

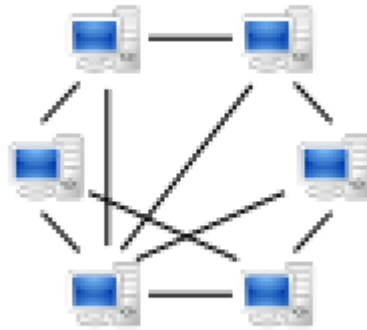
Bitcoin

Sven Moritz 'pesco' Hallberg

Alexander 'copton' Bernauer

Easterhegg 2011

Bitcoin



sourceforge

Motivation



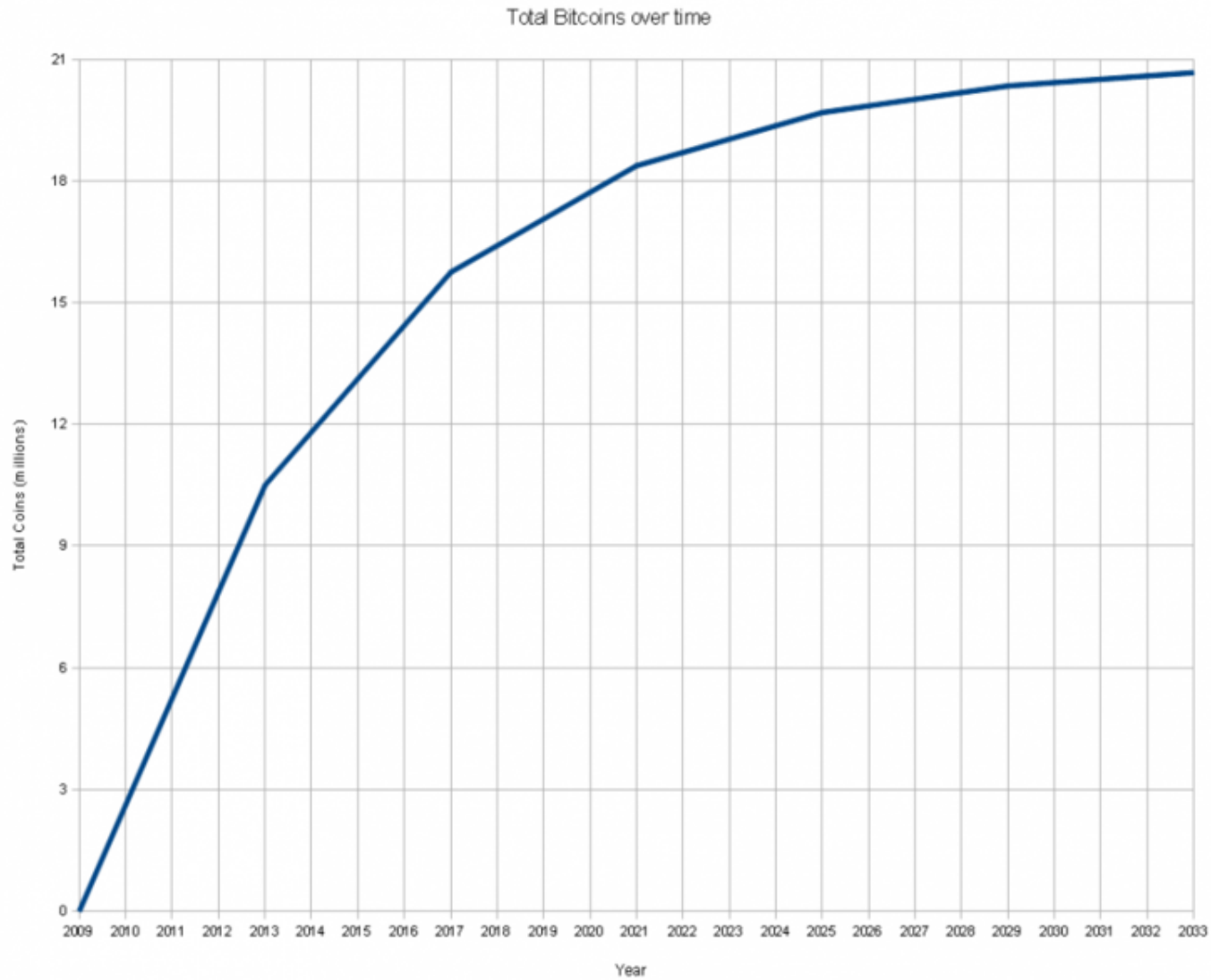
Währung

- fälschungssicher
- speicherbar
- unterteilbar
- tauschbar
- quantifizierbar

Erwerben



Geldmenge



Ausgeben

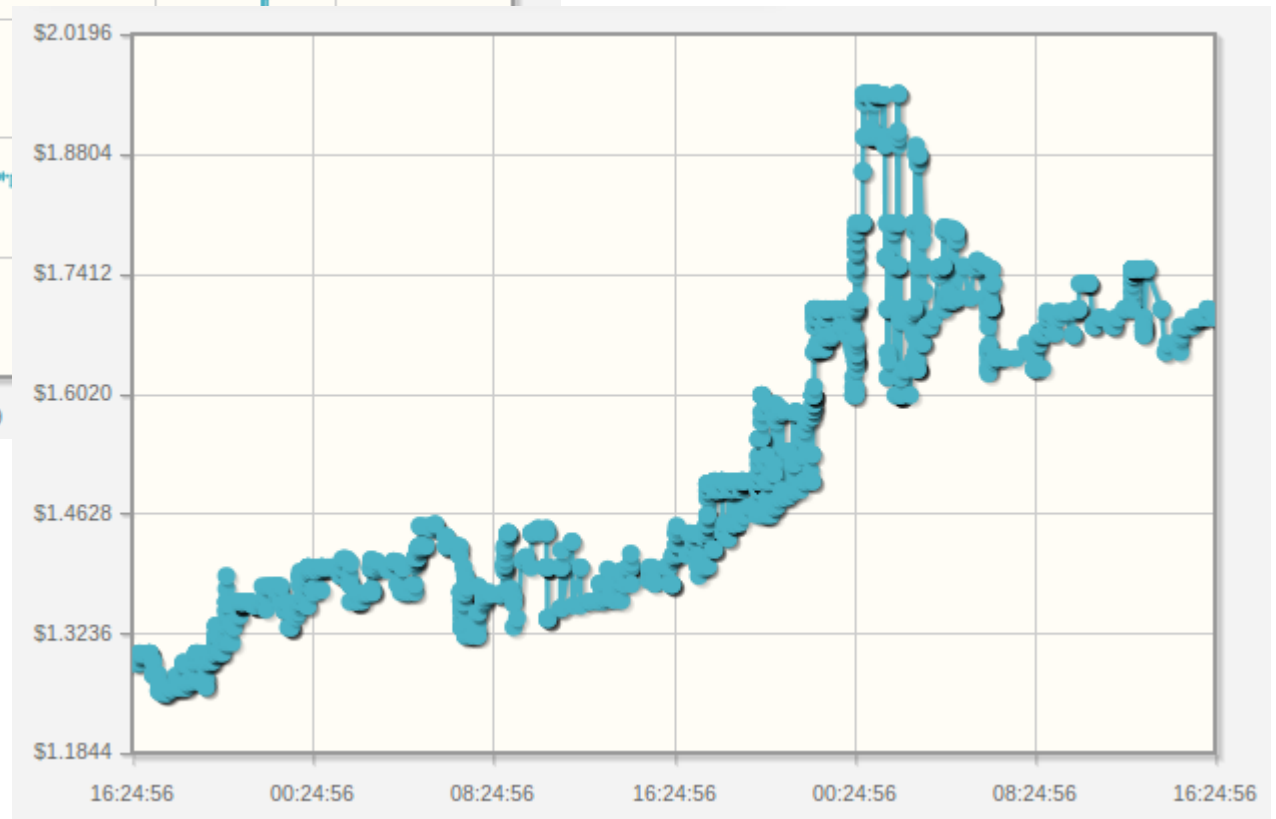
- Internetdienste
- Onlineprodukte
- Materielle Güter
- Dienstleistungen
- Spenden
- Porno
- Gambling
- ...



Entwicklung



Mt. Gox – Bitcoin Exchange



aktuell: 5997200.00000000 BTC

verteilte Datenbank

File Settings Help

Send Coins Address Book

Your Bitcoin Address:

Balance: 0.05

All Transactions Sent/Received Sent Received

Status	Date	Description	Debit	Credit
94 confirmations	04/23/2011 19:22	Received with: 1N73T2WgyNGu... (Your Address)		+0.05

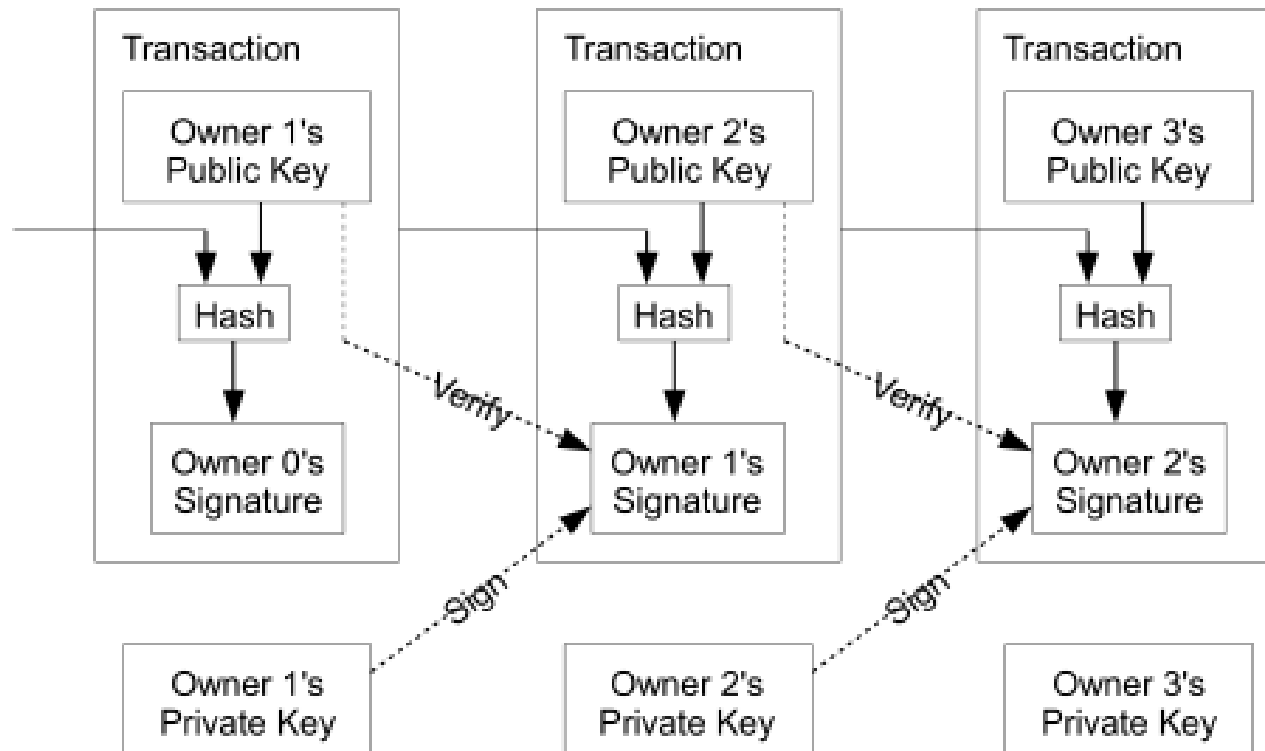
29 connections 119888 blocks 1 transactions



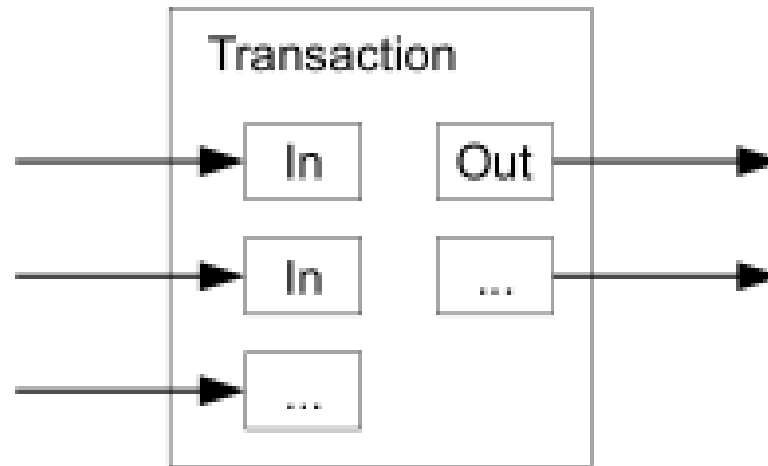
Betrieb

- Broadcast neuer Transaktionen
- Sammlung von Transaktionen in Blöcken
- Erfüllen des Proof-of-Work
- Broadcast einer Lösung
- Akzeptanzchecks neuer Blöcke (double spend)
- Die längste Kette entspricht der Wahrheit

Coin := Kette digitaler Signaturen

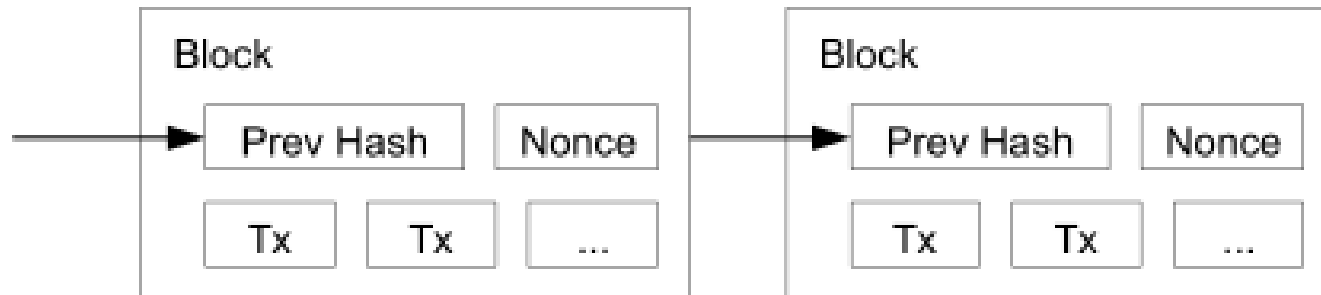


Aufteilung



min: 0.00000001 BTC = 10^{-8} BTC
=> max $\sim 2,1 * 10^{15}$ atomare Einheiten

Proof of Work



Privacy

- öffentlicher Schlüssel ist Pseudonym
- alle Transaktionen sind öffentlich

Eigenschaften





Danke

- <http://bitcoin.org>
- Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, <http://bitcoin.org/bitcoin.pdf>
- Mt. Gox – Bitcoin Exchange: <https://mtgox.com>
- EconTalk-Podcast:
http://www.econtalk.org/archives/2011/04/andresen_on_bit.html
- Omega-Tau-Podcast:
<http://omegataupodcast.net/2011/03/59-bitcoin-a-digital-decentralized-currency/>