BitCoin
eine gänzlich andere Währung

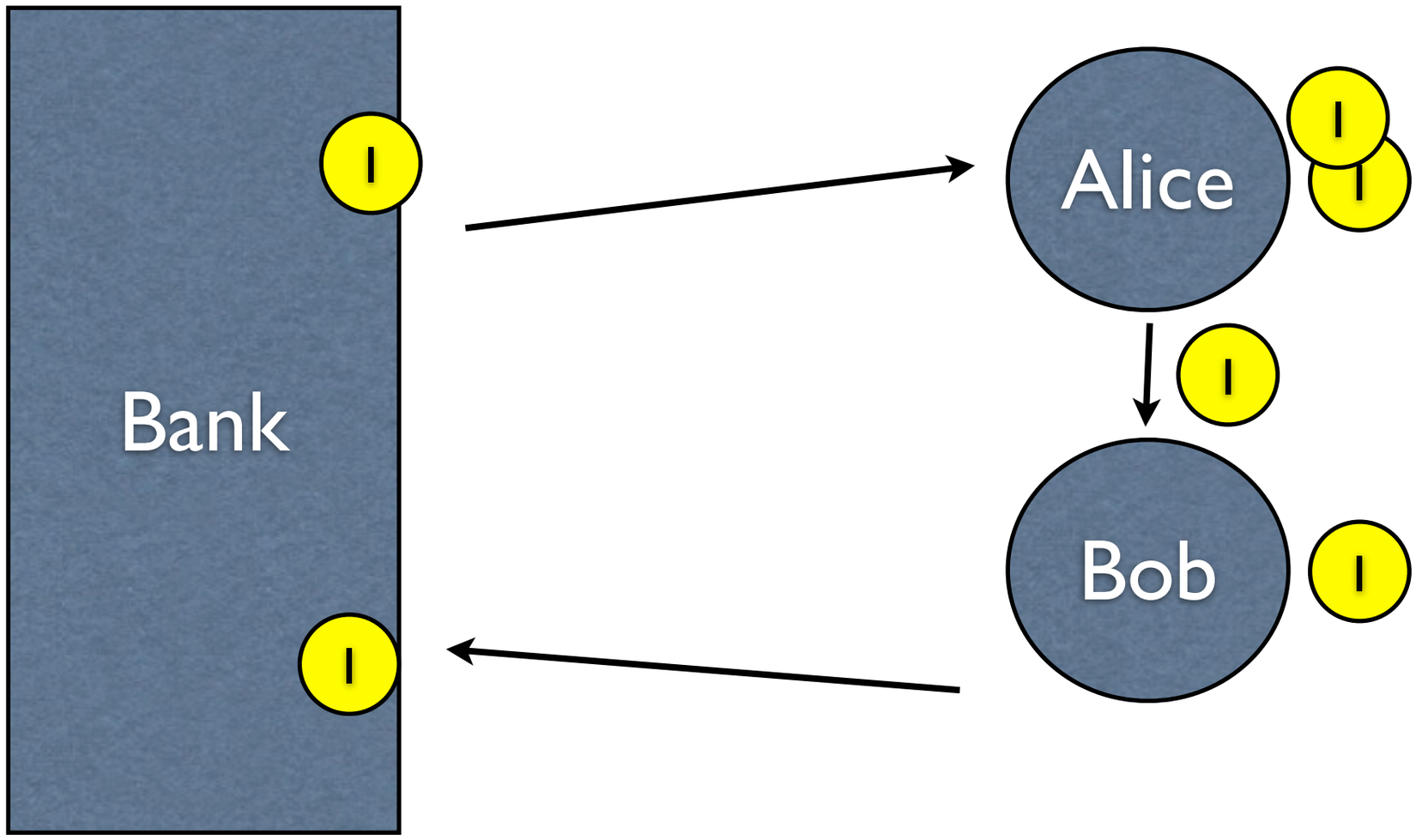
Jens-Christian Fischer
@jcfischer

2012-08-23

Elektronische Zahlungsmittel

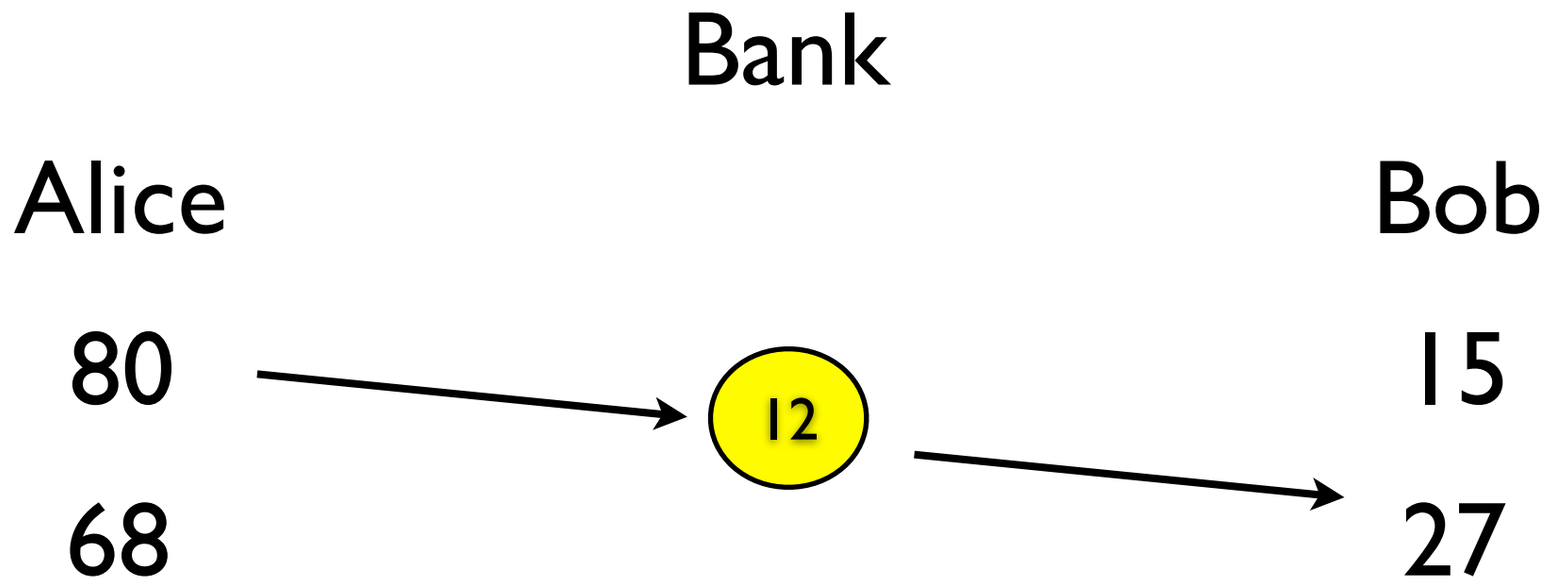
- Einfach
- Anonym?
- Sicher
- Schnell
- Günstig

Diskrete „Münzen“



DigiCash (Chaum), Mojo Nation

Zentrale Kontoführung



World Of Warcraft Gold
Second Life L$

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

http://bitcoin.org/bitcoin.pdf

Probleme

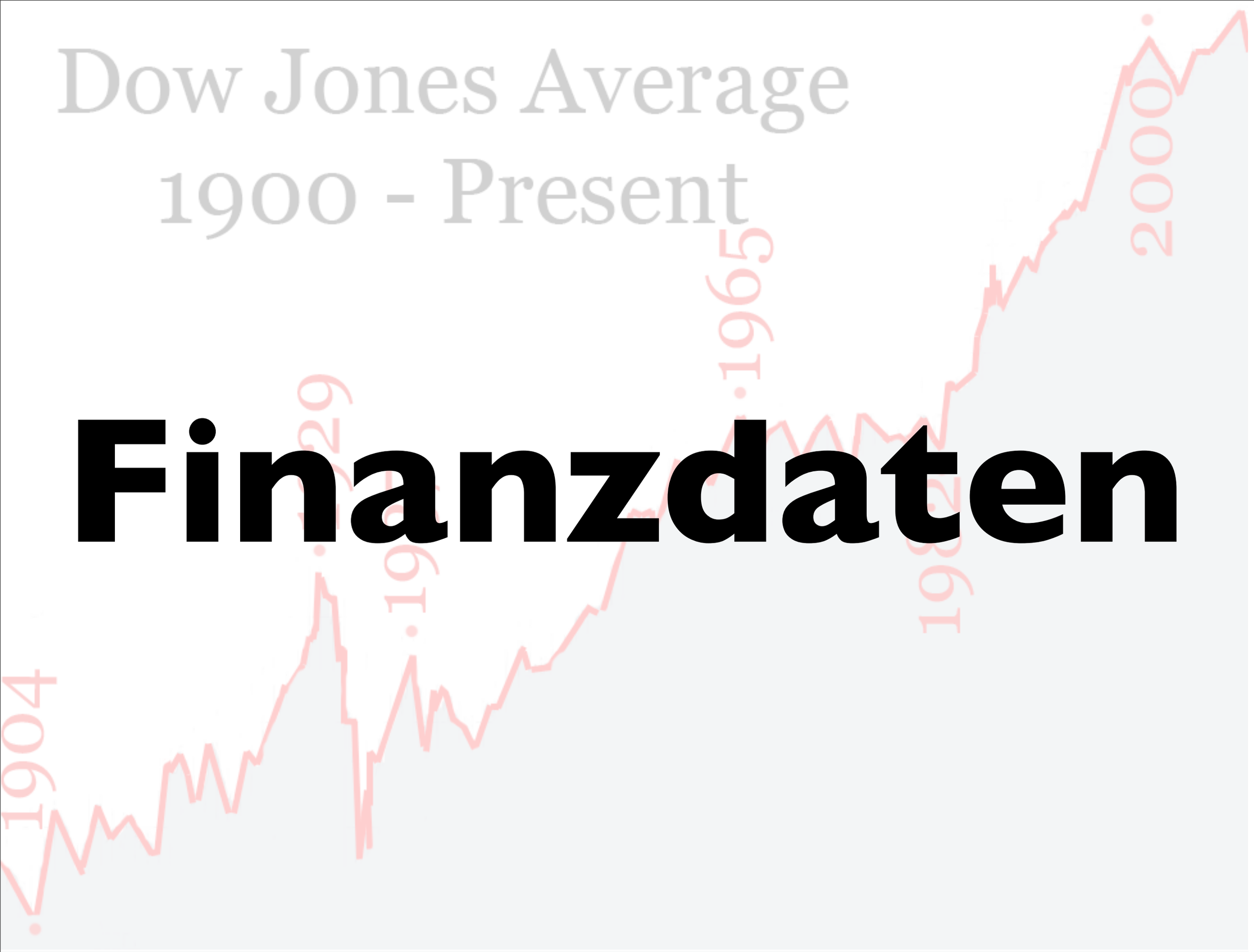
- Geld mehrfach ausgeben
- Erzeugen von Währung (Inflation)
- Bank kann Geld von Benutzern ausgeben
- SPOF

Peer to Peer

- Keine zentrale Ausgabestelle / Bank
- Kein zentrales Vertrauen
- BitCoin ist ein dezentrales Kontobuch, über dass sich alle Parteien einig sind

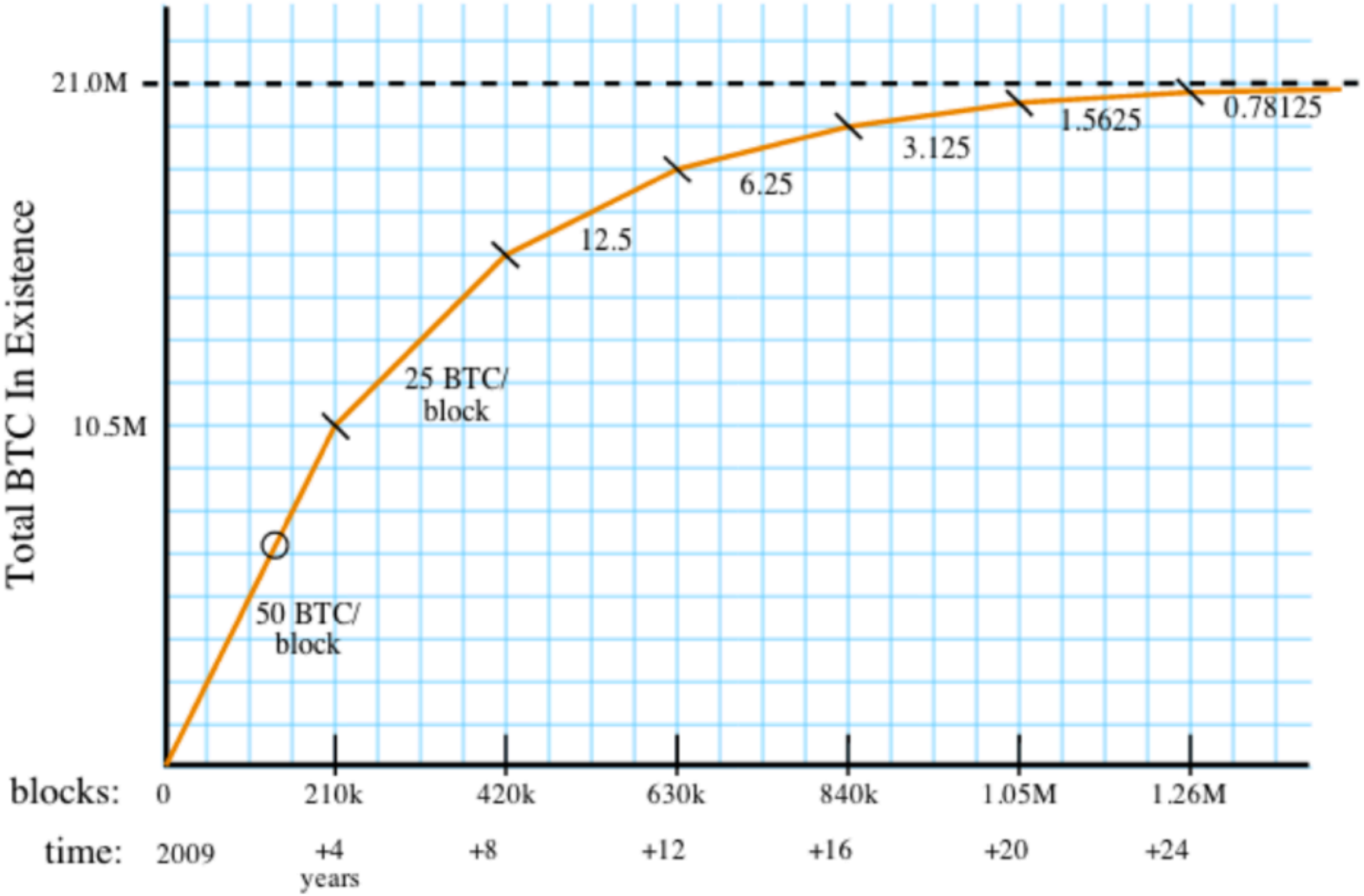
Netzwerk

- Selbstregulierendes Netzwerk
- Knoten die sich nicht vertrauen
- Erreichen Konsens über Gültigkeit von Transaktionen



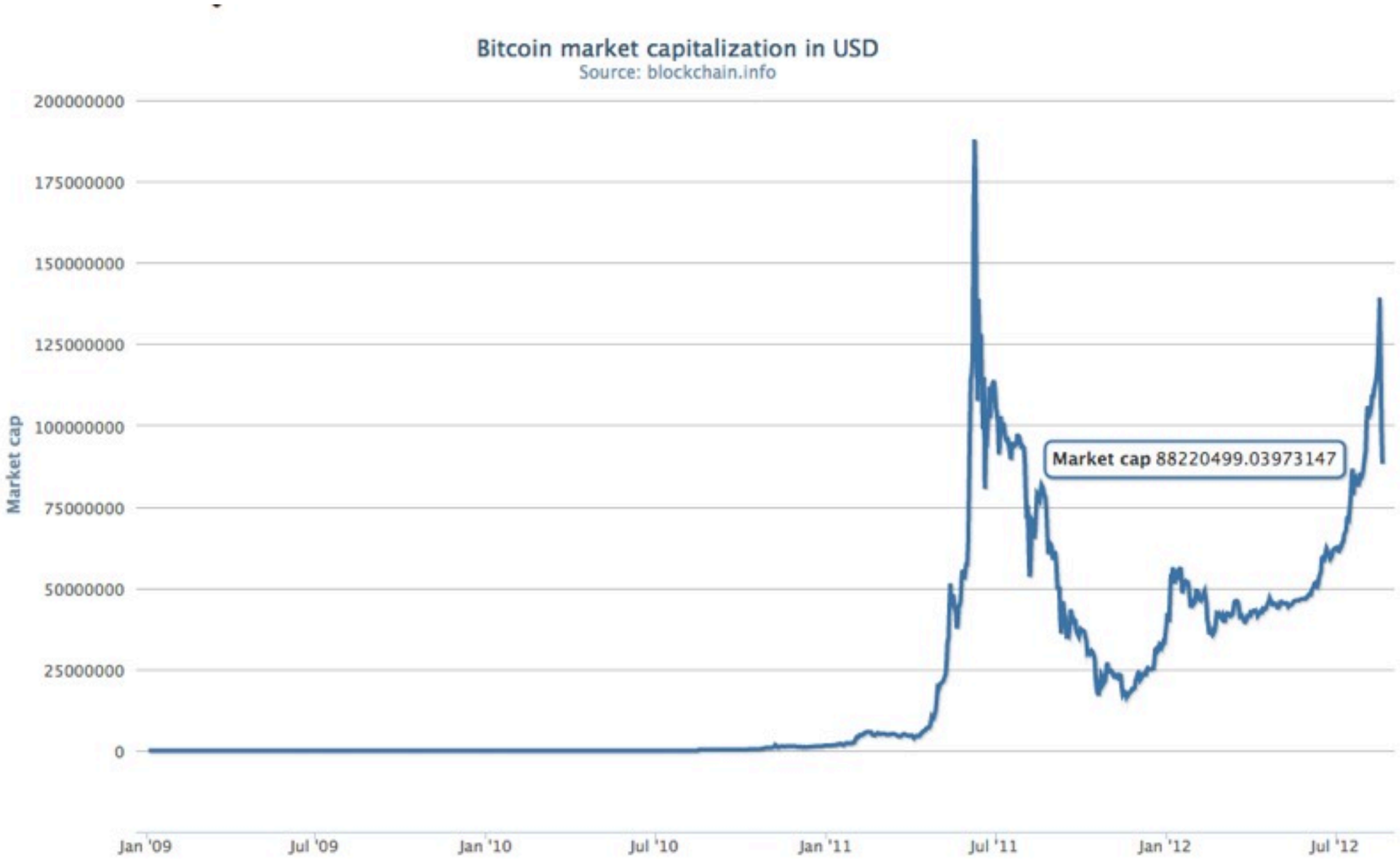
Finanzdaten

BTC Expansion Curve



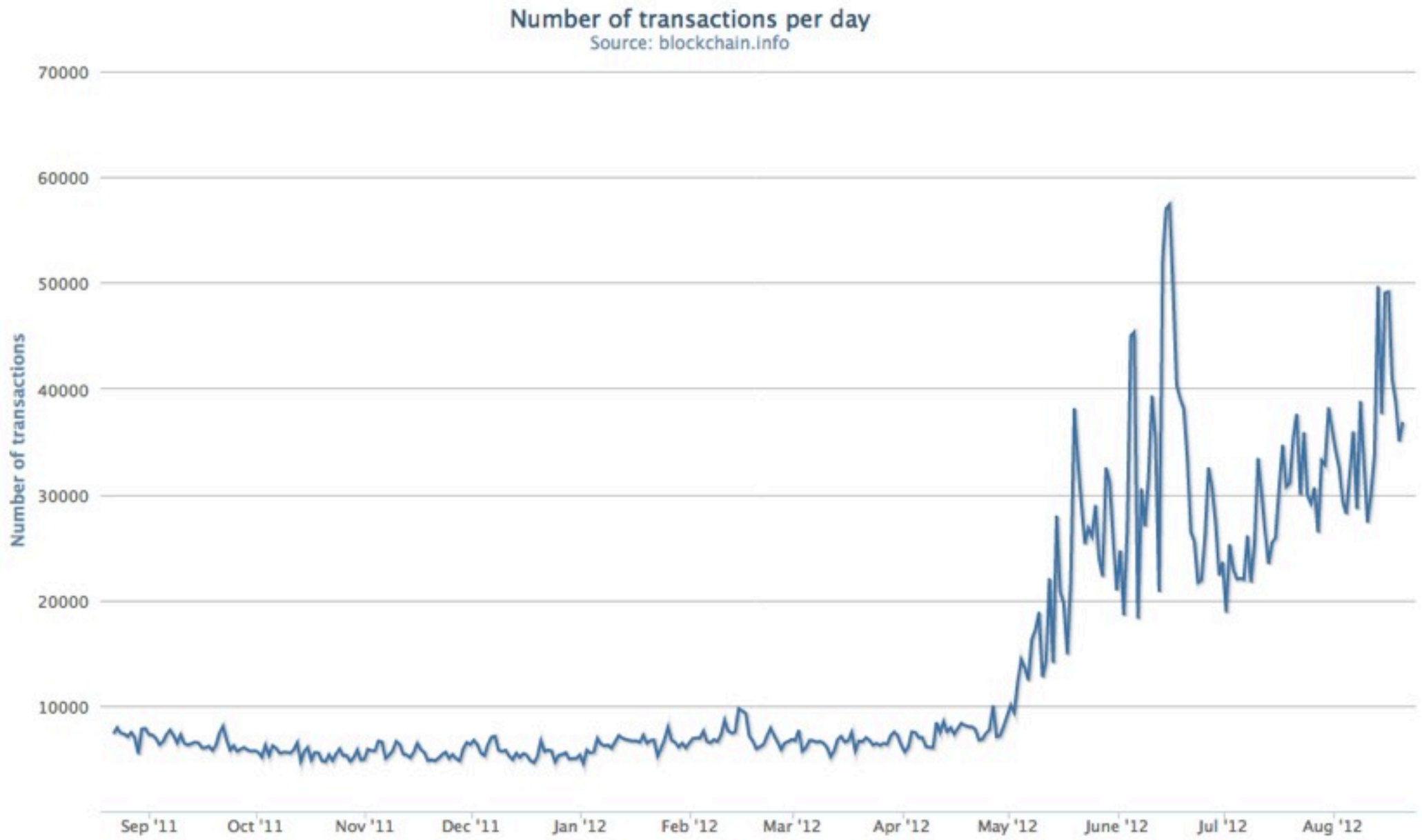
https://people.mozilla.com/~bwarner/bitcoin/slides.html#47

Kapitalisierung

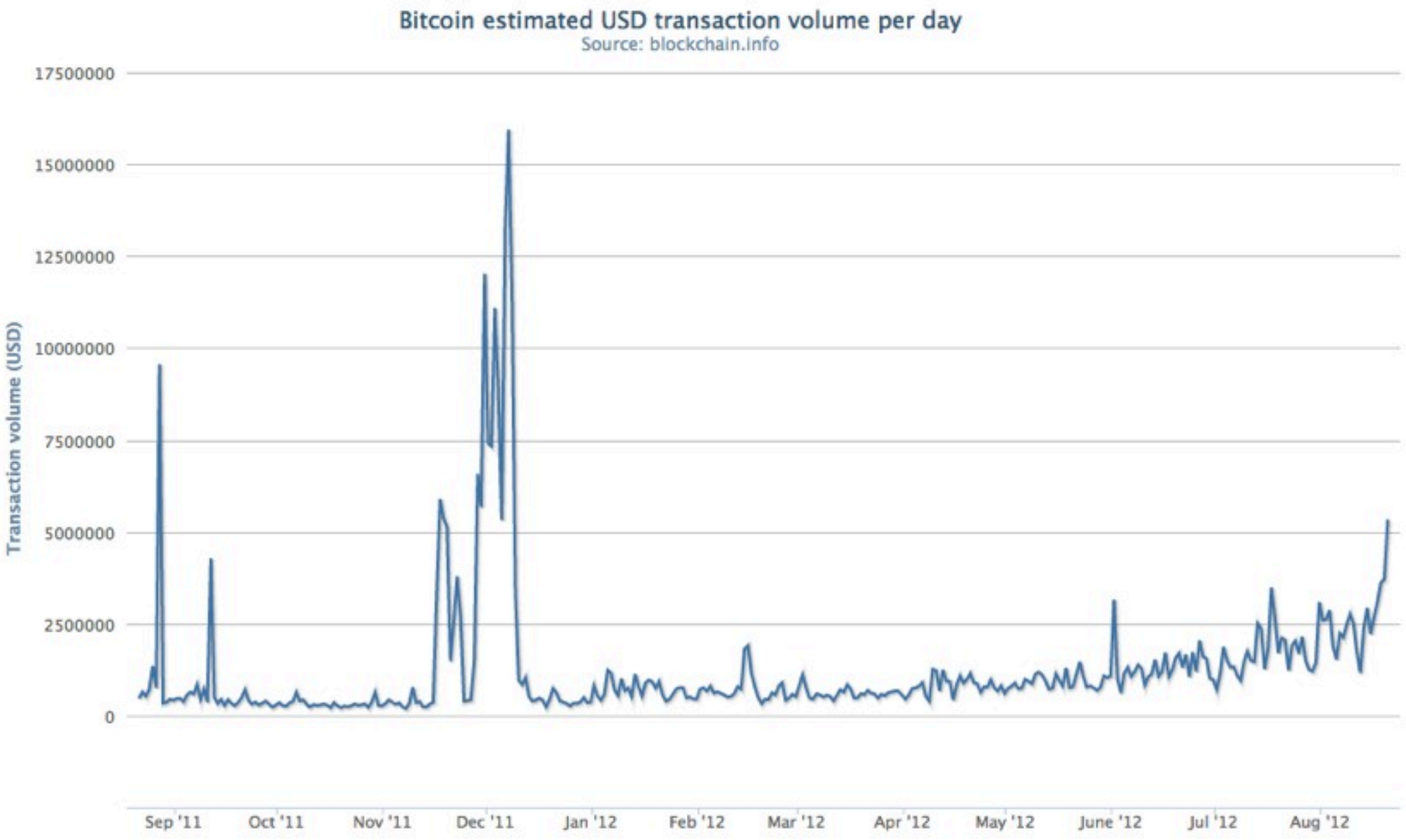


88.2 Millionen USD

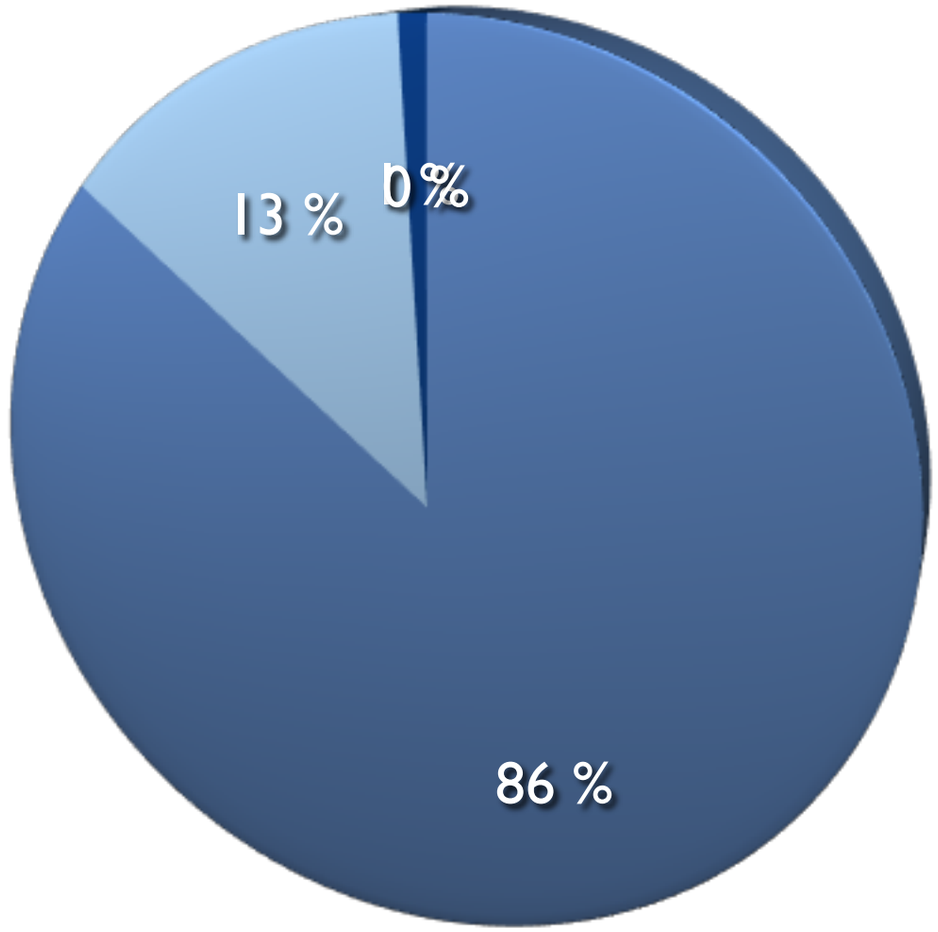
Transaktionen / Tag



Volumen / Tag



5 Mio USD / Tag



USD / EUR
EUR / AUD
USD / CHF
BTC / USD

Währungen	in MRD
USD / EUR *	1101
USD / CHF *	168
EUR / AUD *	12
BTC / USD	0.005

* 2010

http://de.wikipedia.org/wiki/Devisenmarkt

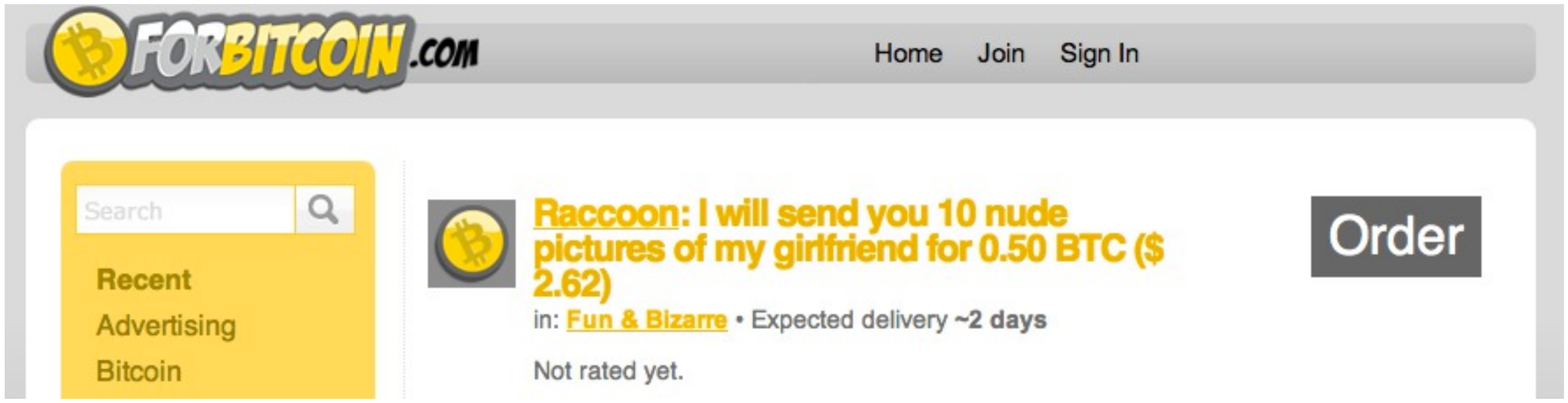
Kaufen / Verkaufen

- Online Dienste, Services
- Spenden (Creative Commons, WikiLeaks,)
- Bed & Breakfast
- Hotels
- Wuala
- ...

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

„Spezielle Angebote“

- Drogen
- Waffen



Wie bekomme ich BTC

- Wechseln (MtGox, ...)
- Selber schürfen (Mining)

Review

TRADE

FUNDING OPTIONS

ACCOUNT HISTORY

CHECKOUT BUTTON

Transactions

Please choose which history you want to see: BTC - USD

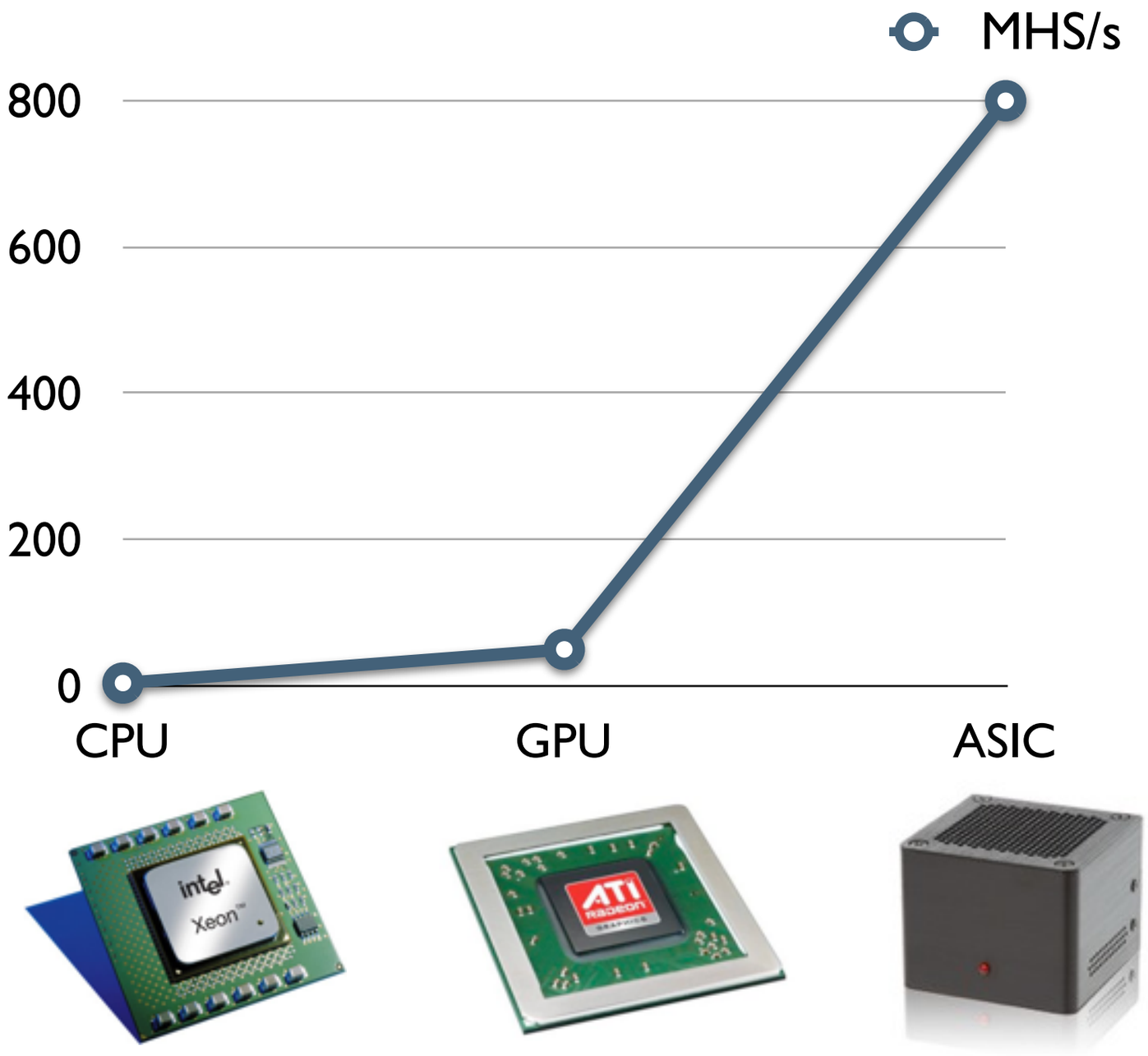
Filters

DATE	TYPE	STATUS	AMOUNT	BALANCE
(3 pages, 134 results)				1 2 3 > >>
2012/08/20 15:07:40	Fee		0.04744984 BTC	35.68839460 BTC
	BTC bought: [tid:1345475260868787] 7.90830721 BTC at $9.44991 (0.6% fee)			
2012/08/20 15:07:40	In		7.90830721 BTC	35.73584444 BTC
	BTC bought: [tid:1345475260868787] 7.90830721 BTC at $9.44991			
2012/08/20 15:06:36	Fee		0.03000000 BTC	27.82753723 BTC
	BTC bought: [tid:1345475196281519] 5.00000000 BTC at $9.44991 (0.6% fee)			
2012/08/20 15:06:36	In		5.00000000 BTC	27.85753723 BTC
	BTC bought: [tid:1345475196281519] 5.00000000 BTC at $9.44991			
2012/08/20 15:06:18	Fee		0.00301000 BTC	22.85753723 BTC
	BTC bought: [tid:1345475178878146] 0.50166716 BTC at $9.44991 (0.6% fee)			
2012/08/20 15:06:18	In		0.50166716 BTC	22.86054723 BTC
	BTC bought: [tid:1345475178878146] 0.50166716 BTC at $9.44991			
	Fee		0.00280789 BTC	22.35888007 BTC

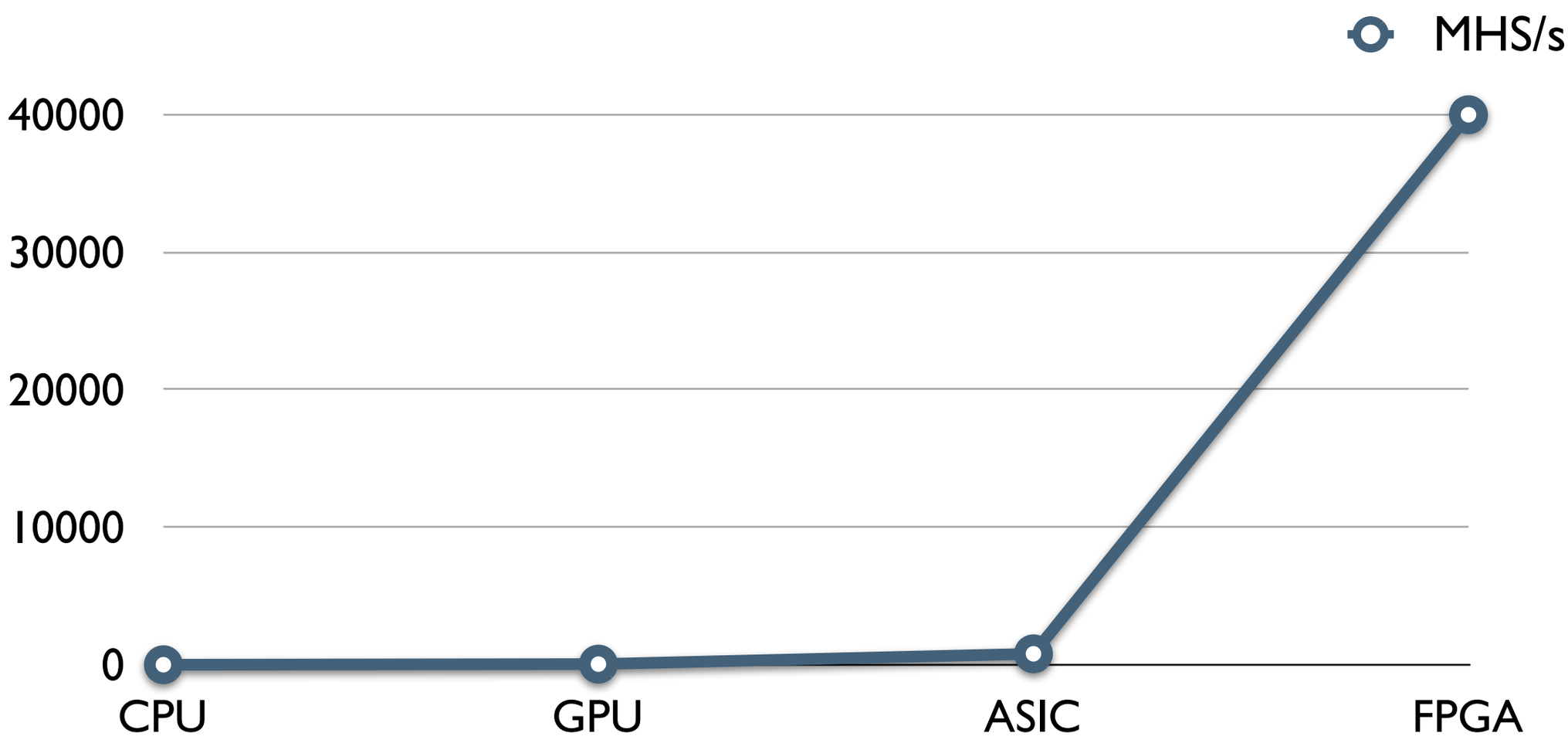
Schürfen

http://philosophyofscienceportal.blogspot.ch/2012/03/south-african-gold-mines-and-miners.html

Spezialisierte Hardware

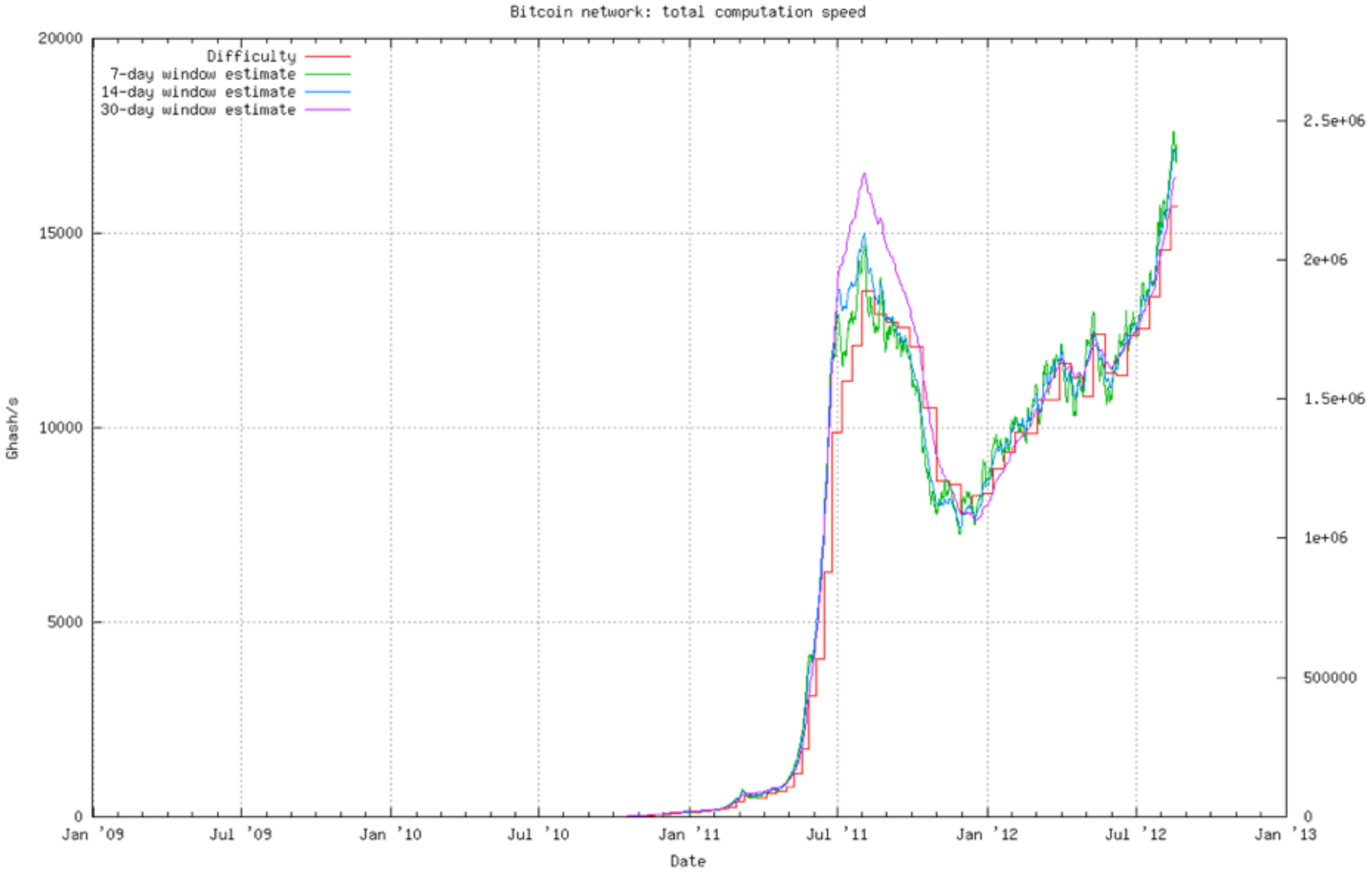


Spezialisierte Hardware



Next

Rechenleistung



Proof of Work

Schwierig zu erzeugen
einfach zu überprüfen

momentan

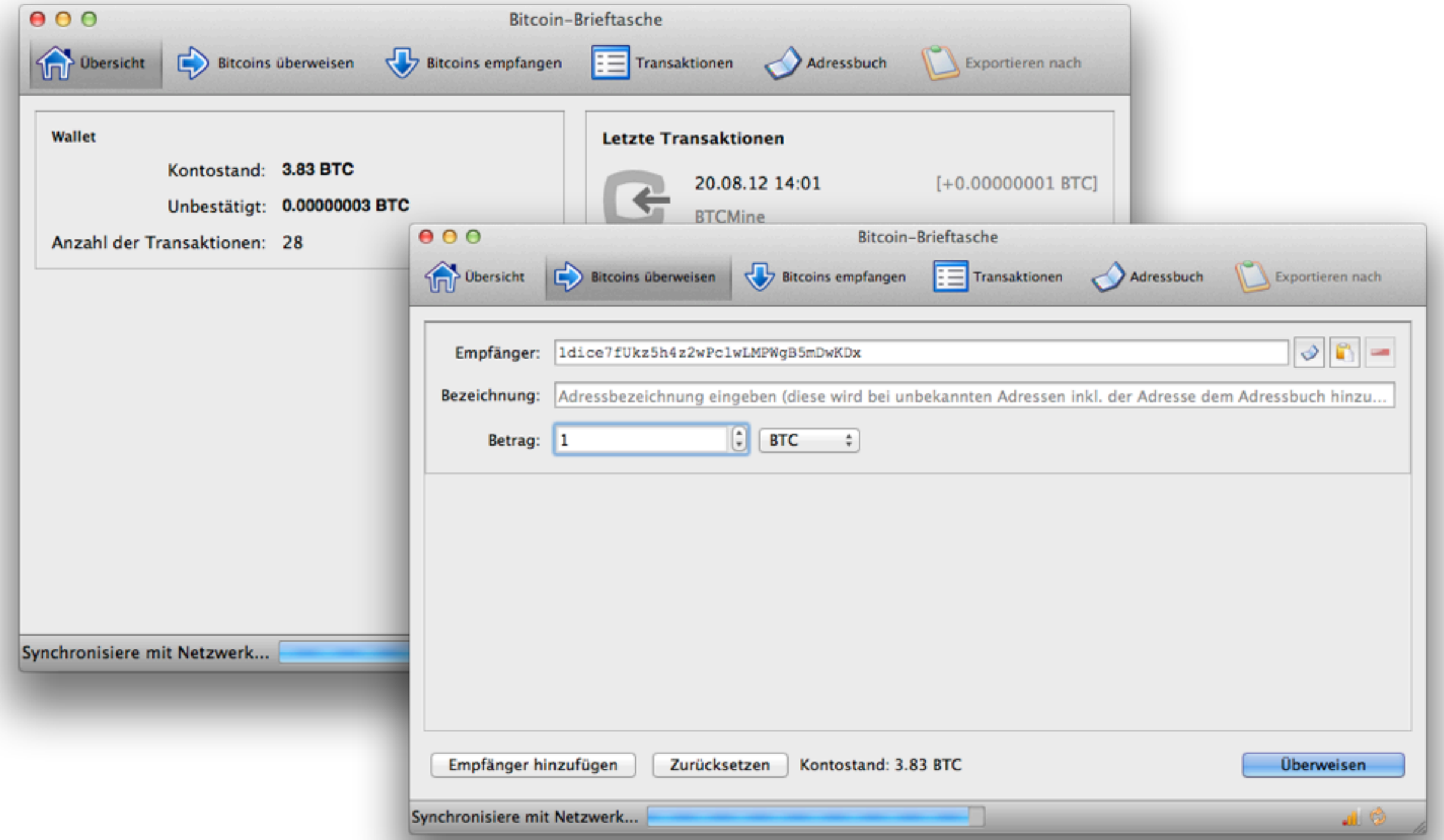
9‘411‘460‘517‘446‘288 Hashes

mit 800 MH/s
130 Tage

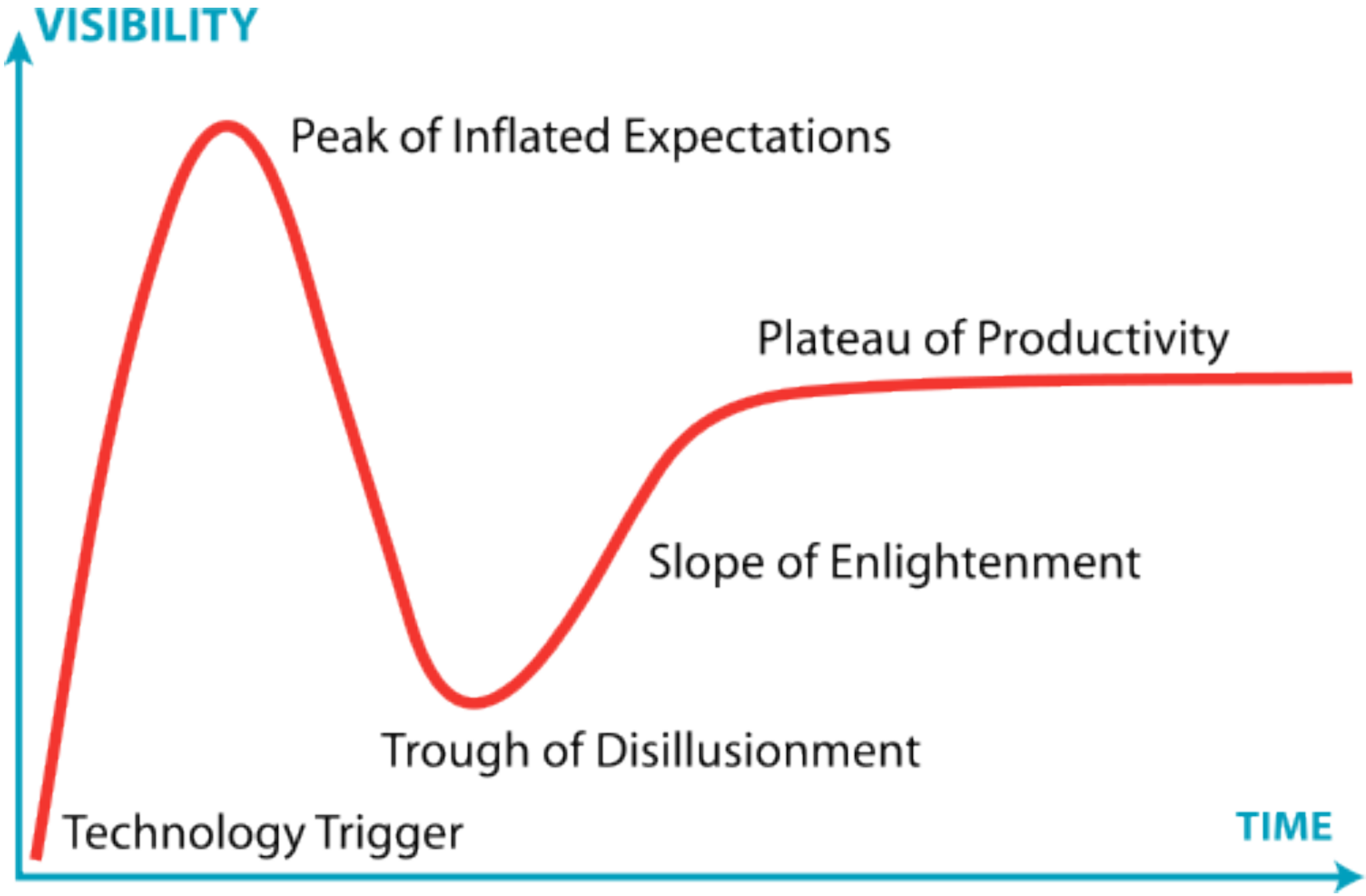
Zukunft

- BitCoin ist in „Hacker-Kreisen“ etabliert
- Vielfältige Dienstleistungen / Services - auch aus dem „normalen“ Leben
- Vielfältige Betrugsmaschen (z.B. High Yield Investment Programs - Ponzi Schema)
- Hoch Spekulativ (Devisenhandel)
- Kreditkarte in naher Zukunft angekündigt

Benutzer-Freundlichkeit




Mt. Gox (USD/dwolla/SEPA)
mtgoxUSD
Aug 20, 2012 – Daily
UTC – http://bitcoincharts.com
Op:8, Hi:10.5, Lo:7.81, Cl:9.68
35
30
25
20
15
10
5
0
Sep 10
Nov
Jan 11
Mar
May
Jul
Sep
Nov
Jan 12
Mar
May
Jul



Gartner „Hype Cycle“

Kontakt

Jens-Christian Fischer
@jcfischer

jens-christian.fischer@simplificator.com
jcf@mobino.com

http://blog.invisible.ch

creative commons

Attribution-NonCommercial-ShareAlike 2.5 Switzerland

You are free:

to Share — to copy, distribute and transmit the work

to Remix — to adapt the work

Under the following conditions:

Attribution. You must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work).

Noncommercial. You may not use this work for commercial purposes.

Share Alike. If you alter, transform, or build upon this work, you may distribute the resulting work only under the same or similar license to this one.

- For any reuse or distribution, you must make clear to others the license terms of this work. The best way to do this is with a link to this web page.
- Any of the above conditions can be waived if you get permission from the copyright holder.
- Nothing in this license impairs or restricts the author's moral rights.