

BIT-ECC: Environment Setup, Installation and Testing

Wahidur Rahman

28th December 2020

INFONET (Prof. Heung-No Lee), GIST

<https://github.com/infonetGIST>

<https://infonet.gist.ac.kr/>

Purpose: The aim of this document is to instruct the readers how to set up the virtual environment, run and test the BIT-ECC [Bitcoin Error Correction Code PoW Blockchain] on local machine.

This document has the following contents.

Contents:

1. Environmental setup
2. Installation of BIT-ECC
3. Test Private Network

1. Environment Setup

In this chapter, we will explain how to install VMware Workstation and how-to setup Ubuntu operating system on the virtual machine. The setup has been prepared for The Windows 10 environment.

1.1 Installation of VMware Workstation:

Download the latest version of a VMware Workstation [The current version is 16.0, downloaded on December 20th, 2020] from the below link and follow the step-by-step instruction to install it on your local machine.

VMware Workstation is available both for Windows and Linux operating systems.

<https://www.vmware.com/kr/products/workstation-player/workstation-player-evaluation.html>

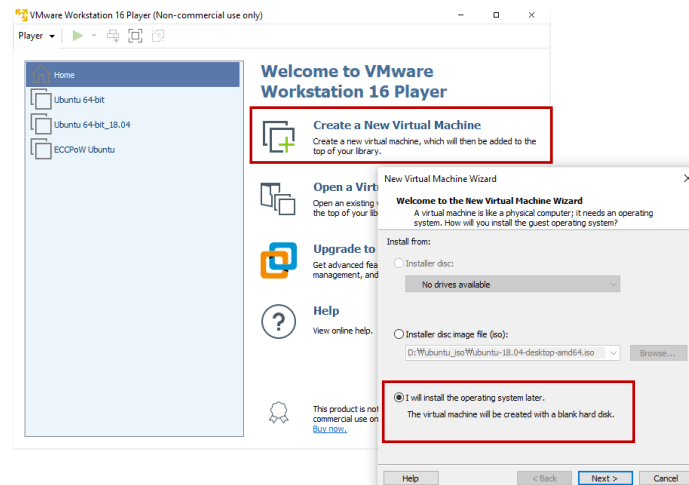
1.2 Download Ubuntu ISO Image file:

Download the Ubuntu 18.04 LTS iso image file from the below link:

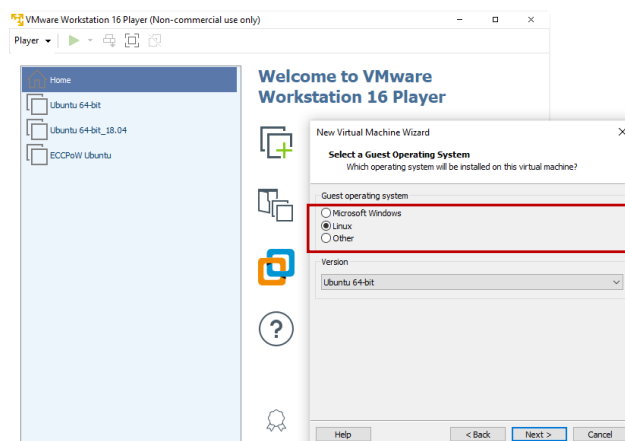
<https://releases.ubuntu.com/18.04/>

1.3 Setup the Linux operating system on VMware Workstation

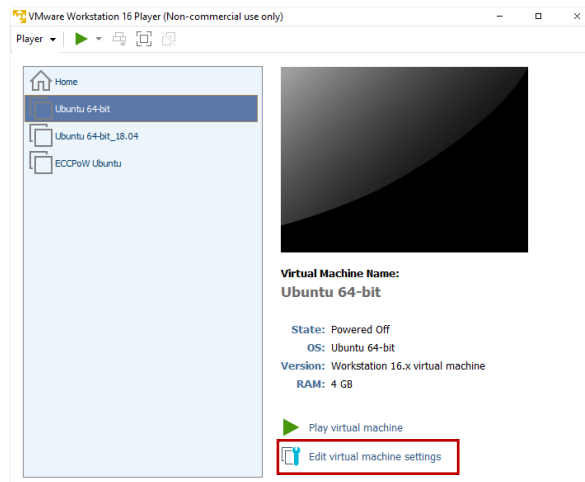
Select the 'Create a New Virtual Machine' tab, then go next. Put a check mark on the but 'I will install the operating system later.' This will create a virtual machine with a blank hard disk.



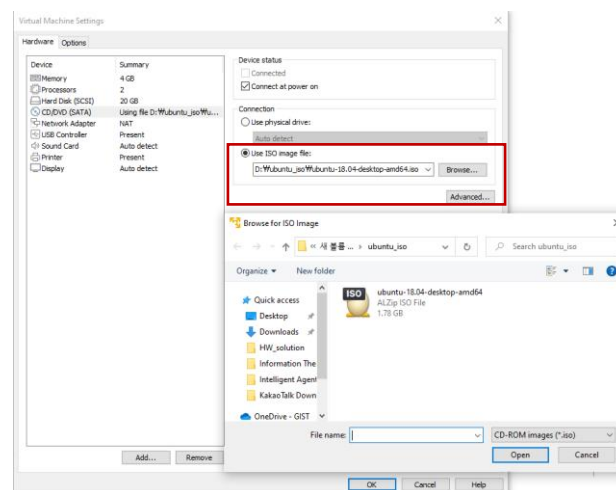
On the next wizard, select the Linux as a guest operating system and keep the version Ubuntu 64-bit.



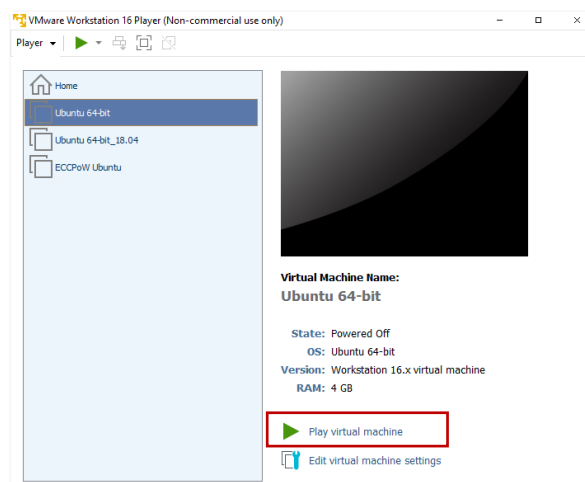
If not required, then keep the installation location as default. Select the disk space as per your requirement. Now select the 'Edit virtual machine settings.'



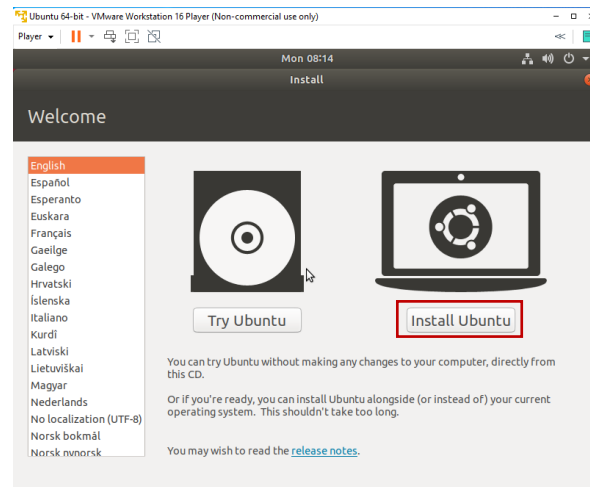
Change the memory and processors as per your requirements. On the CD/DVD (SATA) tab go for the connection tab and use ISO image file as a source of the operating system



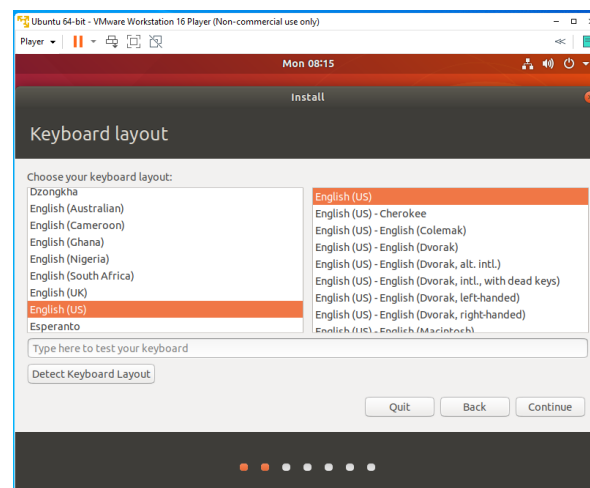
To start the installation process, click on the tab 'Play virtual machine' and follow the instructions.



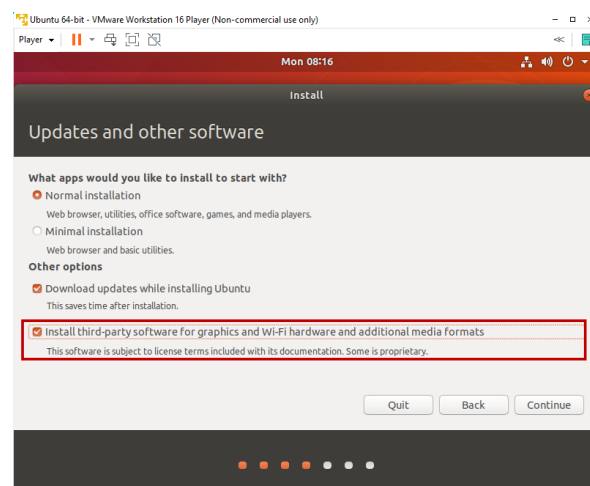
For Ubuntu Setup on virtual machine first select your desire language and select ‘Install Ubuntu’ to start the process



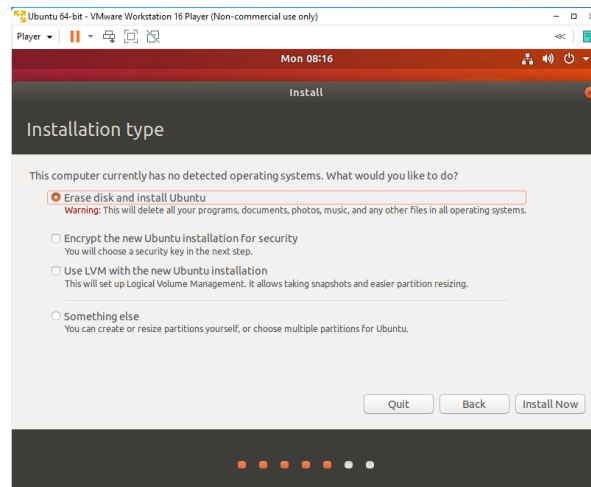
Select your preferable keyboard layout.



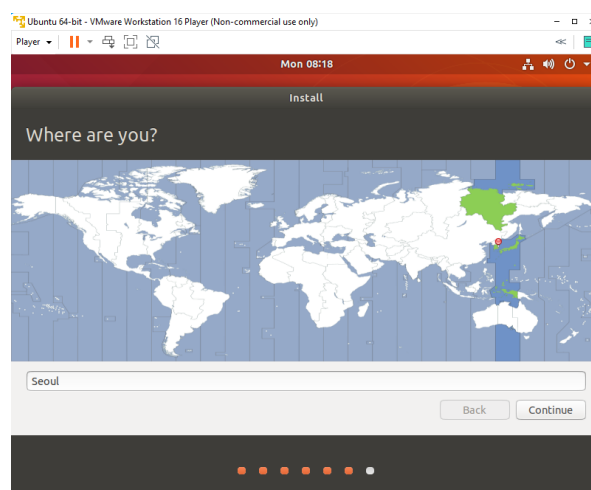
For update and other software check the ‘install third party software’ and keep other options as default



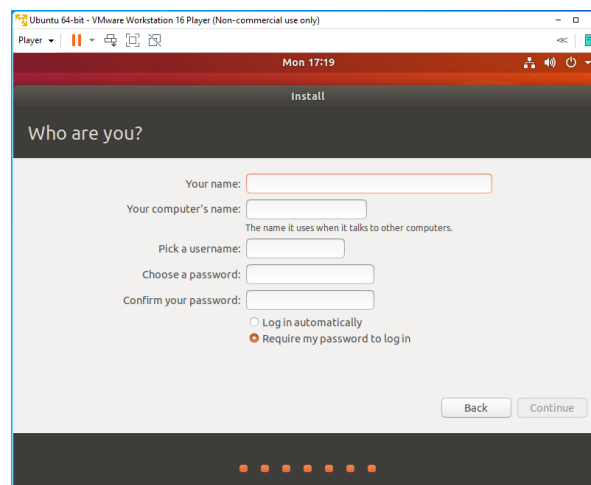
Select 'Erase disk and install Ubuntu' and click 'Install Now'.



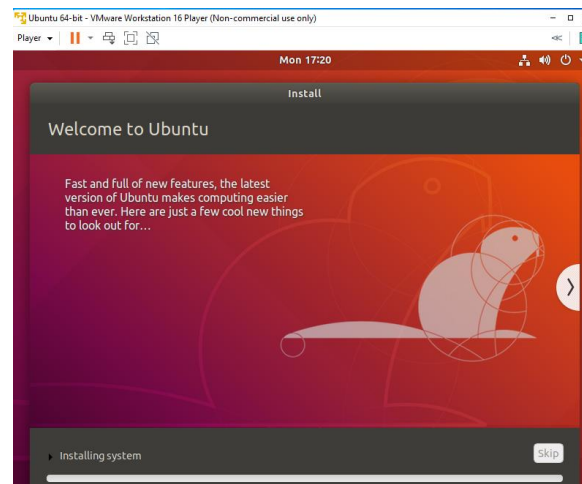
Next select your desired time zone and click on the 'Continue' tab.



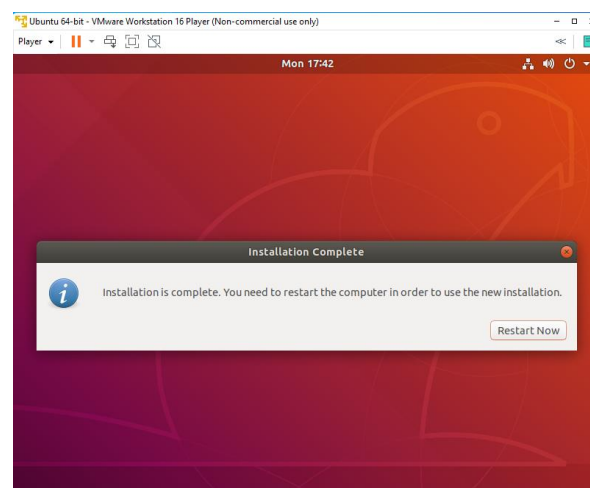
Select the machine name and password.



Now installation process will start, and it will take few minutes to complete the whole installation process.



Click 'Restart Now' to restart the machine for initiating the new process.



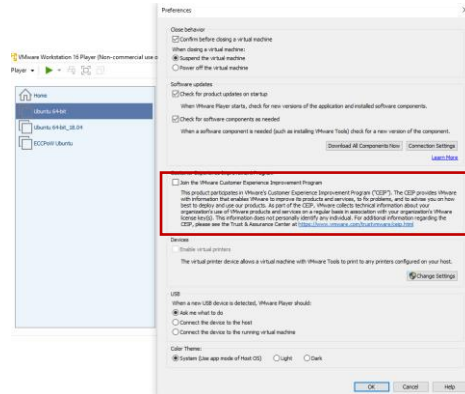
1.4 Two basic commands to fix the screen size.

Open a new terminal and run the below commands.

1. `$ sudo apt-get install open-vm-tools.`
2. `$ sudo apt-get install open-vm-tools-desktop.`

1.5 Enable Copy and Paste Feature in VMware Workstation

Player > File > Performances > Software update > Download all components now.



2. Installation of BIT-ECC

In this chapter, we will describe how to download, install, and run the BIT-ECC on your local machine. Beside that we will install some necessary packages that are prerequisite for this set up.

2.1 Installation of build tool:

1. `$ sudo apt-get install build-essential libtool autotools-dev automake pkg-config bsdmainutils`
2. `$ sudo apt-get install libgrencode-dev autoconf openssl libssl-dev libevent-dev libminiupnpc-dev`

2.2 Installation of boost library:

1. `$ sudo apt-get install libboost-all-dev`

2.3 Installation of Berkeley DB:

1. `$ sudo apt-get install software-properties-common`
2. `$ sudo add-apt-repository ppa:bitcoin/bitcoin`
3. `$ sudo apt-get update`
4. `$ sudo apt-get install libdb4.8-dev libdb4.8++-dev`

2.4 Installation of qt-wallet:

1. `$ sudo apt-get install libqt5gui5 libqt5core5a libqt5dbus5 qttools5-dev qttools5-dev-tools libprotobuf-dev protobuf-compiler libgrencode-dev`

2.5 Installation of git:

1. `$ sudo apt install git`

2.6 Download the most recent version of BIT-ECC blockchain core:

1. `$ git clone https://github.com/cryptoecc/bitcoin_ECC.git`
2. `$ cd bitcoin_ECC`
3. `$ git checkout ecc-0.1.2`

2.7 Build the source code:

1. `$ cd bitcoin_ECC`
2. `$./autogen.sh`
3. `$./configure`
4. `$ make`
5. `$ sudo make install`

2.8 Execute the BIT-ECC core:

```
1. $ bitcoind -txindex -daemon
```

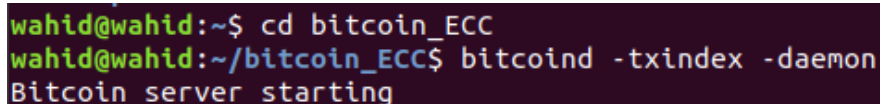
Please see the next chapter.

3. Test Private Network

Open a new terminal under /bitcoin_ECC directory and do the following process to test the private network.

3.1 Execute BIT-ECC/ Run Bitcoin server:

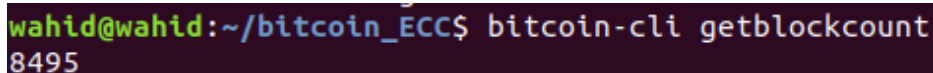
```
1. $ bitcoind -txindex -daemon
```



```
wahid@wahid:~$ cd bitcoin_ECC
wahid@wahid:~/bitcoin_ECC$ bitcoind -txindex -daemon
Bitcoin server starting
```

3.2 Get Block count:

```
1. $ bitcoin-cli getblockcount
```

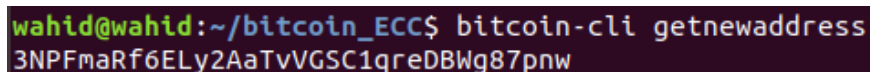


```
wahid@wahid:~/bitcoin_ECC$ bitcoin-cli getblockcount
8495
```

Note: This block count will vary time to time. It is always an increasing number.

3.3 Generate an account/ Generate public address:

```
1. $ bitcoin-cli getnewaddress
```



```
wahid@wahid:~/bitcoin_ECC$ bitcoin-cli getnewaddress
3NPFmaRf6ELy2AaTvVGSC1qreDBWg87pnw
```

3.4 Generate 10 new blocks:

```
1. $ bitcoin-cli generatetoaddress 10
3NPFmaRf6ELy2AaTvVGSC1qreDBWg87pnw
```

```
wahid@wahid:~/bitcoin_ECC$ bitcoin-cli generatetoaddress 10 3NPFmaRf6ELy2AaTvVGSC1qreDBWg87pnw
[
  "63fe74965bed18c4dc4ec729b17cab655f22155c806e0e28b700953995e88dc",
  "2e45d535bc534e5f8d63b65a0e8c33582ab4dd4a4ed4680083e50e1e8e661deb",
  "380080fddac154fb6ff7777aa962bd2c672a9bbb21fb1d41f09e92e6e6b118de",
  "9f753058701ac00d175e6a728901b5a25fe370ec306eb1814dba93098f5fdcea",
  "745aeb57670c41b38fec22b5c11d4834e193fb40350d29720405f98d54f54103",
  "a20888294db16eef1774ae630780abf46ca0c43ff270d49c458be8e169da0a9d",
  "bc494c6673c19df32b8b71419db662ff62b51ae7e88a058638e708bcac536e",
  "470cd2b7a7e067ee9020ea86f7eb805e6bba2879d137067cbb757c176447ad2a",
  "f6449d3df5099b7e9c82e8c032962267bfa15719e2ccaa402c2c44562090550f",
  "fd4fbb26957029e1e30c64c10cf320198bf9ad4ad1ca379640af9b4c4d371a2c"
]
```

3.5 Check blockchain information:

1. \$ bitcoin-cli getblockchaininfo
2. \$ bitcoin-cli getbalance

```
wahid@wahid:~/bitcoin_ECC$ bitcoin-cli getblockchaininfo
{
  "chain": "main",
  "blocks": 8505,
  "headers": 8505,
  "bestblockhash": "fd4fbb26957029e1e30c64c10cf320198bf9ad4ad1ca379640af9b4c4d371a2c",
  "difficulty": 3.479276514130151e+72,
  "mediantime": 1608603701,
  "verificationprogress": 1,
  "initialblockdownload": false,
  "chainwork": "0000000000000000000000000000000000000000000000000000000000000000e17450b94a6a46",
  "size_on_disk": 2560982,
  "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": "failed",
      "startTime": 1462060800,
      "timeout": 1493596800,
      "since": 60
    },
    "segwit": {
      "status": "active",
      "startTime": -1,
      "timeout": 9223372036854775807,
      "since": 0
    }
  },
  "warnings": ""
}
```

```
wahid@wahid:~/bitcoin_ECC$ bitcoin-cli getbalance
1000.00000000
```

3.6 Send Transaction:

Executing a transaction activity is the combination of the below four activities.

1. listunspent
2. createrawtransaction
3. signrawtransaction
4. sendrawtransaction

Here,

Alice public address [Payer]: 3NPFmaRf6ELy2AaTvVGSC1qreDBWg87pnw
Bob public address [Payee]: 3GZ3dAMprHiEk9DUF6m8U8BCaupqiMhNDL
Transfer amount: 0.025 BTC-BTC

3.6.1 Listunspent: Show confirmed outputs (unspent) in Alice address:

1. `$ bitcoin-cli listunspent 0 99999 '["3NPFmaRf6ELy2AaTvVGSC1qreDBWg87pnw"]'`

```
wahid@wahid:~/bitcoin_ECC$ bitcoin-cli listunspent 0 99999 '["3NPFmaRf6ELy2AaTvVGSC1qreDBWg87pnw"]'
[
  {
    "txid": "01cef597444039c160c4559aa5876064a9a6c65327ada706ffa1dcfc8b6a2e19",
    "vout": 0,
    "address": "3NPFmaRf6ELy2AaTvVGSC1qreDBWg87pnw",
    "label": "",
    "redeemScript": "0014d23d5a22c91b1cc25c0dccb7e4fd578d5dd6ae6",
    "scriptPubKey": "a914e2feb63272cd4432c6b6b37d039e42e7ff9b1b0287",
    "amount": 50.00000000,
    "confirmations": 7,
    "spendable": true,
    "solvable": true,
    "desc": "sh(wpkh([fcc4f8f2/0'/0'/2']03c198665acc31856d9553e593fc3272822ab2138857ba8812f653a38cd6005829))#9cqz5j97",
    "safe": true
  },
  {
    "txid": "62c1c698410a1b5ad76c91a622849163c8f20837a9c25946e3a8932ab689291c",
    "vout": 0,
    "address": "3NPFmaRf6ELy2AaTvVGSC1qreDBWg87pnw",
    "label": "",
    "redeemScript": "0014d23d5a22c91b1cc25c0dccb7e4fd578d5dd6ae6",
    "scriptPubKey": "a914e2feb63272cd4432c6b6b37d039e42e7ff9b1b0287",
    "amount": 50.00000000,
    "confirmations": 9,
    "spendable": true,
    "solvable": true,
    "desc": "sh(wpkh([fcc4f8f2/0'/0'/2']03c198665acc31856d9553e593fc3272822ab2138857ba8812f653a38cd6005829))#9cqz5j97",
    "safe": true
  },
  {
    "txid": "0d3ac3f130d82475a7b87d8e6f9794e37289e426c872e40888bf723f4020373e",
    "vout": 0,
    "address": "3NPFmaRf6ELy2AaTvVGSC1qreDBWg87pnw",
    "label": "",
    "redeemScript": "0014d23d5a22c91b1cc25c0dccb7e4fd578d5dd6ae6",
    "scriptPubKey": "a914e2feb63272cd4432c6b6b37d039e42e7ff9b1b0287",
    "amount": 50.00000000,
    "confirmations": 3,
    "spendable": true,
    "solvable": true,
    "desc": "sh(wpkh([fcc4f8f2/0'/0'/2']03c198665acc31856d9553e593fc3272822ab2138857ba8812f653a38cd6005829))#9cqz5j97",
    "safe": true
  },
  {
    "txid": "01dfb723bbb9d40636d6ab83b10db54442b335273350ed3a36f15d0f9c37434f",
    "vout": 0,
    "address": "3NPFmaRf6ELy2AaTvVGSC1qreDBWg87pnw",
    "label": "",
    "redeemScript": "0014d23d5a22c91b1cc25c0dccb7e4fd578d5dd6ae6",
    "scriptPubKey": "a914e2feb63272cd4432c6b6b37d039e42e7ff9b1b0287",
    "amount": 50.00000000,
    "confirmations": 10,
    "spendable": true,
    "solvable": true,
    "desc": "sh(wpkh([fcc4f8f2/0'/0'/2']03c198665acc31856d9553e593fc3272822ab2138857ba8812f653a38cd6005829))#9cqz5j97",
    "safe": true
  }
],
```



```
wahid@wahid:~/bitcoin_ECC$ bitcoin-cli signrawtransactionwithkey "02000000001192e6ab8fcdca1ff06a7ad2753c6a6a9646087a59a55c460c139404497f5ce010000000000fffff02a02526000000000017a914a307fa7979dbb9611079b9a0d18fbde250f3d12d871009df290100000017a914e2feb63272cd4432c6b6b37d039e42e7ff9b1b0287024730440220543c05d66ad4570aa187127989544912214a76b0b65bbbbe546c5d8ec72d24470220157b63e6fec7c7e6e13ff0a3ce37462c925aa54baafaa5cfc92f2a420420b123012103c198665acc31856d9553e593fc3272822ab2138857ba8812f653a38cd600582900000000",
{"hex": "020000000000101192e6ab8fcdca1ff06a7ad2753c6a6a9646087a59a55c460c139404497f5ce010000000017160014d23d5a22c91b1cc25c0dcc1b7e4fd578d5dd6ae6ffffff02a0252600000000000017a914a307fa7979dbb9611079b9a0d18fbde250f3d12d871009df290100000017a914e2feb63272cd4432c6b6b37d039e42e7ff9b1b0287024730440220543c05d66ad4570aa187127989544912214a76b0b65bbbbe546c5d8ec72d24470220157b63e6fec7c7e6e13ff0a3ce37462c925aa54baafaa5cfc92f2a420420b123012103c198665acc31856d9553e593fc3272822ab2138857ba8812f653a38cd600582900000000",
"complete": true
}
```

3.9 Send Raw Transaction:

1. `$ bitcoin-cli sendrawtransaction`
020000000000101192e6ab8fcdca1ff06a7ad2753c6a6a9646087a59a55c460c139404497f5ce010000000017160014d23d5a22c91b1cc25c0dcc1b7e4fd578d5dd6ae6ffffff02a0252600000000000017a914a307fa7979dbb9611079b9a0d18fbde250f3d12d871009df290100000017a914e2feb63272cd4432c6b6b37d039e42e7ff9b1b0287024730440220543c05d66ad4570aa187127989544912214a76b0b65bbbbe546c5d8ec72d24470220157b63e6fec7c7e6e13ff0a3ce37462c925aa54baafaa5cfc92f2a420420b123012103c198665acc31856d9553e593fc3272822ab2138857ba8812f653a38cd600582900000000

```
wahid@wahid:~/bitcoin_ECC$ bitcoin-cli sendrawtransaction 020000000000101192e6ab8fcdca1ff06a7ad2753c6a6a9646087a59a55c460c139404497f5ce010000000017160014d23d5a22c91b1cc25c0dcc1b7e4fd578d5dd6ae6ffffff02a0252600000000000017a914a307fa7979dbb9611079b9a0d18fbde250f3d12d871009df290100000017a914e2feb63272cd4432c6b6b37d039e42e7ff9b1b0287024730440220543c05d66ad4570aa187127989544912214a76b0b65bbbbe546c5d8ec72d24470220157b63e6fec7c7e6e13ff0a3ce37462c925aa54baafaa5cfc92f2a420420b123012103c198665acc31856d9553e593fc3272822ab2138857ba8812f653a38cd600582900000000
f01791cd253e1bef474498905d4f40f127a28e1cf94dee8239ce0e04cfb91dff
```

3.9.1 Verification of the issued transaction in a block.

1. Generate one block
2. Get block information
3. Get transaction information

3.9.1.1 Generate one block: Generate a new block with sender public address.

1. `$ bitcoin-cli generatetoaddress 1`
3NPFmaRf6ELy2AaTvVGSC1qreDBWg87pnw

```
wahid@wahid:~/bitcoin_ECC$ bitcoin-cli generatetoaddress 1 3NPFmaRf6ELy2AaTvVGSC1qreDBWg87pnw
[
  "3f105a645ce5084ad86b1e09315275e3b6f5ad05a23791a4d7c1d64eb67ad2cc"
]
```

```
1. $ bitcoin-cli getblock
3f105a645ce5084ad86b1e09315275e3b6f5ad05a23791a4d7c1d64eb
67ad2cc
```

3.9.1.3 Get transaction information: For the transaction detail run the below command.

15

```

wahid@wahid:~/bitcoin_ECC$ bitcoin-cli gettransaction f01791cd253e1bef474498905d4f40f127a28e1cf94dee8239ce0e04cfb91dff
{
  "amount": 0.00000000,
  "fee": -0.00050000,
  "confirmations": 1,
  "blockhash": "3f105a645ce5084ad86b1e09315275e3b6f5ad05a23791a4d7c1d64eb67ad2cc",
  "blockindex": 1,
  "blocktime": 1608614156,
  "txid": "f01791cd253e1bef474498905d4f40f127a28e1cf94dee8239ce0e04cfb91dff",
  "walletconflicts": [
  ],
  "time": 1608613252,
  "timereceived": 1608613252,
  "bip125-replaceable": "no",
  "details": [
    {
      "address": "3GZ3dAMprHiEk9DUF6m8U8BCaupqiMhNDL",
      "category": "send",
      "amount": -0.02500000,
      "label": "",
      "vout": 0,
      "fee": -0.00050000,
      "abandoned": false
    },
    {
      "address": "3NPFmaRf6ELy2AaTvVGSC1qreDBWg87pnw",
      "category": "send",
      "amount": -49.97450000,
      "label": "",
      "vout": 1,
      "fee": -0.00050000,
      "abandoned": false
    },
    {
      "address": "3GZ3dAMprHiEk9DUF6m8U8BCaupqiMhNDL",
      "category": "receive",
      "amount": 0.02500000,
      "label": "",
      "vout": 0
    },
    {
      "address": "3NPFmaRf6ELy2AaTvVGSC1qreDBWg87pnw",
      "category": "receive",
      "amount": 49.97450000,
      "label": "",
      "vout": 1
    }
  ],
  "hex": "020000000000101192e6ab8fcdca1ff06a7ad2753c6a6a9646087a59a55c460c139404497f5ce010000000017160014d23d5a22c91b1cc25cdcc1b7e4fd578d5dd6ae6ffffff02a02526000000000017a914a307fa7979dbb9611079b9a0d18fbde250f3d12d871009df290100000017a914e2feb63272cd4432c6b6b37d039e42e7ff9b1b0287024730440220543c05d66ad4570aa187127989544912214a76b0b65bbb546c5d8ec72d24470220157b63e6fec7c7e6e13ff0a3ce37462c925aa54baafaa5cfc92f2a420420b123012103c198665acc31856d9553e593fc3272822ab2138857ba8812f653a38cd600582900000000"
}

```