

Bitcoin Core 101

What this covers:

- Intro
- Free learning material
- Full Node (inc. setup script)
- Bitcoin Core commands

<u>Intended audience:</u>

A software developer taking first steps with Bitcoin Core or a pleb with an interest in code.



https://www.youtube.com/@python360

Bitcoin Core
Version vo.17.1

2009-2018 The Bitcon Core developers

Ditcoin Core
Version vo.17.1

2009-2018 The Bitcon Core developers

Ditcoin Core
Version vo.17.1

If you want to get hands-on:

run bitcoin-core on your laptop!

You can use Python code to demonstrate concepts

pip install python-bitcoinlib

View blockchain

Install Bitcoin Core

try out bitcoin-cli -regtest

(+ Run a Full Node if you want to help the network)

Isn't it just funny money?

"Crypto" is a scam

I heard people lost money

It's too slow

It uses too much energy

I thought this was a 'python channel'

https://en.bitcoin.it/wiki/Main_Page

Do you trust government and banks?



https://www.youtube.com/@python360

Bitcoin encompasses more aspects of computer science than you would ever imagine.

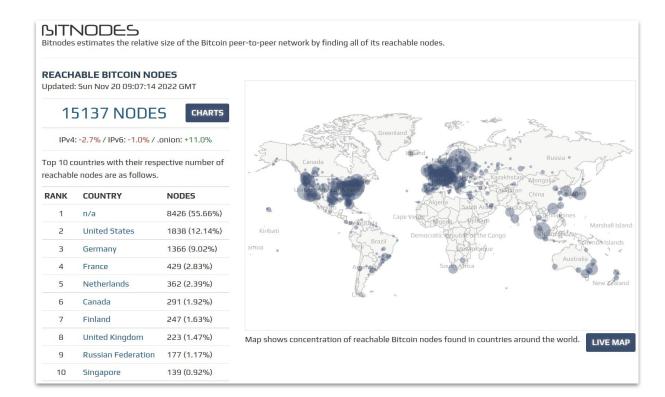
Nothing you learn will be 'redundant'

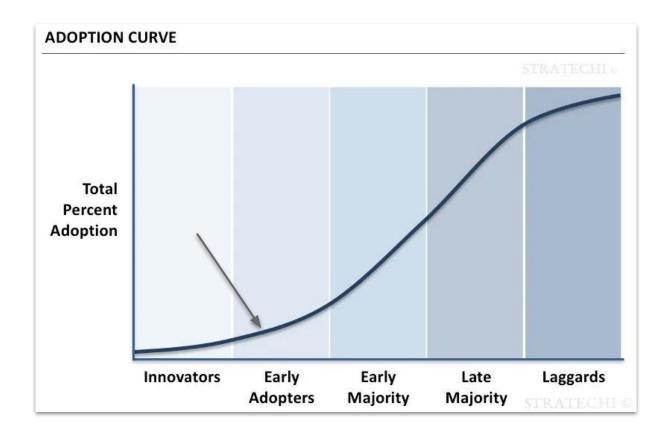
Think TCP/IP - it was niche and now...

TCP/IP was developed in the 1970s and adopted as the protocol standard for ARPANET (the predecessor to the Internet) in 1983.

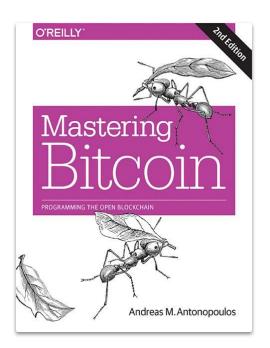


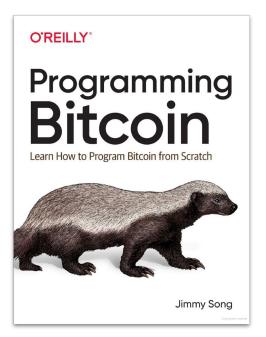
https://www.youtube.com/@python360



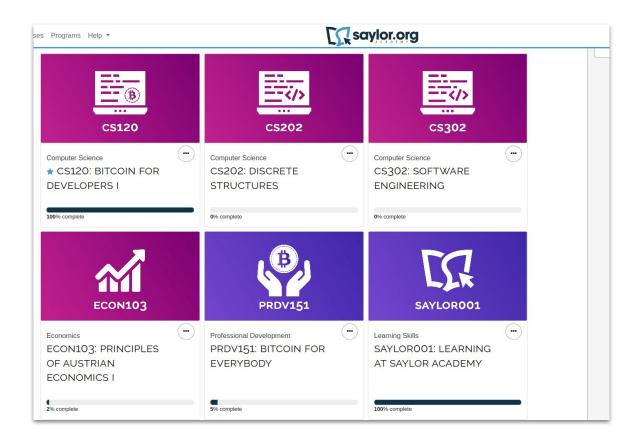


how do I learn more?





Saylor.org



Overview:

All the "Money" (Satoshis) stays on the blockchain, it just gets reallocated to different owners.

The "Price" of Bitcoin is just a conversion rate from FIAT (legacy $\mathfrak{L},\mathfrak{L}$)

Either using software on your phone or computer, or a "hardware wallet" you are able to "talk" to the blockchain and make transactions ("Buy", "Sell").

If you "Buy" or "Earn" some of the Bitcoin, it will be allocated to you, forever....(Until you spend it)



Can I write code in Python?

Yes, although for commercial purposes you would probably use another language (compiled)



```
$ pip install pybtc
import pybtc
a = pybtc.Address()
a.address
'bc1qqd8yzz8fv6aqvzu8xcj8fk5r3kc6qh3nzllmu5'
```



```
IPython 7.13.0 -- An enhanced Interactive Python. Type '?' for help.

In [1]: import pybtc

In [2]: a = pybtc.Address()

In [3]: a.address
Out[3]: 'bc1qgd8yzz8fv6aqvzu8xcj8fk5r3kc6qh3nzllmu5'

In [4]: pybtc.is_address_valid('bc1qgd8yzz8fv6aqvzu8xcj8fk5r3kc6qh3nzllmu5')
Out[4]: True
```

You have just created an address that is more unique than a single atom in the observable universe!

What is it for?

That address can be linked to you (Using software OR a "Hardware Wallet")



What is a full node, and why is it useful as a programmer?

It will allow you to write and test your own code to perform transactions on the blockchain, and understand the workings

I know what a full node is, how can I start trying out some code?

Bitcoind – a daemon program that implements the Bitcoin protocol

> ./bitcoind --daemon

https://en.bitcoinwiki.org/wiki/Bitcoind

https://bitcoincore.org/

https://bitcoincore.org/en/download/

It is free to download.

You can use it to develop code, or run a 'full node'

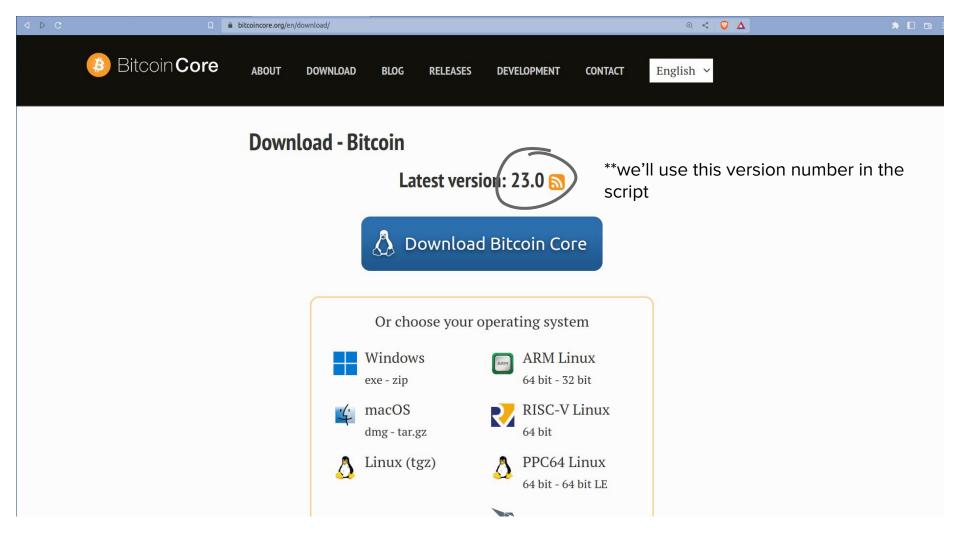


Bitcoin Core is an <u>open source</u> project which maintains and releases Bitcoin client software called "Bitcoin Core".

It is a direct descendant of the original Bitcoin software client released by Satoshi Nakamoto after he published the famous Bitcoin whitepaper.

Bitcoin Core consists of both "full-node" software for fully validating the blockchain as well as a bitcoin wallet. The project also currently maintains related software such as the cryptography library libsecp256k1 and others located at GitHub.

https://bitcoincore.org/en/about/



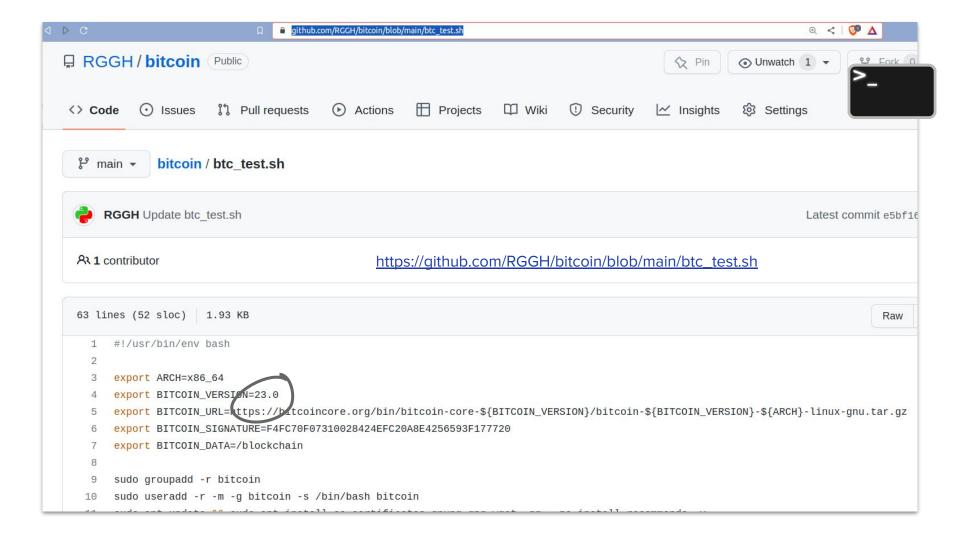


How can I get this set up?

Run a <u>script</u> to do this on Mac, Linux, Raspberry Pi

I have regtest running on a Ubuntu VPS with Webdock

```
This is a webserver based on the Ubuntu Jammy LEMP 8.1 Image
This stack is rocking Git, Composer, Node.js, npm and pip3, so go
ahead and be productive. Read up on how this stack was configured:
https://webdock.io/en/docs/stacks/ubuntu-lemp-81
Last login: Sat Nov 19 11:53:24 2022 from 1
admin@btcx:~$ uname-a
-bash: uname-a: command not found
admin@btcx:~$ uname -a
Linux btcx 5.15.0-52-generic #58-Ubuntu SMP Thu Oct 13 08:03:55 UTC 2022 x86 64 x86 64 x86 64 GNU/Linux
admin@btcx:~$
admin@btcx:~$
Linux btcx 5.15.0-52-generic #58-Ubuntu SMP Thu Oct 13 08:03:55 UTC 2022 x86_64 x86_64 x86_64 GNU/Linux
admin@btcx:~$ uname -a
-bash: uname-a: command not found
admin@btcx:~$ uname-a
```





Once the script has installed bitcoincore:

Bitcoind provides the RPC "interface" in which user can query with bitcoin-cli (or a library in c++).

You must run bitcoind before using bitcoin-cli

> ./bitcoind --daemon

Interacting with "Bitcoin Core":

The official implementation of the full node software...

If remotely installed on another computer: establish a **ssh** connection to the computer running "Bitcoin Core"

Regtest

Regression test mode

A local testing environment in which developers can almost instantly generate blocks on demand for testing events, and can create private satoshis with no real-world value.

Not to be confused with: Testnet (a global testing environment which mostly mimics mainnet)

https://developer.bitcoin.org/glossary.html?highlight=regression

```
admin@btcx:~$ bitcoin-cli -regtest -getinfo
Chain: regtest
Blocks: 1
Headers: 1
Verification progress: 100.0000%
Difficulty: 4.656542373906925e-10
Network: in 0, out 0, total 0
Version: 230000
Time offset (s): 0
Proxies: n/a
Min tx relay fee rate (BTC/kvB): 0.00001000
Balances
0.00000000 my_wallet
                                     bitcoin-cli -regtest -getinfo
0.00000000 my_wallet_pk
0.00000000 moo
```



bitcoin-cli -regtest scantxoutset start

'["raw(76a91411b366edfc0a8b66feebae5c2e25a7b6a5d1cf3188ac)#fm24fxxy"]'

```
admin@btcx:~$ bitcoin-cli -regtest scantxoutset start '["raw(76a91411b366edfc0a8b66feebae5c2e25a7b6a5d1cf3188ac)#fm24fxxy"]'
{
    "success": true,
    "txouts": 1,
    "height": 1,
    "bestblock": "38973495784add9f2519a8ae57fbc8b948e9630aeb7fa6a087698ff47b6188fa",
    "unspents": [
    ],
    "total_amount": 0.000000000
}
admin@btcx:~$ sc
```

"Scans the unspent transaction output set for entries that match certain output descriptors"



\$ bitcoin-cli -regtest createwallet moo \$ bitcoin-cli -regtest -rpcwallet=moo -generate

```
admin@btcx:~$ bitcoin-cli -regtest -generate
error code: -19
error message:
Wallet file not specified (must request wallet RPC through /wallet/<filename> uri-path).
Try adding "-rpcwallet=<filename>" option to bitcoin-cli command line.
admin@btcx:~$ bitcoin-cli -regtest -rpcwallet=moo -generate
{
    "address": "bcrt1ql33rvtslkqn949kge9fxeuv0pca8pf0hm3c55t",
    "blocks": [
        "0036fac0a1ad350615427c19b184d18a1805603d92b397933333b83de67c50d7"
    ]
}
admin@btcx:~$
```



\$ bitcoin-cli -regtest -rpcwallet=moo -generate 2

```
dmin@btcx:~$ bitcoin-cli -regtest -rpcwallet=moo -generate 2
 "address": "bcrt1q4xaudr3k9034u7k2k9reeyh4h52gkk7k0u3fum",
 "blocks": [
   "50e29a67baa7a74664eb04d61529bf04cc7fb96dad2f114cb2aadfaac2ceaa44",
   "4f0dc778f3bbecfb1bf5f3374b7a11bc8db348f233df5662c4088383cdc5a131"
admin@btcx:~$ bitcoin-cli -regtest -rpcwallet=moo getwalletinfo
 "walletname": "moo",
 "walletversion": 169900,
 "format": "sqlite",
 "balance": 0.00000000,
 "unconfirmed balance": 0.00000000
 "immature_balance": 200.00000000,
 "txcount": 4,
 "keypoolsize": 4000,
 "keypoolsize_hd_internal": 4000,
 "paytxfee": 0.000000000
 "private_keys_enabled": true,
 "avoid_reuse": false,
 "scanning": false,
 "descriptors": true,
 "external_signer": false
dmin@btcx:~$
```

\$ bitcoin-cli -regtest -rpcwallet=moo getwalletinfo

```
admin@btcx:~$ bitcoin-cli -regtest -rpcwallet=moo getwalletinfo
  "walletname": "moo",
  "walletversion": 169900,
  "format": "sqlite",
  "balance": 7850.00000000,
  "unconfirmed_balance": 0.00000000,
  "immature balance": 2500.00000000,
  "txcount": 265,
  "keypoolsize": 4000,
  "keypoolsize hd internal": 4000,
  "paytxfee": 0.00000000,
  "private keys enabled": true,
  "avoid reuse": false,
  "scanning": false,
  "descriptors": true,
  "external signer": false
```

https://www.youtube.com/@python360



\$ bitcoin-cli -regtest -rpcwallet=moo -generate 2
\$ bitcoin-cli -regtest -rpcwallet=moo getblockcount

```
admin@btcx:~$ bitcoin-cli -regtest -rpcwallet=moo -generate 2
{
    "address": "bcrt1qxsz8wq4k5aw3hgwxm2yl8fuavmn7m4wm04u2ha",
    "blocks": [
    "7912147023ec2c18c2b2f9f02bd1bd5d31f0d20dd8e2adbcca2a1cc1aaa3f44f",
    "7647bfd05f9e68c3b3130a1fece231e977bc17e4737c3e0e50bf7f50f7c4572b"
    ]
}
admin@btcx:~$ bitcoin-cli -regtest getblockcount
6
```



Examples:

- > bitcoin-cli createrawtransaction "[{\"txid\":\"myid\",\"vout\":0}]" "[{\"address\":0.01}]"
- > bitcoin-cli createrawtransaction "[{\"txid\":\"myid\",\"vout\":0}]" "[{\"data\":\"00010203\"}]"
- > curl --user myusername --data-binary '{"jsonrpc": "1.0", "id": "curltest", "method": "createrawtransaction", "params":
- ["[{\"txid\":\"myid\",\"vout\":0}]", "[{\"address\":0.01}]"]}' -H 'content-type: text/plain;' http://127.0.0.1:8332/
- > curl --user myusername --data-binary '{"jsonrpc": "1.0", "id": "curltest", "method": "createrawtransaction", "params":
- ["[{\"txid\":\"myid\",\"vout\":0}]", "[{\"data\":\"00010203\"}]"]}' -H 'content-type: text/plain;' http://127.0.0.1:8332/

```
Examples:

> bitcoin-cli createrawtransaction "[{\"txid\":\"myid\",\"vout\":0}]" "[{\"address\":0.01}]"

> bitcoin-cli createrawtransaction "[{\"txid\":\"myid\",\"vout\":0}]" "[{\"data\":\"00010203\"}]"

> curl --user myusername --data-binary '{"jsonrpc": "1.0", "id": "curltest", "method": "createrawtransaction",

0.01}]"]}' -H 'content-type: text/plain;' http://127.0.0.1:8332/

> curl --user myusername --data-binary '{"jsonrpc": "1.0", "id": "curltest", "method": "createrawtransaction",

0010203\"}]"]}' -H 'content-type: text/plain;' http://127.0.0.1:8332/
```

find a block's hash, then retrieve it

>_

- \$ bitcoin-cli -regtest getblockhash 1
- \$ bitcoin-cli -regtest getblock 38973495784add9f2519a8ae57fbc8b948e9630aeb7fa6a087698ff47b6188fa

```
admin@btcx:~$ bitcoin-cli -regtest getblockhash 1
38973495784add9f2519a8ae57fbc8b948e9630aeb7fa6a087698ff47b6188fa
admin@btcx:~$ bitcoin-cli -regtest getblock 38973495784add9f2519a8ae57fbc8b948e9630aeb7fa6a087698ff47b6188fa
 "hash": "38973495784add9f2519a8ae57fbc8b948e9630aeb7fa6a087698ff47b6188fa",
 "confirmations": 13,
 "height": 1,
 "version": 536870912,
 "versionHex": "20000000",
 "merkleroot": "5b12d4058c63e8003994640779340ead0acd7186fd9182a1b93f08788663b59e",
 "time": 1668723549,
 "mediantime": 1668723549,
 "nonce": 0,
 "bits": "207ffffff",
 "difficulty": 4.656542373906925e-10,
 "nTx": 1,
 "previousblockhash": "0f9188f13cb7b2c71f2a335e3a4fc328bf5beb436012afca590b1a11466e2206",
 "nextblockhash": "0036fac0a1ad350615427c19b184d18a1805603d92b397933333b83de67c50d7",
 "strippedsize": 213,
 "size": 249,
 "weight": 888,
 "tx": [
   "5b12d4058c63e8003994640779340ead0acd7186fd9182a1b93f08788663b59e'
admin@btcx:~$
```



find the tx and then you can look up the raw transaction next

```
admin@btcx:-$ bitcoin-cli -regtest getblock 38973495784add9f2519a8ae57fbc8b948e9630aeb7fa6a087698ff47b6188fa
 "hash": "38973495784add9f2519a8ae57fbc8b948e9630aeb7fa6a087698ff47b6188fa",
 "confirmations": 13,
 "height": 1,
 "version": 536870912,
 "versionHex": "20000000",
 "merkleroot": "5b12d4058c63e8003994640779340ead0acd7186fd9182a1b93f08788663b59e",
 "time": 1668723549,
 "mediantime": 1668723549,
 "nonce": 0,
 "bits": "207fffff",
 "difficulty": 4.656542373906925e-10,
 "nTx": 1,
 "previousblockhash": "0f9188f13cb7b2c71f2a335e3a4fc328bf5beb436012afca590b1a11466e2206",
 "nextblockhash": "0036fac0a1ad350615427c19b184d18a1805603d92b397933333b83de67c50d7",
 "strippedsize": 213,
 "size": 249,
 "weight": 888,
 "tx": [
   "5b12d4058c63e8003994640779340ead0acd7186fd9182a1b93f08788663b59e"
admin@btcx:~$
```

https://www.youtube.com/@python360



```
admin@btcx:~$ bitcoin-cli -regtest getblockchaininfo
 "chain": "regtest",
 "blocks": 13,
 "headers": 13.
 "bestblockhash": "34cfa092f6988aead20f162f8a2d49dbc63520a4de38aed82051136badc13af6",
 "difficulty": 4.656542373906925e-10,
 "time": 1668776368,
 "mediantime": 1668776367,
 "verificationprogress": 1,
 "initialblockdownload": false,
 "size on disk": 4167,
 "pruned": false,
 "warnings": ""
                              https://www.youtube.com/@python360
```

>_

Bitcoin

bitcoin-cli -regtest -rpcwallet=moo generatetoaddress 101 \$(bitcoin-cli -regtest -rpcwallet=moo getnewaddress)

```
"097f3e9c6d0641534aff0a2421a84a07511b2df3d21ad80e6de3e2f38048a165",  
"74283b982a6829069b10b4c3b0261425278f7c675334728b2795925e758efceb",  
"0daa1e2b283b1831d3c3c69f4aee244a5fcd2cc6870e0d711f082db549b2767d",  
"52ca5ffc82907d10716a26c31eff8f752ac550a00677466db988f44ff277dbce",  
"7b4923aebe48c2eda850cdcc261c751b69b83b7034bef6e33ff3056763c80666",  
...
```

Mine blocks immediately to a specified address



bitcoin-cli -regtest -rpcwallet=moo listunspent

```
"txid": "814a2422666794e71e7d0aeff5b81a8aaccc815154e7b3e5e324f04bd8e45400".
"vout": 0,
"address": "bcrt1q7yl6prcjj4k62tw46sszrrpettmazj0kzspkt8",
"label": "".
"scriptPubKey": "0014f13fa08f12956da52dd5d420218c395af7d149f6",
"amount": 50.00000000.
"confirmations": 135.
"spendable": true,
"solvable": true.
"desc": "wpkh([84bdebb1/84'/1'/0'/0/6]03d06b384cc175071c64999c79f08425600e6824b42932f47dfd01d8448eca334d)#n6fzfnl9",
"safe": true
"txid": "62f7bbcc7c3f6477530b2632b4f0af8ad04ff9fa3b0e33fe8a8e360873afe001",
"vout": 0.
```

https://www.youtube.com/@python360



```
admin@btcx:~$ bitcoin-cli -regtest -rpcwallet="moo" createrawtransaction '[{ "txid": "9c42a8167e88c5f566ae0a4d10e17fa70081691d14b91938aaf83df9cedf4d07", "vout": 1}]' '{"bcrt1qc2f4e3kq3xeunhk5csuguufgtka7hz8g9x40kp": 0.111, "bcrt1q8vculfa05wr6vhyh70nyw55jgd8aau2qxrl3nf": 49.888}'
```

*get your txid from a UTXO in your wallet

admin@btcx:~\$ bitcoin-cli -regtest -rpcwallet="moo" createrawtransaction '[{ "txid": "9c42a8167e88c5f566ae0a4d10e17fa70081691d14b91938aa
f83df9cedf4d07", "vout": 1}]' '{"bcrt1qc2f4e3kq3xeunhk5csuguufgtka7hz8g9x40kp": 0.111, "bcrt1q8vculfa05wr6vhyh70nyw55jgd8aau2qxrl3nf": 4
9.888}'

 $0200000001074 ddfcef93 df8aa3819b9141d698100a77fe1104d0aae66f5c5887e16a8429c0100000000fffffff62605fa9000000000160014c2935cc6c089b3c9ded4\\c4388e71285dbbeb88e8000c5b29010000001600143b31cfa7afa387a65c97f3e6475292434fdef14000000000$

admin@btcx:~\$



bitcoin-cli -regtest -rpcwallet="moo" signrawtransactionwithwallet

020000001074ddfcef93df8aa3819b9141d698100a77fe1104d0aae66f5c5887e16a8429c0100000000fffffff02605fa900000000160014c2 935cc6c089b3c9ded4c4388e71285dbbeb88e8000c5b29010000001600143b31cfa7afa387a65c97f3e6475292434fdef14000000000

```
admin@btcx:~$ bitcoin-cli -regtest -rpcwallet="moo" signrawtransactionwithwallet 0200000001074ddfcef93df8aa3819b9141d698100a77fe1104d0aa
e66f5c5887e16a8429c01000000000fffffffff02605fa90000000000160014c2935cc6c089b3c9ded4c4388e71285dbbeb88e8000c5b29010000001600143b31cfa7afa38
7a65c97f3e6475292434fdef14000000000
  "hex": "0200000001074ddfcef93df8aa3819b9141d698100a77fe1104d0aae66f5c5887e16a8429c0100000000ffffffff02605fa9000000000160014c2935cc6c0
89b3c9ded4c4388e71285dbbeb88e8000c5b29010000001600143b31cfa7afa387a65c97f3e6475292434fdef14000000000",
  "complete": false,
  "errors": [
      "txid": "9c42a8167e88c5f566ae0a4d10e17fa70081691d14b91938aaf83df9cedf4d07",
     "vout": 1,
      "witness": [
      "scriptSig": "",
     "sequence": 4294967295,
      "error": "Input not found or already spent"
admin@btcx:~$
```

https://developer.bitcoin.org/examples/testing.html

https://developer.bitcoin.org/examples/transactions.html



Bitcoin

\$ bitcoin-cli -regtest -rpcwallet=moo getbalance

3200.00000000

bitcoin-cli -regtest -rpcwallet="testx" getnewaddress bcrt1qc2f4e3kq3xeunhk5csuguufgtka7hz8g9x40kp

```
admin@btcx:~$ bitcoin-cli -regtest -rpcwallet=moo getunconfirmedbalance
0.00000000
admin@btcx:~$ bitcoin-cli -regtest -rpcwallet=moo getbalance
7850.00000000
```



```
admin@btcx:~$ bitcoin-cli -regtest -rpcwallet="testx" getnewaddress
bcrt1qc2f4e3kq3xeunhk5csuguufgtka7hz8g9x40kp
```

```
admin@btcx:~$ bitcoin-cli -regtest validateaddress bcrt1qc2f4e3kq3xeunhk5csuguufgtka7hz8g9x40kp
{
    "isvalid": true,
    "address": "bcrt1qc2f4e3kq3xeunhk5csuguufgtka7hz8g9x40kp",
    "scriptPubKey": "0014c2935cc6c089b3c9ded4c4388e71285dbbeb88e8",
    "isscript": false,
    "iswitness": true,
    "witness_version": 0,
    "witness_program": "c2935cc6c089b3c9ded4c4388e71285dbbeb88e8"
}
admin@btcx:~$
```



General Info

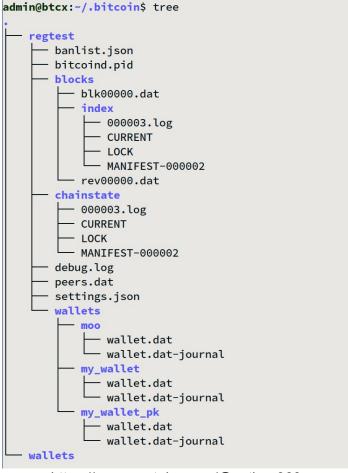
getblockchaininfo getmininginfo getpeerinfo

Block Info

getblockcount getbestblockhash getblock hash getblockhash index

Transaction Info

getrawmempool getrawtransaction txid decoderawtransaction rawtx



https://www.youtube.com/@python360



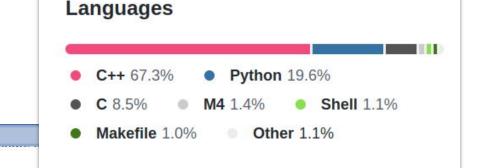


admin@btcx:~/.bitcoin/regtest/wallets/my_wallet\$ tree
.
—— wallet.dat
— wallet.dat-journal

To be on the safe side, core wallet clients store their private keys in the wallet.dat file, acting as a master private key. The wallet.dat files hold your private keys, addresses, and transaction data. When these private keys or wallet.dat files are lost, it's impossible to recover your wallet and the funds in it.

DC

README.md



There are also regression and integration tests, written in Python. These tests can be run (if the test dependencies are installed) with: test/functional/test_runner.py

@ github.com/bitcoin/bitcoin

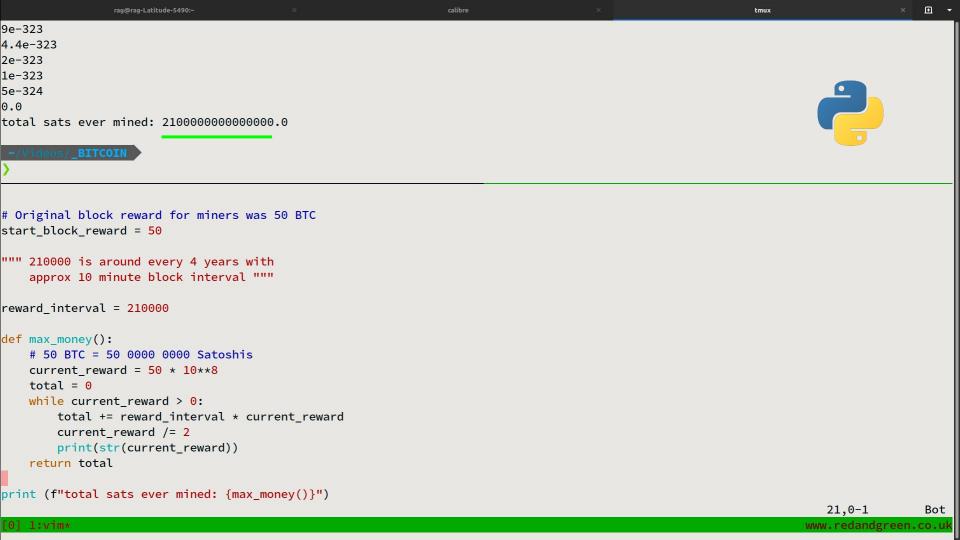
The CI (Continuous Integration) systems make sure that every pull request is built for Windows, Linux, and macOS, and that unit/sanity tests are run automatically.

Manual Quality Assurance (QA) Testing

Changes should be tested by somebody other than the developer who wrote the code. This is especially important for large or high-risk changes. It is useful to add a test plan to the pull request description if testing the changes is not straightforward.

```
# Original block reward for miners was 50 BTC
start block reward = 50
""" 210000 is around every 4 years with
    approx 10 minute block interval """
reward interval = 210000
def max money():
    # 50 BTC = 50 0000 0000 Satoshis
    current_reward = 50 * 10**8
    total = 0
    while current_reward > 0:
        total += reward interval * current reward
        current reward /= 2
        print(str(current reward))
    return total
print (f"total sats ever mined: { max money()}")
```





not your keys, not your coins...





