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

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

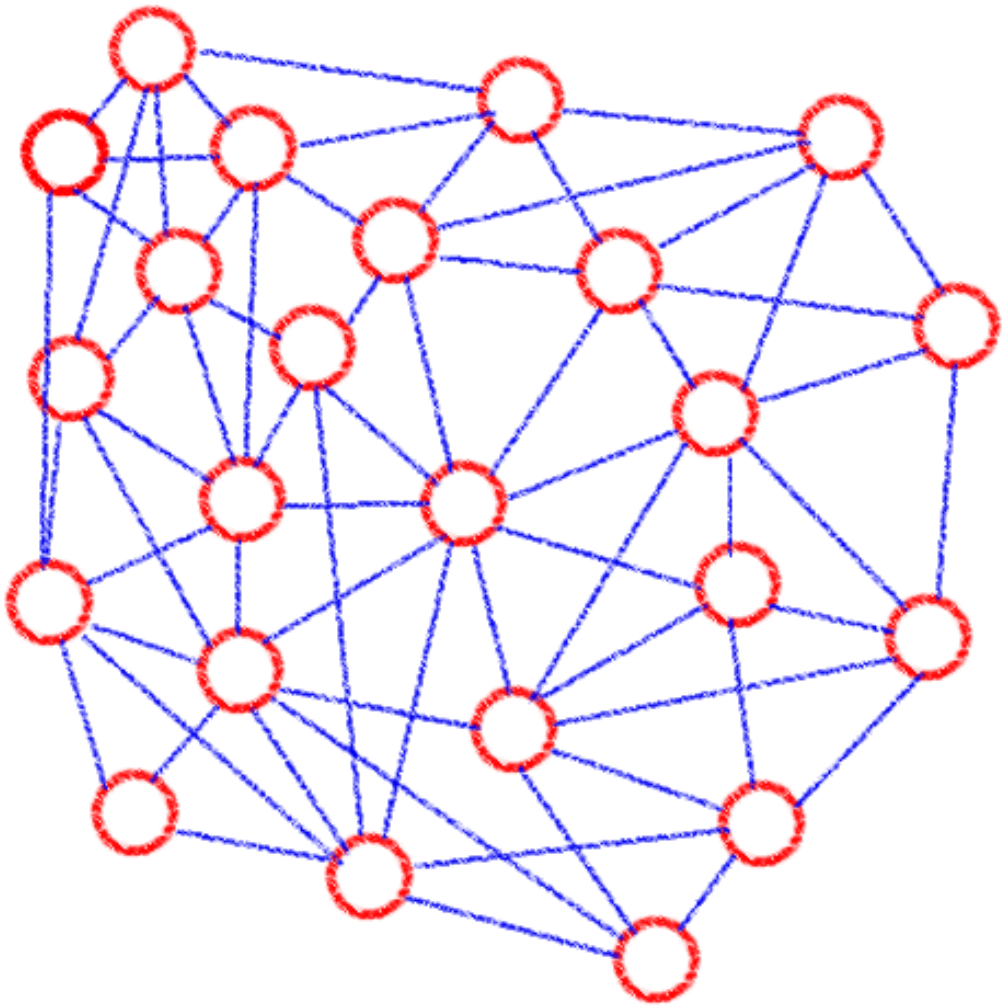
Bitcoin

- 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”

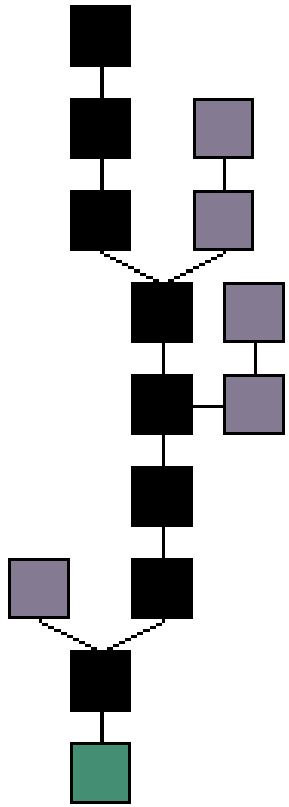
clearing every transaction individually: inefficient. . .

- transactions are grouped into *blocks*

the “block chain”

clearing every transaction individually: inefficient. . .

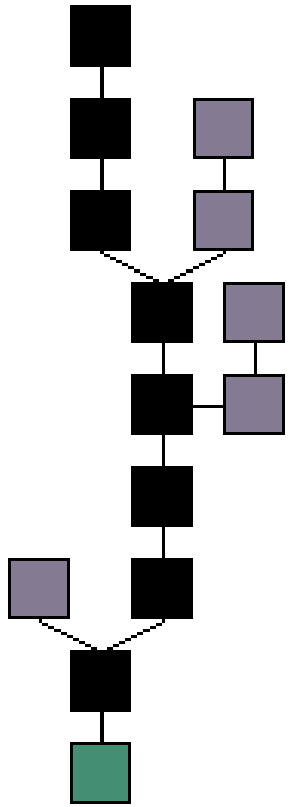
- transactions are grouped into *blocks*
- blocks are linked (hash of predecessor)



the “block chain”

clearing every transaction individually: inefficient. . .

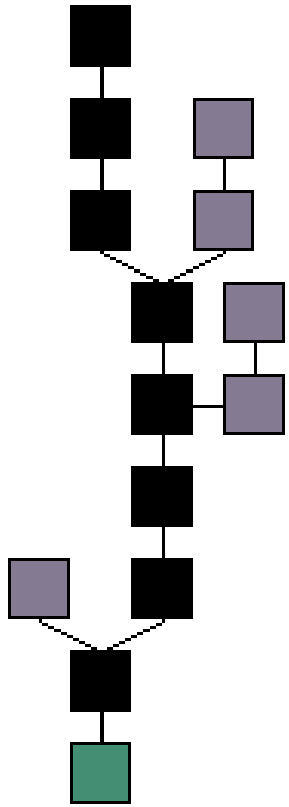
- transactions are grouped into *blocks*
- blocks are linked (hash of predecessor)
- making a block is hard



the “block chain”

clearing every transaction individually: inefficient. . .

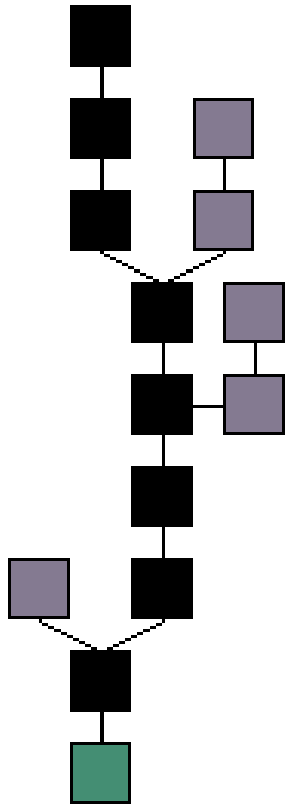
- transactions are grouped into *blocks*
- blocks are linked (hash of predecessor)
- making a block is hard
- first one wins



the “block chain”

clearing every transaction individually: inefficient. . .

- transactions are grouped into *blocks*
- blocks are linked (hash of predecessor)
- making a block is hard
- first one wins
- $\longrightarrow$ “mining”



mining

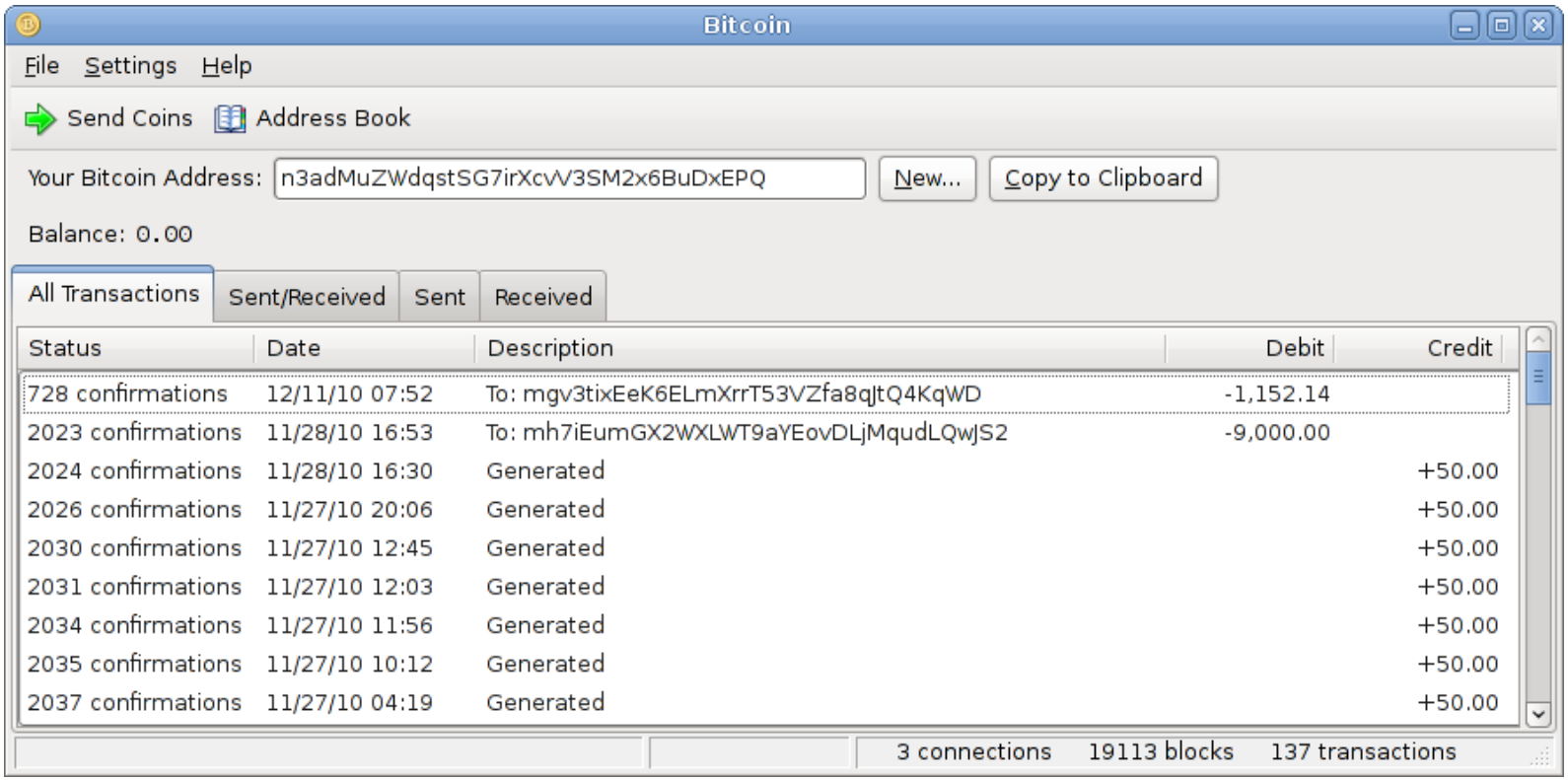
- blocks give money to their creator

mining

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

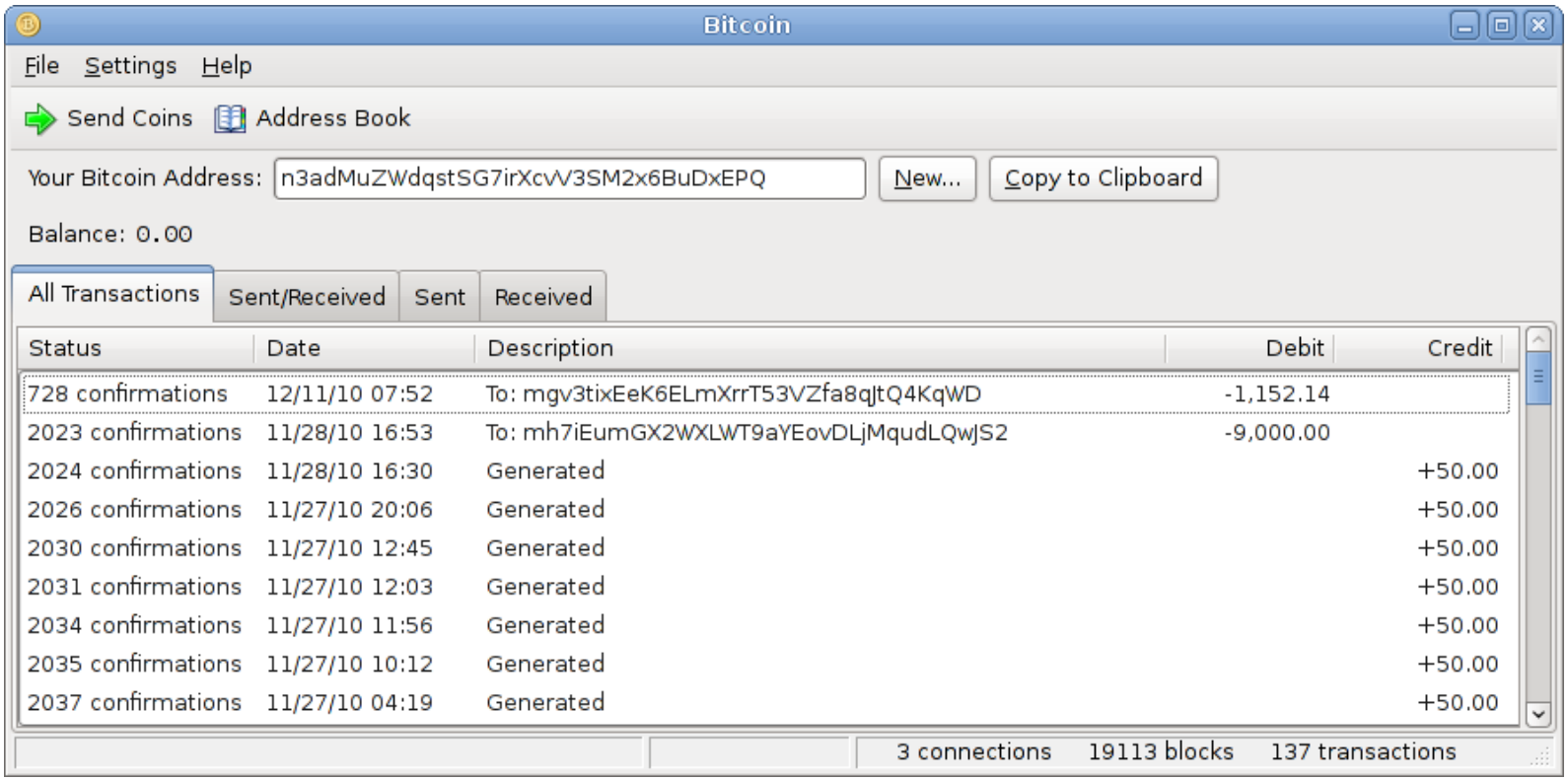
using bitcoin

- Bitcoin client = wallet = network node



using bitcoin

- Bitcoin client = wallet = network node



- or online wallet at `mybitcoin.com`

currency exchanges

trage BTC for USD/EUR/...

currency exchanges

trage BTC for USD/EUR/...

- `mtgox.com`

currency exchanges

trage BTC for USD/EUR/...

- `mtgox.com`
- `tradehill.com`

currency exchanges

trage BTC for USD/EUR/...

- `mtgox.com`
- `tradehill.com`
- `britcoin.co.uk`

currency exchanges

trage BTC for USD/EUR/...

- `mtgox.com`
- `tradehill.com`
- `britcoin.co.uk`
- `bitcoin7.com`

currency exchanges

trage BTC for USD/EUR/...

- `mtgox.com`
- `tradehill.com`
- `britcoin.co.uk`
- `bitcoin7.com`
- `...`

currency exchanges

trage BTC for USD/EUR/...

- `mtgox.com`
- `tradehill.com`
- `britcoin.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`