PROJECT 7
BITCOIN SETTING UP A PRIVATE REGTEST

SPRING TRIMESTER 2022

By

NIKHIL PATEL

Overview :- In this lab we will get to know how to set up our own private blockchain with the current version of bitcoin using a test network which is “ regtest ” and get to know how blockchain technology works.

Procedure :-

Step 1 : First of all we will create a config file for setting up with bitcoin. Open a console and type following commands:

```
Cd
Mkdir .bitcoin
Nano .bitcoin/bitcoin.conf
```

Step 2 : Secondly, as soon as you hit enter after the last cmd new empty file will open. Then, in that file you have to add the following lines which are user name and password.

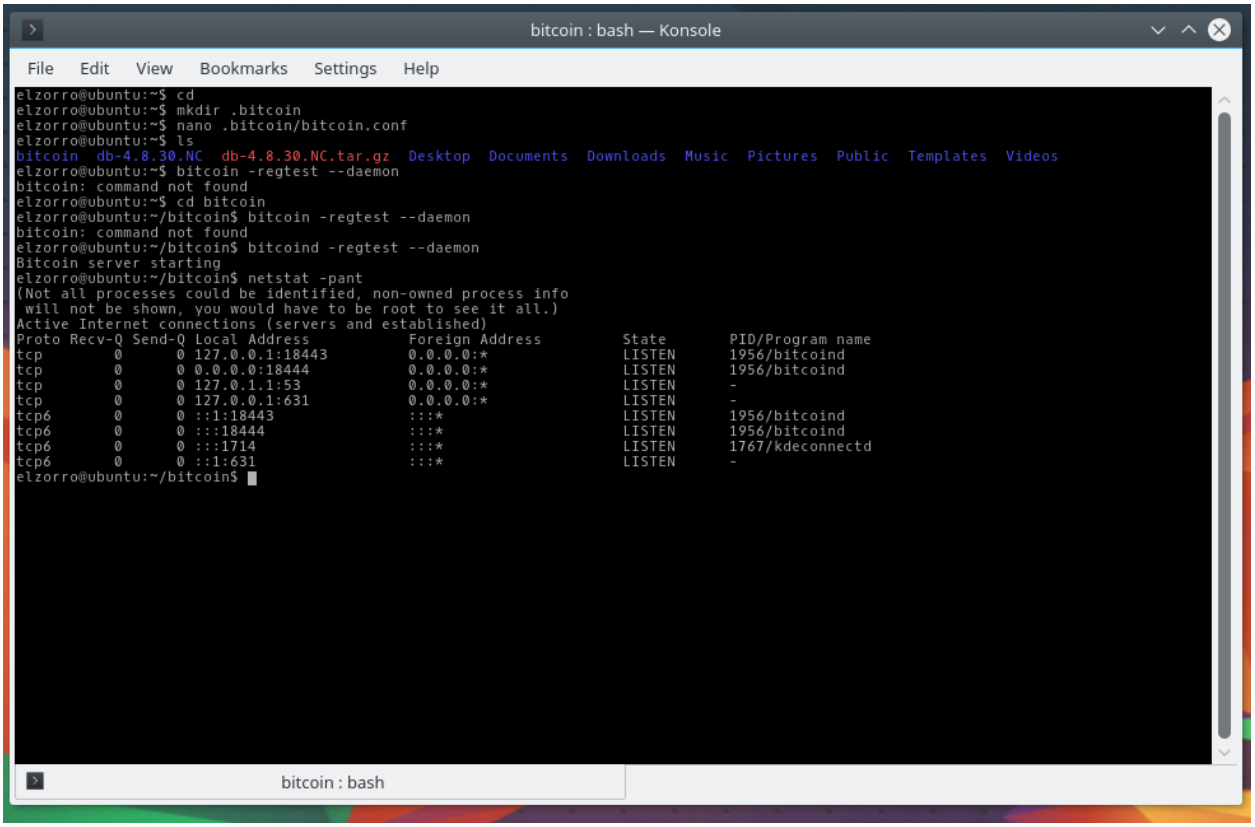
```
rpcuser=bitcoinrpc
rpcpassword=7bLjxV1CKhNJmdxTUMxTpF4vEemWCp49kMX9CwvZabYi
```

NOTE : All the cmds has to be written as it is in the console other you will see and error says no such file in the directory.

After copying the above cmd in the file then hit ctrl + X to exit and then Y to save the file make sure you keep the path of the file and file name in mind or note it down somewhere for further use.

Step 3 : Now, we will setup the bitcoin daemon(which means to implement the bitcoin protocol) this can be done by executing two cmd:

```
bitcoind -regtest --daemon
netstat –pant
```

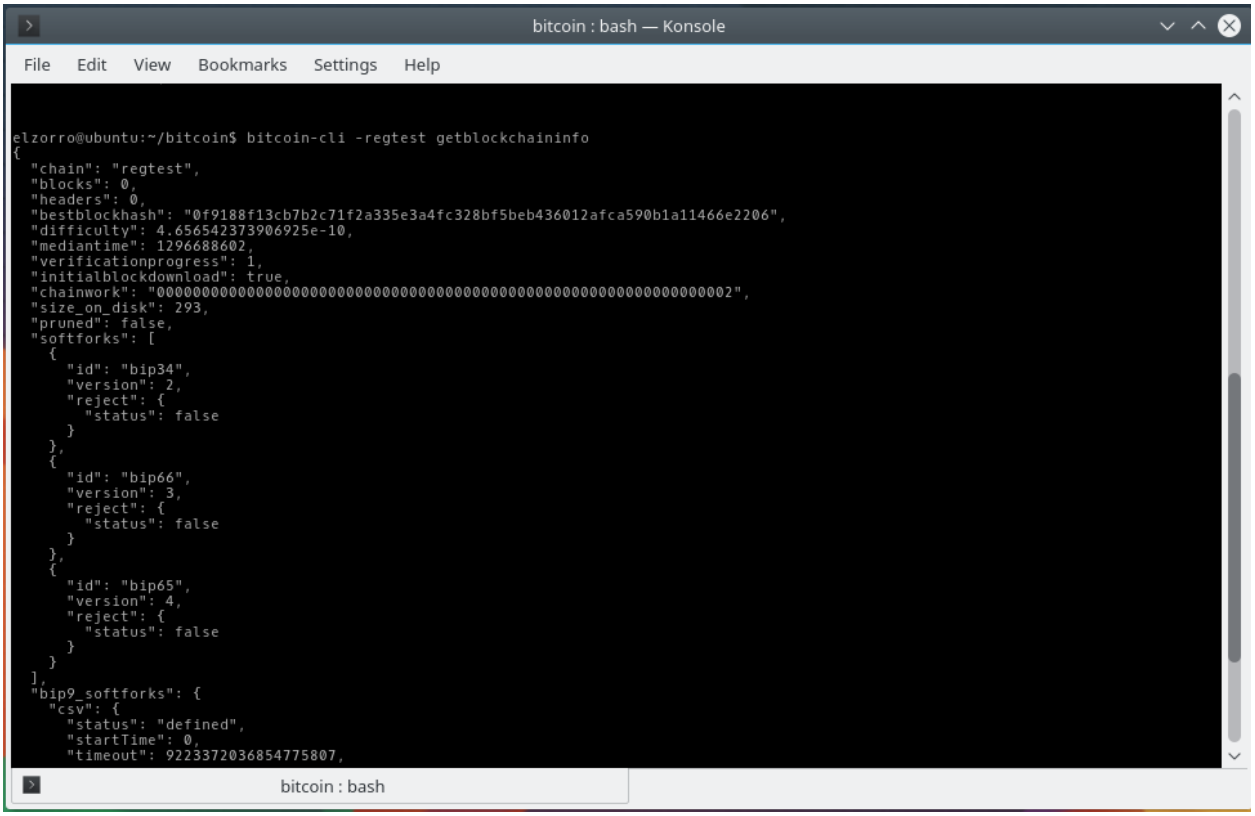


```
elzorro@ubuntu:~$ cd
elzorro@ubuntu:~$ mkdir .bitcoin
elzorro@ubuntu:~$ nano .bitcoin/bitcoin.conf
elzorro@ubuntu:~$ ls
bitcoin  db-4.8.30.NC  db-4.8.30.NC.tar.gz  Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
elzorro@ubuntu:~$ bitcoin -regtest --daemon
bitcoin: command not found
elzorro@ubuntu:~$ cd bitcoin
elzorro@ubuntu:~/bitcoin$ bitcoin -regtest --daemon
bitcoin: command not found
elzorro@ubuntu:~/bitcoin$ bitcoind -regtest --daemon
Bitcoin server starting
elzorro@ubuntu:~/bitcoin$ netstat -pant
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:18443         0.0.0.0:*               LISTEN      1956/bitcoind
tcp        0      0 0.0.0.0:18444           0.0.0.0:*               LISTEN      1956/bitcoind
tcp        0      0 127.0.1.1:53            0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      -
tcp6       0      0 ::1:18443               :::*                    LISTEN      1956/bitcoind
tcp6       0      0 :::18444                :::*                    LISTEN      1956/bitcoind
tcp6       0      0 :::1714                 :::*                    LISTEN      1767/kdeconnectd
tcp6       0      0 ::1:631                 :::*                    LISTEN      -
elzorro@ubuntu:~/bitcoin$ 
```

Above image shows the bitcoin daemon for our own regtest network and the listening port for that is 18444.

Step 4: Now, we will get an information regarding blockchain by executing the following commands :

bitcoin-cli -regtest getblockchaininfo



```
elzorro@ubuntu:~/bitcoin$ bitcoin-cli -regtest getblockchaininfo
{
  "chain": "regtest",
  "blocks": 0,
  "headers": 0,
  "bestblockhash": "0f9188f13cb7b2c71f2a335e3a4fc328bf5beb436012afca590b1a11466e2206",
  "difficulty": 4.656542373906925e-10,
  "mediantime": 1296688602,
  "verificationprogress": 1,
  "initialblockdownload": true,
  "chainwork": "0000000000000000000000000000000000000000000000000000000000000002",
  "size_on_disk": 293,
  "pruned": false,
  "softforks": [
    {
      "id": "bip34",
      "version": 2,
      "reject": {
        "status": false
      }
    },
    {
      "id": "bip66",
      "version": 3,
      "reject": {
        "status": false
      }
    },
    {
      "id": "bip65",
      "version": 4,
      "reject": {
        "status": false
      }
    }
  ],
  "bip9_softforks": {
    "csv": {
      "status": "defined",
      "startTime": 0,
      "timeout": 9223372036854775807,
```

Above image shows the blockchain information, which contains zero blocks for now.

Step 5: After getting info about the blockchain now we will get the status of our wallet. Hit following cmd in console

bitcoin-cli -regtest getwalletinfo

Step 6: Next step is to encrypt our wallet so that if someone steals your wallet, they have to decrypt the wallet to get the bitcoin. Execute the command to encrypt our wallet and here i am using password as P@ssw0rd you can use your own strong password to encrypt your wallet.

bitcoin-cli -regtest encryptwallet P@ssw0rd

Step 7: Wait for a few seconds for service to stop automatically and the encryption is done successfully. After the service is stop then restart the server and see the wallet status again so that you will get to know whether the new password has been applied to the wallet or not.

bitcoind -regtest -daemon
bitcoin-cli -regtest getwalletinfo

<u>Step 8:</u> Execute the command to unlock your wallet for a specific time, here i am unlocking it for 6 min which is 360 seconds and see the wallet status.

```
bitcoin-cli -regtest walletpassphrase P@ssw0rd 360
bitcoin-cli -regtest getwalletinfo
```

<u>Step 9:</u> Now, we will learn how to back up and restore our bitcoin wallet. We will create a file named "wallet.backup" for the backup.

```
bitcoin-cli -regtest backupwallet wallet.backup
ls -1 ~/wal*
```

Note : if the last cmd doesn't work then for checking up the backup wallet go to the Bitcoin folder in the console then type " ls " to search the backup file.

<u>Step 10:</u> We will dump the wallet into a human-readable file which means converting the wallet file from Binary to Readable text file. You will see a file header and some addresses.

```
bitcoin-cli -regtest dumpwallet wallet.txt
head wallet.txt
```

<u>Step 11:</u> We will get a new address and you can have as many addresses as you wish to have. That would be difficult for others to detect where your money is going.

```
bitcoin-cli -regtest getnewaddress
```

<u>Step 12:</u> Mining a block is an important part of bitcoin mining for that you need a high end pc with the best processor to generate a block, because in reality mining a block is time consuming and difficult. Execute cmd to mine a block and then get info of blockchain :

```
bitcoin-cli -regtest generate 1
bitcoin-cli -regtest getblockchaininfo
```

Step 13: Execute the command to get the information of the all the transactions :

```
bitcoin-cli -regtest listtransactions
```

You will see one transaction for the amount of 50 bitcoins. This is our reward for the first block.To view balance execute :

```
bitcoin-cli -regtest getbalance
```

Step 14: In step 13 you get to know you have 0 balance to get money you need to generate more blocks. We will mine more 100 blocks to check whether we get any amount or not. For that type following cmd :

```
bitcoin-cli -regtest generate 100
bitcoin-cli -regtest getblockchaininfo
```

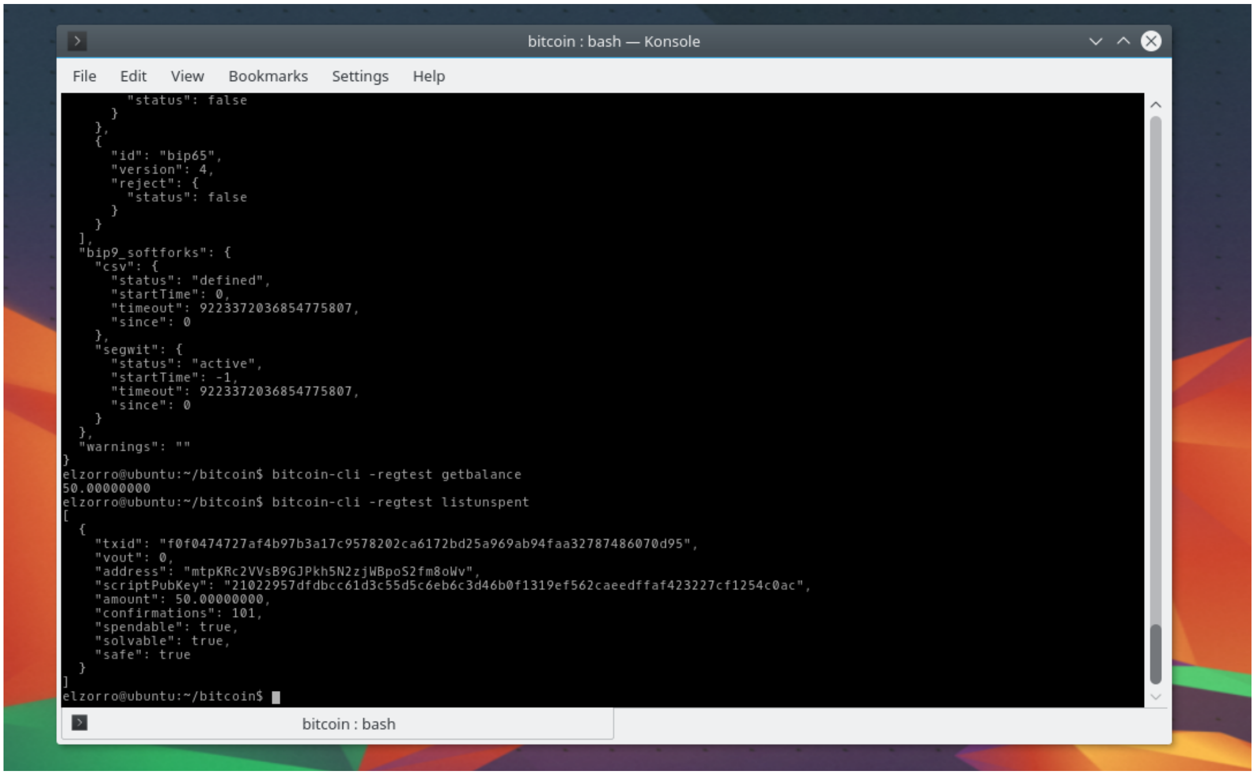
Now, we have 101 blocks, check the balance now :

```
bitcoin-cli -regtest getbalance
```

Step 15: Now we will see how much bitcoin is spendable or is left with us. For that type :

```
bitcoin-cli -regtest listunspent
```

Make sure you see two like “amount and spendable : true “ to confirm that much is left with us.



```
        "status": false
      }
    },
    {
      "id": "bip65",
      "version": 4,
      "reject": {
        "status": false
      }
    }
  ],
  "bip9_softforks": {
    "csv": {
      "status": "defined",
      "startTime": 0,
      "timeout": 9223372036854775807,
      "since": 0
    },
    "segwit": {
      "status": "active",
      "startTime": -1,
      "timeout": 9223372036854775807,
      "since": 0
    }
  },
  "warnings": ""
}
elzorro@ubuntu:~/bitcoin$ bitcoin-cli -regtest getbalance
50.00000000
elzorro@ubuntu:~/bitcoin$ bitcoin-cli -regtest listunspent
[
  {
    "txid": "f0f0474727af4b97b3a17c9578202ca6172bd25a969ab94faa32787486070d95",
    "vout": 0,
    "address": "mtpKRc2VVsB9GJPkh5N2zjWBpoS2fm8oWv",
    "scriptPubKey": "21022957dfdbcc61d3c55d5c6eb6c3d46b0f1319ef562caeedffaf423227cf1254c0ac",
    "amount": 50.00000000,
    "confirmations": 101,
    "spendable": true,
    "solvable": true,
    "safe": true
  }
]
elzorro@ubuntu:~/bitcoin$ 
```

The final image shows the bitcoins left with us.

<u>Conclusion :</u> In this lab we learned how to make our own private blockchain on the test network ‘ regtest ‘ which was completely private and under our control and we got to know about how blockchain technology works. The coin which has been created can’t be used in real life but the purpose of generating those coins was to know how it is created. But,as we say in reality, bitcoin is hard to generate because the difficulty level to create a single block is higher as compared to a test network. For that we need a high-end pc and lots of energy to generate bitcoin, and we can’t guarantee the amount we invested will be refunded in terms of profit.