Bitcoin - eine digitale, verteilte, anonyme Währung

AGENDA

- Geschichte
- Eigenschaften
- Transaktionen
- Blöcke
- Hashes
- Mining
- Demos
- MT Gox Hack

Der besondere Reiz an den Bitcoins ist ihre Konstruktion:

Bitcoins sind digital und global sowie pseudonym handelbar, vorbei an jeder Kontrolle - sei sie staatlich oder durch Banken und Zahlungsdienstleister.

Weder können Konten eingefroren werden, noch Zahlungsflüsse nachvollzogen werden, im Gegensatz zu globalen Transaktionen bei anderen Konten sind Überweisungen umsonst.

Der Blogger Jason Calacanis bezeichnete die Währung daher schon als

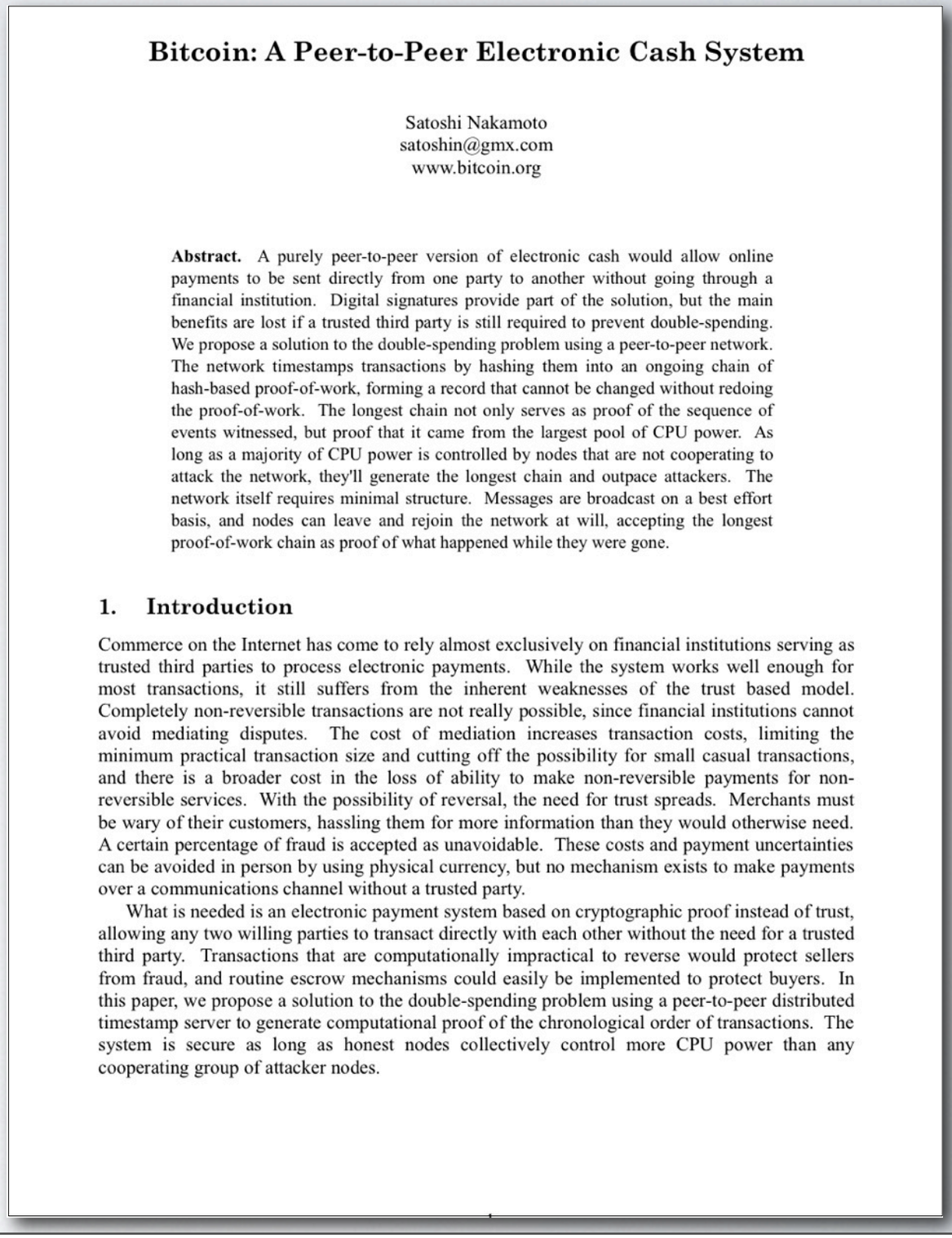
"das gefährlichste Open-Source-Projekt aller Zeiten".

Er rechnet früher oder später mit dem Verbot der Parallelwährung, die sich jeder Kontrolle entzieht.

http://www.golem.de/1105/83829.html

GESCHICHTE

- 2008, Whitepaper von Satoshi Nakamoto
- Das Konzept „anonymen digitalen Geldes, basierend auf asymmetrischen Kryptosystemen“ ist älter (1958)
- Beginn der Entwicklung Anfang 2009



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.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

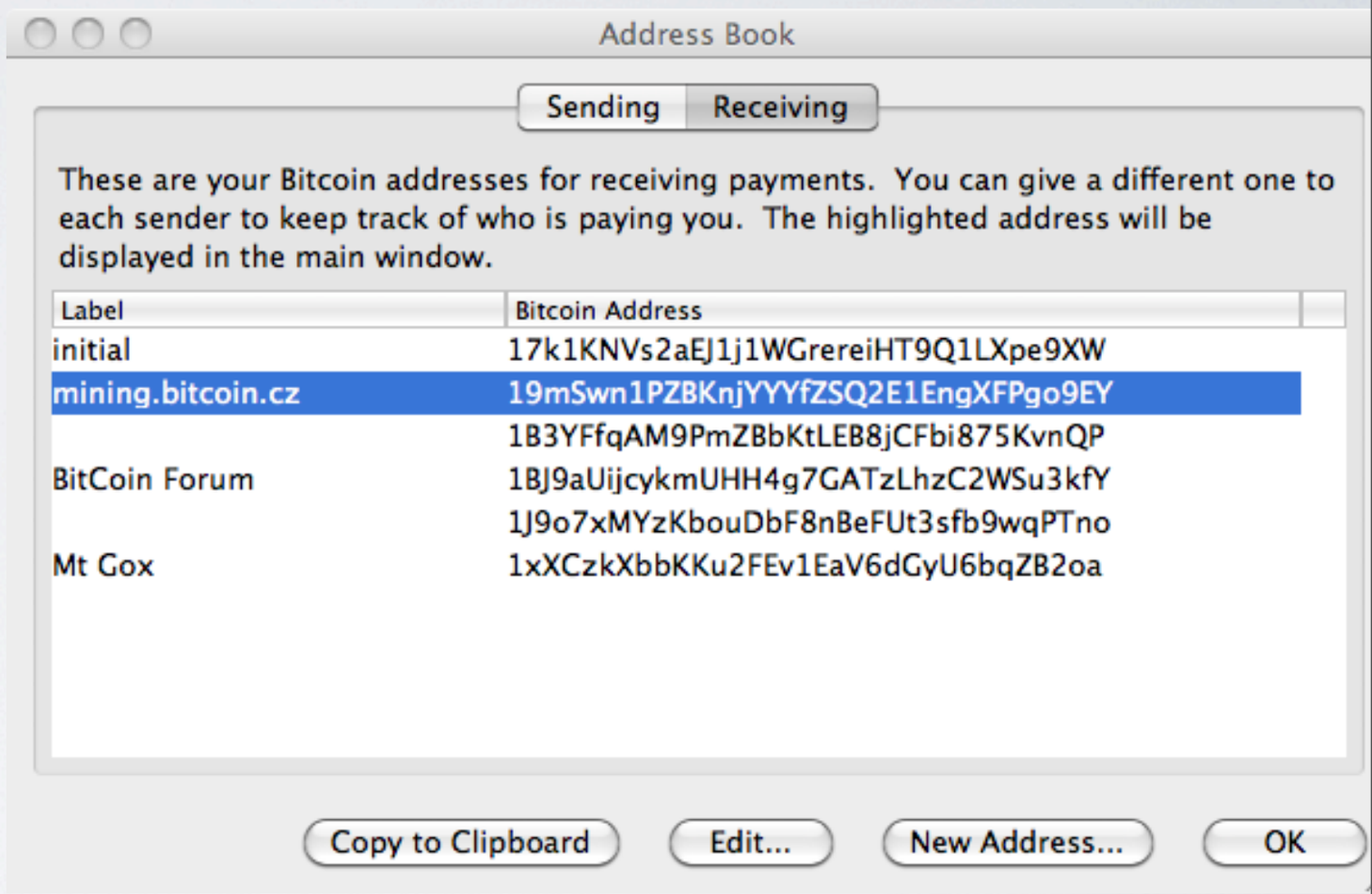
What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

EIGENSCHAFTEN

- Sicher
  Asymmetrische Verschlüsselung (Elliptic Curve DSA)
- Unabhängig
  Geldtransfer ohne Beteiligung von Dritten (Banken)
- Dezentral
  Eine zentrale Stelle, das Pendant zur Noten- oder Zentralbank, wird nicht benötigt.
- Anonym
  (für jeden Transfer ist eine neue Adresse möglich)
- Portabel
  Das Guthaben wird lokal in Form einer elektronischen Geldbörse (Wallet gesichert).
- Transparent
  Client ist komplett Open-Source, alle Transaktionen sind öffentlich.

SCHLÜSSEL

- Beim ersten Start erzeugt der Client ein Schlüsselpaar:
- Ein öffentlicher Schlüssel, der wie eine Kontonummer funktioniert (später können noch weitere generiert werden)
- Ein privater Schlüssel (wallet), der die Überweisungen frei schaltet



TRANSAKTIONEN

All Transactions | Sent/Received | Sent | Received

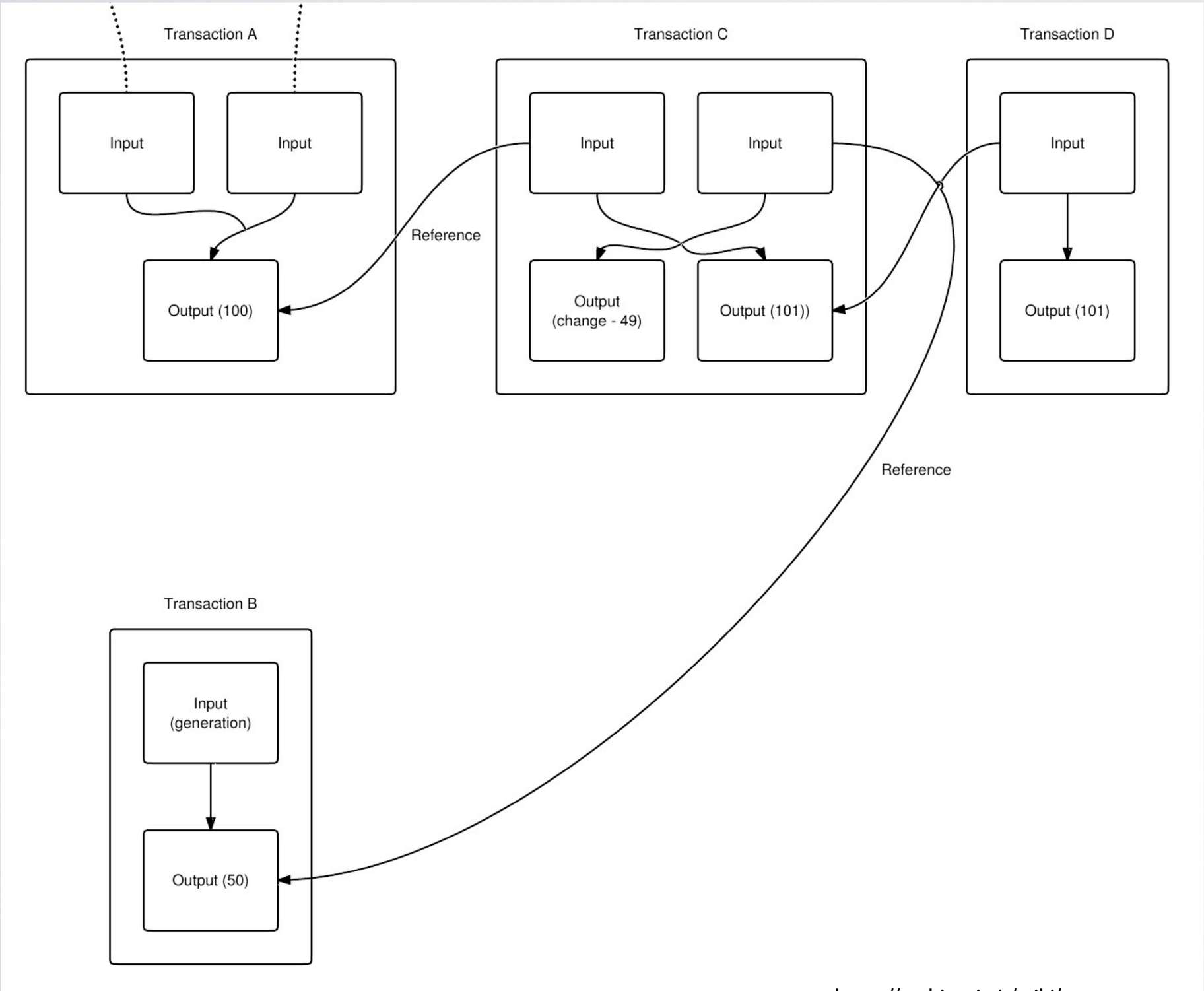
Status	Date	Description	Debit	Credit
22 confirmations	18.06.2011 01:33	Received with: 19mSwn1PZBKn... (mining.bitcoin.cz)		+0.01
25 confirmations	18.06.2011 01:05	Received with: 19mSwn1PZBKn... (mining.bitcoin.cz)		+0.01
84 confirmations	17.06.2011 17:35	Received with: 19mSwn1PZBKn... (mining.bitcoin.cz)		+0.01
108 confirmations	17.06.2011 15:07	Received with: 19mSwn1PZBKn... (mining.bitcoin.cz)		+0.01
114 confirmations	17.06.2011 13:34	Received with: 19mSwn1PZBKn... (mining.bitcoin.cz)		+0.02
157 confirmations	17.06.2011 07:34	Received with: 19mSwn1PZBKn... (mining.bitcoin.cz)		+0.01
168 confirmations	17.06.2011 05:59	Received with: 19mSwn1PZBKn... (mining.bitcoin.cz)		+0.01
172 confirmations	17.06.2011 05:09	Received with: 19mSwn1PZBKn... (mining.bitcoin.cz)		+0.01
179 confirmations	17.06.2011 04:08	Received with: 19mSwn1PZBKn... (mining.bitcoin.cz)		+0.03
297 confirmations	16.06.2011 13:37	Received with: 19mSwn1PZBKn... (mining.bitcoin.cz)		+0.01
306 confirmations	16.06.2011 12:36	Received with: 19mSwn1PZBKn... (mining.bitcoin.cz)		+0.02
314 confirmations	16.06.2011 12:08	Received with: 19mSwn1PZBKn... (mining.bitcoin.cz)		+0.01
319 confirmations	16.06.2011 11:35	Received with: 19mSwn1PZBKn... (mining.bitcoin.cz)		+0.01
343 confirmations	16.06.2011 07:06	Received with: 19mSwn1PZBKn... (mining.bitcoin.cz)		+0.02
542 confirmations	15.06.2011 12:17	Received with: 19mSwn1PZBKn... (mining.bitcoin.cz)		+0.02
1882 confirmations	09.06.2011 22:12	Received with: 1xXCzkXbbKKu... (Mt Gox)		+0.25
1989 confirmations	09.06.2011 09:33	Received with: 19mSwn1PZBKn... (mining.bitcoin.cz)		+0.01
2056 confirmations	09.06.2011 02:46	Received with: 1xXCzkXbbKKu... (Mt Gox)		+0.24
2309 confirmations	07.06.2011 18:34	Received with: 19mSwn1PZBKn... (mining.bitcoin.cz)		+0.01
2486 confirmations	06.06.2011 17:36	Received with: 19mSwn1PZBKn... (mining.bitcoin.cz)		+0.01
2619 confirmations	06.06.2011 04:36	To: 1J9QqpdC2iTSCAHJP4XCCXsYZd6ZVRFPh2	-5.00	
2881 confirmations	05.06.2011 01:04	Received with: 19mSwn1PZBKn... (mining.bitcoin.cz)		+0.01
3122 confirmations	03.06.2011 21:43	Received with: 17k1KNVs2aEJ... (initial)		+5.18
3544 confirmations	01.06.2011 19:21	Received with: 19mSwn1PZBKn... (mining.bitcoin.cz)		+0.01

17 connections 131533 blocks 24 transactions

TRANSAKTIONEN

- Alle Transaktionen sind öffentlich bekannt.
- Alle Knoten sind Teil der gleichen Historie in deren Reihenfolge die Transaktionen durchgeführt werden.

TRANSAKTIONEN



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

- A sendet 100 BTC to C
- C generiert 50 BTC.
- C sendet 101 BTC an D und sendet sich selbs eine Differenz (-49 BTCs)

DEMO
BITCOINMONITOR

BLOCK

- Im Bitcoin Netzwerk werden fortlaufend die laufenden Transaktionen in Form von Blöcken gespeichert.

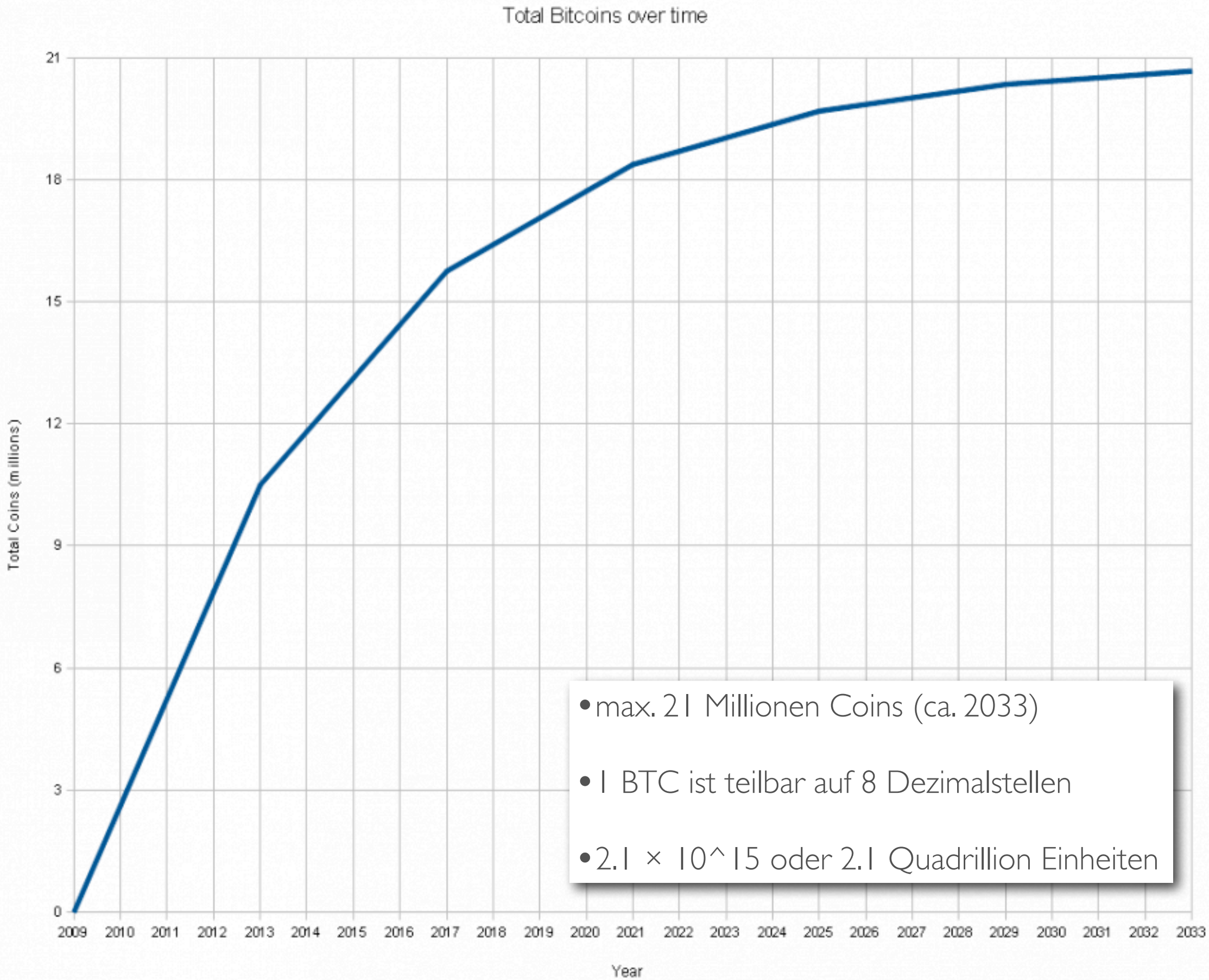
- Blöcke werden alle 10 Minuten erstellt.

BLOCK

- Jeder Block enthält:
  die letzten Transaktionen
  eine Nonce (random Number)
  der Hash des vorherigen Blocks
- Die erste Transaktion in einem Block enthält neue Bitcoins für den Knoten, der den Block generiert hat (Reward).
- aktuell sind dies 50 BTCs (diese Anzahl halbiert sich alle 210,000 Blöcke).

BLOCK

- neue Blöcke können alle 10 Minuten erstellt werden.
- Aktuell existieren ca. 136.000 Blöcke (http://blockexplorer.com/q/getblockcount)



- max. 21 Millionen Coins (ca. 2033)
- 1 BTC ist teilbar auf 8 Dezimalstellen
- 2.1 × 10^15 oder 2.1 Quadrillion Einheiten

BLOCK-EXPLORER

Block 71036[?]

Short link: http://blockexplorer.com/b/71036

Hash[?]: 00000000000997f9fd2fe1ee376293ef8c42ad09193a5d2086dddf8e5c426b56

Previous block[?]: 00000000009c516fac28019301e50b478f335e2fce14856f0b487f1cbb547da2

Next block[?]: 0000000000955acd68880d5d8a8d813e2f5f2cf7b1b7e0b7f10c31fc70b87c94

Time[?]: 2010-07-29 21:08:29

Difficulty[?]: 244.213223 ("Bits"[?]: 1c010c5a)

Transactions[?]: 7

Total BTC[?]: 167.82

Size[?]: 14.027 kilobytes

Merkle root[?]: f1cbd5d18720cd775f3ce92480c9cb2643b0cda98781e28004d0a903e0e24e25

Nonce[?]: 174619651

Raw block[?]

Transactions

Transaction[?]	Fee[?]	Size (kB)[?]	From (amount)[?]	To (amount)[?]
cfd753d7f3...	0	0.135	Generation: 50 + 0 total fees	15Gd5vbVzbKJHEq7a6ixL33E9ton4p9X3D: 50
98d1a7aee3...	0	0.257	1NZx2C2L1hjoZGhD6sieyHGiwhssZHxtQA: 13.7	12AvTd3Le5sUgJuX8mnLprufSojvEEUrGX: 0.05 19rnqSBGFnAQA6kceebjQbANGv7ZxuF6fc: 13.65
b1317f150b...	0	0.372	1JYajUKkEk8xTQzTRbDZU5XKyEWWeADtvZ: 49 1PR68ieryoKf8mmQe3bQPtuNyS51FxgCAN: 50	1ASAqSL7U2syVw27hozixtHaCoV1AMKP96: 90 19WnrbR73chSXm7m6wUzVT7PW3yBkMtNR5: 9
e411dbebd2...	0	4.304	1EFFSQKVrsq7KgmqxRB8gyLzccLFj3KzLk: 0.05	13fQzp1E8yhd1UUhW43kYX5Lfknv4TWp5: 0.04 Unknown: 0.01

Eigenschaften eines Blocks

alle Transaktionen des Blocks

DEMO
BLOCK-EXPLORER

GENERIERUNG VON BITCOINS

MINING

SYBIL ATTACK

„The Sybil attack in computer security is an attack wherein a reputation system is subverted by forging identities in peer-to-peer networks. It is named after the subject of the book Sybil, a case study of a woman with multiple personality disorder.“

http://en.wikipedia.org/wiki/Sybil_attack

PROOF OF WORK (POW)

- Um das System nicht durch eine große Anzahl falscher Identitäten zu kompromittieren („Sybil Attack“), ist es während der Generierung eines Blocks notwendig ein „proof-of-work“ Problem zu lösen.
- Knoten, die diese Arbeit durchführen heißen Miner.

POW

```
loop:
  var blockheader = DoGetWorkRPCCall()
  var target = ExtractTarget(blockheader)
  for nonce in 0..4294967295:
    var attempt = ModifyNonce(blockheader, nonce)
    var hash = SHA256(SHA256(attempt))
    if (hash < target)
      ReportSolution(attempt)
```

Ein Block gilt als „gelöst“
(veröffentlich und akzeptiert bei allen anderen Peers),

wenn der SHA-256 Hash des gesamten Blocks
(nummerisch) kleiner ist als das aktuelle Target.

VERSCHIEDENE MINER

- CPU
- GPU
- FPGA

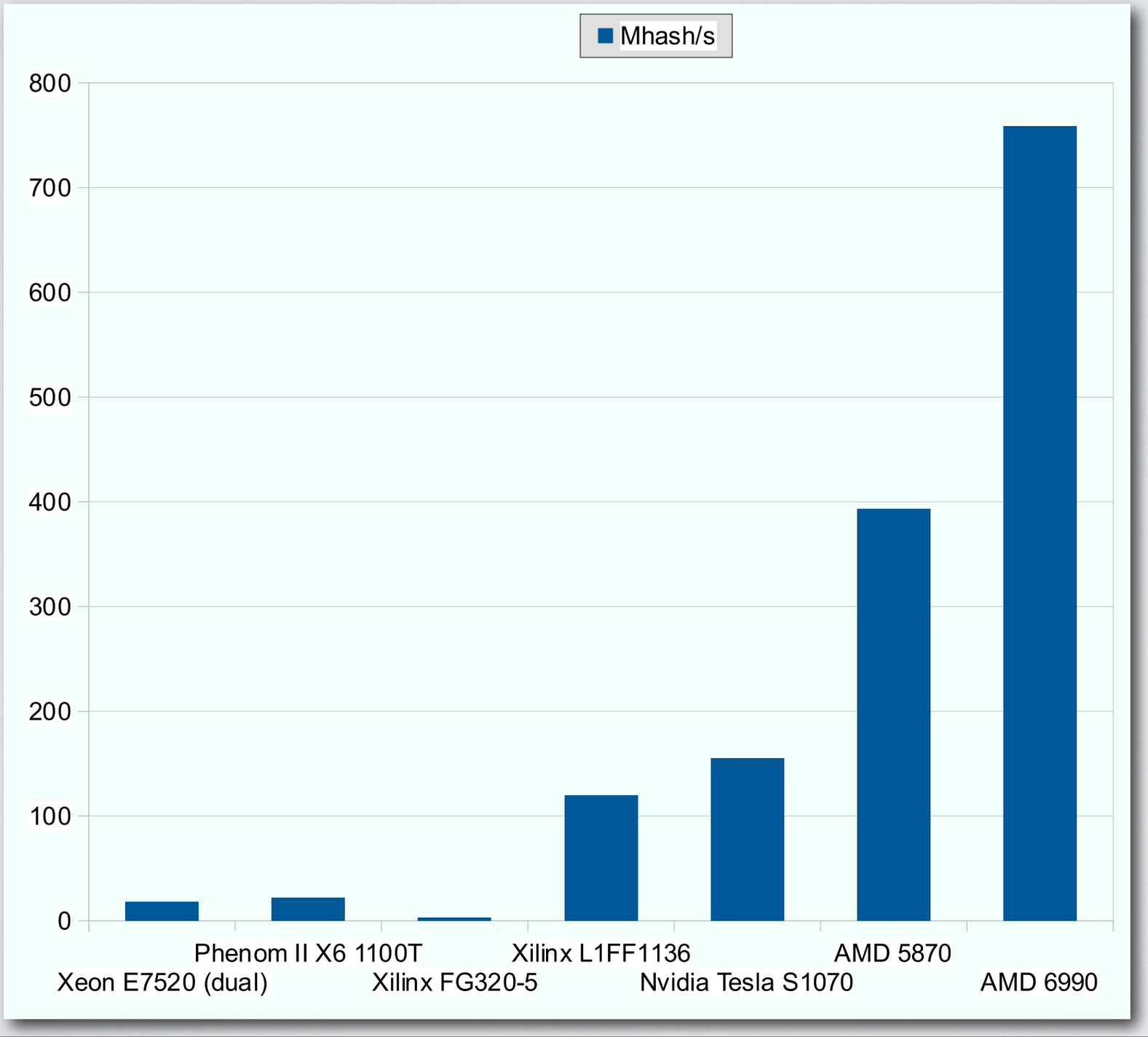
- Durchsatz (MHashes/s)
- Verbrauch (Watt)
- Betrieb (Wärm/Strom)

HARDWARE - VERGLEICH

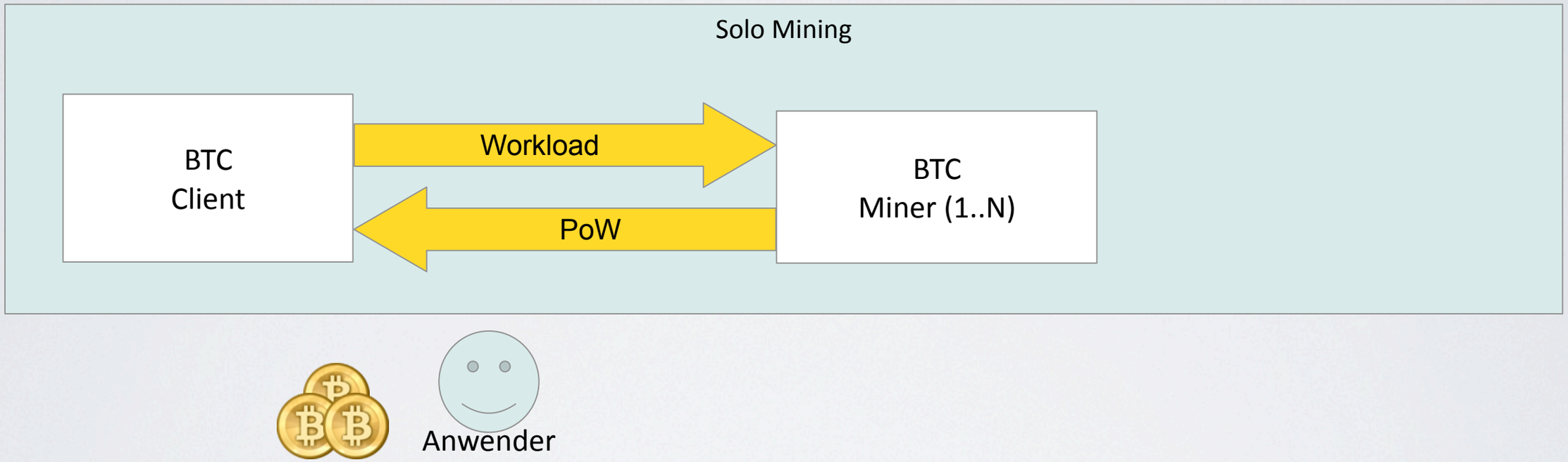
	Mhash/s	W
CPU		
Phenom II X6 1100T	22	125
Xeon E7520 (dual)	18	95
FPGA		
Xilinx XC3S500E-FG320-5	3.125	0.78
Xilinx XC5VLX110T-1FF1136	120	0.78
GPU		
Nvidia Tesla S1070	155.2	150
AMD 5870	393.46	150
AMD 6990	758.82	346

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

HARDWARE

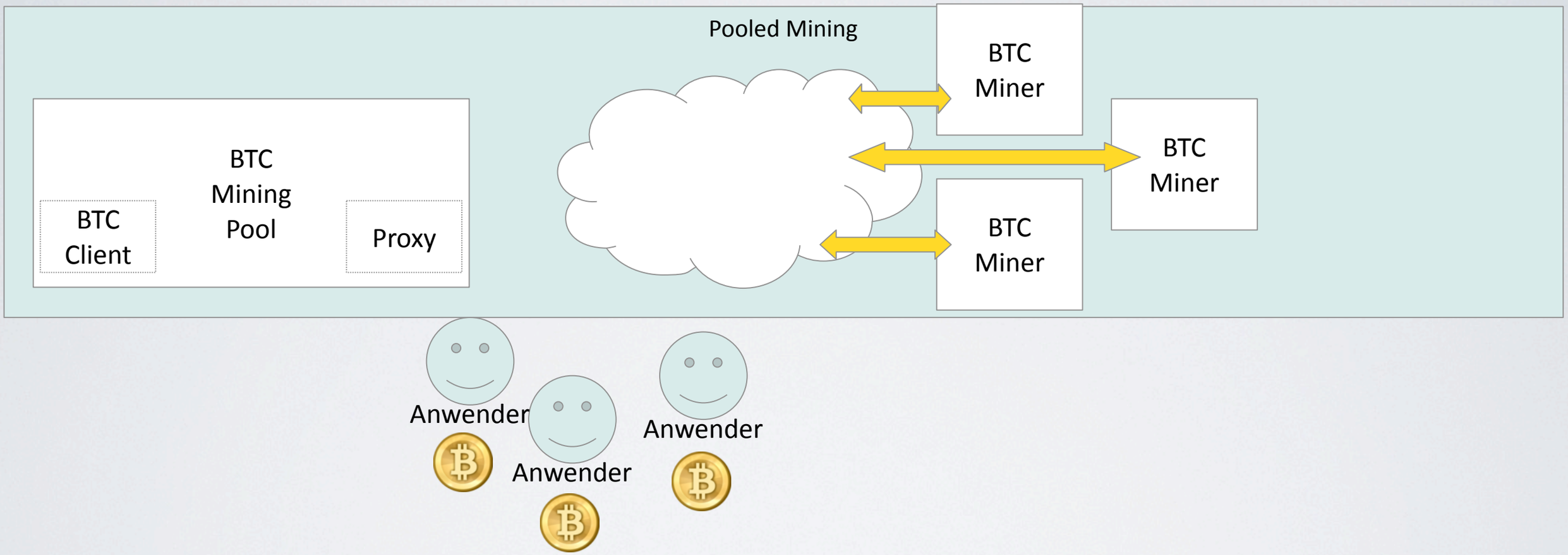

Mhash/s
800
700
600
500
400
300
200
100
0
Xeon E7520 (dual)
Phenom II X6 1100T
Xilinx FG320-5
Xilinx L1FF1136
Nvidia Tesla S1070
AMD 5870
AMD 6990

SOLO-MINING



50 BTCs für einen User

POOLED MINING



Anwender erhalten je nach eingebrachter Rechenzeit einen Anteil

BEWERTUNG

Solo-Mining

- hoher Ertrag
- mehr Aufwand
- weniger regelmäßig

Pooled-Mining

- Geringerer Ertrag
- Auch mit weniger Rechenleistung erfolgreich
- regelmäßigeres „Einkommen“

DEMO
SOLO MINING

HOWTO

- Einrichten des BTC-Clients als Server
- Client muss alle aktuellen Blöcke herunter geladen haben
- Installation eines Miners (CPU/GPU)

BITCOIN.CONF

- Location:

  MacOS:
  /Users/<user>/Library/Application Support/Bitcoin

  Windows:
  c:\Benutzer\<user>\AppData\Roaming\Bitcoin

  Linux:
  /home/<user>/.bitcoin

BITCOIN.CONF

```
#versch. Nodes (schnelleres Scanning)
addnode=69.164.218.197
addnode=64.22.103.150
addnode=173.242.112.53

#Server ist aktiv
server=1

rpcuser=user
rpcpassword=pass
rpcport=8332
rpcallowip=192.168.178.*

#Client generiert BTCs?
#gen=1
#Gen-Algo
#4way=1

paytxfee=0.00
min=1
```

DEMO
POOLED MINING

HOWTO

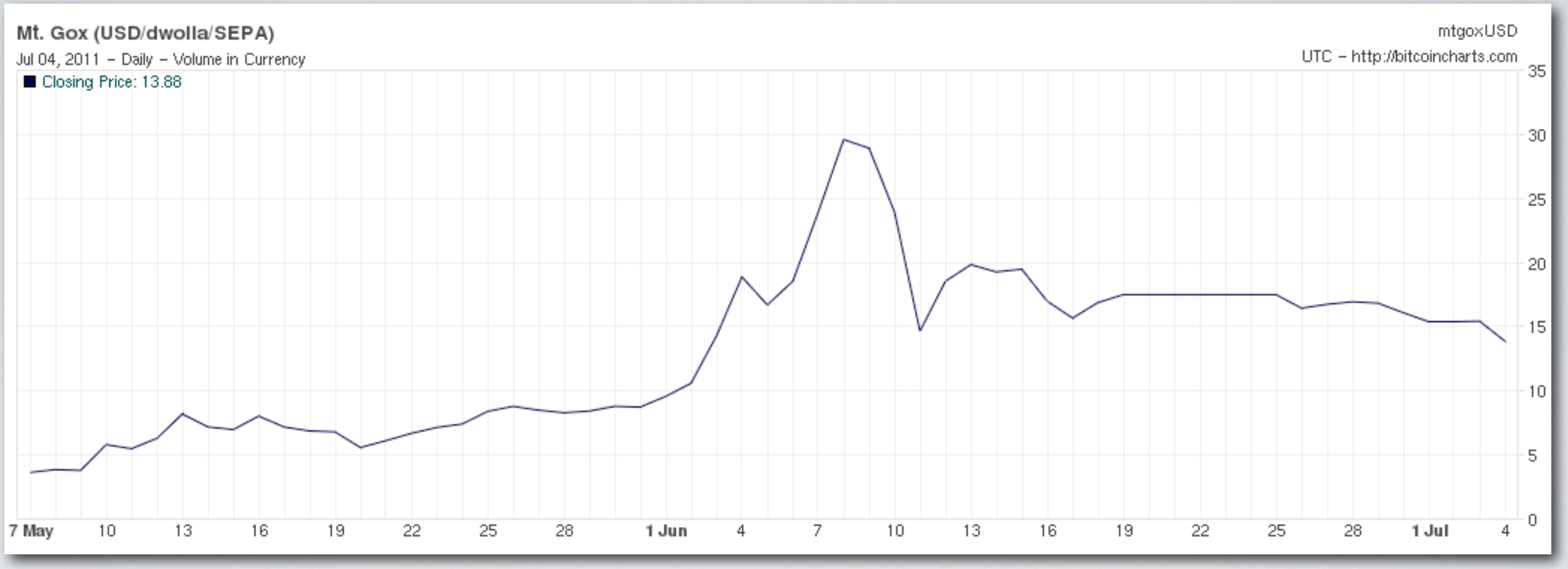
- Wahl eines Mining Pools (z.B. Slush Pool)
- Einrichten eines Accounts
- Eintrag eines Empfänger-Keys
- Einrichten eines Miners (oder mehrere)

„EMPFEHLUNGEN“

- CPU-Mining lohnt nicht, GPU Mining auf AMD Karten hat den größten Effekt.
- Solo-Mining lohnt sich aktuell ab ca. 1000 MHashes/s
- (ca. 1BTC/Tag ~ $17) – allerdings: ca 1000W Verbrauch und man braucht keine Heizung mehr :-).
- Pool-Mining ist gut um mal „eigene“ BTCs zu besitzen (eher Promille-Bereich).
- Für geringere Beträge lassen sich auch BTCs kaufen (und ggf. vermehren → Day-Trading)

TRADING

CHARTS


Mt. Gox (USD/dwolla/SEPA)
Jul 04, 2011 – Daily – Volume in Currency
Closing Price: 13.88
mtgoxUSD
UTC – http://bitcoincharts.com
35
30
25
20
15
10
5
0
7 May
10
13
16
19
22
25
28
1 Jun
4
7
10
13
16
19
22
25
28
1 Jul
4

TRADING PORTALE

Symbol	Latest Price	Previous Close	Volume	30d Volume	Day low/high		Open	Bid	Ask	30 days
mtgoxUSD USD (dwolla/SEPA)	13.81 Jul 4, 2011, 23:13:38	15.44049 -1.63049 -10.56%	51,408.47 744,898.71 USD	1,345,628.20 25,770,967.96 USD	13.14	15.48988	15.4407	13.83001	13.8756	
thUSD USD	13.84 Jul 4, 2011, 23:11:12	15.2 -1.36 -8.95%	5,170.88 75,656.49 USD	77,255.62 1,253,215.18 USD	13.26	15.85	15.24	13.70001	13.84	
bitomatPLN PLN (wire)	38.15 Jul 4, 2011, 22:47:29	40.65 -2.5 -6.15%	1,572.53 61,459.28 PLN	49,494.48 2,874,613.92 PLN	36.06	41.5	40.68	37.24	38.15	
britcoinGBP GBP (wire)	8.8221 Jul 4, 2011, 23:14:01	9.9 -1.0779 -10.89%	1,123.58 10,458.39 GBP	18,187.23 217,665.05 GBP	8.8	12.699	9.8864	8.8221	5	
bitmarketEUR EUR (wire)	10.49 Jul 4, 2011, 22:44:48	11 -0.51 -4.64%	424.42 4,772.59 EUR	17,201.39 248,624.41 EUR	10.1	16.9	11	10.11	10.3	
b7USD USD	14.4 Jul 4, 2011, 21:59:27	15.27 -0.87 -5.70%	1,104.20 15,798.71 USD	12,767.44 196,741.32 USD	13.75	15.3	14.58	13.8	14.4	
virwoxSLL SLL (Second Life)	3160 Jul 4, 2011, 23:10:23	4174 -1014 -24.29%	375.00 1,352,604.00 SLL	11,171.00 62,323,655.80 SLL	2940	4175	4175	3160	3891	
bitmarketUSD USD (wire/PayPal)	15.5 Jul 4, 2011, 22:07:47	16.8 -1.3 -7.74%	162.77 2,585.92 USD	3,961.01 80,154.50 USD	15	17	16.85	15.5	15.9	
btcexUSD USD (wire)	13.6865 Jul 4, 2011, 23:04:22	14.1032 -0.4167 -2.96%	125.90 1,800.08 USD	1,726.72 29,568.88 USD	13.0087	15.3	14.1277	13	13.7	
thLRUSD USD (Liberty Reserve)	13.6 Jul 4, 2011, 21:03:09	14.5 -0.9 -6.21%	142.90 2,069.68 USD	1,565.62 23,292.55 USD	13.6	15.19	15.19	13	14.34980654	
bitmarketGBP GBP (wire)	10 Jul 4, 2011, 18:30:48	10 0 0%	9.00 90.04 GBP	1,299.06 17,225.46 GBP	10	10.01	10.01	9	9.8	
b7EUR EUR	9.7 Jul 4, 2011, 21:07:54	10.71 -1.01 -9.43%	95.93 977.31 EUR	1,029.79 14,409.04 EUR	9.7	11	10.71	9.5	9.7	
exchbUSD	13.8587	15.3	45.22	1,009.01	13.5	15.5638	15.5638	13.5	14.1783	

http://bitcoinwatch.com/

TRADING API

All these URLs return JSON results.

Fetching Public Data	
Ticker Data	http://mtgox.com/code/data/ticker.php
Market Depth	http://mtgox.com/code/data/getDepth.php
Recent Trades	http://mtgox.com/code/data/getTrades.php

The following take your Mt Gox username and password as parameters. They must be sent as a POST.

Placing Orders	
Get your current balance	**https://mtgox.com/code/getFunds.php?name=blah&pass=blah**
Place an order to Buy BTC	**https://mtgox.com/code/buyBTC.php?name=blah&pass=blah&amount=#&price=#** returns a list of your open orders
Place an order to Sell BTC	**https://mtgox.com/code/sellBTC.php?name=blah&pass=blah&amount=#&price=#** returns a list of your open orders
Fetch a list of your open Orders	**https://mtgox.com/code/getOrders.php?name=blah&pass=blah** oid: Order ID type: 1 for sell order or 2 for buy order status: 1 for active, 2 for not enough funds
Cancel an order	**https://mtgox.com/code/cancelOrder.php?name=blah&pass=blah&oid=#&type=#** oid: Order ID type: 1 for sell order or 2 for buy order
Send BTC	**https://mtgox.com/code/withdraw.php?name=blah&pass=blah&group1=BTC&btca=bitcoin_address_to_send_to&amount=#**

DEMO
MT GOX

HISTORY

- January 3, 2009
Genesis block established at 18:15:05 GMT

- May 22, 2010
first pizza for Bitcoins 10,000 BTC for ~$25

- July 11, 2010
Bitcoin slashdoted

- December 7, 2010
first Mobile to Mobile Transaction (Nokia N900)

- December 16, 2010
first Block found with pooled Mining

- January 28, 2011
1/4 of 21 million generated.

- February 9, 2011
$1 per BTC at MtGox.

- February 14, 2011 First vehicle was offered for BTCs

- April 16, 2011
TIME does an article on Bitcoin.

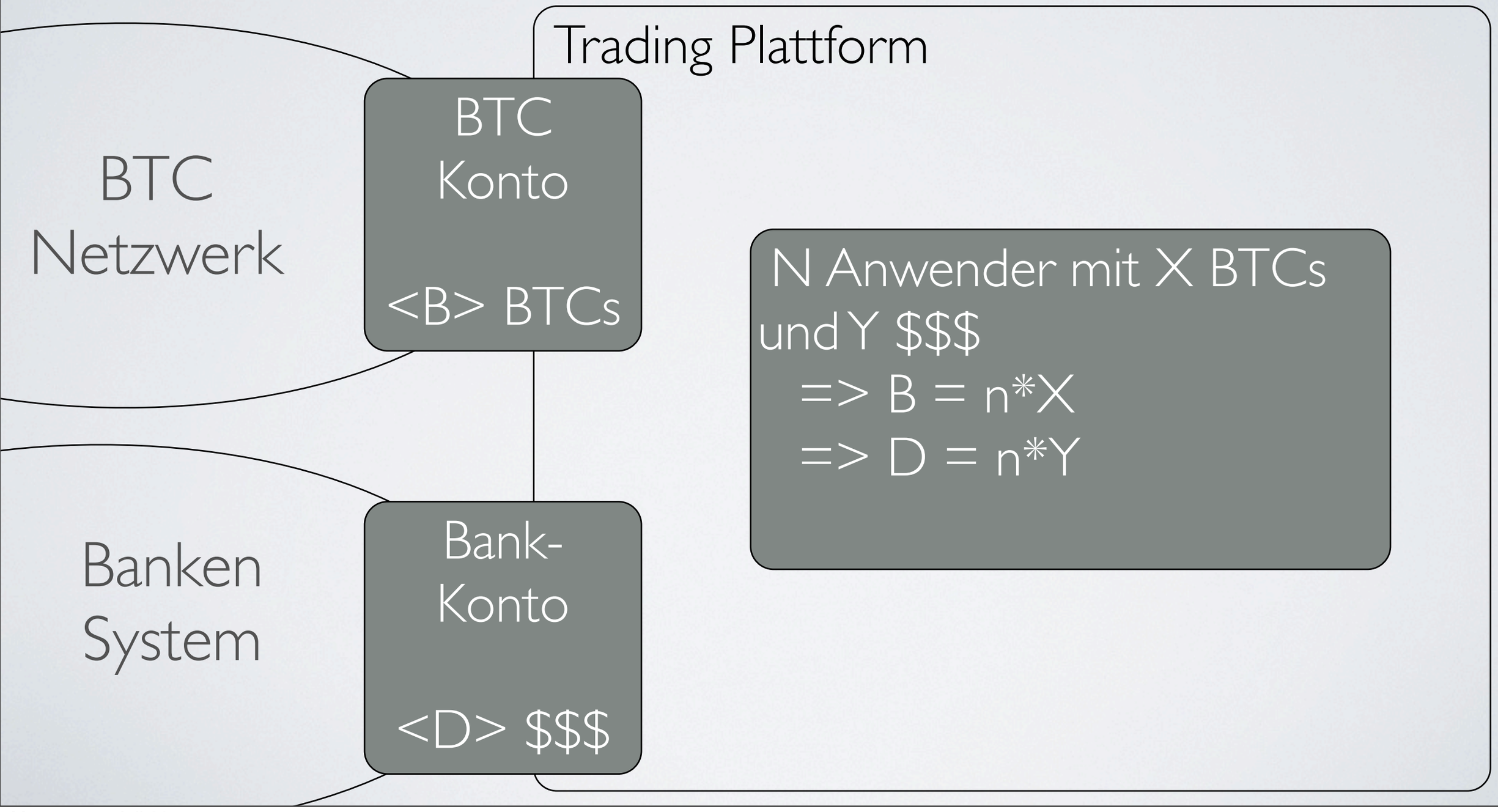
- June 10, 2011
exchange rate above 31 USD

- June 19, 2011
The MtGox database was hacked

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

MT GOX HACK

WIR FUNKTIONIERT EINE TRADING PLATTFORM?



FOLGEN

- intern kann die Plattform alle Abläufe steuern (DB-Operationen)
- Dauerhafte Transaktionen erfolgen erst beim Abbuchen von Dollars/BTCs
- Das Vertrauen in so eine Trading-Plattform muss groß sein.

MT GOX HACK VERMUTUNG

Username	Email	Password (md5 Hash)	Amount $	Amount BTC
test	test@example.com	2a3.....4gr34	10	234
user	user@domain.com	f13.....4gr3fs	20	12
...				

FOLGEN

- Durch den Hack wurden die Verhältnisse der Nutzer untereinander verändert.
- Die DB konnte auf einen früheren Zustand zurück gerollt werden.
- BTCs wurden scheinbar nicht in größerem Rahmen transferiert.
- Hashing-Algorithmus der Passwörter ist nun SHA256

LINKS

http://www.bitcoin.org
Projektseite mit Bitcoin-Clients

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

http://www.bitcoinmonitor.com
Live-Ansicht aller Transaktionen im P2P Netz

http://blockexplorer.com
Untersuchung aller im System vorhandener Blöcke

http://bitcoinwatch.com/
Echtzeit Informationen über das Bitcoin Netzwerk

Eine der größten BTCs-Trading-Plattformen
https://mtgox.com

Algorithmus für BTC Keys
http://en.wikipedia.org/wiki/Elliptic_Curve_DSA