

an introduction to Bitcoin

Sven Moritz Hallberg
<pesco@khjk.org>

Chaos Computer Club Hamburg

july 2011

outline

context

what is Bitcoin?

technical details

using Bitcoin

in the future. . .

context

context

▶ money

context

- ▶ money
- ▶ medium of exchange

context

- ▶ money
- ▶ medium of exchange
- ▶ fiat currency

context

- ▶ money
- ▶ medium of exchange
- ▶ fiat currency
- ▶ central banks

Bitcoin

- ▶ electronic *currency*



Bitcoin

- ▶ electronic *currency*
- ▶ a distributed bank, kind of
- ▶ *not* untraceable



Bitcoin

- ▶ electronic *currency*
- ▶ a distributed bank, kind of
- ▶ *not* untraceable
- ▶ but anonymous



Bitcoin

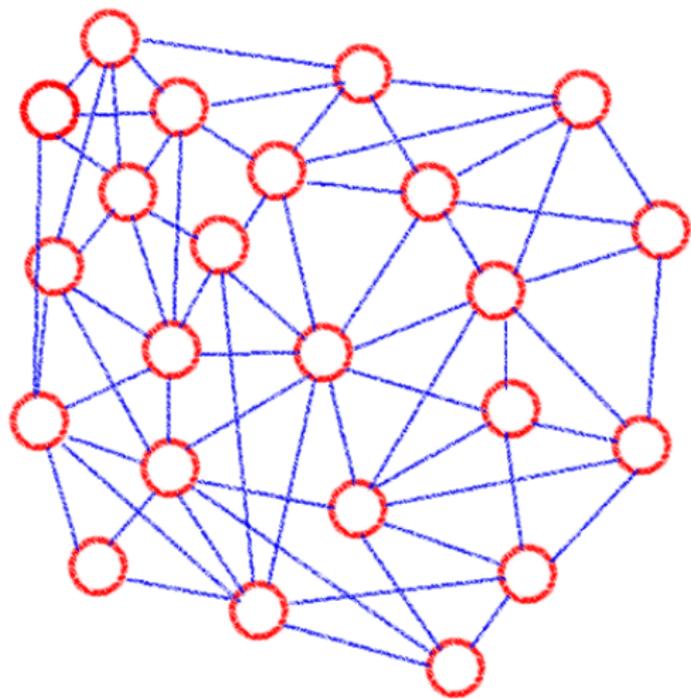
- ▶ electronic *currency*
- ▶ a distributed bank, kind of
- ▶ *not* untraceable
- ▶ but anonymous
 - ▶ *if* you are careful
- ▶ limited long-term supply



now: technical stuff...

(distributed network, accounts, keys
transactions, blocks, mining)

the Bitcoin network



the Bitcoin network

- ▶ distributed network
- ▶ nodes connected via TCP/IP

the Bitcoin network

- ▶ distributed network
- ▶ nodes connected via TCP/IP
- ▶ broadcast transactions

the Bitcoin network

- ▶ distributed network
- ▶ nodes connected via TCP/IP
- ▶ broadcast transactions
- ▶ distributed database

the Bitcoin network

- ▶ distributed network
- ▶ nodes connected via TCP/IP
- ▶ broadcast transactions
- ▶ distributed database

- ▶ nodes join/leave at any time
- ▶ request any info that they miss

accounts and keys

- ▶ asymmetric cryptography, think PGP

accounts and keys

- ▶ asymmetric cryptography, think PGP
- ▶ account numbers \approx public keys
- ▶ private key = access to money

accounts and keys

- ▶ asymmetric cryptography, think PGP
- ▶ account numbers \approx public keys
- ▶ private key = access to money
- ▶ accounts are cheap

the “block chain”

clearing every transaction individually: inefficient. . .

the “block chain”

clearing every transaction individually: inefficient. . .

- ▶ transactions are grouped into *blocks*

mining

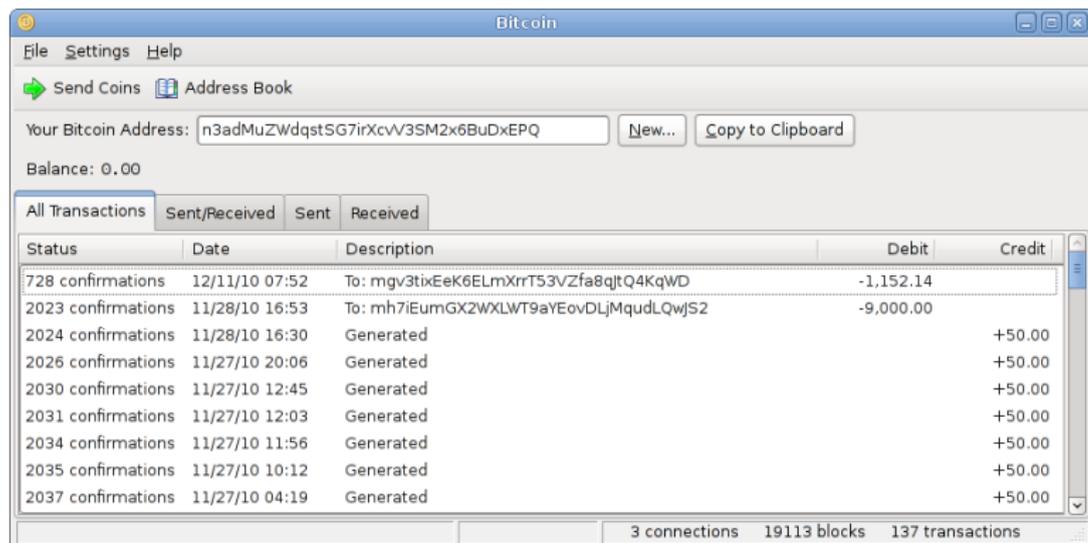
- ▶ blocks give money to their creator

mining

- ▶ blocks give money to their creator
- ▶ 50 BTC each right now
- ▶ less later
- ▶ but also *transaction fees*

using bitcoin

- ▶ Bitcoin client = wallet = network node



The screenshot shows the Bitcoin client interface. At the top, there is a menu bar with "File", "Settings", and "Help". Below the menu bar, there are buttons for "Send Coins" and "Address Book". The "Your Bitcoin Address:" field contains the address "n3adMuZwDqstSG7irXcvV3SM2x6BuDxEPQ", with "New..." and "Copy to Clipboard" buttons next to it. The "Balance:" is displayed as "0.00".

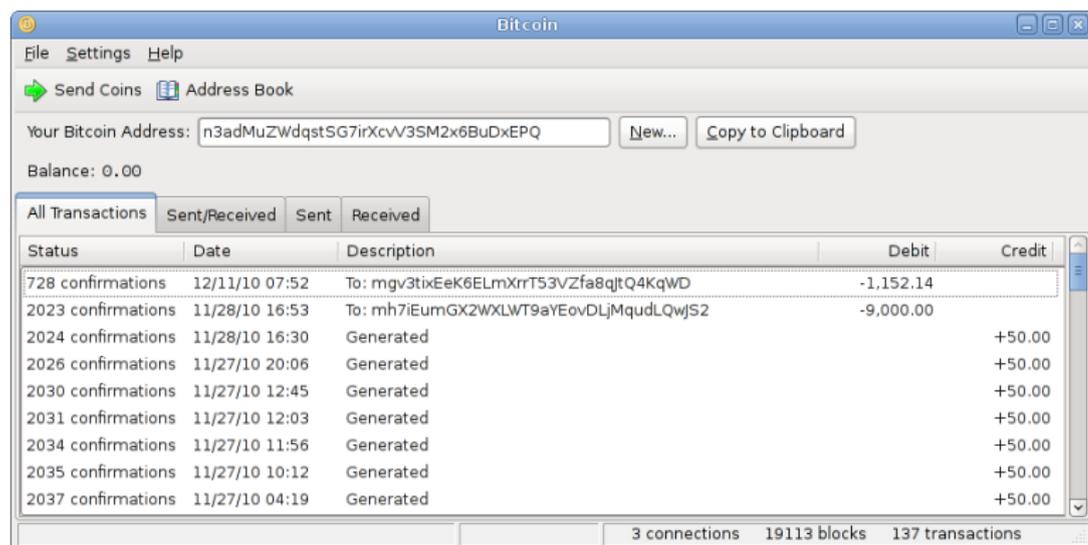
The main area shows a list of transactions with tabs for "All Transactions", "Sent/Received", "Sent", and "Received". The "All Transactions" tab is selected, showing a table of transactions:

Status	Date	Description	Debit	Credit
728 confirmations	12/11/10 07:52	To: mgv3tixEeK6ELmXrrT53VZfa8qjtQ4KqWD	-1,152.14	
2023 confirmations	11/28/10 16:53	To: mh7iEumGX2WXLWT9aYEovDLjMqudLQwjS2	-9,000.00	
2024 confirmations	11/28/10 16:30	Generated		+50.00
2026 confirmations	11/27/10 20:06	Generated		+50.00
2030 confirmations	11/27/10 12:45	Generated		+50.00
2031 confirmations	11/27/10 12:03	Generated		+50.00
2034 confirmations	11/27/10 11:56	Generated		+50.00
2035 confirmations	11/27/10 10:12	Generated		+50.00
2037 confirmations	11/27/10 04:19	Generated		+50.00

At the bottom of the window, the status bar shows "3 connections", "19113 blocks", and "137 transactions".

using bitcoin

- ▶ Bitcoin client = wallet = network node



The screenshot shows the Bitcoin client window with the following details:

- Menu: File, Settings, Help
- Buttons: Send Coins, Address Book
- Your Bitcoin Address: n3adMuZwdqstSG7irXcvV3SM2x6BuDxEpQ (with New... and Copy to Clipboard buttons)
- Balance: 0.00
- Transaction List:

Status	Date	Description	Debit	Credit
728 confirmations	12/11/10 07:52	To: mgv3tixEeK6ELmXrrT53VZfa8qtQ4KqWD	-1,152.14	
2023 confirmations	11/28/10 16:53	To: mh7iEumGX2WXLWT9aYEovDLjMqudLQwjS2	-9,000.00	
2024 confirmations	11/28/10 16:30	Generated		+50.00
2026 confirmations	11/27/10 20:06	Generated		+50.00
2030 confirmations	11/27/10 12:45	Generated		+50.00
2031 confirmations	11/27/10 12:03	Generated		+50.00
2034 confirmations	11/27/10 11:56	Generated		+50.00
2035 confirmations	11/27/10 10:12	Generated		+50.00
2037 confirmations	11/27/10 04:19	Generated		+50.00

Bottom status bar: 3 connections 19113 blocks 137 transactions

- ▶ or online wallet at mybitcoin.com

currency exchanges

trade BTC for USD/EUR/...

currency exchanges

trade BTC for USD/EUR/...

▶ mtgox.com

currency exchanges

trade BTC for USD/EUR/...

- ▶ mtgox.com
- ▶ tradehill.com

currency exchanges

trade BTC for USD/EUR/...

- ▶ mtgox.com
- ▶ tradehill.com
- ▶ bitcoin.co.uk

currency exchanges

trade BTC for USD/EUR/...

- ▶ mtgox.com
- ▶ tradehill.com
- ▶ bitcoin.co.uk
- ▶ bitcoin7.com

currency exchanges

trade BTC for USD/EUR/...

- ▶ mtgox.com
- ▶ tradehill.com
- ▶ bitcoin.co.uk
- ▶ bitcoin7.com
- ▶ ...

currency exchanges

trade BTC for USD/EUR/...

- ▶ mtgox.com
- ▶ tradehill.com
- ▶ bitcoin.co.uk
- ▶ bitcoin7.com
- ▶ ...
- ▶ see the wiki for more.

merchants / services

buy stuff for BTC. . .

merchants / services

buy stuff for BTC. . .

- ▶ server hosting

merchants / services

buy stuff for BTC. . .

- ▶ server hosting
- ▶ books

merchants / services

buy stuff for BTC. . .

- ▶ server hosting
- ▶ books
- ▶ music

merchants / services

buy stuff for BTC. . .

- ▶ server hosting
- ▶ books
- ▶ music
- ▶ coffee

merchants / services

buy stuff for BTC. . .

- ▶ server hosting
- ▶ books
- ▶ music
- ▶ coffee
- ▶ clothing

merchants / services

buy stuff for BTC. . .

- ▶ server hosting
- ▶ books
- ▶ music
- ▶ coffee
- ▶ clothing
- ▶ . . .

merchants / services

buy stuff for BTC. . .

- ▶ server hosting
- ▶ books
- ▶ music
- ▶ coffee
- ▶ clothing
- ▶ . . .

- ▶ see the wiki for *much* more!

outlook

problems / challenges:

outlook

problems / challenges:

- ▶ regulation

outlook

problems / challenges:

- ▶ regulation
- ▶ acceptance

outlook

problems / challenges:

- ▶ regulation
- ▶ acceptance
- ▶ deflation?

outlook

problems / challenges:

- ▶ regulation
- ▶ acceptance
- ▶ deflation?
- ▶ bugs, hacks, attacks

outlook

problems / challenges:

- ▶ regulation
- ▶ acceptance
- ▶ deflation?
- ▶ bugs, hacks, attacks
- ▶ ...

the end

questions?

see also: www.bitcoin.org