



Exchange Digital Money using Bitcoin and Python

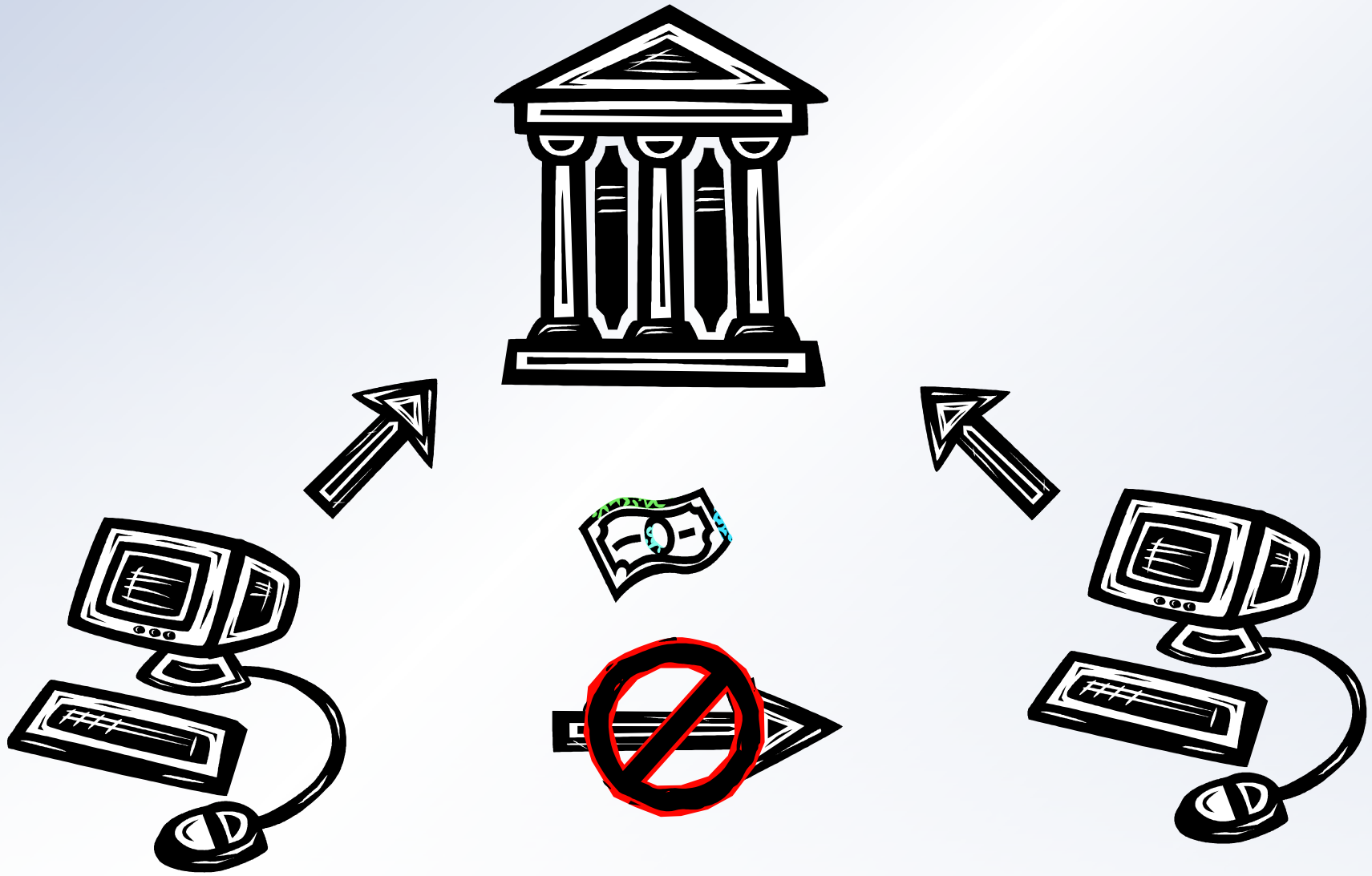
31 July 2011

David Steele
@dsteele
(+)dsteele@gmail.com

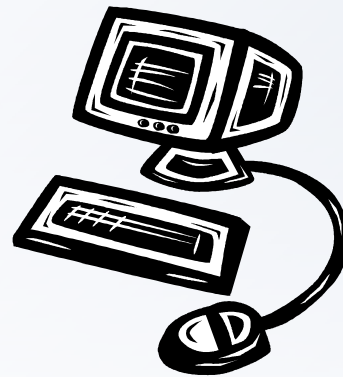
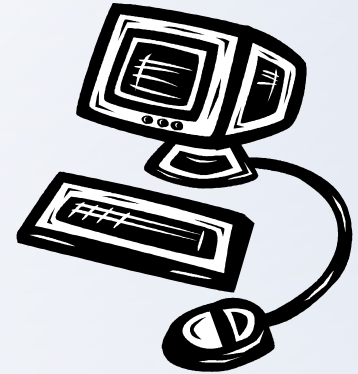
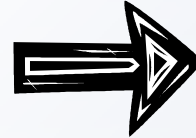
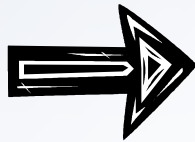
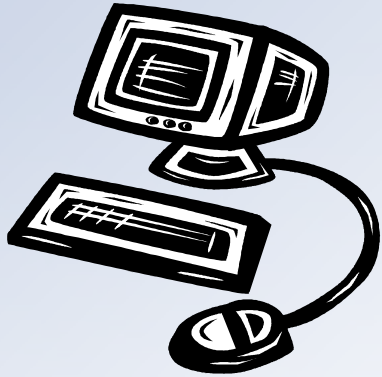
Resources

- Presentation
 - <http://davesteele.github.com/python-bitcoin-talk/>
- Software
 - {apt-get|yum} install git python-simplejson python-irclib pygame Django
 - Or 'easy_install simplejson python-irclib pygame Django'
 - git clone git://github.com/davesteele/python-bitcoin-talk.git











Block

1/3/09

t - 10 min

t



Transaction

Debit		Credit	
Address	AMT	Address	AMT
1LqRY...	17.21	avHR7...	5.00
		1LqRY...	12.21

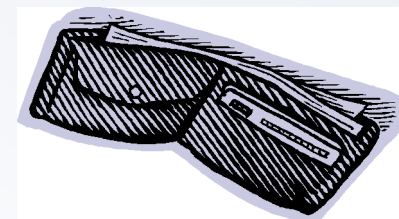
Address

1LqRY...

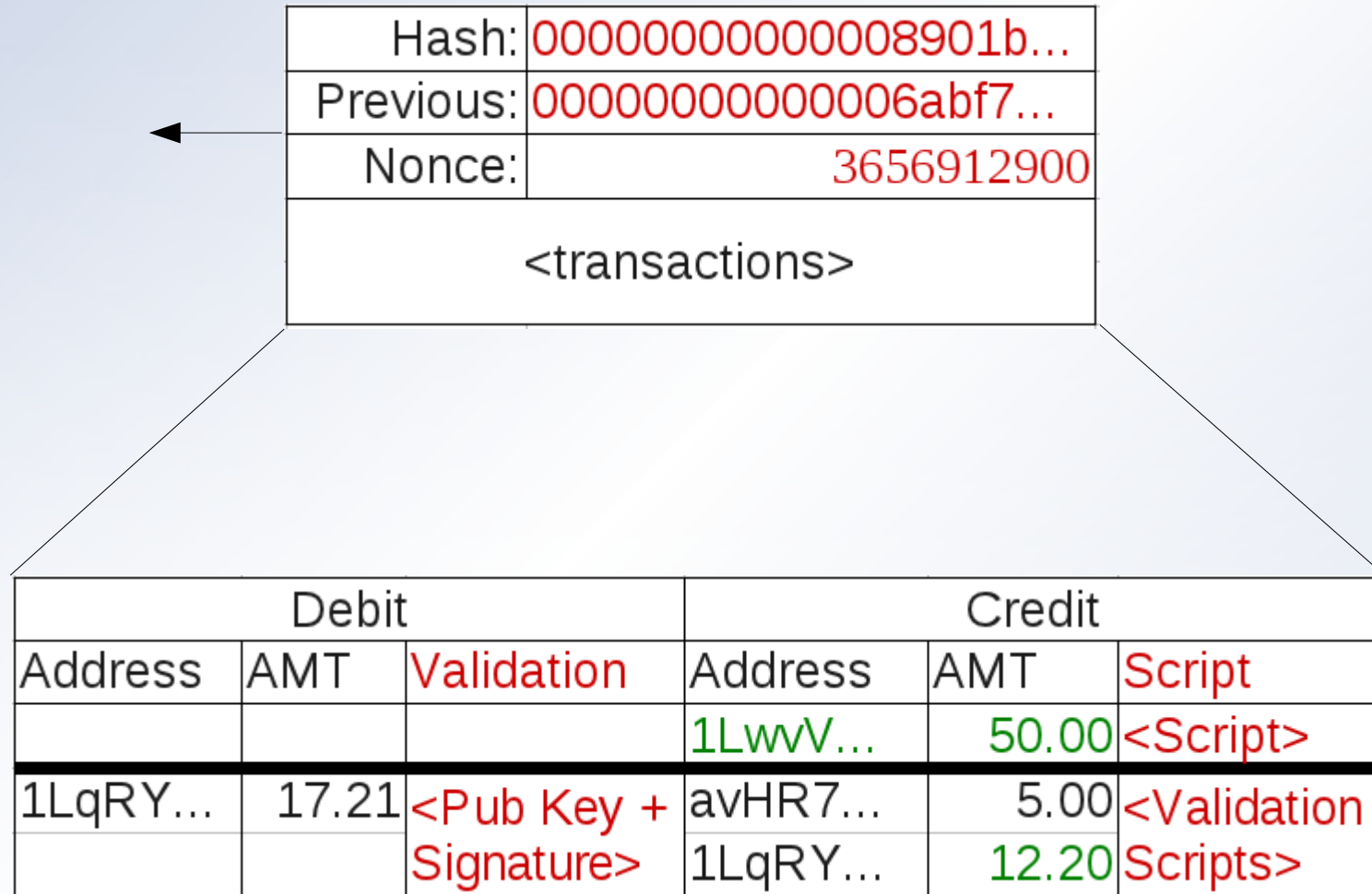
Public Key

Private Key

Hash



The Secret Sauce...



Terminology

- The Bitcoin ledger consists of a communally-maintained chain of Blocks containing Transactions which record balance transfers between Addresses
- Addresses are derived from a hash of the public key for a public/private key pair stored in the private Wallet
- Transactions are Confirmed as they become embedded in the Longest Block Chain
- Addresses can be aggregated locally in the Wallet using text Labels, also called Accounts

The screenshot shows a web browser window with two tabs: "Tx acba2d6864... - Bitcoin" and "Bitcoin P2P Virtual Curren...". The address bar shows "bitcoin.org". The browser's bookmark bar includes "GTD", "English", "Send Link", "Instapaper Text", "newsmap", and "Other Bookmarks".

bitcoin

P2P Virtual Currency

Bitcoin is a peer-to-peer currency. Peer-to-peer means that no central authority issues new money or tracks transactions. These tasks are managed collectively by the network.

Resources

- [What is Bitcoin?](#)
- [FAQ](#)
- [Wiki / Help](#)
- [Forum](#)
- [Sites That Accept Bitcoin](#)
- [Merchant Howto](#)
- [Bitcoin Charts / Markets](#)

Download

Bitcoin 0.3.24

- [Windows \(zip\)](#) 5.8MB
- [Windows \(exe\)](#) 5.8MB
- [Linux](#) 9.8MB
- [Mac OS X](#) 7.7MB (0.3.23)

Latest source code: [GitHub](#)

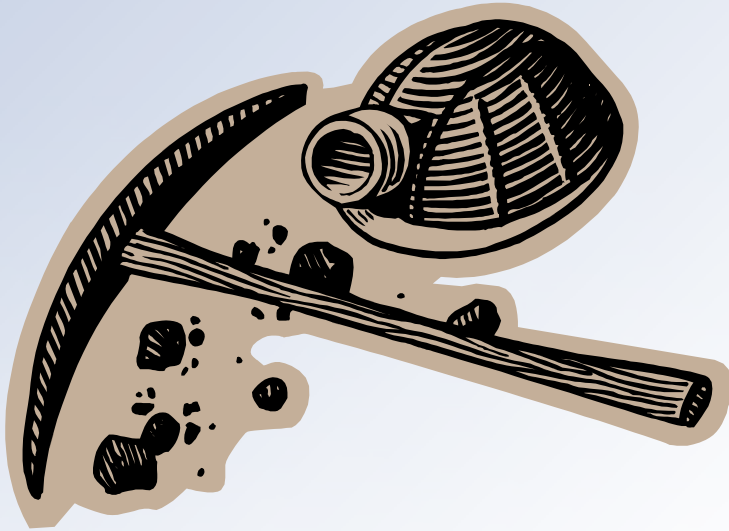
Project

- Community-driven open source, released under the [MIT license](#)
- Based on Satoshi Nakamoto's paper [Bitcoin: A Peer-to-Peer Electronic Cash System](#)
- Project Developers
 - Satoshi Nakamoto
 - Gavin Andresen - gavinandresen@gmail.com ([PGP](#))
 - Amir Taaki - genjix@riseup.net ([PGP](#))
 - Pieter Wuille
 - Nils Schneider - nils.schneider@gmail.com
 - Jeff Garzik - jgarzik@exmulti.com ([PGP](#))
- Press mailing list for presentation and interview requests: bitcoin-press@lists.sourceforge.net

Community

- Join the [Bitcoin Forum](#)
- Join the project's lively IRC channels on the [FreeNode](#) network or use the [FreeNode Web IRC](#).
 - [#bitcoin](#) (General Bitcoin-related)
 - [#bitcoin-dev](#) (Development and technical)
 - [#bitcoin-otc-foyer](#) (Over The Counter exchange)
 - [#bitcoin-market](#) (Live quotes from markets)
 - [#bitcoin-mining](#) (GPU mining related)
- [Twitter Search](#)
- [Facebook Page](#)

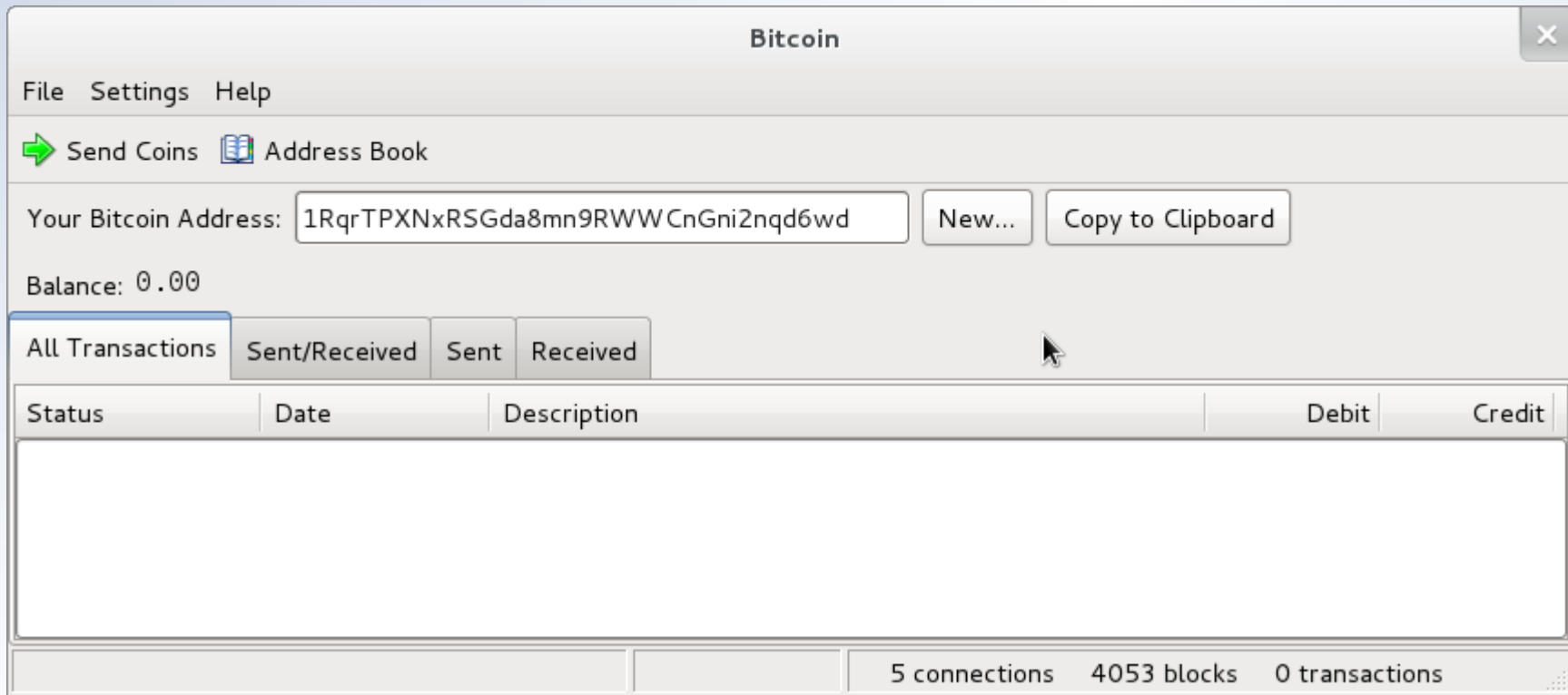
Getting Bitcoins



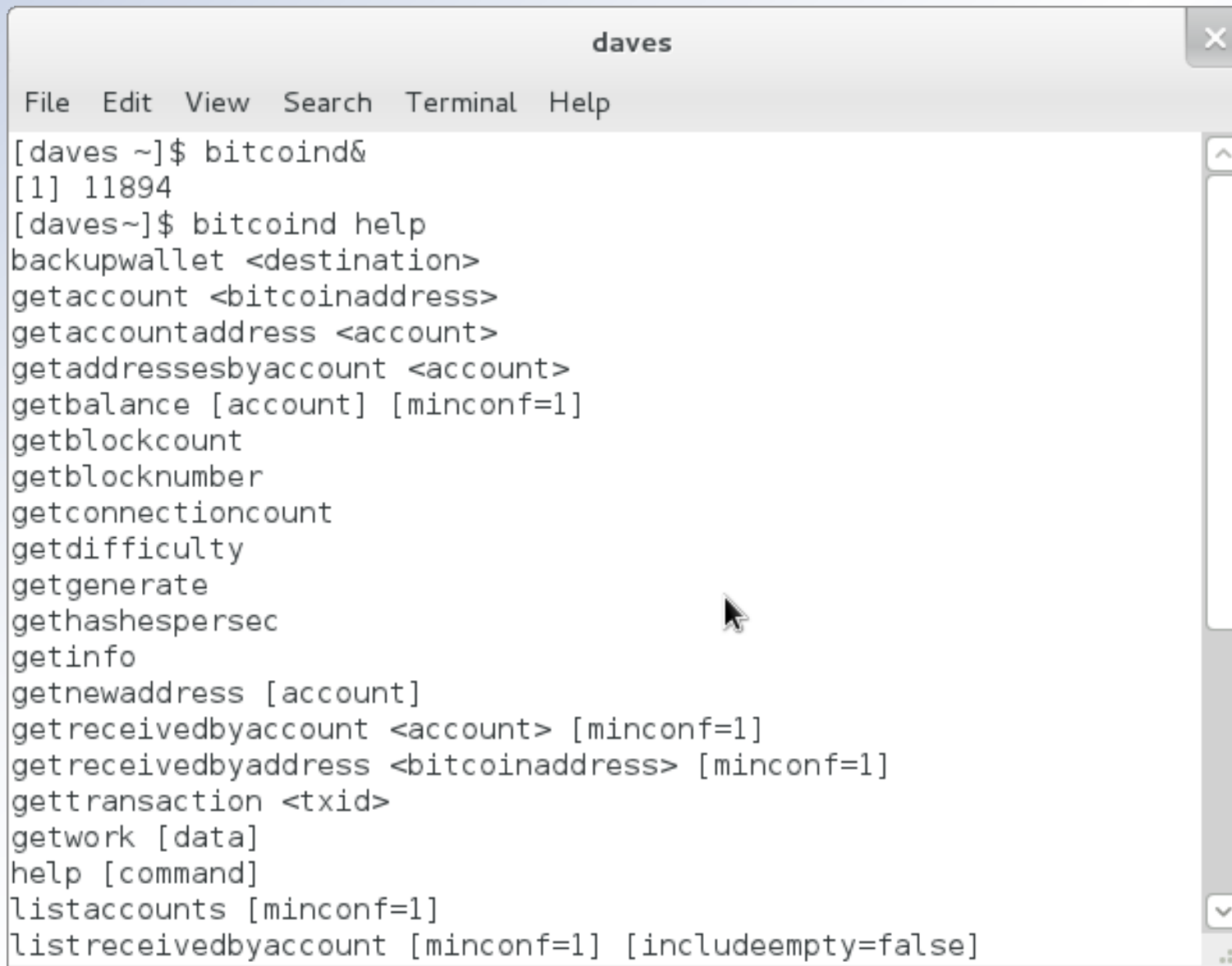
OR



GUI Client



bitcoind

A terminal window titled "daves" with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the execution of "bitcoind" and "bitcoind help", resulting in a list of bitcoind commands and their options. A mouse cursor is visible over the terminal text.

```
daves
File Edit View Search Terminal Help
[daves ~]$ bitcoind&
[1] 11894
[daves~]$ bitcoind help
backupwallet <destination>
getaccount <bitcoinaddress>
getaccountaddress <account>
getaddressesbyaccount <account>
getbalance [account] [minconf=1]
getblockcount
getblocknumber
getconnectioncount
getdifficulty
getgenerate
gethashespersec
getinfo
getnewaddress [account]
getreceivedbyaccount <account> [minconf=1]
getreceivedbyaddress <bitcoinaddress> [minconf=1]
gettransaction <txid>
getwork [data]
help [command]
listaccounts [minconf=1]
listreceivedbyaccount [minconf=1] [includeempty=false]
```

bitcoind JSON-RPC using Python

- rpcuser and rpcpassword defined in
~/.bitcoin/bitcoin.conf

- Install python-bitcoinrpc

<https://github.com/jgarzik/python-bitcoinrpc>

- bitcoind running

- Ports 8332 and 8333 accessible

- API Calls are defined at

https://en.bitcoin.it/wiki/Original_Bitcoin_client/API_Calls_list

```
bitcoinclishort.py x
#!/usr/bin/python

from jsonrpc import ServiceProxy

PROXY = ServiceProxy( "http://me:mypassword@127.0.0.1:8332" )

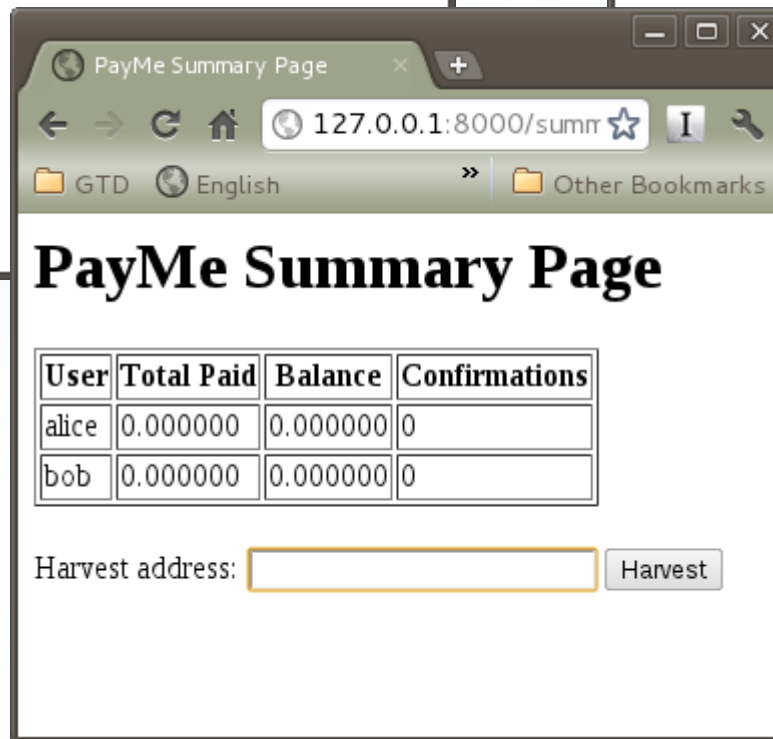
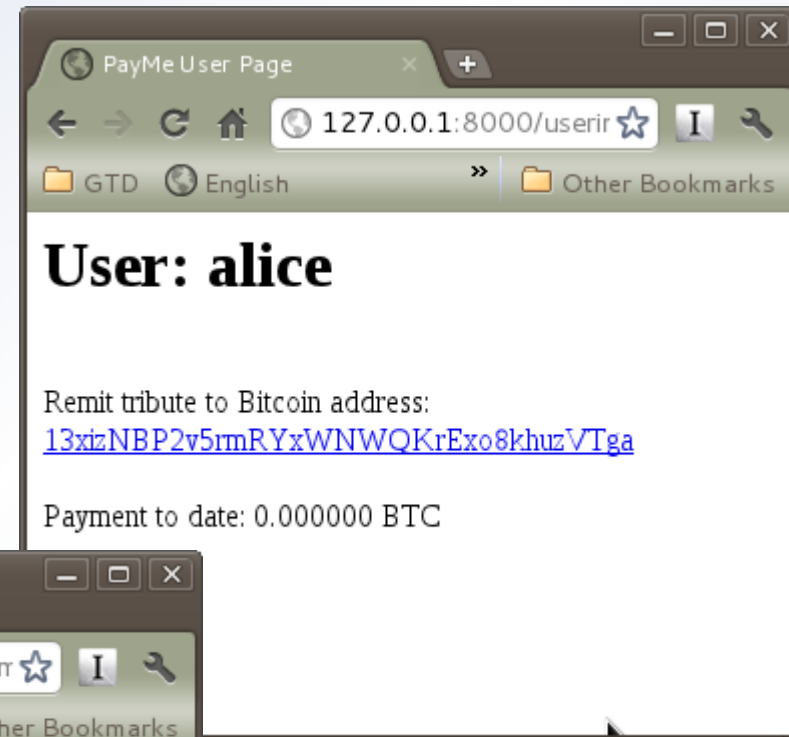
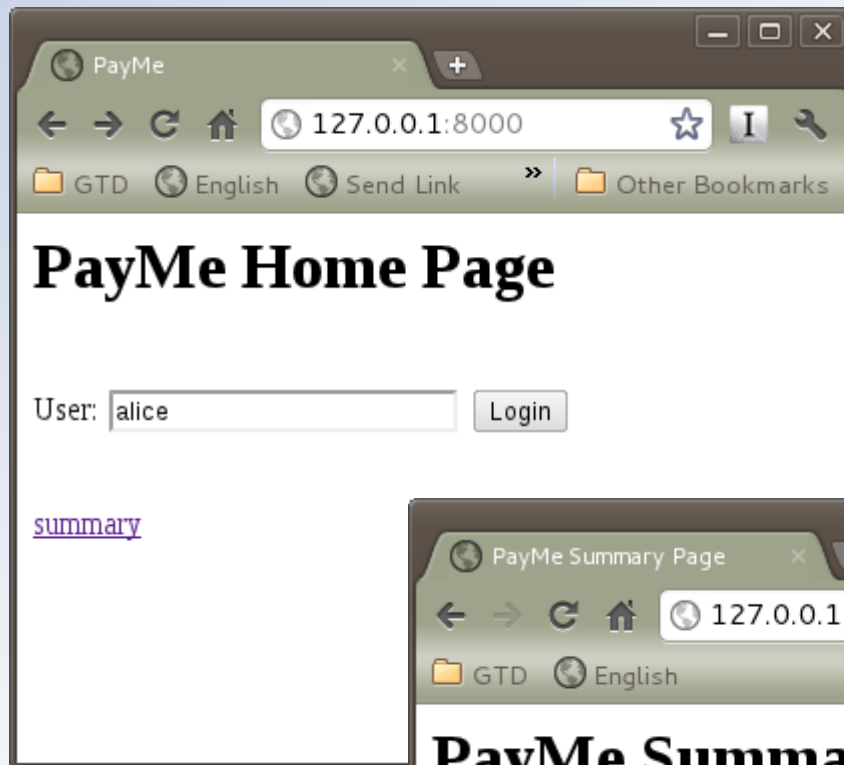
BTINFO = PROXY.getinfo()

print "BitCoin stats"

for key in BTINFO.keys():
    print "    %s; %s" % ( key, BTINFO[key] )

print "See https://en.bitcoin.it/wiki/Original_Bitcoin_client/API_Calls_list"
print "for the full list of functions available"
```

Example Django Website



"Bitcoin Watch" Monitor

The image shows a screenshot of an IRC window titled "FreeNode: #bitcoin-watch". The window displays a list of Bitcoin transactions with their IDs, amounts, and addresses. Below the IRC window, a terminal window titled "daves:~/bitcointalk" is open, showing the Python code for a bot named "BitcoinWatchBot".

```
FreeNode: #bitcoin-watch
freenode | Streaming Bitcoin Transactions/Markets || Thanks to bitcoincharts.com for the data feed. || LR=Liberty Reserve, MB=Money Bookers, PX=Pecunix, PP=PayPal, YX=Yandex, WM=WebMoney || Support this service...
#bitcoin-watch
[22:08] Txn e40a403f4da071ad332cd4102f6ae6dc9f94cb223c4c3917b074dc1abe1bbf04: 1Ab730xqvE7vtj4DPzdZqmuJswAv7kuaEK 0.16 BTC, 1HmkQ59haTqBraawLxPHKiKyzgAMeEr5FN 0.0395 BTC
[22:08] Txn 9cac293f057332fc67a844ae5abfc3837e7cb22d6a18df850269859ec19c8032: 15K629Uuiy1fw2bDbHN2r7aTsdRuRYSDpvv 0.16 BTC, 1AVh5DaauZnZqpNgSFuDe2n7DcF2YDH0eq 0.0395 BTC
[22:08] Txn 2e9f214f065fa6237fc0cea175d4986658cdc79e4505bb67fed3c53c415ff071: 1GunEjMq1CXNjR1EnMDM29k8k6wxvVKuzx 40.19648305 BTC, 1B335NoZLZaStfwefJBcE17RpSfDsTN8j 0.17 BTC
[22:08] Txn 87a07b18df98568467d9db449169db5b19e478d9248921b8176840b67e9c26d: 1Ab730xqvE7vtj4DPzdZqmuJswAv7kuaEK 0.16 BTC, 1GrPTHvTaiFRBQ4V7Y5GmUSyG6HPkqDo 0.0395 BTC
[22:08] Txn bff43551f8215d051147f07623fce46d49a1e87333d44b34cb08ec723c960b00: 13Rf00wvEqZuR8vBwYhrEzNmM9ofNXNRCT 1.00 BTC, 1En4VU4EX3FwC7p12U1tdztWkoMqzG2Fvt 0.32 BTC
[22:08] Txn f605b20be38997e9f7f04fd57730387a67b0086b081ec31e93a141eb79d6244e: 16o11Cqs59HpoHABVe2S6W817QtBTYxwkT 0.20 BTC, 12rZL2QujB81Rf88TJKnwXZiVAXaCb020 0.029 BTC
[22:08] Txn 1cc7c122505dff00f62b7c11db30bb321b7877cb9e379ac01ffa69c0cf2450fa: 1Ab730xqvE7vtj4DPzdZqmuJswAv7kuaEK 0.20 BTC, 1CSrTvr4u4yzrdNDzTGwwUDqCBvAHjT6V4 0.0995 BTC
[22:08] Txn 39d2a312ebe5fb67eaa028bb4552b1f7f6bdafb902f19c8d49916a22a0996f69: 1GQ3EznNznhxqHATFr3ngsFKVtY5AtcZCU 40.071 BTC, 12xDHkJcbFmyFhdogHDUHMKYHA9Z6r34cY 0.51 BTC
[22:08] Txn de51ec8ae43b47fb2fac07bf8d658c4a810f87ab7155cbf7807d8e01982aad3c: 1Ab730xqvE7vtj4DPzdZqmuJswAv7kuaEK 0.16 BTC, 1BmeFmqbGPPCNBL8DX96ud81VhtCdSohES 0.0395 BTC
[22:08] Txn 18b201b121b98e8d990b5f91bbfab361e14de6237b8ac9acebb1420fbe17f6b5: 13LLyZwtFDDPRHRXGAYffMYGTqYfa1Diq 0.10 BTC, 1BghuN3TjEw6PqPd69xDUjChckrySxybX 0.039 BTC
[22:08] Txn 809428b206d584fd97f1be0eecbba2dce417d87e3de8057f72c3b064473986c: 1GEZX1rEgwiVr7qbj3cZhoC9L1cZ9gBzvf 39.75041754 BTC, 18oipuHx35jpkqW20JH7npjUnR23YDzcf 1.01 BTC
[22:08] Txn f63c188cb68...
[22:08] Txn d7ab6026070...
trade ExchngBCs:
[22:09] trade ExchngBCs:
[22:09] trade ExchngBCs:
[22:09] trade ExchngBCs:
[22:09] Txn 32e7708cf05...
[22:09] Txn 920c3cec950...
[22:09] Txn a72d33edcf8...
BTC

92 Users daves
0.1s lag

daves:~/bitcointalk
File Edit View Search Terminal Help
#!/usr/bin/env python
""" module to monitor realtime Bitcoin transactions via the freenode
#Bitcoin-Watch channel - https://en.bitcoin.it/wiki/Bitcoin-Watch

requires irclib (repo)
and ircbot
(http://code.google.com/p/ircbot-collection/source/browse/trunk/ircbot.py?r=66)

pygame is used by the demo main routine"""

from ircbot import SingleServerIRCBot
from irclib import nm_to_n
import re
import random

class BitcoinWatchBot(SingleServerIRCBot):
    """ Bitcoin transaction watching bot. See main() for usage example """

    def __init__(self, channel="#Bitcoin-Watch",
                 nickname="bcbot",
                 server="chat.freenode.net",
                 port=6667,
                 realname="Bitcoin monitoring bot <webpage>"):
        16,7 Top
```


Opportunity – URI Scheme Handler

bitcoin:1Lg7peCQCBBRsmZJ5MoXikuQ25oZ4voBit?amount=5X8&
label=Bitcoin%20Watch&
message=Donation%20for%20watch%20service



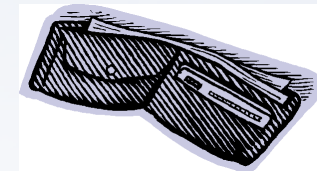
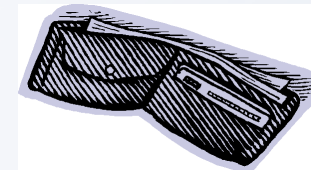
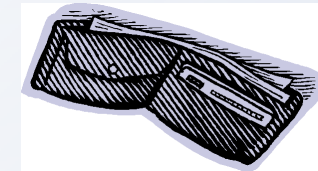
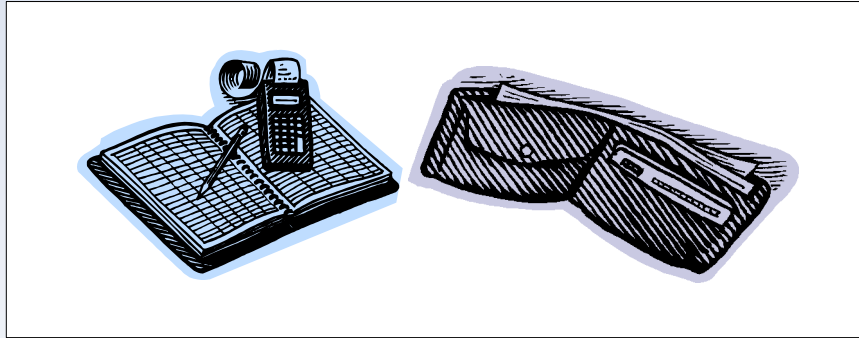
The image shows a screenshot of a Bitcoin payment dialog box. The dialog has a white background and a blue border. At the top, it says "Bitcoin Payment". Below that, it lists the recipient as "To: Bitcoin Watch", the amount as "Amount: 5.0", and the memo as "Memo: Donation for watch service". There is a "From Account:" label followed by a dropdown menu showing "Alice" with a downward arrow. At the bottom, there are two buttons: "Cancel" and "Pay".

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

Vending



Opportunity – Wallet Apps



Different:
- Security Levels
- Users
- Use Cases

<http://gitorious.org/pycoin> - Bitcoin P2P Implementation

Is it Money? - Aristotle's Qualities of a Good Money



Durable	✓	✓
Portable	✓	✓
Divisible	✓	✓
Intrinsic Value	✗	?

The Market View

PyOhio Saturday, July 30 a x Bitcoin Charts / Markets / x

bitcoincharts.com/markets/mtgoxUSD_trades.html

bitcoin charts Bitcoin Markets Charts About

Blocks 137577 Difficulty Jul 23, 2011 02:18:02 (UTC)
 Total BTC 6.879 Estimated 1731331 in 1527 blks Bloc

Symbol

mtgoxUSD ↓
 USD (dwoila/SEPA)

thUSD ↓
 USD

bitomatPLN ↑
 PLN (wire)

b7USD ↓
 USD

bitcoinGBP ↓
 GBP (wire)

bitmarketEUR ↓
 EUR (wire)

virtexCAD ↓
 CAD (EMT/Direct)

virwoxSLL ↑
 SLL (Second Life)

btcexUSD ↑
 USD (Liberty Reserve)

exchbUSD ↑
 USD (dwoila/wire)

bitmarketUSD ↑
 USD (wire/PayPal)

cbxUSD ↑
 USD (dwoila)

thLRUSD ↓
 USD (Liberty Reserve)

b7EUR ↑

Mt. Gox (USD/dwoila/SEPA)

Summary Trade History Market Depth

TRADE FOREX WITH A LEADING BANK

- Consistent spreads from 1.2 pips*
- Trade with a leading FX bank
- Metatrader 4 with full functionality

>> Try the FREE demo

*See website for details Trading Forex Involves a high degree of risk

Trade History 60d 30d 10d 5d 2d

Jul 23, 2011 - Daily

Op:13.7, Hi:13.7, Lo:13.6, Cl:13.63 Vol: 2.01K

Recent Trade Volume				Trades		
Interval	Volume (BTC)	Volume (USD)	Weighted Price	Date	Price	Volume
15min	91.26	1,245.27	13.6458	Jul 23, 2011, 02:17:21	13.63500	7.79
1h	1,196.40	16,301.45	13.6254	Jul 23, 2011, 02:17:13	13.63534	0.05
4h	3,426.00	46,803.17	13.6612	Jul 23, 2011, 02:17:13	13.63998	20.21
12h	6,743.97	92,027.13	13.6458	Jul 23, 2011, 02:17:13	13.63999	27.15
1d	15,841.42	216,402.88	13.6606	Jul 23, 2011, 02:17:13	13.63999	0.11
2d	40,759.84	556,545.42	13.6543	Jul 23, 2011, 02:17:13	13.64000	5.00
7d	258,133.75	3,492,512.15	13.5299	Jul 23, 2011, 02:17:13	13.64997	5.00
20d	870,840.21	11,214,732.80	12.8856	Jul 23, 2011, 02:17:13	13.65082	0.20

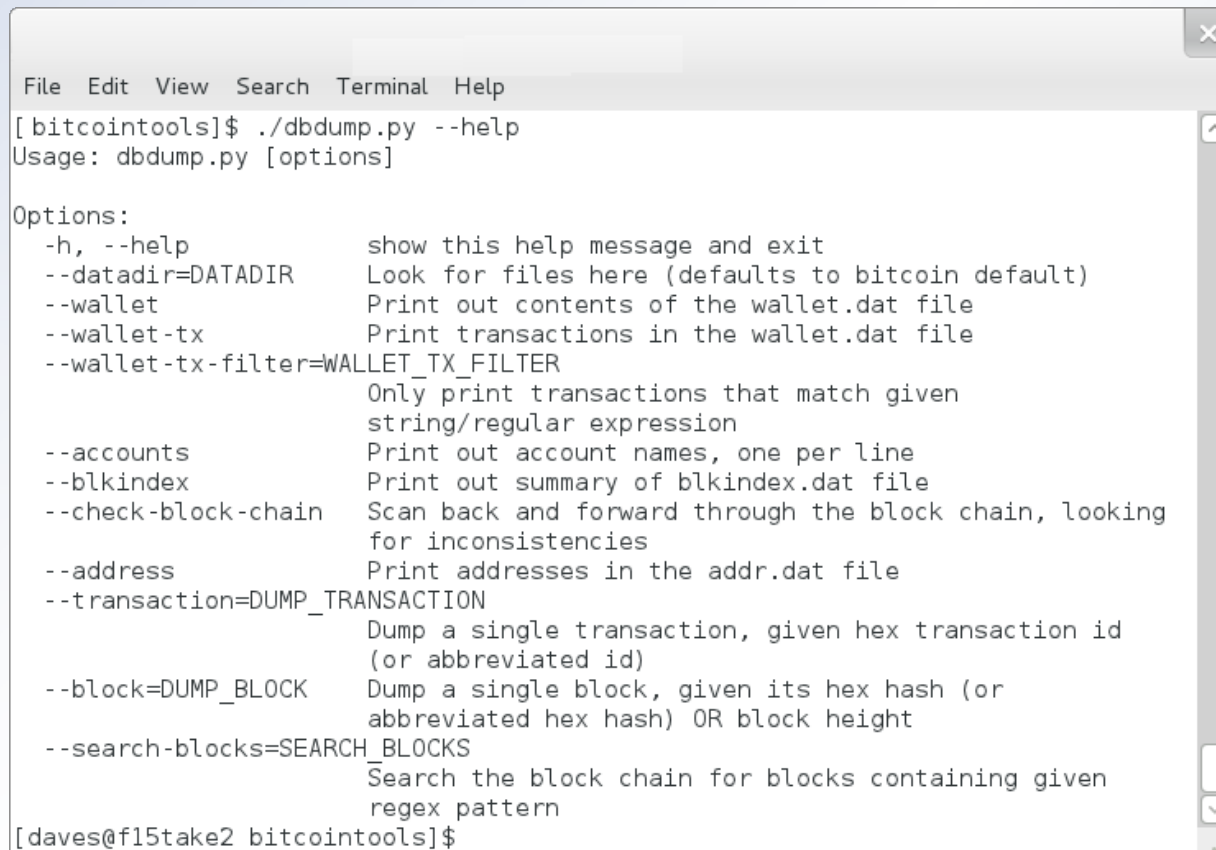
Ledger Analysis

- Metrics for a better idea of Bitcoin economy health
 - Difficulty vs time?
 - % Mining Pools
 - BTC Velocity?
 - Tx Velocity?
 - Median Tx BTC?
 - Addresses
 - Reuse?
 - Account detection metric

<http://blockexplorer.com/>

Ledger Analysis using Python

- The bitcointools module parses local bitcoin data files



```
File Edit View Search Terminal Help
[bitcointools]$ ./dbdump.py --help
Usage: dbdump.py [options]

Options:
  -h, --help                show this help message and exit
  --datadir=DATADIR        Look for files here (defaults to bitcoin default)
  --wallet                  Print out contents of the wallet.dat file
  --wallet-tx               Print transactions in the wallet.dat file
  --wallet-tx-filter=WALLET_TX_FILTER
                           Only print transactions that match given
                           string/regular expression
  --accounts                Print out account names, one per line
  --blkindex                Print out summary of blkindex.dat file
  --check-block-chain       Scan back and forward through the block chain, looking
                           for inconsistencies
  --address                 Print addresses in the addr.dat file
  --transaction=DUMP_TRANSACTION
                           Dump a single transaction, given hex transaction id
                           (or abbreviated id)
  --block=DUMP_BLOCK        Dump a single block, given its hex hash (or
                           abbreviated hex hash) OR block height
  --search-blocks=SEARCH_BLOCKS
                           Search the block chain for blocks containing given
                           regex pattern

[daves@f15take2 bitcointools]$
```

<https://github.com/gavinandresen/bitcointools>

Bitcoin Links

- Market – Bitcoin Charts
 - <http://bitcoincharts.com>
- Plumbing – Block Explorer
 - <http://blockexplorer.com/>
 - Stats - <http://blockexplorer.com/q>
- Technical – Bitcoin Wiki
 - https://en.bitcoin.it/wiki/Main_Page
 - Addresses, Transactions, Signing, Blocks, Peer Protocol
- Community - <http://forum.bitcoin.org/>
- News
 - <http://www.bitcoinnews.com/>
 - http://www.****coins.com/

