Seminar Web Science

฿ Bitcoins ฿

Nico Merten

nmerten@uni-koblenz.de

16.05.2012

Überblick

- Satoshi Nakamoto - 2009 - Bitcoin: A Peer-to-Peer Electronic Cash System
- Über den Autor:
  - Frau oder Mann?
  - Anagram: Katoshi Namasoto
  - Kleingruppe von Mitarbeitern eines Geheimdienstes
  - **SA**msung, **TOSHI**ba, **NAKA**michi und **MOTO**rola

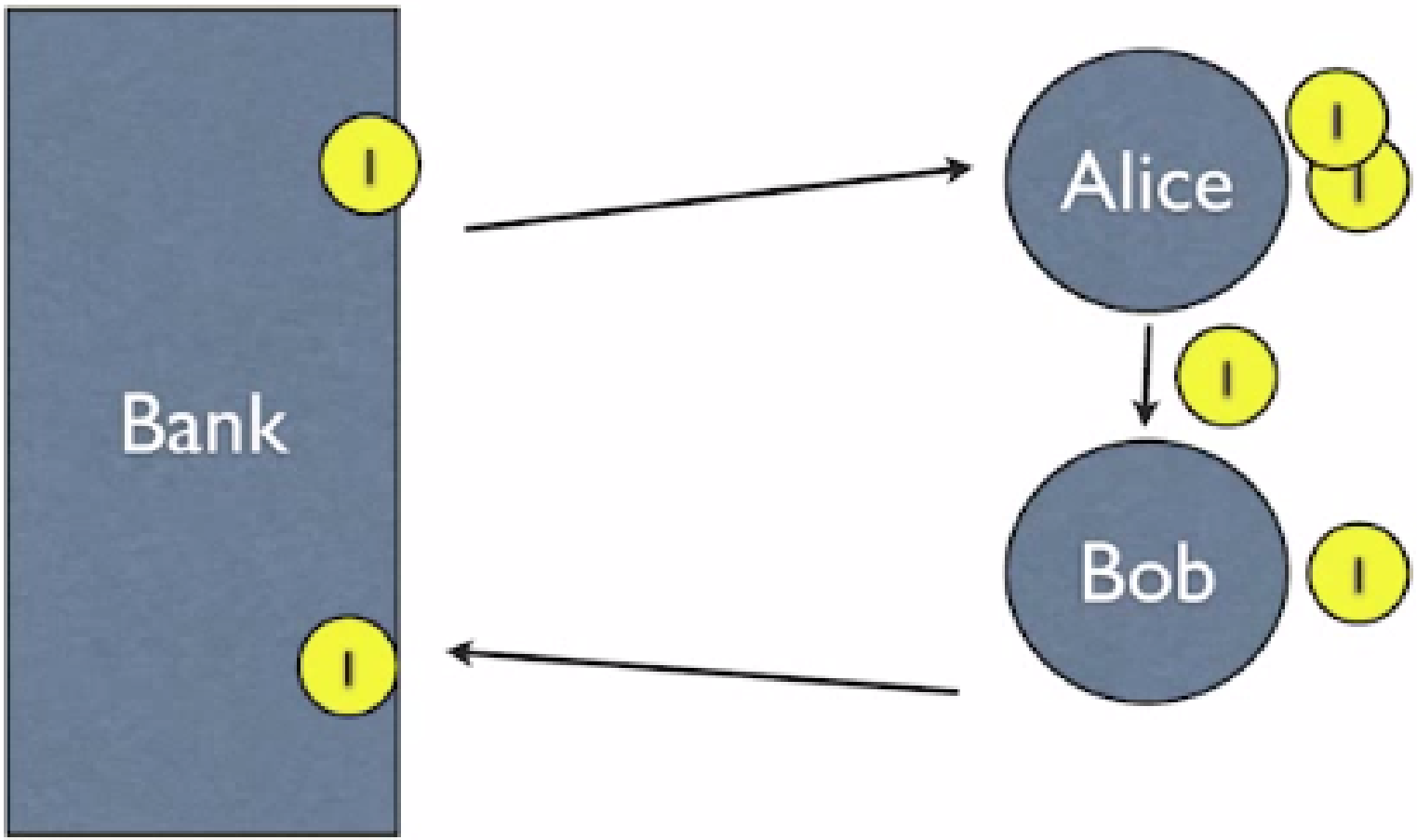
Idee

Elektronische Zahlungsmittel sollten...

- einfach,
- anonym,
- sicher,
- schnell und
- günstig

sein.

Elektronische Ideen - DigiCash (David Chaum)



Elektronische Ideen - WoW Gold, SecondLife L$

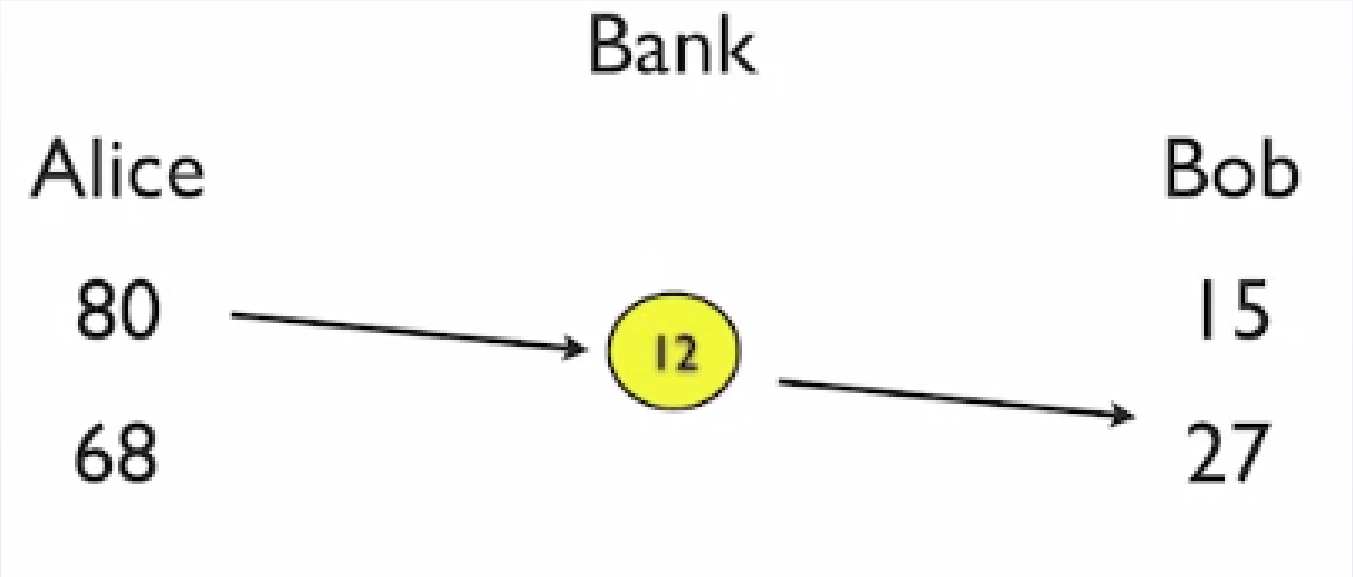


Abbildung: Schema einer Rollenspiel Währung

Probleme bei elektronischem Geld

- Geld mehrfach ausgeben (Double-Spending Problem)
- Erzeugen von Währung (Inflation)
- Bank kann Geld von Benutzern ausgeben
- SPOF (Single Point of Failure)

Funktionen gegenübergestellt

	Echte Banken	Bitcoin
Geld aufbewahren	Konten	Wallets
Geld transferieren	Überweisungen	Transactions
Geld schöpfen	Drucken und Prägen	Mining
Geld wechseln	Tausch	Anbieter

Geld aufbewahren

	Echte Banken	Bitcoin
Geld aufbewahren	**Konten**	**Wallets**
Geld transferieren	Überweisungen	Transactions
Geld schöpfen	Drucken und Prägen	Mining
Geld wechseln	Tausch	Anbieter

Wallet

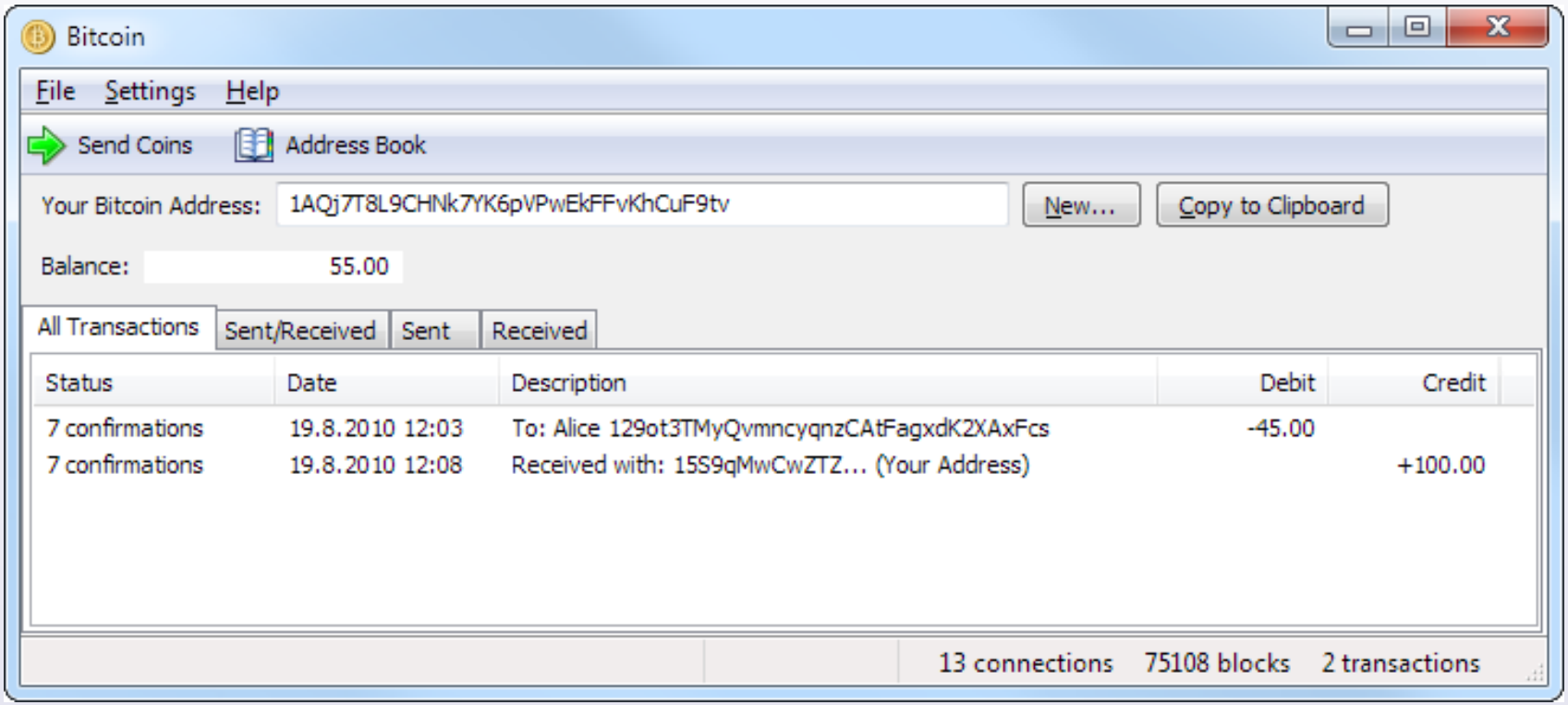


Abbildung: Wallet in der Bitcoin Software

Geld transferieren

	Echte Banken	Bitcoin
Geld aufbewahren	Konten	Wallets
Geld transferieren	**Überweisungen**	**Transactions**
Geld schöpfen	Drucken und Prägen	Mining
Geld wechseln	Tausch	Anbieter

Transaktionen

Beim Öffnen der Software bekommt man eine automatisch generierte Transaktionsadresse.
Beispiel: 13jUhd3nXaRhVgDoqnqh84tX237Fw7ooVm (und QR Code)

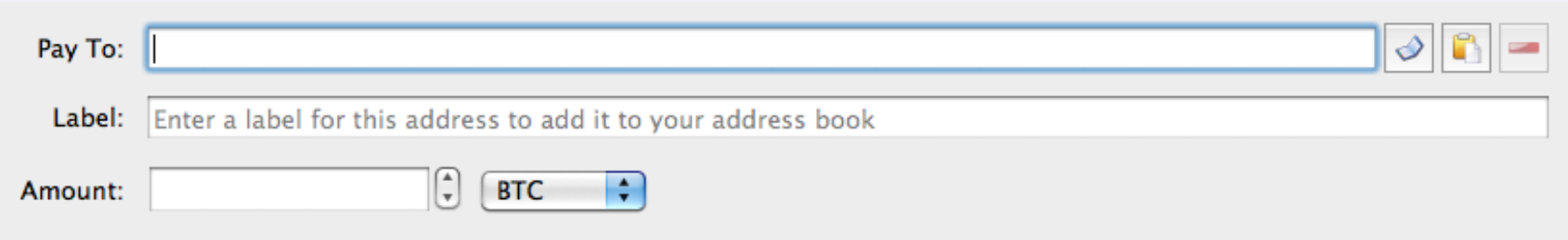


Abbildung: Transactions in der Bitcoin Software

Viele Adressen pro Wallet sind erstellbar. In Wirklichkeit werden ein **privater** und ein **öffentlicher** Schlüssel generiert.

	Echte Banken	Bitcoin
Geld aufbewahren	Konten	Wallets
Geld transferieren	Überweisungen	Transactions
Geld schöpfen	**Drucken und Prägen**	**Mining**
Geld wechseln	Tausch	Anbieter

Überweisungen und Blöcke

Transaktionen werden in Blöcken zusammengefasst.

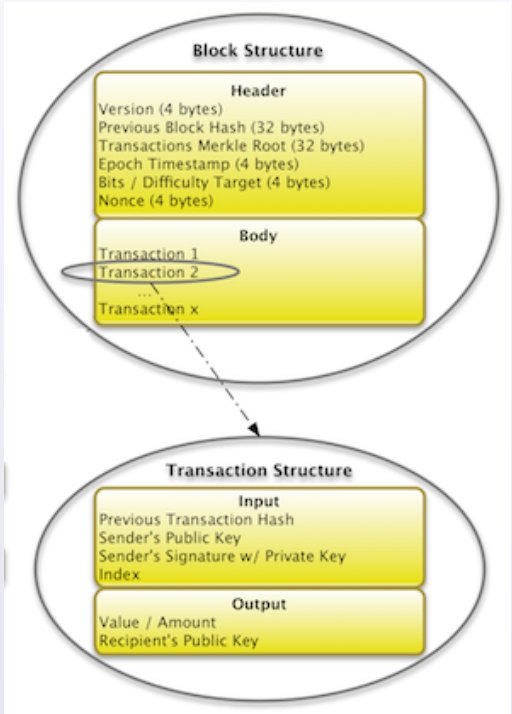


Abbildung: Ein Block mit Header und Body

Block Header

Die Informationen aus dem Header werden konkateniert und gehasht:
headerHex = (Version + Hash des vorherigen Blocks + Merkle Root der Transaktionen + Zeitstempel + Schwierigkeit + Nonce)
Doch diese Informationen ändern sich stetig...

Feld	Änderung
Version	Neuer Block, neue Version
Hash Block	Vorheriger Block
Merkle Root	Transaktion ist akzeptiert
Zeitstempel	Alle paar Sekunden
Schwierigkeit	Alle zwei Wochen ca.
Nonce	Inkrimentell bei einem Hashing

Blockhistory

Number[?]	Hash[?]	Time[?]	Transactions[?]	Total BTC[?]	Size (kB)[?]
215294	d5254101f9...	2013-01-05 17:11:33	154	2996.82755357	87.042
215293	57493d2c65...	2013-01-05 17:06:05	15	321.59409895	5.774
215292	265b6db6a1...	2013-01-05 17:05:46	94	172.21088976	44.118
215291	a9bdff8f8b...	2013-01-05 17:05:36	376	17090.60729009	172.687
215290	48012d3ad6...	2013-01-05 17:00:33	546	8978.3697827	298.041
215289	513687a4c9...	2013-01-05 16:44:00	101	6471.54552688	47.098
215288	d8d94c3274...	2013-01-05 16:39:02	410	12387.36203034	166.298

Abbildung: Blockexplorer mit kleiner History

Konkreter Block 215402

Block 215402[?]

Short link: http://blockexplorer.com/b/215402

Hash[?]: 000000000000057d4b1ca89b8f5f12b0ddd7f1106ea1b60d76c4709d9fb396d7

Previous block[?]: 000000000000029e3fb0134055d202205b4ca438de5715afcc48186bab28663

Time[?]: 2013-01-06 11:21:53

Difficulty[?]: 2 979 636.616938 ("Bits"[?]: 1a05a16b)

Transactions[?]: 115

Total BTC[?]: 1072.24714959

Size[?]: 48.942 kilobytes

Merkle root[?]: 59ca8785b4e0ac2e372283a4d669f5d71d624c7adaa4f37b44a64c3fa08eb3e7

Nonce[?]: 203235384

Abbildung: Block 215402 aus Block-URL

Wiederholung: Hashing

Bei Bitcoin wird die kryptographische Hash Funktion SHA-256 benutzt (keine Kollision!). Das sieht so aus:

Hello, world!0 => 1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64
Hello, world!1 => e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8
Hello, world!2 => ae37343a357a8297591625e7134cbea22f5928be8ca2a32aa475cf05fd4266b7
...
Hello, world!4248 => 6e110d98b388e77e9c6f042ac6b497cec46660deef75a55ebc7cfdf65cc0b965
Hello, world!4249 => c004190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6
Hello, world!4250 => 0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9

Bei Versuch 4251 wurden (durch Zufall) vier 0en am Anfang erzeugt!

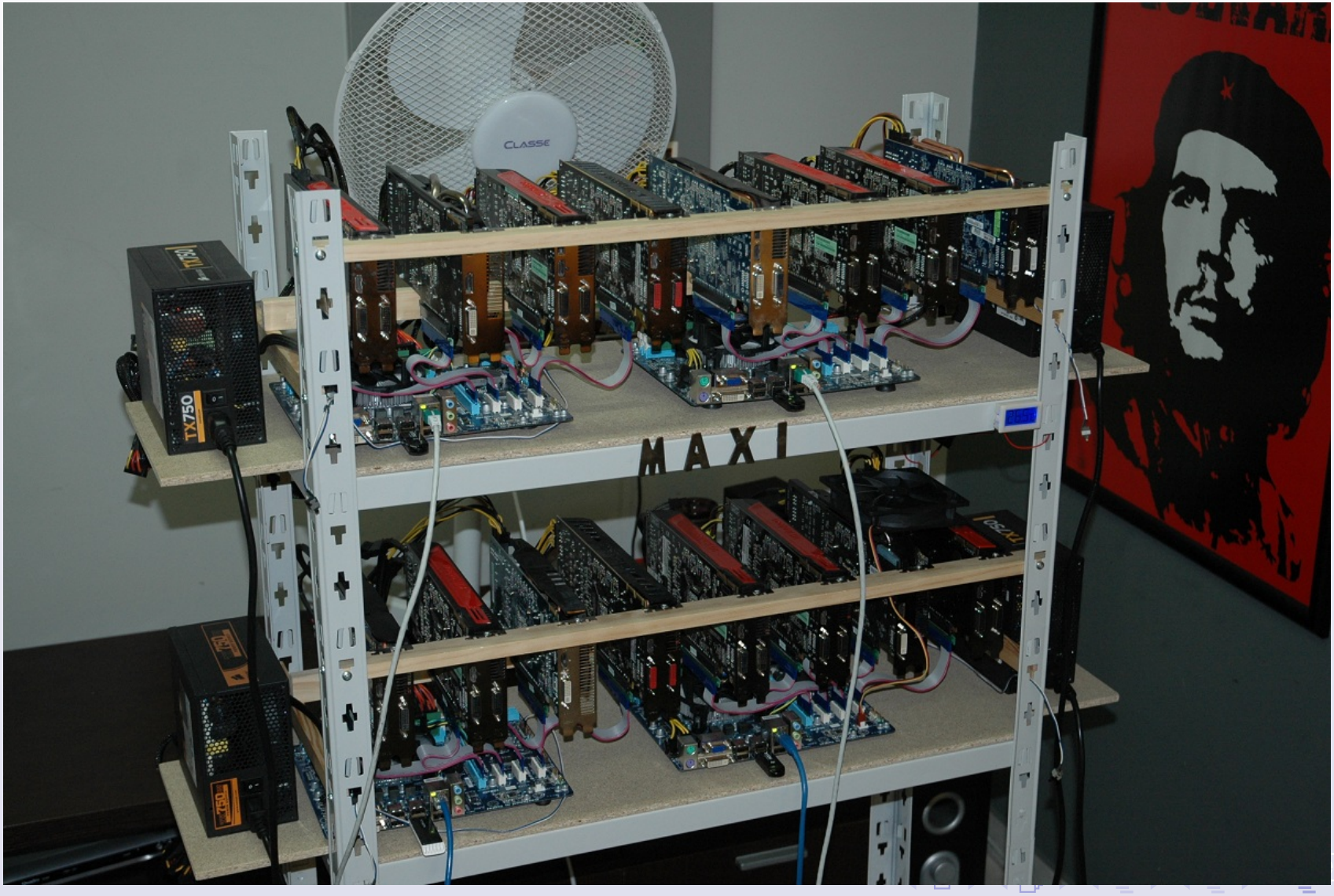
Wird der Hash des aktuellen (noch nicht bestätigtem Blocks) getroffen oder unterboten, so ruft er ins Netzwerk und alle Nodes bestätigen einen neuen Block (sofern er nicht schummelt...).

Probleme...

Derjenige der einen Block erzeugt hat, bekommt als Belohnung n-viele Bitcoins (siehe später). Aber man könnte doch schummeln, oder?

- Double-Spending (nein, weil Transaktionen *begraben* sind)
- Durch starke Hardware sich einen Vorteil erkaufen (Netzwerk adjustiert Schwierigkeit)
- Beim aktuellen Block eigene Wahrheit einpflegen (kann derjenige durch Hashing nur raten)

Mining Rig



Kurze Wiederholung Mining

Mining: Vereinfacht in fünf Schritten

- Transaktionen werden durchgeführt und vom Netzwerk bestätigt
- Transaktionen werden in Blöcken zusammengefasst
- Blöcke werden durch ihre Header-Informationen repräsentiert und gehasht
- Durch raten versuchen Mining-Nodes das Target (Ziel Hash) zu treffen oder zu unterbieten. Das Netzwerk bestätigt bei Richtigkeit diesen Block.
- Derjenige der das schafft, bekommt eine Belohnung in Form von Bitcoins

Geld wechseln

	Echte Banken	Bitcoin
Geld aufbewahren	Konten	Wallets
Geld transferieren	Überweisungen	Transactions
Geld schöpfen	Drucken und Prägen	Mining
Geld wechseln	**Tausch**	**Anbieter**

Tausch: Echtes Geld <-> Bitcoins

Diesen Service bietet das System von sich aus nicht, aber andere Dienstleister: Zum Beispiel Mt.Gox.

Symbol	Latest Price	30 days	Average	Volume	Low	High	Bid	Ask	24h Avg.	Volume
mtgoxUSD USD (dwolla/SEPA)	13.41151 1 min ago		13.42 -0.01 -0.04%	782,763.01 10,501,959.44 USD	12.74919 13.314 (24h)	13.90119 13.52999 (24h)	13.41151	13.45734	13.44 -0.03 -0.20%	19,947.80 268,054.32 USD
bitstampUSD USD (SEPA converted)	13.06 49 min ago		13.22 -0.16 -1.22%	78,087.20 1,032,377.34 USD	12.75 13.03 (24h)	13.94 13.15 (24h)	13.1	13.14	13.13 -0.07 -0.52%	1,084.30 14,235.35 USD
btceUSD USD (CC, LR)	13.095 3 min ago		13.15 -0.06 -0.45%	65,917.60 867,124.21 USD	12.63 13.086 (24h)	13.887 13.199 (24h)	13.095	13.1	13.13 -0.03 -0.23%	1,799.61 23,620.78 USD
mtgoxEUR EUR	10.2084 0 min ago		10.31 -0.11 -1.03%	64,431.71 664,593.23 EUR	9.84986 10.10142 (24h)	10.8 10.289 (24h)	10.2084	10.27	10.19 0.02 0.22%	1,333.74 13,585.99 EUR
virwoxSLL SLL (Second Life)	3556.4 2 min ago		3452.87 103.53 3.00%	52,356.00 180,778,701.50 SLL	3054 3367.8 (24h)	3675 3586 (24h)	3398.6	3555.5	3492.30 64.10 1.84%	1,974.00 6,893,807.10 SLL
btcdeEUR EUR	10.03 5 min ago		10.49 -0.46 -4.36%	42,451.16 445,172.74 EUR	5 10 (24h)	10000 11 (24h)	10.12	10.2	10.32 -0.29 -2.83%	858.70 8,863.25 EUR
mtgoxAUD AUD	13.09 33 min ago		13.08 0.01 0.06%	38,345.10 501,657.78 AUD	12.42001 12.7988 (24h)	13.45154 13.17645 (24h)	13.0186	13.11725	13.00 0.09 0.71%	300.47 3,905.21 AUD

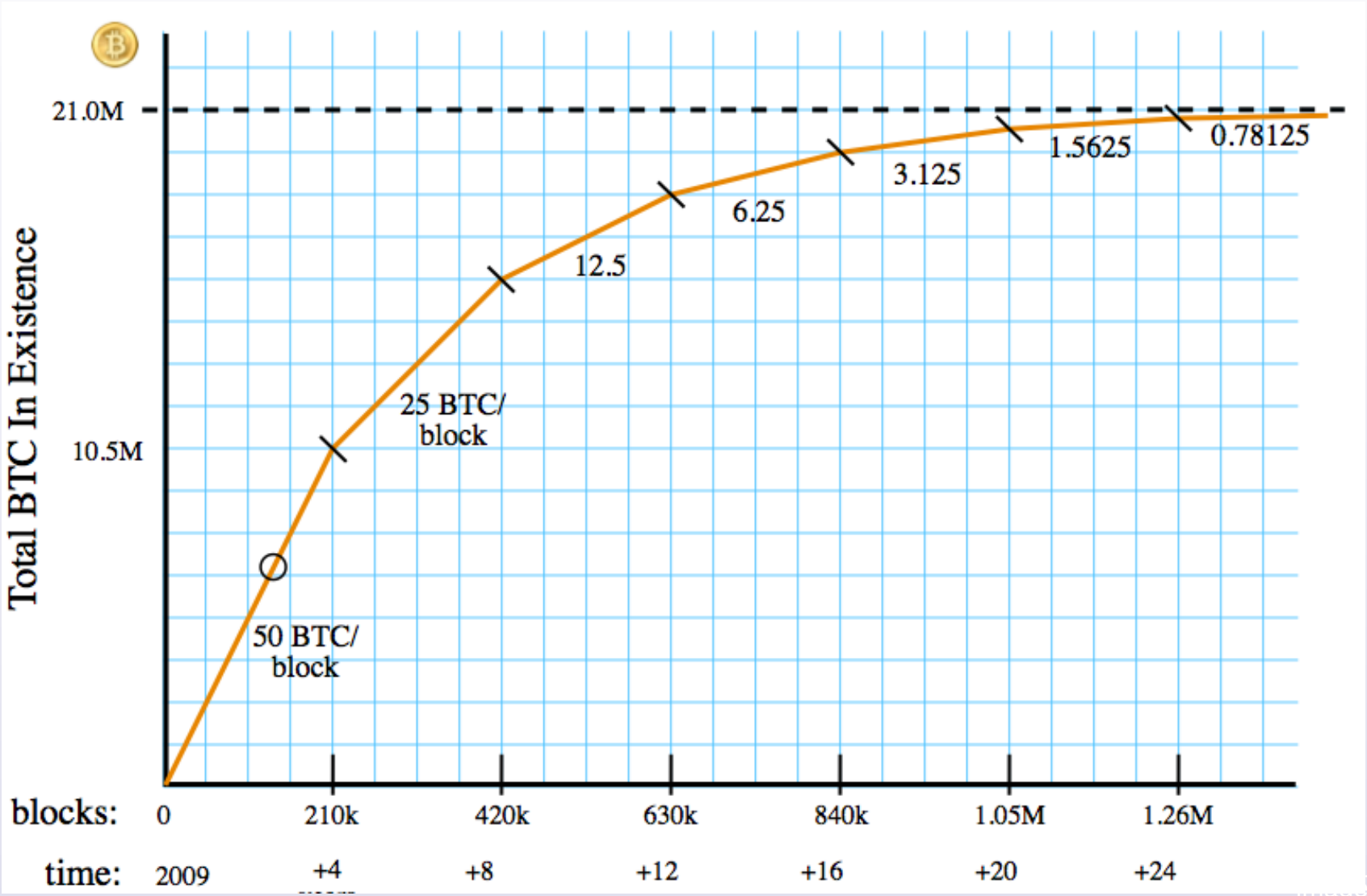
Abbildung: Verschiedene Märkte für echte Währungen und Bitcoins

Währungen: EUR, USD, CHF, DKK, JPY, GBP, LD, ...
Liste hier.

Eigenschaften von Bitcoins

- Dezentral (Keine dritte Person, keine Bank)
- Geld ist einfach zu verschicken und zu erhalten
- Sicher (siehe Mining)
- Fester Endwert an Bitcoins (21 Millionen)
- Öffentliches Kontobuch (jeder kennt alle Transaktionen)
- Man hat ein Pseudonym, aber ist nicht anonym

Bitcoins: Erzeugung und gesamter Pool



Statistiken; Stand 06. Januar 2013

- 10.635.575 BTC
- 109.227.355 Euro
- 1532.67 Transaktionen/Stunde
- 44.538,56 BTC/Stunde
- 6,08 Blöcke/Stunde (Schwierigkeit wird steigen...)
- 22,89 Terahash/Sekunde ($= 22,89 * 10^{12}$)

Handel

Hier eine riesige Liste von Tauschdiensten. Was kann ich für Bitcoins kaufen?

- Musik, Kunst, Software ...
- Bücher, Marmelade, Pizza, Socken aus Alpakka-Fell, ...
- Psychotherapien, Drogen, Waffen, Sex ...
- Spenden (WikiLeaks, ...)
- ...

Fazit

Bitcoins sind ein spannendes Thema, welches sich aus vielen Disziplinen bedient.
Schlau durchdachtes komplexes Thema, ohne wirklichen Urheber.
Wird sich das Projekt halten? Das entscheidet die Community.
Wird es das letzte Wort zum Thema digitale Währung sein? Sicherlich nicht!

Quellen

- Bitcoin Wiki
- Einfaches Schema als Bild
- SHA-2 Hashing
- Bitcoin Charts
- Block Explorer
- Wire - The Rise and Fall of Bitcoin

Und zum Schluss!

Danke ...

... für Eure Aufmerksamkeit!

Aber ...

... gibt es noch Fragen?