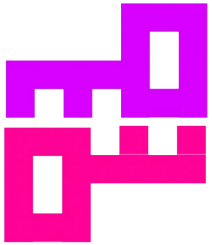


Am Golde hängt's,
zum Golde drängt's doch alle

Coin oder Bitcoin, das ist hier die Frage

V 0.2 150216 Bonn
Jochim Selzer
Jselzer@vorratsdatenspeicherung.de
https://cryptoparty.in/cryptopartykbn
a57a 4e28 a59d 0385 d33d 6301 763d ce1b 65f4 c445

Was soll Geld leisten?

- limitiert, schwer zu vervielfältigen, kann nur einmal ausgegeben werden (double-spend)
- transportabel
- aufteilbar
- dauerhaft haltbar
- vertrauenswürdig

Was hätten wir gern?

- Anonymität

Was ist Bitcoin?

- Digitale Währung
- Dezentral, Peer-to-Peer
- Für alle transparent, Community-kontrolliert

Was ist Bitcoin nicht?

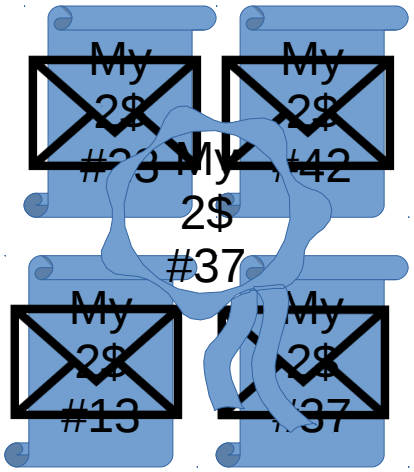
- anonym
- durch Goldreserververen o.ä. gedeckt
- Bits, die zwischen Konten verschoben werden
- Bits, die man durch „Mining“ ausgräbt

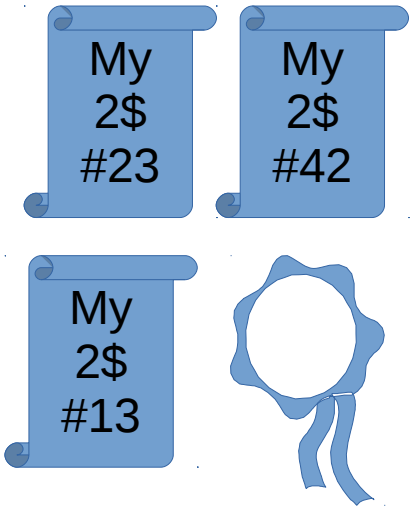
Was ist Bitcoin denn nun?

- ein Logbuch
- von allen geführt (zumindest theoretisch)
- von allen überprüfbar
- enthält alle Transaktionen seit Beginn des Bitcoin-Projekts

Geldscheine selber drucken (Blinding, E-Cash von Digicash)

Bank

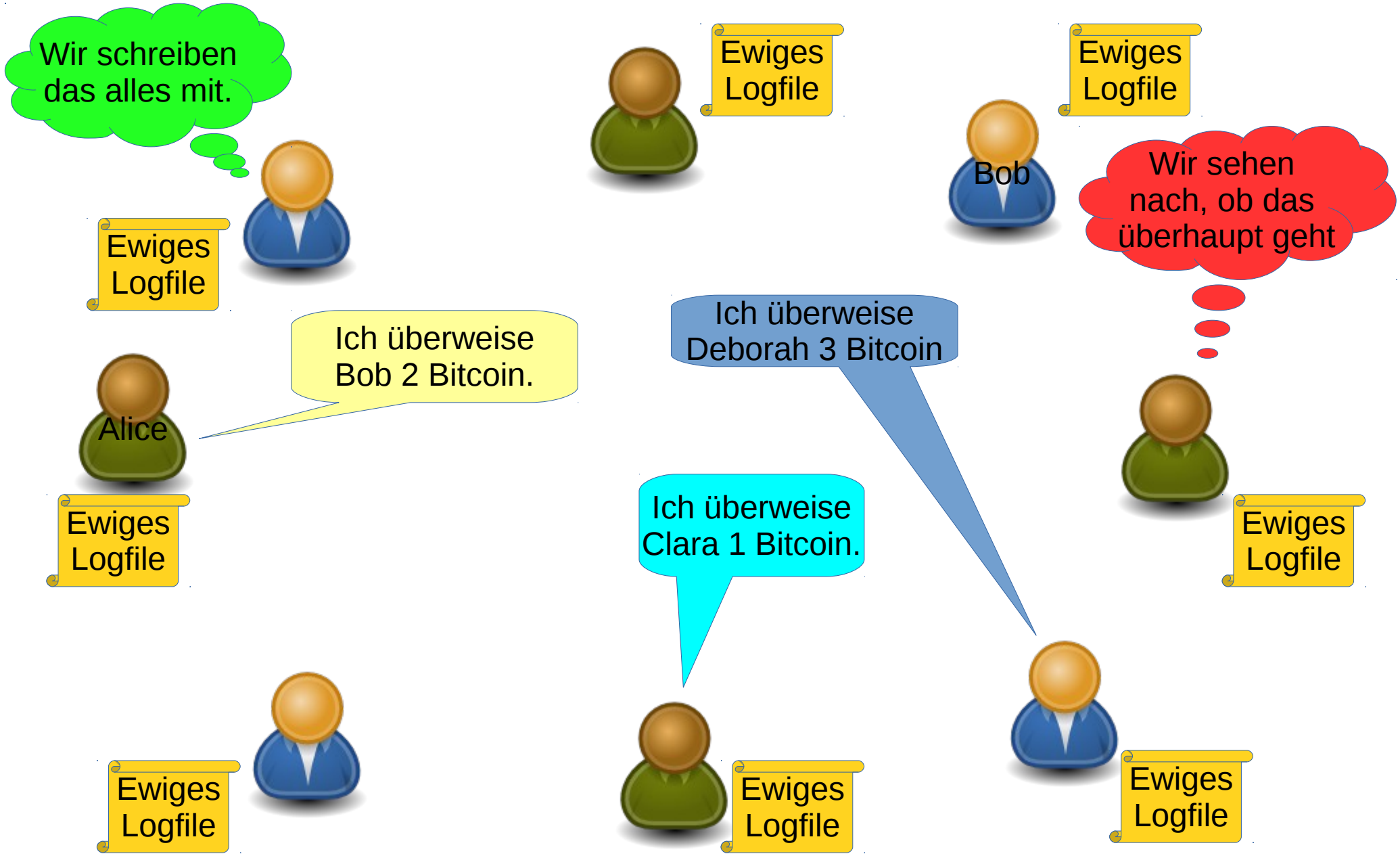




Secret Splitting

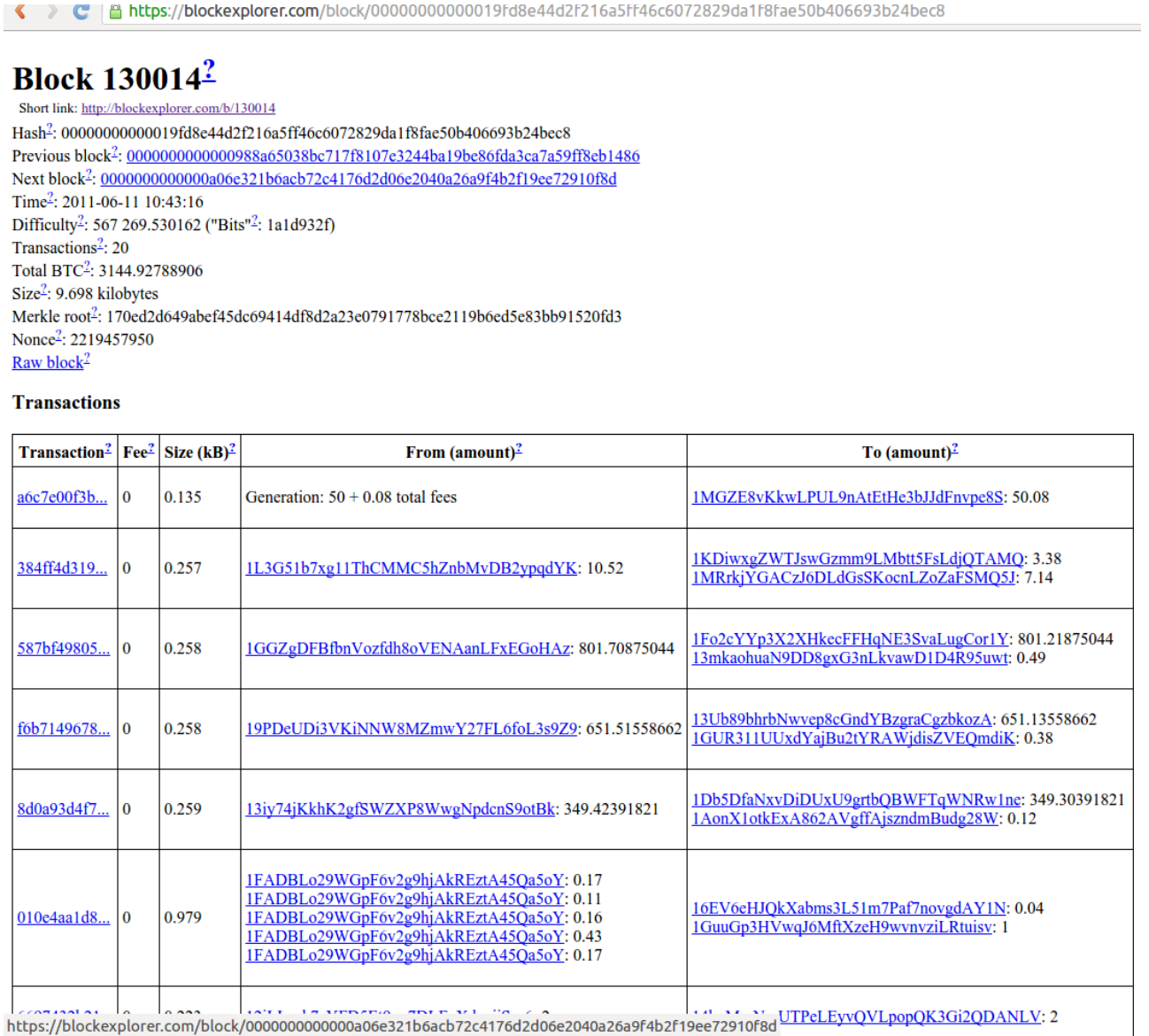
- Alice spaltet ihren Namen hundert mal auf zwei Umschläge auf.
- Bob entscheidet bei den hundert Paaren, welchen Umschlag er haben will
- Das Gleiche passiert mit Claude
- Wenn Bob oder Claude einen Betrug feststellen, schließen sich zusammen und finden Alices Identität heraus.

Peer-to-Peer-Geld



Block

https://blockexplorer.com/block/00000000000019fd8e44d2f216a5ff46c6072829da1f8fae50b406693b24bec8



https://blockexplorer.com/block/00000000000019fd8e44d2f216a5ff46c6072829da1f8fae50b406693b24bec8

Block 130014

Short link: http://blockexplorer.com/b/130014

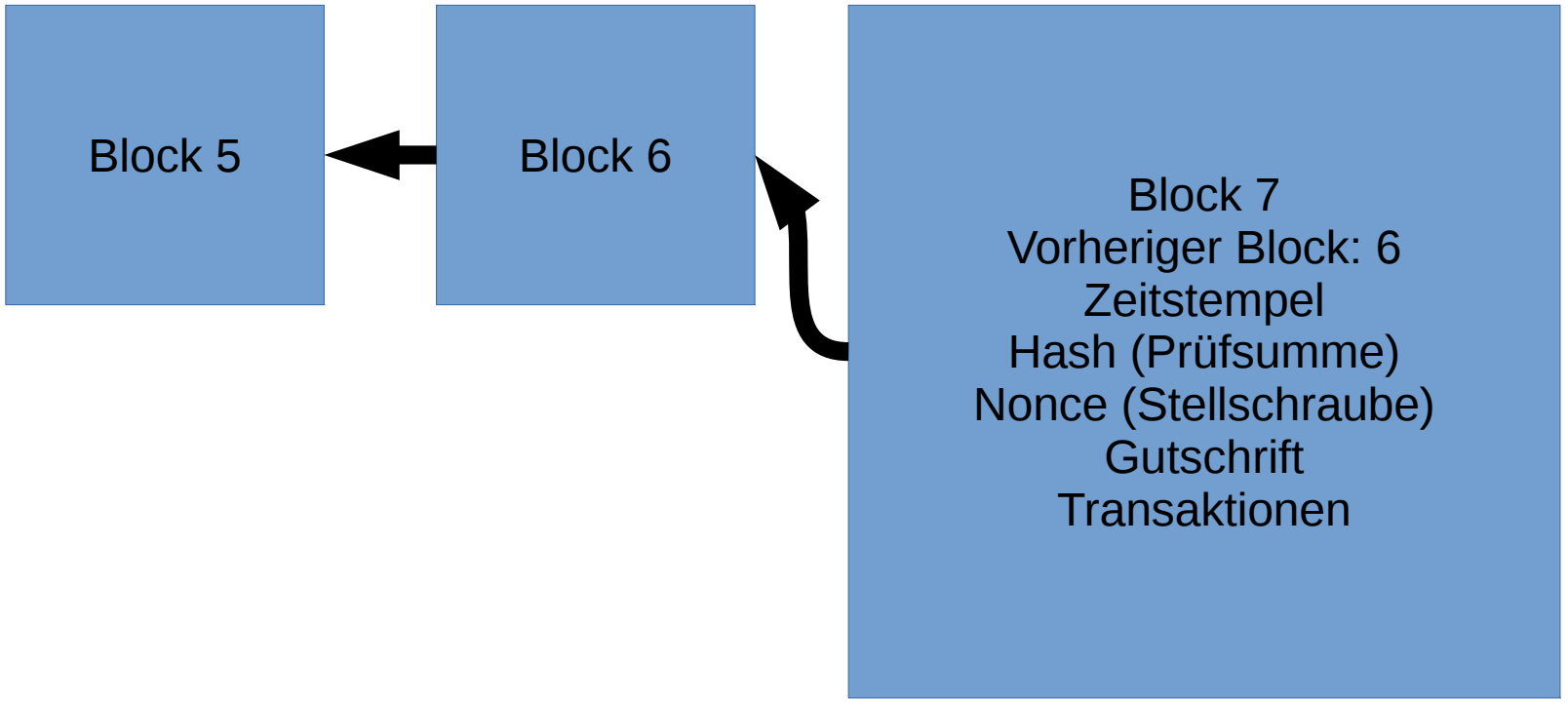
Hash: 00000000000019fd8e44d2f216a5ff46c6072829da1f8fae50b406693b24bec8
Previous block: 000000000000000988a65038bc717f8107e3244ba19be86fda3ca7a59ff8eb1486
Next block: 0000000000000a06e321b6acb72c4176d2d06e2040a26a9f4b2f19ee72910f8d
Time: 2011-06-11 10:43:16
Difficulty: 567 269.530162 ("Bits": 1a1d932f)
Transactions: 20
Total BTC: 3144.92788906
Size: 9.698 kilobytes
Merkle root: 170ed2d649abef45dc69414df8d2a23e0791778bce2119b6ed5e83bb91520fd3
Nonce: 2219457950
Raw block

Transactions

Transaction	Fee	Size (kB)	From (amount)	To (amount)
a6c7e00f3b...	0	0.135	Generation: 50 + 0.08 total fees	1MGZE8vKkwLPUL9nAtEtHe3bJJdFnvpe8S: 50.08
384ff4d319...	0	0.257	1L3G51b7xg11ThCMMC5hZnbMvDB2ypqdYK: 10.52	1KDiwxgZWTJswGzmm9LMbtt5FsLdjQTAMQ: 3.38 1MRrkjYGACzJ6DLdGsSKocnLZoZaFSMQ5J: 7.14
587bf49805...	0	0.258	1GGZgDFBfbnVozfdh8oVENAanLFxEGoHAz: 801.70875044	1Fo2cYYp3X2XHkecFFHqNE3SvaLugCor1Y: 801.21875044 13mkaohuaN9DD8gxG3nLkvawD1D4R95uwt: 0.49
f6b7149678...	0	0.258	19PDeUDi3VKiNNW8MZmwY27FL6foL3s9Z9: 651.51558662	13Ub89bhrbNwvep8cGndYBzgraCgzbkozA: 651.13558662 1GUR311UUxdYajBu2tYRAWjdisZVEQmdiK: 0.38
8d0a93d4f7...	0	0.259	13iy74jKkhK2gfSWZXP8WwgNpdcnS9otBk: 349.42391821	1Db5DfaNxvDiDUxU9grtbQBWFTqWNRw1ne: 349.30391821 1AonX1otkExA862AVgffAjszndmBudg28W: 0.12
010e4aa1d8...	0	0.979	1FADBLo29WGpF6v2g9hjAkREztA45Qa5oY: 0.17 1FADBLo29WGpF6v2g9hjAkREztA45Qa5oY: 0.11 1FADBLo29WGpF6v2g9hjAkREztA45Qa5oY: 0.16 1FADBLo29WGpF6v2g9hjAkREztA45Qa5oY: 0.43 1FADBLo29WGpF6v2g9hjAkREztA45Qa5oY: 0.17	16EV6eHJQkXabms3L51m7Paf7novgdAY1N: 0.04 1GuuGp3HVwqJ6MftXzeH9wvnvziLRtuisv: 1
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]UTPeLEyvQVLpopQK3Gi2QDANLV: 2

https://blockexplorer.com/block/0000000000000a06e321b6acb72c4176d2d06e2040a26a9f4b2f19ee72910f8d

Blockchain


Block 5
Block 6
Block 7
Vorheriger Block: 6
Zeitstempel
Hash (Prüfsumme)
Nonce (Stellschraube)
Gutschrift
Transaktionen

Was zeichnet einen Hash aus?

- Prüfsumme
- Nicht umkehrbar
- Sehr ähnliche Eingaben erzeugen möglichst unterschiedliche Ausgaben.
- aufwändig zu berechnen.
- kollisionsarm

Nonce

1$ from Alice to Bob
2$ from Mike to Clara
1.5$ from Dorothy to Peter
0.75$ from Shaun to Martin

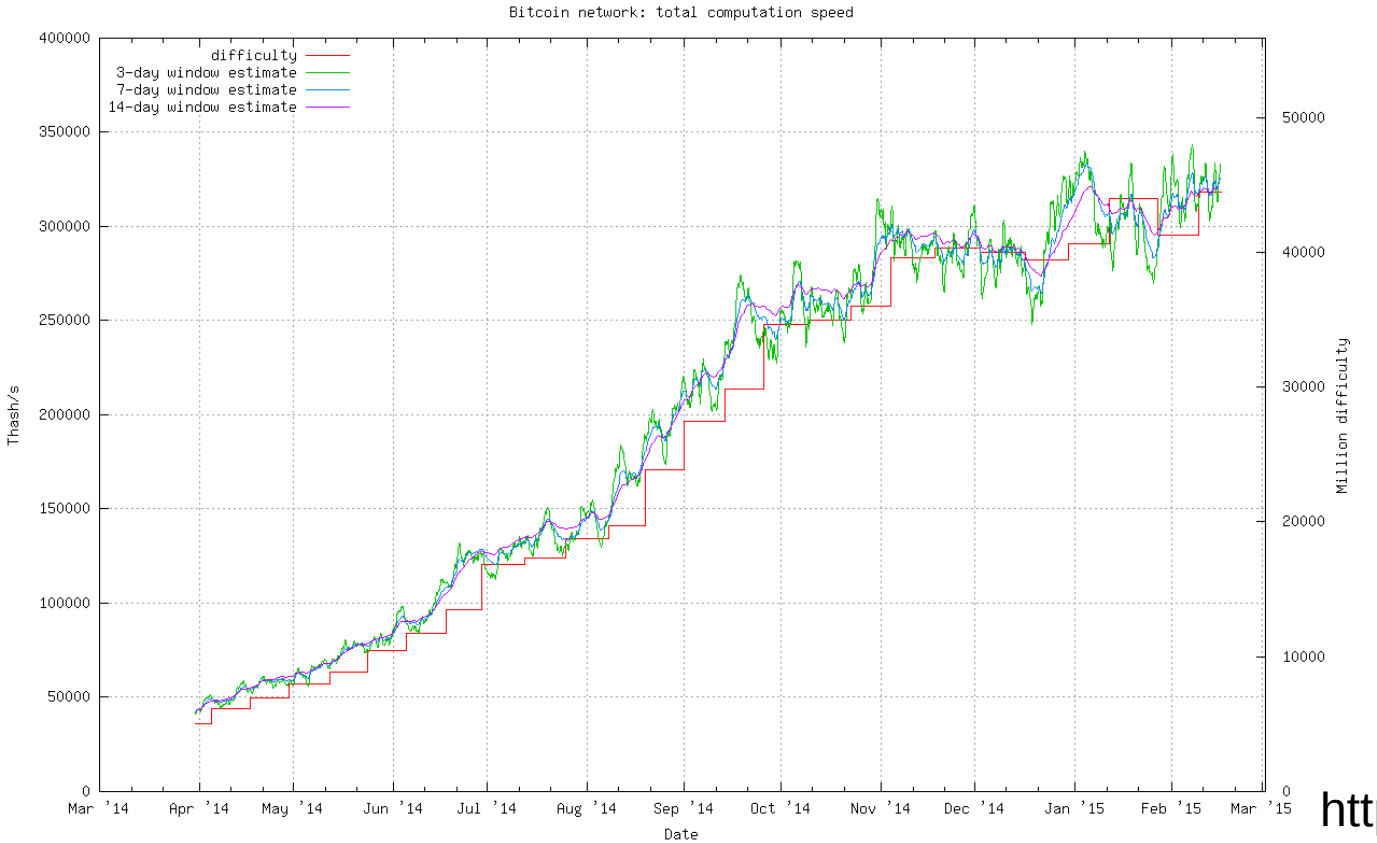
0

SHA
256

```
74e84500c2589b393fea828edd65021ce8faf452bf6161a4ba35cc06e0b33604
8584a13542dfcac24d1696f66a6ab6be50e26c568dc6e58ad04624fdc95db1d9
b95809ff9ef1dead9d5952a4a7fbe4aeb4615948f74af0a91fb918ffc9200e44
3: beb319f9688c9c087e6a3d57186cc2a31cc5a9208263a705f524da408ef87b8c
4: 526d86b5bdc2e698559fa5afefc7a44ffe3d45fcec04bf02225fb0622c463ff6
5: f69229736d7ffe25927047c5e5e6369a8fc56872fc40ffbdc4c1ed046a348d72
6: 476e3f4444ff900975d2ce5f2d6797e7b36918a7d259d2e1f4f7475f92545739
7: faa77ce2b17e5b585bba0bbf3687a2e7cdf543233a11fcb4b55573b11607c130
8: 24e796a0143ffa05b9f6e9f9ebe5dceb94940f378a13e4922f9e35efa57fc0da
1ad1e9cce38d5ea81528a074f493d85518e56acacc0343a3d0398a4cb5817308
```

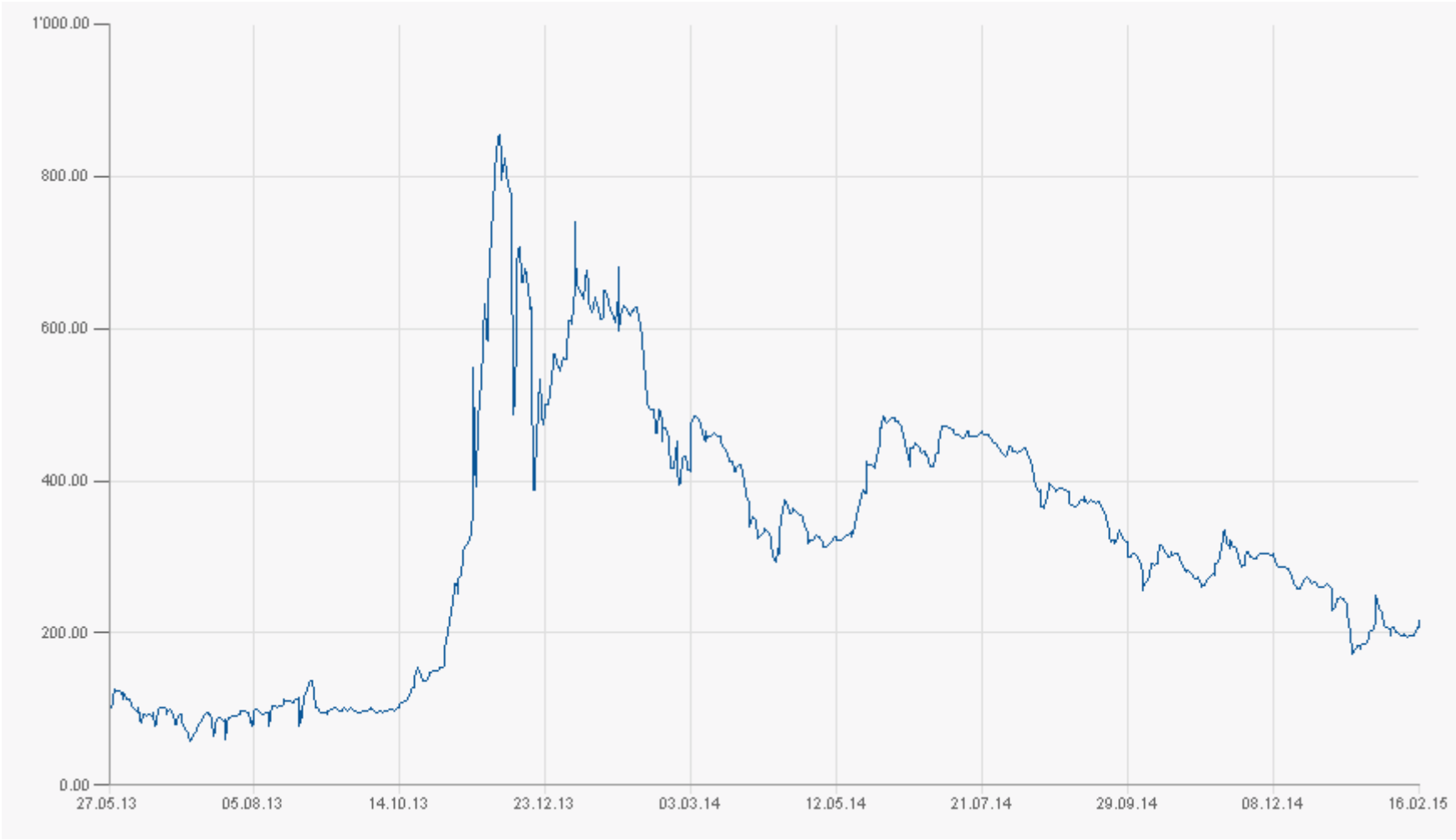
Berechnungen

- Alle 10 Minuten wird ein Block fertig (Stichwort Lottospiel)
- Wenn nicht, wird am Schwierigkeitsgrad ged



http://bitcoin.sipa.be/

Wechselkurs BTC/EUR



http://www.finanzen.net/devisen/bitcoin-euro/chart

Wechselkurs BTC/USD

http://www.ariva.de/btc-usd-bitcoin-us-dollar-kurs/chart?layout=klassisch&t=all&size=XL&volume=1&boerse_id=167

Was passiert, wenn...

- jemand einen umgearbeiteten Client einsetzt, der z.B. mehr Bitcoins insgesamt zulässt?
  - Es bildet sich ein neuer Bitcoin-Zweig, von dem man nur unter Totalverlust auf den alten Zweig zurückkommt.
- jemand Geld zweimal ausgibt?
  - Es bilden sich zwei Zweige der Blockchain, aber nur einer wird von der Mehrheit weiterentwickelt.

Weitere Anwendungen

- Dokumentation eines erzeugten Dokuments

Links

- Vortrag auf der FrOSCon
- Joerg Platzer: Bitcoin kurz & gut, O'Reilly
- CRE 182