

BTCD

BitDevs Meetup

John C. Vernaleo, Ph.D.

Senior Developer
Conformal Systems
jcv@conformal.com

04/22/2014

What is it?

btcd - An alternative, full node Bitcoin implementation in Go by Conformal Systems.

And friends.

Also wallet (btcwallet) and GUI (btcdgui).

Why?

- ▶ Trouble using bitcoind on OpenBSD.
- ▶ Limitations on the json-rpc interface.
- ▶ Did not want to build things against the main C++ codebase.
- ▶ We really like Go.
- ▶ Diversity is good.

Who?

▶ Conformal Systems

- ▶ Most of team has background with OpenBSD/Bitrig.
- ▶ Security and Privacy Focused.
- ▶ History of Open Source software.
- ▶ Authors of Cyphertite - zero knowledge backup system.

▶ Me

- ▶ <http://www.netpurgatory.com>
- ▶ Mainly worked on rpc server and json interface for btcd.
- ▶ Mostly working on Coinvoice now.

The Code

`https://github.com/conformal/btcd`

Community

irc.conformal.com:6697

ssl required

channel #btcd

Main Features

- ▶ Go
 - ▶ Other than btcgui, pure go.
- ▶ Open Source (ISC license)
- ▶ Modular (Build your own tools!)
 - ▶ The Executables
 - ▶ The Code
- ▶ Portable
 - ▶ *BSD
 - ▶ Linux
 - ▶ Windows
 - ▶ OSX
 - ▶ Plan 9
- ▶ Compatible + Extensions

Why we trust btcd:

- ▶ Very high rate of unit test coverage.
- ▶ Passes all block or regression tests already available to bitcoin community.
- ▶ Modular so we can worry about validating piece by piece.
- ▶ Been running side by side with bitcoind for months now.

We use it.

- ▶ Blocksafari
- ▶ Coinvoice
- ▶ Other things we aren't ready to talk about yet.

Block Safari - Welcome - Mozilla Firefox

Block Safari - Welcome

yoshi:8080

ixquick Search Engine WebPage for John C... Twitter / Home Netpurgatory Blog Tiny Tiny RSS

Bitcoin Block Safari

This site is written in [Go](#). It uses JSON to fetch and parse this data from [btcd](#) on-demand.

Number	Hash	Time	Transactions	Total BTC	Size (kB)
297019	3420f67ea5	2014-04-21 13:28:08	614	6935.24335651	290.656
297018	104a9a9c7f	2014-04-21 13:14:02	80	175.34527959	35.513
297017	7945e5eb31	2014-04-21 13:12:30	161	1976.37054675	72.614
297016	54dfc1c837	2014-04-21 13:10:24	50	1414.55879077	19.360
297015	5904eb18b7	2014-04-21 13:09:28	737	8696.35992962	343.457
297014	8f1b8a1ef7	2014-04-21 12:51:26	120	2532.48917267	50.375
297013	3a5ff01ea0	2014-04-21 12:48:05	164	3909.85219658	90.908
297012	8b888e57e7	2014-04-21 12:43:41	227	1033.94576439	106.814
297011	83bca2cfe9	2014-04-21 12:39:44	60	928.37316176	58.502
297010	2ab23376d3	2014-04-21 12:35:33	315	5625.92681224	226.006
297009	5da11ca3ac	2014-04-21 12:28:00	394	7053.08684558	247.155
297008	506b3ca386	2014-04-21 12:20:25	604	3053.39173060	346.832
297007	8ebe6f7964	2014-04-21 12:16:35	490	3673.43425886	485.698
297006	7ece5e2314	2014-04-21 12:12:53	1036	11769.48834747	349.073
297005	8053027921	2014-04-21 12:00:12	444	7337.18886220	226.977

<https://coinvoice.com>

The screenshot shows a Mozilla Firefox browser window displaying the Coinvoice website. The browser's address bar shows the URL <https://coinvoice.com>. The website's header features the Coinvoice logo (two interlocking circles) and the text "COINVOICE". Navigation links include "ABOUT", "FAQ", "CONTACT", "SIGN UP" (highlighted in an orange box), and "LOGIN".

The main content area has a teal background with a repeating pattern of Bitcoin symbols. The primary text reads: "Invoice in USD or BTC, Get paid in USD or BTC. Liberate your business with Bitcoin". Below this text is a circular "Sign up" button. To the right, there is a graphic of a yellow envelope with a Bitcoin symbol and the word "PAID" written on it, surrounded by several gold Bitcoin coins. A white circle with a black dollar sign (\$) is also visible in the background.

At the bottom of the page, there is a section with the text "Integrate bitcoins into any business" and a diagram showing the Coinvoice logo between two green boxes, with arrows indicating integration. The URL <https://coinvoice.com/register> is visible in the bottom left corner of the page content.

Packages

- ▶ btcjson
- ▶ btcws
- ▶ btcwire
- ▶ btcchain
- ▶ btcscript
- ▶ btcec
- ▶ btcdb
- ▶ btcutil

Websockets

- ▶ Compatible the the json-rpc interface, but that is limited.
- ▶ We added a new json interface done over websockets.
- ▶ Allows you to interact with a running btcd in more complex ways without modifying or even linking to our code.

WebSocket Notifications

- ▶ notifyblocks
- ▶ notifyreceived
- ▶ notifyspent
- ▶ notifynewtransactions
- ▶ rescan

WS Sample

```
addrs := []string{"17XhEvq9Nahdj7Xe1nv6oRe1tEmaHUuynH"}
rescanCmd, _ := btcws.NewRescanCmd(1, 276000, addrs, nil)
sendCmd <- rescanCmd
for {
    reply := <- marshaledReplies
    n, _ := btcjson.ParseMarshaledCmd([]byte(reply));
}
```


Wire Sample

```
pver := btcwire.ProtocolVersion  
btcnet := btcwire.MainNet  
msg, rawPayload, err := btcwire.ReadMessage(conn, pver, btcnet)
```

↑ _ □ ×
btcgui [TESTNET]

File Settings Help

Overview | Send Coins | Receive Coins | Transactions

Wallet

Balance: **10.10002212 BTC**

Unconfirmed: **0.00000000 BTC**

Recent Transactions

←	Apr 16, 2014 at 12:56 PM	8.90626856
	Receive (mr9wrAyg3m9FeYFxDPieTjfuRTQ3f5pxWj)	
←	Apr 16, 2014 at 12:56 PM	0.04328204
	Receive (mivy7mhkPnkB1HStmo7GEwDnrDrAsHmz94)	
→	Apr 16, 2014 at 12:56 PM	-0.04328204
	Send (mivy7mhkPnkB1HStmo7GEwDnrDrAsHmz94)	
→	Apr 16, 2014 at 12:56 PM	-8.90626856
	Send (mr9wrAyg3m9FeYFxDPieTjfuRTQ3f5pxWj)	
←	Apr 16, 2014 at 12:50 PM	8.94965060
	Receive (n3h7pNB2d2KBPAbjBqgKqwGTDkW4ny5wBc)	

225936 blocks

Why 3 programs instead of 1?

- ▶ Keep blockchain (19G and growing) on big machine.
- ▶ Wallet and GUI can go on other machine.
- ▶ Share blockchain but not wallet.

Conclusion

Please give btcd a try if you can and let us know what you think on irc or github.

- ▶ Still a work in progress, but other than the GUI and a few features still in progress, very far along.