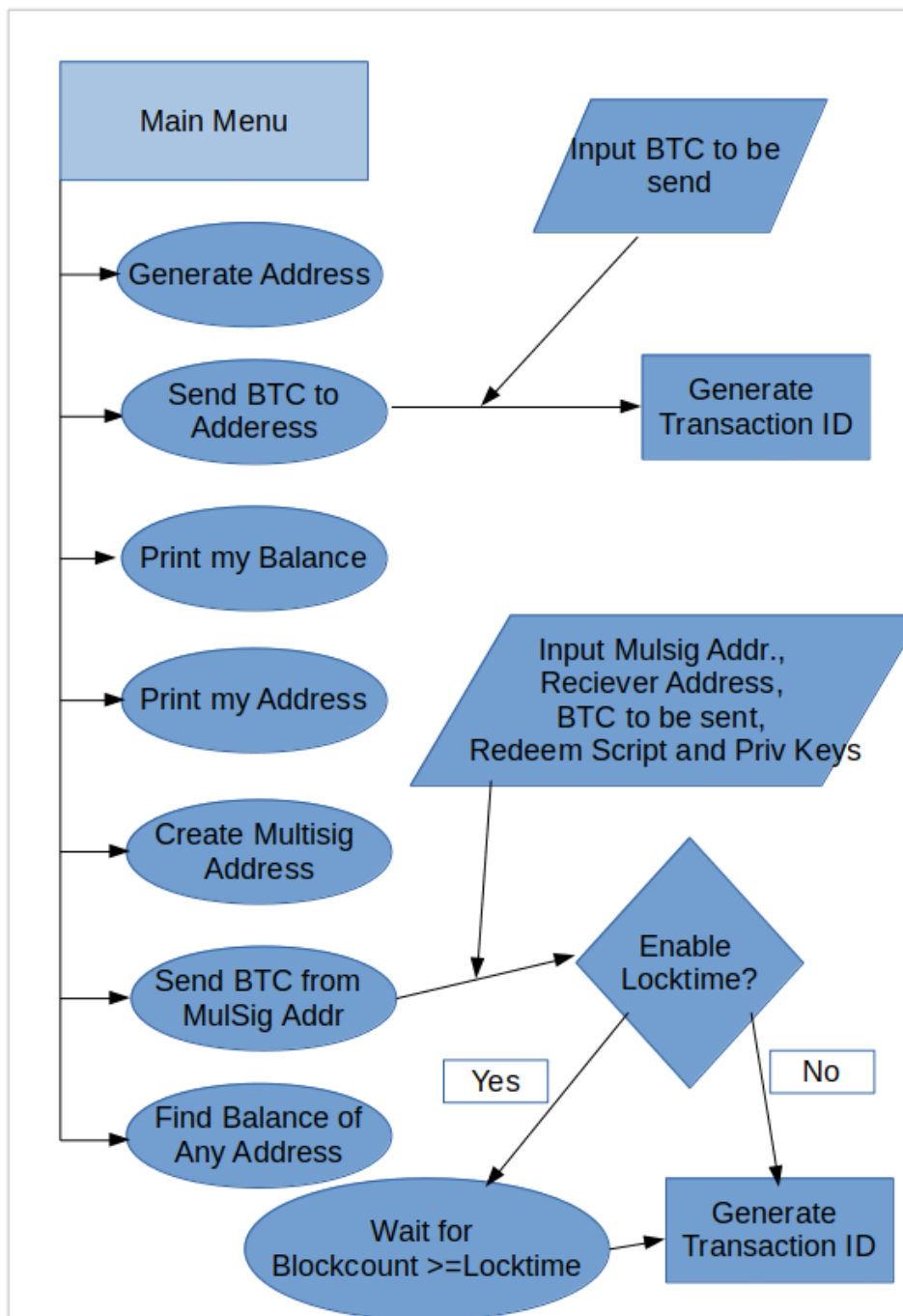
Akash Banerjee (CS18MTECH11023)

Outline : This is a simple application made on command line interface. The main motive is to focus on implementation of the various functionalities of the Blockchain transaction.

This application allows user to transfer some Bitcoins to an address. This also has the functionality to send some Bitcoins from Multisig address. This also includes the feature to provide a Locktime in a transaction.

We have implemented a 2 of 3 Multisig Transaction in this application.

Block Diagram :



Execution Results:

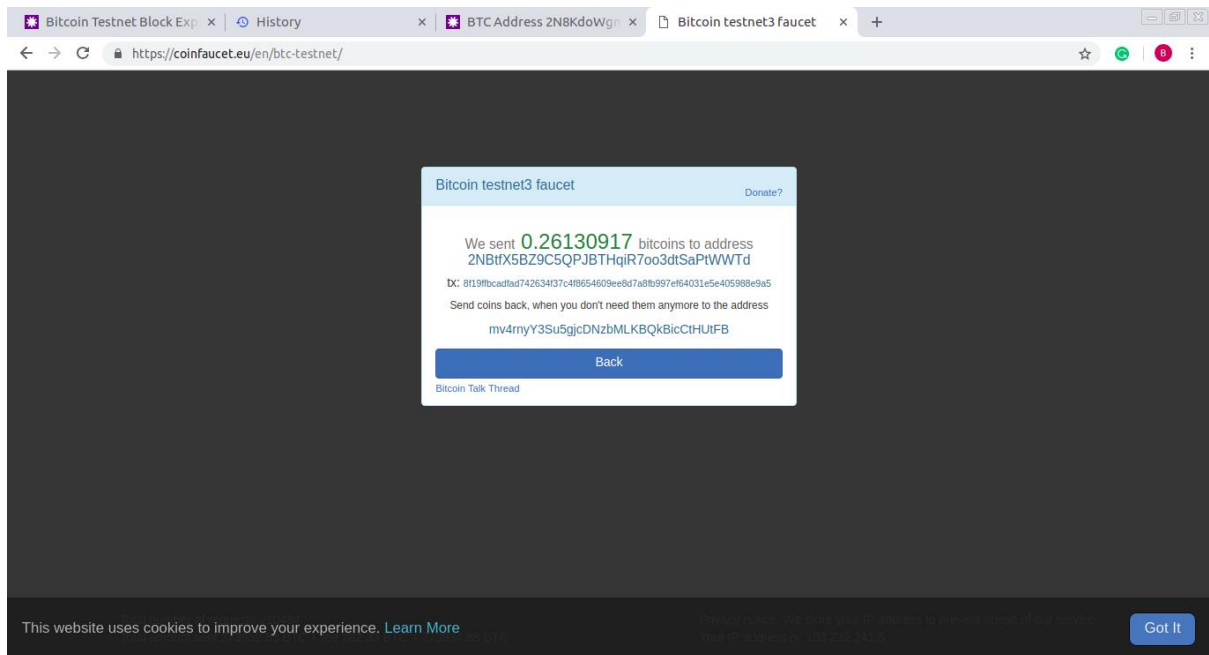
1. Creation of Mutisig Address:

```
bhavesh@bhavesh-HP-Notebook: ~/blockchain-basics
File Edit View Search Terminal Help
root@3aee6ea23320:/code# ruby bitcoin_rpc.rb
What would you like to do?
1: Print My Address
2: Generate new Address
3: Create Multisig Address
4: Print my Balance
5: Send BTC to Address
6: Send BTC from multisig address
7: Find Balance of any address
10: Exit
3
Multisig Redeem Script : 522103e6fbd596e7b8cfed03ea05f062e897c1666d6bf312c5ff90989d4675a8efd7e921025ffca93ff6d5b9eec2094de91081e150cd795b434d63ba2aa1
89a860cc9812ca210355718a785f06a6ef67bf19a9e9de2c2e838d6ba9743d243f185cea7b4754f9ea53ae
Multisig Address : 2NBtFX5BZ9C5QPJBTHqIR7oo3dtSaPtWMTd
Would you like to see the private keys for this address?Yes / No :
Yes
"cTxG6Cm9e4uL4P8ctL1Wyd7JWEftrKGMQMWLi3Z4RTqy5SuyBfe"
"cMnnzuQyFXcXUeWanz8a6S1FSmLtUgrp9mmvwik1Jx368Xm8ms2"
"cQdbkANwBjLobihVLyKs18v986WGLQ2FaqVbVVK9tdp7gVXYn12"
What would you like to do?
1: Print My Address
2: Generate new Address
3: Create Multisig Address
4: Print my Balance
5: Send BTC to Address
6: Send BTC from multisig address
7: Find Balance of any address
10: Exit
```

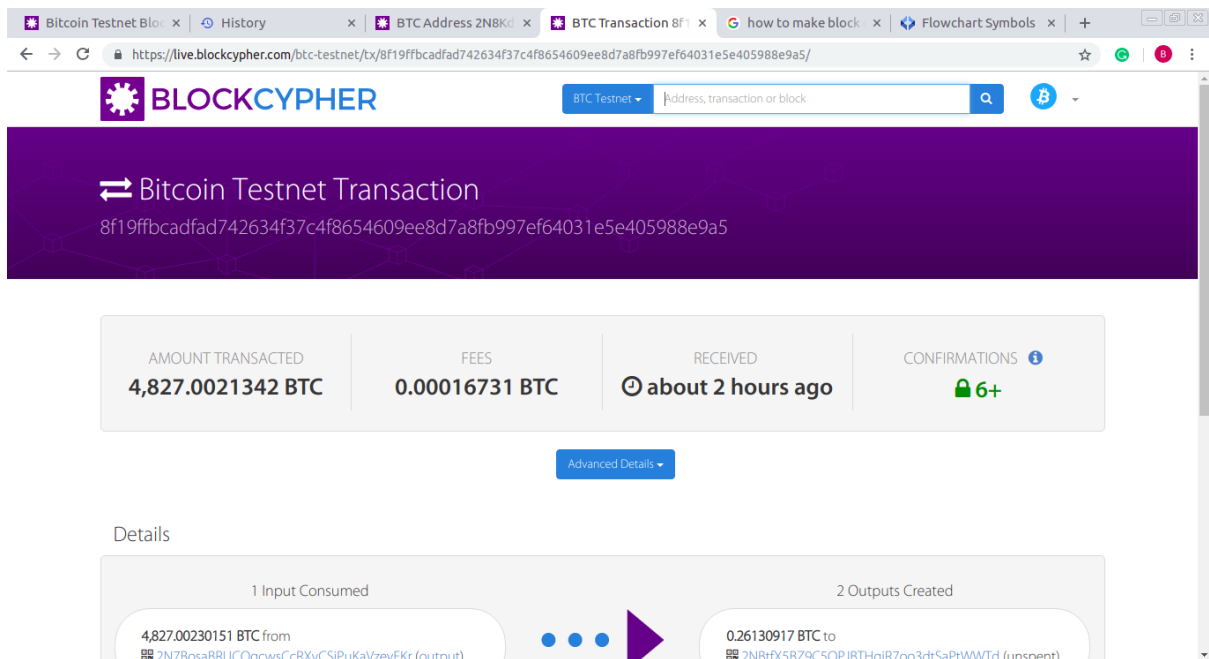
2. Checking Balance of Multisig Address

```
bhavesh@bhavesh-HP-Notebook: ~/blockchain-basics
File Edit View Search Terminal Help
6: Send BTC from multisig address
7: Find Balance of any address
10: Exit
3
Multisig Redeem Script : 522103e6fbd596e7b8cfed03ea05f062e897c1666d6bf312c5ff90989d4675a8efd7e921025ffca93ff6d5b9eec2094de91081e150cd795b434d63ba2aa1
89a860cc9812ca210355718a785f06a6ef67bf19a9e9de2c2e838d6ba9743d243f185cea7b4754f9ea53ae
Multisig Address : 2NBtFX5BZ9C5QPJBTHqIR7oo3dtSaPtWMTd
Would you like to see the private keys for this address?Yes / No :
Yes
"cTxG6Cm9e4uL4P8ctL1Wyd7JWEftrKGMQMWLi3Z4RTqy5SuyBfe"
"cMnnzuQyFXcXUeWanz8a6S1FSmLtUgrp9mmvwik1Jx368Xm8ms2"
"cQdbkANwBjLobihVLyKs18v986WGLQ2FaqVbVVK9tdp7gVXYn12"
What would you like to do?
1: Print My Address
2: Generate new Address
3: Create Multisig Address
4: Print my Balance
5: Send BTC to Address
6: Send BTC from multisig address
7: Find Balance of any address
10: Exit
7
Please enter an address:
2NBtFX5BZ9C5QPJBTHqIR7oo3dtSaPtWMTd
Balance : 0
What would you like to do?
1: Print My Address
2: Generate new Address
3: Create Multisig Address
4: Print my Balance
5: Send BTC to Address
6: Send BTC from multisig address
7: Find Balance of any address
10: Exit
```

3. Transferring Bitcoins to Multisig Address



4. Coin Transfer Transaction has been Successful



5. Checking Balance After Bitcoin Transfer:

```
bhaves@bhaves-HP-Notebook: ~/blockchain-basics
File Edit View Search Terminal Help
What would you like to do?
1: Print My Address
2: Generate new Address
3: Create Multisig Address
4: Print my Balance
5: Send BTC to Address
6: Send BTC from multisig address
7: Find Balance of any address
10: Exit
7
Please enter an address:
2NBtFX5BZ9C5QPJBTHqLR7oo3dtSaPtMWTd
Balance : 0

What would you like to do?
1: Print My Address
2: Generate new Address
3: Create Multisig Address
4: Print my Balance
5: Send BTC to Address
6: Send BTC from multisig address
7: Find Balance of any address
10: Exit
7
Please enter an address:
2NBtFX5BZ9C5QPJBTHqLR7oo3dtSaPtMWTd
Balance : 0.26130917

What would you like to do?
1: Print My Address
2: Generate new Address
3: Create Multisig Address
4: Print my Balance
5: Send BTC to Address
6: Send BTC from multisig address
7: Find Balance of any address
10: Exit
```

6. Creating new Address to transfer bitcoins:

```
bhaves@bhaves-HP-Notebook: ~/blockchain-basics
File Edit View Search Terminal Help
10: Exit
2
New Address : mgkVrj7ZgnVbo0LHxxKZLXngFt2B7N6XbZ

What would you like to do?
1: Print My Address
2: Generate new Address
3: Create Multisig Address
4: Print my Balance
5: Send BTC to Address
6: Send BTC from multisig address
7: Find Balance of any address
10: Exit
1
Address : mgkVrj7ZgnVbo0LHxxKZLXngFt2B7N6XbZ

What would you like to do?
1: Print My Address
2: Generate new Address
3: Create Multisig Address
4: Print my Balance
5: Send BTC to Address
6: Send BTC from multisig address
7: Find Balance of any address
10: Exit
4
Balance : 0

What would you like to do?
1: Print My Address
2: Generate new Address
3: Create Multisig Address
4: Print my Balance
5: Send BTC to Address
6: Send BTC from multisig address
7: Find Balance of any address
10: Exit
```

7. Sending Bitcoins from Multisig Address to the new Address (Locktime is enabled):

```
bhaves@bhaves-HP-Notebook: ~/blockchain-basics
File Edit View Search Terminal Help
4: Print my Balance
5: Send BTC to Address
6: Send BTC from multisig address
7: Find Balance of any address
10: Exit
4
Balance : 0

What would you like to do?
1: Print My Address
2: Generate new Address
3: Create Multisig Address
4: Print my Balance
5: Send BTC to Address
6: Send BTC from multisig address
7: Find Balance of any address
10: Exit
6
Please enter multisig address you would like to send BTC FROM
2NBtFX5BZ9C5QPJBTHqLR7oo3dtsaPtMMTD
Please enter address you would like to send BTC TO...
mgkVrj7ZgnVbooiHxxKZLXngft2B7N6xbZ
How many Bitcoins would you like to send?
0.01
Please enter any two private keys for the multisig address:
cTxG6Cm9e4uL4P8ctL1Myld7JWEfTRkGQMwli3Z4RTqy5SuyBfe
Enter another private key:
cMnnzuQyFxcXUeWanZ8a6S1F5mLtUgrp9mmvwk1Jx368XWm8ms2
Please enter the Redeem Script for the multisig address:
522103e6fbd59e7b8cfb03ea05f062e897c166d6bf312c5ff90989d4675a8efd7e921025ffca93ff6d5b9ecc2094de91081e150cd795b434d63ba2aa189a860cc9812ca210355718a78
5f06a6ef67bf19a9e9de2c2e838d6ba9743d243f185cea7b4754f9ea53ae
Would you like to have a Locktime on the transaction?
Yes/No:
Yes
Current Block Height : 1415227
What would you like to set as LockTime?
1415228
```

8. Transaction will be completed when the block count exceeds the locktime value:


```
bhaves@bhaves-HP-Notebook: ~/blockchain-basics
File Edit View Search Terminal Help
5: Send BTC to Address
6: Send BTC from multisig address
7: Find Balance of any address
10: Exit
4
Balance : 0


What would you like to do?
1: Print My Address
2: Generate new Address
3: Create Multisig Address
4: Print my Balance
5: Send BTC to Address
6: Send BTC from multisig address
7: Find Balance of any address
10: Exit
6
Please enter multisig address you would like to send BTC FROM
2NBtFX5BZ9C5QPJBTHqLR7oo3dtsaPtMMTD
Please enter address you would like to send BTC TO...
mgkVrj7ZgnVbooiHxxKZLXngft2B7N6xbZ
How many Bitcoins would you like to send?
0.01
Please enter any two private keys for the multisig address:
cTxG6Cm9e4uL4P8ctL1Myld7JWEfTRkGQMwli3Z4RTqy5SuyBfe
Enter another private key:
cMnnzuQyFxcXUeWanZ8a6S1F5mLtUgrp9mmvwk1Jx368XWm8ms2
Please enter the Redeem Script for the multisig address:
522103e6fbd59e7b8cfb03ea05f062e897c166d6bf312c5ff90989d4675a8efd7e921025ffca93ff6d5b9ecc2094de91081e150cd795b434d63ba2aa189a860cc9812ca210355718a78
5f06a6ef67bf19a9e9de2c2e838d6ba9743d243f185cea7b4754f9ea53ae
Would you like to have a Locktime on the transaction?
Yes/No:
Yes
Current Block Height : 1415227
What would you like to set as LockTime?
1415228
```

Sun 21:24

Bit x His x BT x BT x G ho x Flo x +

https://live.blockcypher.com/btc-testnet/

BLOCKCYPHER

payCent DASH Pay ZERO transaction fee*
Buying DASH is now easier with PayCent! Buy and Sell Instantly

Recent Blocks

Height	Age	Transactions	Total Sent	Total Fees	Block Size (in bytes)
1415227	13 minutes ago	89	50,531.231 BTC	0.078 BTC	17,800
1415226	34 minutes ago	15	409.241 BTC	0.008 BTC	4,910
1415225	54 minutes ago	49	23,865.315 BTC	0.023 BTC	33,710
1415224	an hour ago	58	78,907.079 BTC	0.032 BTC	21,949
1415223	an hour ago	57	40,401.088 BTC	0.017 BTC	17,547

Current Fee Estimates < API Call > API Docs

9. Block count is equal to Locktime , so Transaction Id is generated:

The terminal window shows the following commands and outputs:

```
5: Send BTC to Address
6: Send BTC from multisig address
7: Find Balance of any address
10: Exit
6
Please enter multisig address you would like to send BTC FROM
2NBtFX5B29C5QPJBTHqIR7oo3dtSaPtWtd
Please enter address you would like to send BTC TO...
mgkVrj72gnVboohHxxKZLXngft2B7N6xbZ
How many Bitcoins would you like to send?
0.01
Please enter any two private keys for the multisig address:
cTxG6Cm9e4uL4P8ctL1Myld7JMEftrKQWMMil324RTqy5SuyBfe
Enter another private key:
cMnnzuQyFxcXUeWanz8a651F5mLtUgrp9mmvwlk1Jx368XWm8ms2
Please enter the Redeem Script for the multisig address:
522103e6fbd596e7b8cfed03ea05f062e897c166d6bf312c5ff90989d4675a8efd7e92102
5ffca93ff6d5b9e2c2094de91081e150cd795b434d63ba2aa189a860cc9812ca210355718a
785f06a6ef67bf19a9e9de2c2e838d6ba9743d243f185cea7b4754f9ea53ae
Would you like to have a Locktime on the transaction?
Yes/No:
Yes
Current Block Height : 1415227
What would you like to set as LockTime?
1415228
Transaction ID: 4e5c3ed1b4de350fbedb87792f2f588cabd22e201e4f15db47a7474ddcbf1a26
What would you like to do?
1: Print My Address
2: Generate new Address
3: Create Multisig Address
4: Print my Balance
5: Send BTC to Address
6: Send BTC from multisig address
7: Find Balance of any address
10: Exit
```

The web browser shows the Bitcoin Testnet Explorer interface. The URL is <https://live.blockcypher.com/btc-testnet/>. The page displays the Bitcoin logo and the text "Bitcoin Testnet Explorer". Below this, there is a section for "Recent Blocks" with a table showing the following data:

Height	Age	Transactions	Total Sent	Total Fees	Block Size (in bytes)
1415228	11 seconds ago	50	42,019.501 BTC	0.014 BTC	10,347
1415227	20 minutes ago	89	50,531.231 BTC	0.078 BTC	17,800
1415226	40 minutes ago	15	409.241 BTC	0.008 BTC	4,910
1415225	an hour ago	49	23,865.315 BTC	0.023 BTC	33,710
1415224	an hour ago	58	78,907.079 BTC	0.032 BTC	21,949

10. Transaction will be confirmed after a confirmations

The screenshot shows the Bitcoin Testnet Explorer interface for a specific transaction. The URL is <https://live.blockcypher.com/btc-testnet/tx/4e5c3ed1b4de350fbedb87792f2f588cabd22e201e4f15db47a7474ddcbf1a26/>. The transaction details are as follows:

AMOUNT TRANSACTED	FEES	RECEIVED	CONFIRMATIONS
0.01 BTC	0.25130917 BTC	about a minute ago	0/6

Below the table, there are two circular gauges: "Confidence" at 37.39% and "Miner Preference" at HIGH. To the right, there is a table with the following data:

Size	Lock Time	Version	Relayed By:
340 bytes	1415228	2	78.47.230.62:18333

At the bottom, there is a section for "Details" showing the transaction flow: "1 Input Consumed" (0.26130917 BTC from 2NBtFX5B29C5QPJBTHqIR7oo3dtSaPtWtd) and "1 Output Created" (0.01 BTC to mgkVrj72gnVboohHxxKZLXngft2B7N6xbZ (unspent)).

TXID : 4e5c3ed1b4de350fbedb87792f2f588cabd22e201e4f15db47a7474ddcbf1a26

P.S.- See the details of the transaction on <https://live.blockcypher.com/btc-testnet/> for evidence.