

A bitcoin lab.

- Practice receiving and sending bitcoin transactions
- Practice signing and verifying messages

Section Download, Configuration, and Installation:

Bitcoin terms:

Bitcoin has three types of network

Bitcoin **Mainnet**: live transactions take place (peer to peer)

Bitcoin **Testnet**: provides a test environment (peer to peer)

Bitcoin **Regnet**: for testing bitcoin applications (no peers)

Let's first use a test environment. You need to create a Bitcoin configuration file inside the Bitcoin core directory since the configuration file is not automatically created, and then we download and install the bitcoin application.

This configuration file helps to access the network and to provide directions to the Bitcoin core application. Bitcoin looks for the configuration file in the bitcoin data directory. The configuration tells the Bitcoin core to load the application into the **Testnet** or **Regnet** network rather than into the main network.

To create a configuration file **bitcoin.conf** file. The configuration file consists of `option=value` entries. One per line, and remove any whitespaces. A value of the given option is required e.g, `testnet=1`, or `regtest=1`.

Windows :

C:\Users\username\AppData\Roaming\Bitcoin\bitcoin.conf

Linux:

/home/username/.bitcoin/bitcoin.conf

macOS:

/Users/username/Library/Application
Support/Bitcoin/bitcoin.conf

```
Bitcoin — -bash — 80x24
[Anwars-MBP-2:Bitcoin pcanw$ pwd
/Users/pcanw/Library/Application Support/Bitcoin
[Anwars-MBP-2:Bitcoin pcanw$
[Anwars-MBP-2:Bitcoin pcanw$ cat bitcoin.conf
testnet=1
Anwars-MBP-2:Bitcoin pcanw$
```

Click on the link below to download and install a bitcoin application

<https://bitcoin.org/en/download>

After you install the application and run it, you will see Bitcoin core [test].

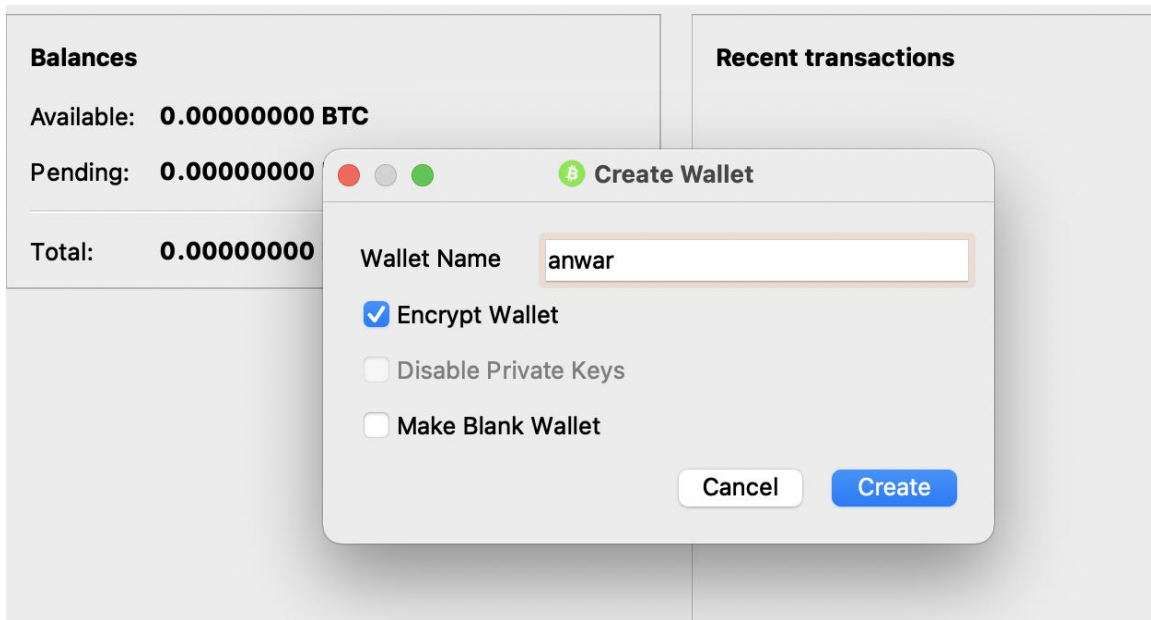


[Source](#)

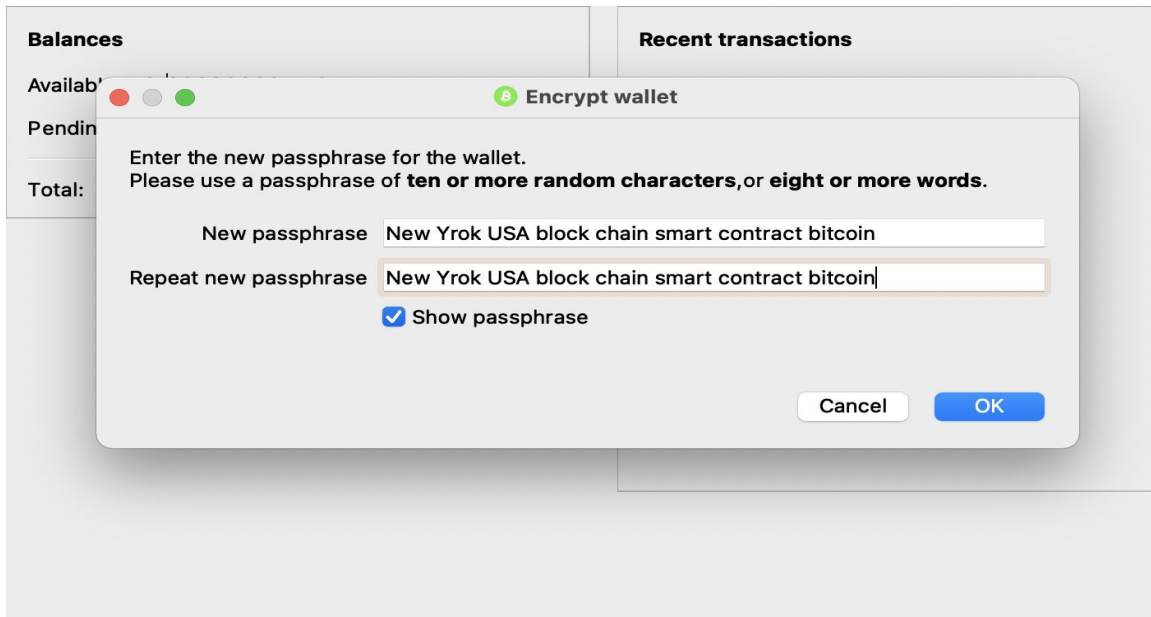
Section 2) Create Wallet and Receive bitcoin

Create a new wallet from the file menu choose create a wallet, and then write the name of the wallet :

File menu → Create Wallet



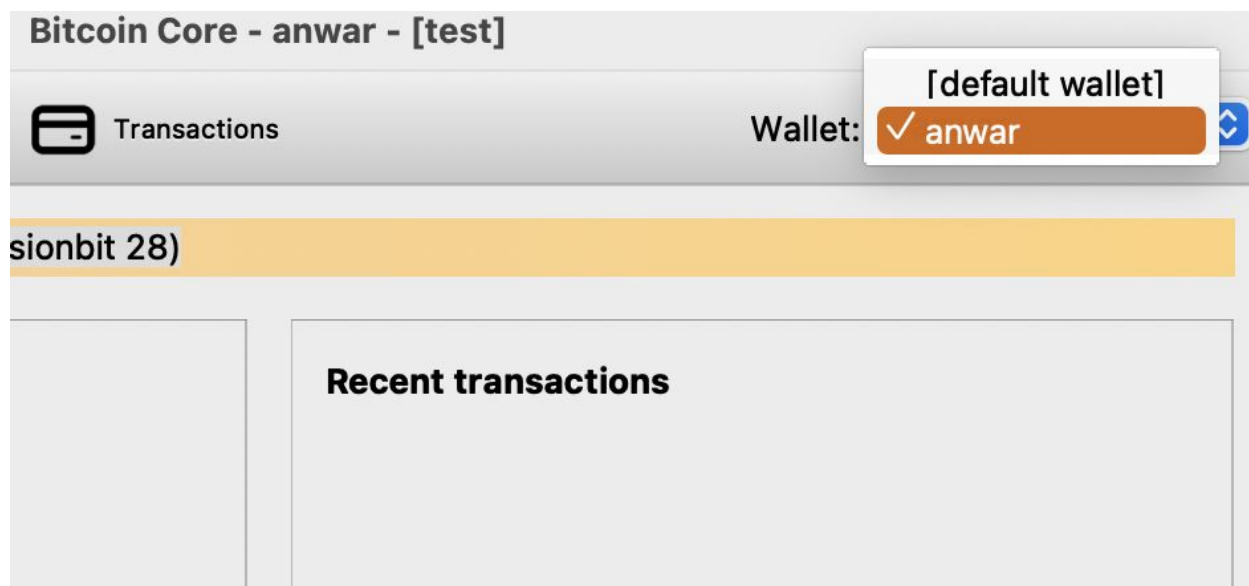
Encryption wallet allows you to enter a new passphrase for the wallet.



Warning:

The passphrase can be any word or sentence. It is case-sensitive. You **MUST** keep your passphrase in a safe place and if you lose it or forget it, you will **LOSE** your wallet and your coins. When you encrusted your wallet that does not mean that your coin is protected from being stolen by malware. It is better to keep your wallet in a safe place.

To backup your wallet you need to select the wallet name on the wallet selection:



And then from the file menu → Backup Wallet.

Also if you go to the bitcoin directory and since you use the testnet network you can find block and wallet files in `/Bitcoin/testnet3/` directory.

```
-bash
Anwars-MBP-2:testnet3 pcanw$ pwd
/Users/pcanw/Library/Application Support/Bitcoin/testnet3
Anwars-MBP-2:testnet3 pcanw$
Anwars-MBP-2:testnet3 pcanw$ ls
banlist.dat          chainstate           mempool.dat
bitcoind.pid         debug.log            peers.dat
blocks              fee_estimates.dat   wallets
Anwars-MBP-2:testnet3 pcanw$
```

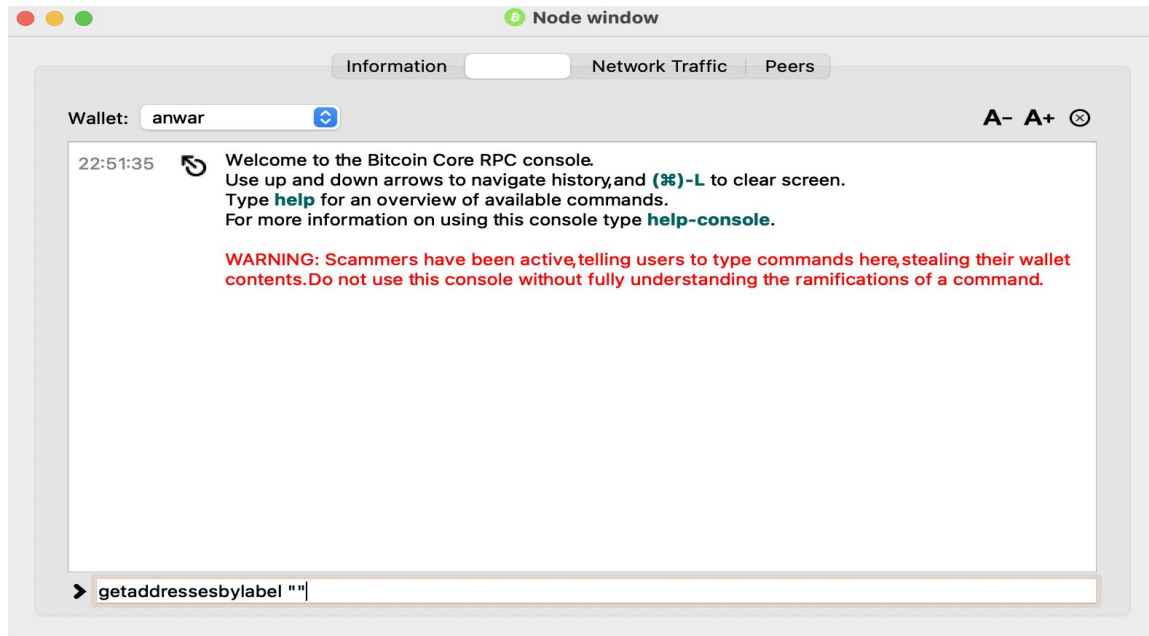
So if you want to backup `wallet.dat` file since by default contains the private keys, you can find it under the wallets directory inside **the wallet name directory**.

Warning: if you lose or delete your wallet file, you lose your coins.

```
-bash
Anwars-MBP-2:testnet3 pcanw$ pwd
/Users/pcanw/Library/Application Support/Bitcoin/testnet3
Anwars-MBP-2:testnet3 pcanw$ ls
banlist.dat          chainstate           mempool.dat
bitcoind.pid         debug.log            peers.dat
blocks              fee_estimates.dat   wallets
Anwars-MBP-2:testnet3 pcanw$ cd wallets/
Anwars-MBP-2:wallets pcanw$
Anwars-MBP-2:wallets pcanw$ ls
anwar                database             db.log              wallet.dat
Anwars-MBP-2:wallets pcanw$ cd anwar/
Anwars-MBP-2:anwar pcanw$
Anwars-MBP-2:anwar pcanw$ ls
database             db.log              wallet.dat
Anwars-MBP-2:anwar pcanw$ █
```

To receive bitcoin, you need your public address or you could create a new receiving address. You need to use the console in the application so you can write the command line which is the interface for the bitcoin application.

From Window menu → Console, you will see this windows below.



You MUST select the wallet name then write **getaddressesbylabel ""** to show the default receiving wallet address.

You can create a new receiving address by:

```
getnewaddress ( "label" "address_type" )
```

Returns a new Bitcoin address for receiving payments.

Arguments:

1. Label: (string, optional, default="") The label name for the address to be linked to. It can also be set to the empty string "" to represent the default label. The label does not need to exist, it will be created if there is no label by the given name.
2. Address_type: (string, optional, default=set by -addresstype) The address type to use. Options are "legacy", "p2sh-segwit", and "bech32".

legacy is the P2PKH address type. The **P2PKH** stands for “Pay to Public Key Hash”. The Public Key Hash is one of many formats of the Bitcoin address.

Example:

```
getnewaddress "anwar" "legacy"
```

To return the new receiving wallet address:

```
getaddressesbylabel "label"
```

Returns the list of addresses assigned the specified label.

Example:

getaddressesbylabel "anwar"

```
22:51:59 ➡ getaddressesbylabel ""
22:51:59 ⬅ {
  "tb1qesukk2n088vld6wpp8szxq99yd8et83hdudq7h": {
    "purpose": "receive"
  }
}
22:56:00 ➡ getaddressesbylabel "anwar"
22:56:00 ⬅ {
  "mt7JFYmEnijJ5myZ97MP4s4wr3CapXNU7h": {
    "purpose": "receive"
  },
  "n26MVA42xF1kZsjPvy2iw6gAHEY2YPy8W2": {
    "purpose": "receive"
  }
}
```

In this example we have those addresses above.

To receive a test Bitcoin to yourself, you can use this website and put any one of the addresses

<https://bitcoina faucet.uo1.net/>

Current wallet balance is ₿ 483.255. You can get up to ₿ 0.00075.

KeepKey - it's time to take control of your crypto. Check out the premier wallet for the new ShapeShift Platform

₿ bitcoin address, e.g. 2MsZQSzRirq6N6jjKkZQ9D5gpjdnjEvJnAy

0.0001

Send testnet bitcoins

Last Transactions

17200caf4d29f9401dff167d4572077f2fd7982dfd57f1d0fb0ee3e12068b394	Wed, 23 Dec 2020 03:43:08
tb1qesukk2n088vld6wpp8szxq99yd8et83hdudq7h	-0.0001
pending	0.00000141 fee

4b258427e4fcd1f945e0e53e33f1ae6e2fbf67f6b622666fc177c5e586cde736	Wed, 23 Dec 2020 03:41:56
n26MVa42xF1kZsjPvy2iw6gAHEY2YPy8W2	-0.0001
pending	0.00000144 fee

As you can see the transaction is pending on the memory pool “unconfirmed transaction” so we need to wait until the transactions get confirmed.

Pending transactions or unconfirmed transactions means these the transactions have not been included in a block so they have not been confirmed.

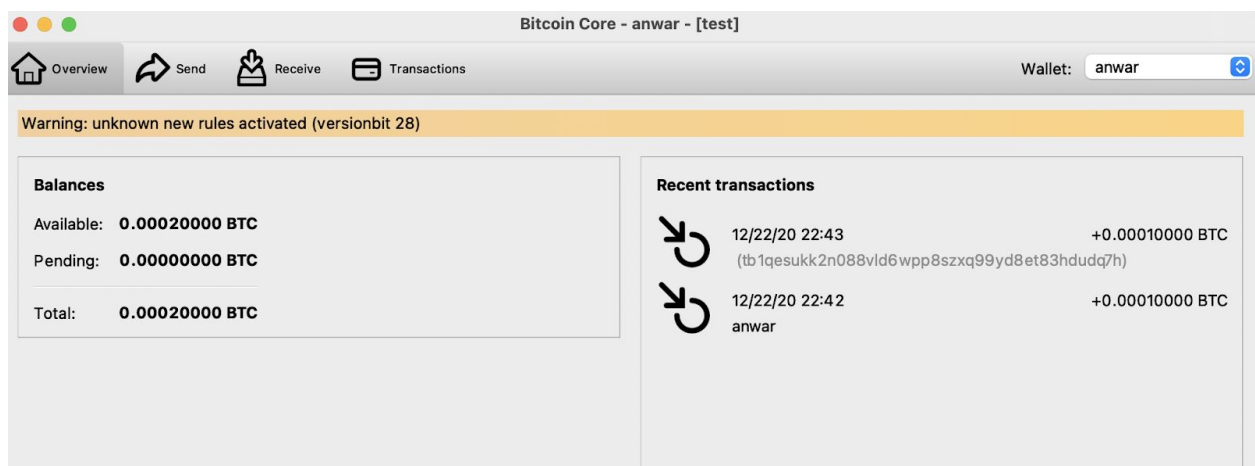
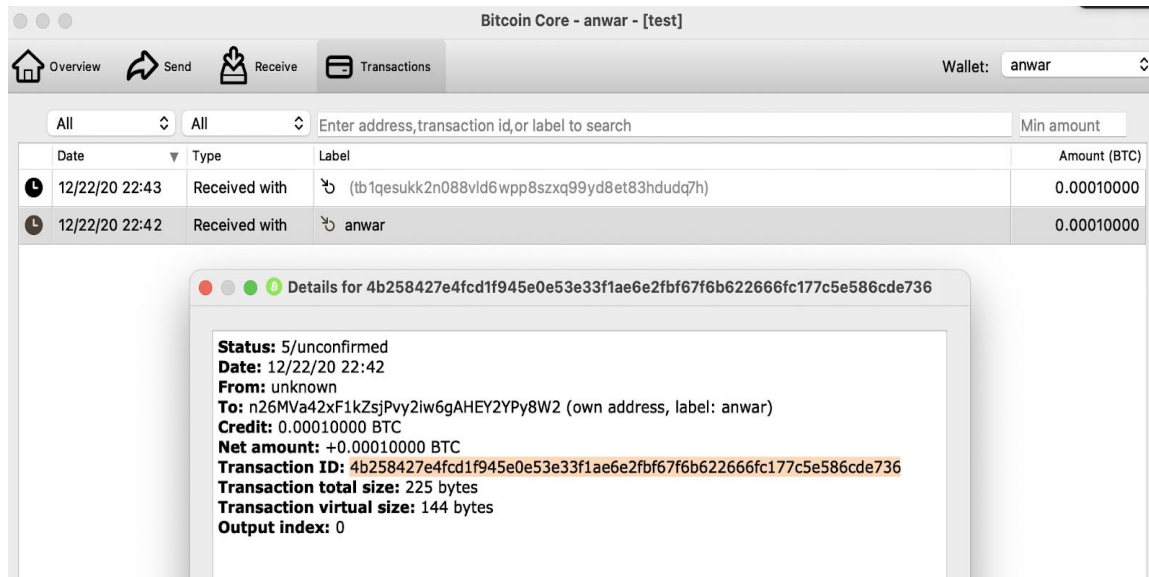
Transaction Details:

You can see transaction Id on the website and the bitcoin application:

[4b258427e4fcd1f945e0e53e33f1ae6e2fbf67f6b622666fc177c5e586cde736](#)

17200caf4d29f9401dff167d4572077f2fd7982dfd57f1d0fb0ee3e12068b394	Wed, 23 Dec 2020 03:43:08
tb1qesukk2n088vld6wpp8szxq99yd8et83hdudq7h	-0.0001
5 confirmations	0.00000141 fee

4b258427e4fcd1f945e0e53e33f1ae6e2fbf67f6b622666fc177c5e586cde736	Wed, 23 Dec 2020 03:41:56
n26MVa42xF1kZsjPvy2iw6gAHEY2YPy8W2	-0.0001
5 confirmations	0.00000144 fee



Nice! We received our test bitcoin.

You can see the details of the transaction on the bitcoin test explore. The advanced details show you more about block hash, index, size, and other details. You need to scroll further down so you can see more detail. It gives a breakdown of the transaction input and output, and you can navigate the network and get an idea of the structure of data available on the blockchain.

<https://live.blockcypher.com/btc-testnet/tx/4b258427e4fcd1f945e0e53e33f1ae6e2fbf67f6b622666fc177c5e586cde736/>

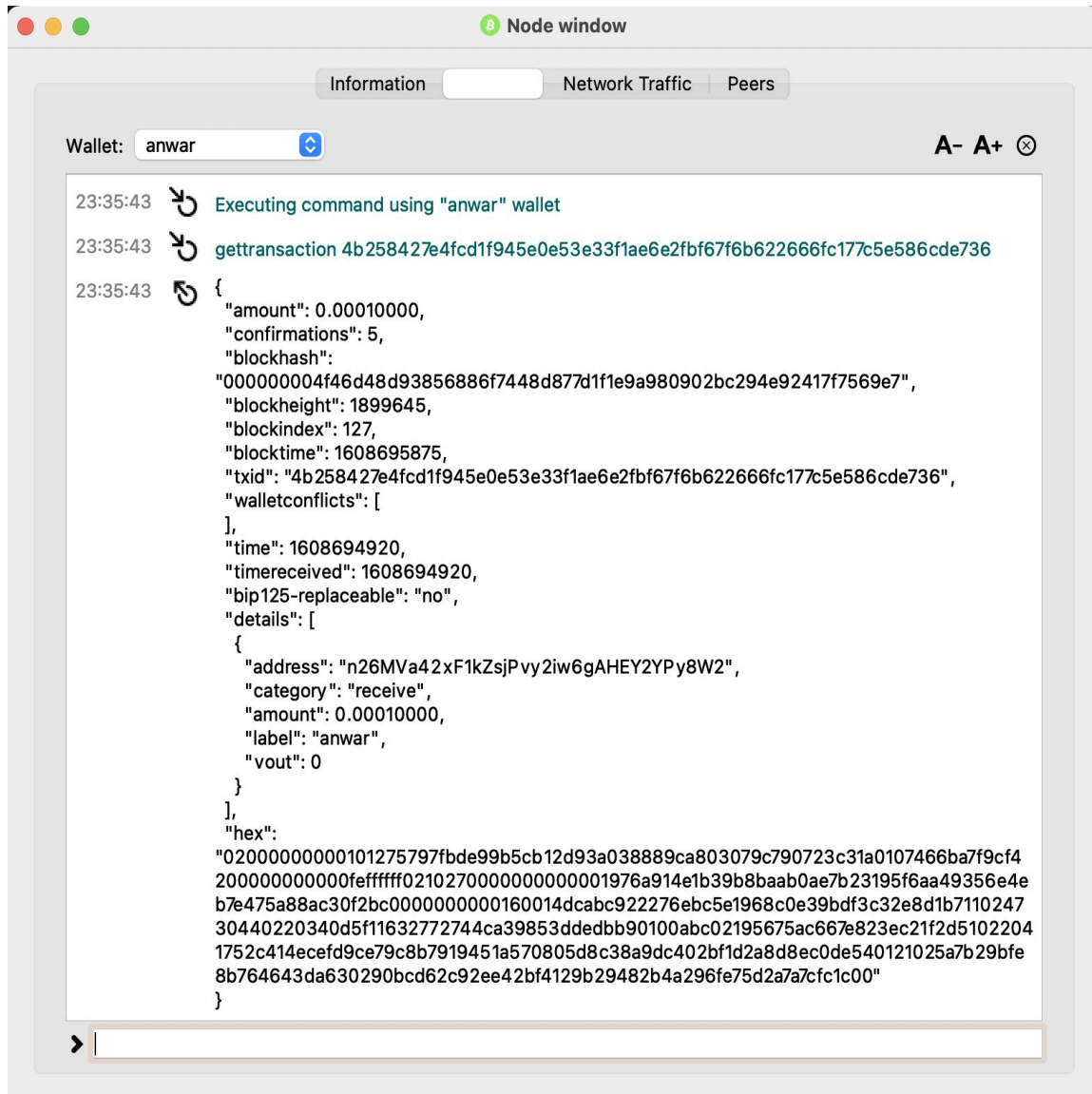
Also you can get detailed information about a transaction in the console

```
gettransaction "txid"
```

```
Get detailed information about in-wallet transaction <txid>  
txid (string, required) The transaction id
```

Example:

```
gettransaction 4b258427e4fcd1f945e0e53e33f1ae6e2fbf67f6b622666fc177c5e586cde736
```



Note: make sure to select your wallet name.

Also you can get information about the block if you use the `getblock` command line.

 `gettransaction 4b258427e4fcd1f945e0e53e33f1ae6e2fbf67f6b622666fc177c5e586cde736`



```
{
  "amount": 0.00010000,
  "confirmations": 420,
  "blockhash":
  "000000004f46d48d93856886f7448d877d1f1e9a980902bc294e92417f7569e7",
  "blockheight": 1899645,
  "blockindex": 127,
  "blocktime": 1608695875,
  "txid": "4b258427e4fcd1f945e0e53e33f1ae6e2fbf67f6b622666fc177c5e586cde736",
  "walletconflicts": [
  ],
  "time": 1608694920,
  "timereceived": 1608694920,
  "bip125-replaceable": "no",
  "details": [
  {
    "address": "n26MVa42xF1kZsjPvy2iw6gAHEY2YPy8W2",
    "category": "receive",
    "amount": 0.00010000,
    "label": "anwar",
    "vout": 0
  }
  ],
  "hex":
  "02000000000101275797fbde99b5cb12d93a038889ca803079c790723c31a0107466ba7f9cf4
  200000000000feffffff0210270000000000001976a914e1b39b8baab0ae7b23195f6aa49356e4e
  b7e475a88ac30f2bc000000000160014dcabc922276ebc5e1968c0e39bdf3c32e8d1b7110247
  30440220340d5f11632772744ca39853ddedbb90100abc02195675ac667e823ec21f2d5102204
  1752c414ecef9d9ce79c8b7919451a570805d8c38a9dc402bf1d2a8d8ec0de540121025a7b29bfe
  8b764643da630290bcd62c92ee42bf4129b29482b4a296fe75d2a7a7cfc1c00"
}
```

Copy the `blockhash` value to get information about the block

`getblock`

`000000004f46d48d93856886f7448d877d1f1e9a980902bc294e92417f7569e7`

Wallet: anwar

A- A+ X

10:38:57 ↻ getblock 000000004f46d48d93856886f7448d877d1f1e9a980902bc294e92417f7569e7

10:38:57 ↻ {

"hash": "000000004f46d48d93856886f7448d877d1f1e9a980902bc294e92417f7569e7",

"confirmations": 410,

"strippedsize": 34668,

"size": 57841,

"weight": 161845,

"height": 1899645,

"version": 536870912,

"versionHex": "20000000",

"merkleroot":

"48896eb5a5a27375ef3448600982ac6b26b012441c3aa9ee4c1fcde489249ee3",

"tx": [

"2d4d8c68604854b151461a6b303f7879a7c618ee339a0b3691a423d9fadada30",

"bfa1aadb68c4e128b84582c78b127502da777a59410036f8fd81c8b8dfc8bbfc",

"8462605b246f4c8b9097f71c006af65025edde3c629ef5de63b7122ec7e18c17",

"50fcd28868afc8e0517e9695eef84426ea55051f092221cbe5b3f94ed79e0966",

"57fad6ccaec37b7b4f0b22f4e8c22ea5678f4032c3f649924912a01e3c05fe03",

"0d36f040d2407359824ed55c39d04cfd62e034d827a977aa08c4dc7536682922",

"7ab015629afc07239dab54be1472f0f4b8d856a01a34f764472698e9e79f0fc8",

"f0a1371aabe399ca478afa755c85bbe59a838411c9aaf489c8ee0897bc46a8a6",

"9ec39ea8c4811aaa50d002daed8cb28140e1aead604a507ca02f8b04b66e8566",

"bccfebb5170e801975c945a81903f1b80815131ce7ed764197b1f573016b0509",

"2e50f6760c644a416dd40ffb7266c8f48520a082042b705c1037e1b2c8557914",

"99c56bf0959e0d079d056c70fbb705e6794fe9f58e4cbe9551a8d0a635addf70",

"a150208a2ce40c7538c87cd469cceb935cf0573f5523f1087bd8aed7cc1bf31c",

"1314a3cf0da8ad61f0baa94c450af22b8614ef31c9bafb3cd8f3cfb1a023ccf4",

"2566a709cec962fed32f73eaffc3463641e514c9ac29ad4b8c9da33c932d5c1f",

"581d023f3fc2dc5990893071be9094e59f05b869cb14c4848bcc146b6291465e",

"4aa7b22d861110eb0a07b0a8d46416c6ee67cbe8d8bf585ecbb8ab19734cb948",

"c5c5235c685aad531257544abcb90a83db0976d0d3178ddaf178069ce1844f3d",

"13f0946d886d0477be52571ebfd55de2053b44e30c1b7f5c7263770701bce7f4",

"4395fdd2fc286a12a2650910372b7cd1c96fcec8400082d79988cbe00a108427",

"c7db8824a29fc320f6ce42ca8967212ebd3d2cc9c8c5a99e80ef7e8e18d8bf39",

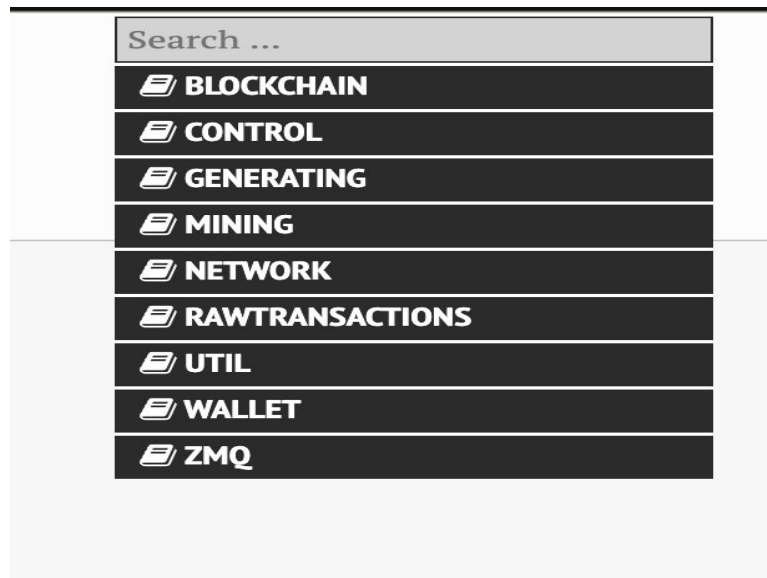
As you can see there are 410 transactions that were confirmed in this block.

In order to receive the coins, the Bitcoin core application has to be synchronized completely with the Tesnet network. It will be delayed until the network is synchronized.

All bitcoin core application command lines can be found in this website:

<https://bitcoincore.org/en/doc/0.17.0/rpc/>

We only used wallets and transaction information command lines, there are more such as general Information (getblockchaininfo, getmininginfo, getpeerinfo) and block information (getblockcount, getblock hash, getblockhash index)



Signing and Verifying message:

The digital signature is used for authenticating transactions by hashing a value of a message. When someone sent this message, that means this person had to be in possession of the private key in order to send the message, and the result anyone can verify the transaction.

The signing algorithm $(s) \leftarrow \text{Sign}(\text{message}, \text{private key})$ takes a message (m) and the private key (piv) and outputs a signature (s). This algorithm has to be processed on the client side because the users must use their (piv).

From the console, we need to create a P2PKH address to sign a message.

To create a new P2PKH address type

```
getnewaddress "anwar" "legacy"
```

To return your P2PKH address

```
getaddressesbylabel "anwar"
```

Note: Make sure you write your wallet name.

Sign message:

First you need to input the address and you can select any of your addresses from the contact book o

This is the P2PKH address:

myT7W362772ytDRyzrRxbEbx3sKuy25qe8

Message: Hello there

Signature: H3NRxR5BYh7WGpj392Nuua9jHVmsttqp323enchX5zYrE8B6VTRZKpcgVj0QXq4eV19AXe6XeKIm7UzMBvMCqhA=

Signatures - Sign / Verify a Message

Verify Message

You can sign messages/agreements with your addresses to prove you can receive bitcoins sent to them. Be careful not to sign anything vague or random, as phishing attacks may try to trick you into signing your identity over to them. Only sign fully-detailed statements you agree to.

1 myT7W362772ytDRyzrRxbEbx3sKuy25qe8 show your address

The Bitcoin address to sign the message with

2 Hello there Enter your message here

Signature

H3NRxR5BYh7WGpj392Nuua9jHVmsttqp323enchX5zYrE8B6VTRZKpcgVj0QXq4eV19AXe6XeKIm7UzMBvMCqhA=

3 Sign Message Sign the message Clear All

Message signed.

Verify a message:

The signature verification algorithm $\text{validity} \leftarrow \text{signVer}(m, s)$ requires a public key (pub), a message (m), and a signature (s) and returns true if $\text{hash}(m)$ corresponds with the signature. A string transaction is true if $\text{signVer}(\text{piv}, m, \text{Sign}(\text{pub}, m)) = \text{true}$, and otherwise the output is invalid.

Signatures - Sign / Verify a Message

Sign Message

Enter the receiver's address, message (ensure you copy line breaks, spaces, tabs, etc. exactly) and signature below to verify the message. Be careful not to read more into the signature than what is in the signed message itself, to avoid being tricked by a man-in-the-middle attack. Note that this only proves the signing party receives with the address, it cannot prove sendership of any transaction!

myT7W362772ytDRyzrRxbEbx3sKuy25qe8

Hello there

H3NRxR5BYh7W6pj392Nuua9jHVMsttqp323enchX5zYrE8B6VTRZKpcgVj0QXq4eV19AXe6XeKIm7UzMBvMCqhA=

? Verify Message ⊗ Clear All **Message verified.**

Look if we changed the signature that was given when the message was signed we received an error. Also if we changed the message, we got an error too.

Signatures - Sign / Verify a Message

Sign Message

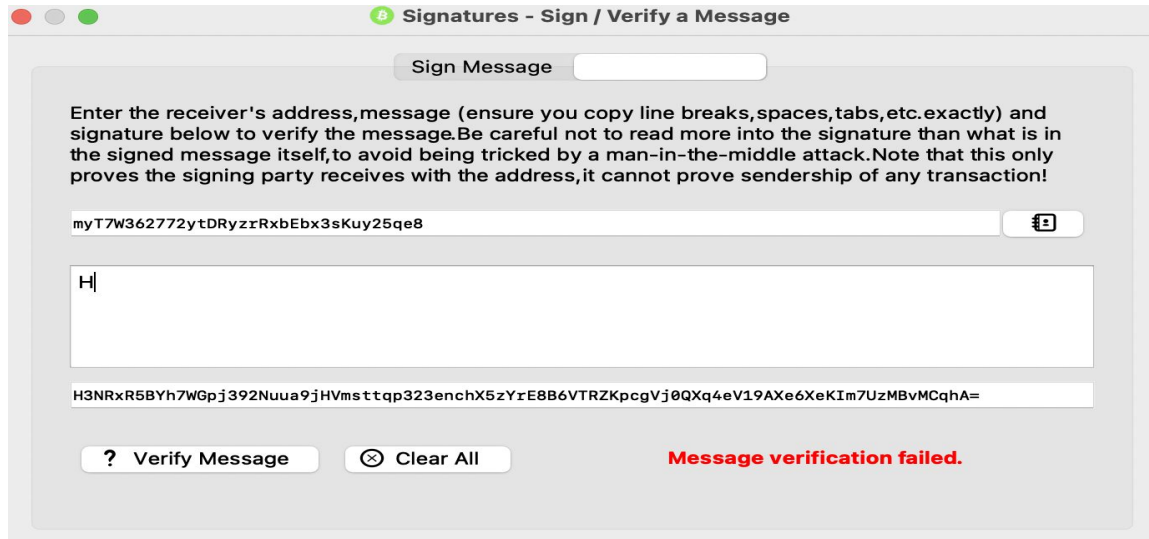
Enter the receiver's address, message (ensure you copy line breaks, spaces, tabs, etc. exactly) and signature below to verify the message. Be careful not to read more into the signature than what is in the signed message itself, to avoid being tricked by a man-in-the-middle attack. Note that this only proves the signing party receives with the address, it cannot prove sendership of any transaction!

myT7W362772ytDRyzrRxbEbx3sKuy25qe8

Hello there

H3NRxR5BYh7W6pj392Nuua9jHVMsttqp323enchX5zYrE8B6VTRZKpcgVj0QXq4eV19AXe6XeKIm7UzMBvMCqhA=

? Verify Message ⊗ Clear All **The signature could not be decoded. Please check the signature and try again.**



Homework:

- Create your own wallet and send bitcoin test to your address and then send **0.0005 - 0.0001** bitcoin to this address :

Also you need to find your transaction using this website
<https://live.blockcypher.com> and share the link of your transaction.

Note: when you don't need the coins anymore please send them back:

[tb1qm5tfegjevjj27yvna9elym9lnzcf0zraxgl8z2](https://bitcoinfaucet.uol.net)

<https://bitcoinfaucet.uol.net>