Clemens H. Cap
Universität Rostock
clemens .cap (at) uni-rostock (dot) de

BITCOIN
DAS DIGITALE OPEN-SOURCE GELD DES INTERNET-ZEITALTERS

Clemens Cap about electronic bitcoin wallet at EuroBit

bitgroups | Subscribe | 13 videos

HMD
Praxis der Wirtschaftsinformatik
ISSN 1436-3011

HMD 283, 49. Jahrgang, Februar 2012

Open Source - Konzepte, Risiken, Trends

Herausgeber: Susanne Strahringer

Bitcoin - das Open-Source-Geld

Clemens H. Cap

Product: Print | Save

Bitcoin – Digital Open Source Money of the Internet Age

Product

It is astonishing that in the Internet age we still settle our bills with physical objects (bills or coins), But also account-based money has its problems, since the user must trust the bank and its governance....
Read more

Exhibitor

Uni Rostock

Universitätsplatz 1
18055 Rostock
Germany

Phone: +49 381 498 0
Fax: +49 381 498 1216

Exhibition stand

Hall 26, Stand A34

Topic: Mecklenburg-Vorpommern Pavilion

Erstes akademisches Workshop & Tutorial

GMDS 2012 / INFORMATIK 2012 · 16. bis 21. SEPTEMBER 2012

57. Jahrestagung der Deutschen Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V. (GM
42. Jahrestagung der Gesellschaft für Informatik e.V. (GI)

Informatik 2012 > Workshop "Bitcoin"

.: Workshop & Tutorial Bitcoin :.

Call for Papers

The English version of the call for papers can be found here.

Halbägiges Tutorial und **halbtägiger Workshop** an der Jahrestagung der **Gesellschaft für Informatik** (GI), 20. September 2012, Braunschweig

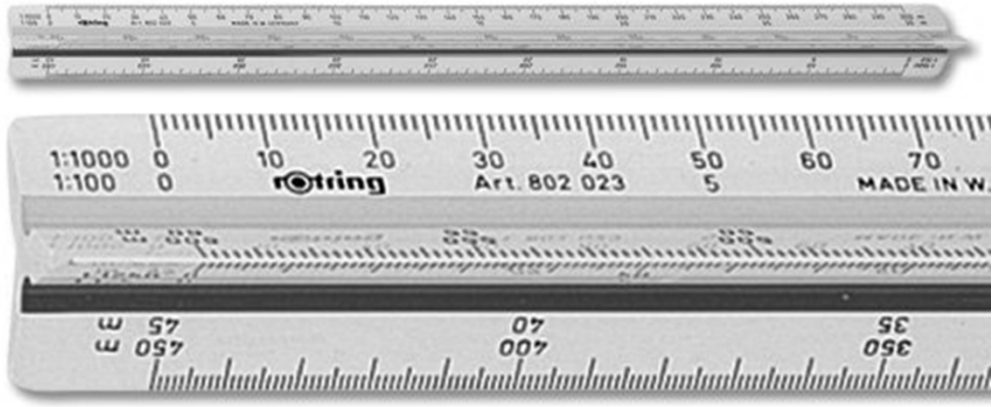
Verlängerte Deadline zur Einreichung: 30.04.2012

Koordinator: Clemens Cap (Universität Rostock), clemens.cap@uni-rostock.de

WAS IST GELD ÜBERHAUPT?

WAS IST GELD ÜBERHAUPT?

1. Wertmaßstab



Problem:

- **Wie viel ist eine Stunde "Vorlesung Cap" wert?**
- **"Tausche 60 Minuten Vortrag gegen X Minuten Zahnarzt"**

Verbleibende Problemquellen:

- **Gibt es den objektiven Wertmaßstab?**
- **Wie entsteht er?**
- **Wie wird stabiles Vertrauen darin etabliert?**

2. Tauschmittel

Problem

- Lehrer bietet Unterricht und will ein Steak
- Schüler will Unterricht, hat aber nur eine ganze Kuh

2. Tauschmittel

Lösung

- Geld vereinfacht mehrfache Tauschketten
- Geld ermöglicht die Aufteilung der Kuh in kleine Teile

Geeignete Tauschmittel

Lösung

- Geld vereinfacht mehrfache Tauschketten
- Geld ermöglicht die Aufteilung der Kuh in kleine Teile

Ungeeignete Tauschmittel

Ungeeignete Tauschmittel

Ungeeignetes Tauschmittel
Gibt es diesen Schein wirklich ???

Ungeeignete Tauschmittel


Provinz Berlin
50
Millionen
Mk.
1923


GUTSCHEIN
DEUTSCHE REICHSBAHN
FÜNF
BILLIONEN
MARK
Die Scheine werden von sämtlichen Reichsbahnkassen des Direktionsbezirks in Zahlung genommen und nach Bekanntgabe durch die Karlsruher Zeitung und durch Anschlag auf den Bahnhöfen zum vollen Nennwert eingelöst
Karlsruhe, den 15. November 1923
Reichsbahndirektion
Lit. C
№ 06692

Problemquellen

Wodurch entsteht die (möglichst universelle Akzeptanz)?

Bedrohungen:

- Wert-Verlust, Inflation (Bsp: 5 Billionen Mark)
- System-Crash (Bsp: Lehman Brothers)
- Denial of service (Bsp: Wikileaks)


LEHMAN
BROTHERS
LACOSTE
LACOSTE
ESCADA


LEHMAN
BROTHERS


Price $/Share
100
90
80
70
60
50
40
30
20
10
0
2005
2006
2007
2008
Lehman Brothers
2005 - 2008

Kreditkartenfirmen

Ku-Klux-Klan ja, Wikileaks nein

(Headline der Süddeutschen Zeitung)

3. Wertaufbewahung

Aufgeschoebener Tausch

- Tausch jetzt – Rücktausch später
- Heute Unterricht
- Morgen Opernbesuch
- In 20 Jahren in die Rente.

NOCHMAL:
WAS IST GELD ABSTRAKT?

Was ist Geld?
Digital (1)

Ein **Recht** zur Ausführung einer bestimmten Transaktion

das von seinem **Träger**

genau einmal ausgeübt werden kann

und **nur durch** die Ausübung auf **andere übergeht**

"Träger"

▪ An **Name** gebunden	Konto ad personam
▪ An **Kenntnis** gebunden	Nummernkonto, PIN, TAN
▪ An ein **Pseudonym**	Public – private Key Paar
▪ An den Besitz eines **Objekts**	Münze, Goldbarren, Juxten Bon
▪ An den **Körper**	Biometrie, Fingerabdruck

Was ist Geld?
Digital (2)

Ein **Recht** zur Ausführung einer Transaktion

das von seinem **Träger**

genau einmal ausgeübt werden kann

und **nur durch** die Ausübung auf **andere übergeht**

"Genau einmal … von seinem Träger"

- **Anti-Bsp:** Perfekte digitale Kopie einer digitalen Münze
- Kein **Double Spending**
- **Weitergabe** möglich (Übergang des Rechts)
- **Backup** möglich
  - sinnvoller Vorteil von digitalem Geld

Was ist Geld?
Digital (3)

Ein **Recht** zur Ausführung einer Transaktion

das von seinem **Träger**

genau einmal ausgeübt werden kann

und **nur durch** die Ausübung auf **andere übergeht**

"Nur durch"

- **Anti-Bsp:** Geld selber fertigen
- Kein Erzeugen von Geld-Einheiten ohne

Gegenleistung in Zeit, Energie, Gold	**Wert-Deckung**
Gesellschaftlich /rechtliche Befugnis	**Regelungs-Deckung**
Gesellschaftliche Akzeptanz	**De Facto Deckung**

Was ist Geld?
Digital (4)

Ein **Recht** zur Ausführung einer Transaktion

das von seinem **Träger**

genau einmal ausgeübt werden kann

und **nur durch** die Ausübung auf **andere übergeht**

"auf andere übergeht"

- Einer verliert, einer bekommt das Recht
- Übertragung kann **mit Zwischen-Instanz** geschehen

  Bsp: Bank mit Buchgeld und Konto
- Übertragung kann **ohne Zwischen-Instanz (Peer-2-Peer)** geschehen

  Bsp: Bargeld, Edelmetalle

Woher kommt im Geld der "Wert"

Langandauernden Konvertierbarkeit in Waren & Dienstleistungen

Unmittelbare Konvertierbarkeit

- Energieträger: Universelle physikalische Eigenschaft
- Nahrungsmittel: Universelle Nachfrage

Akzeptanz & Nachfrage Was nimmt der Tauschpartner?

- Brot, Wasser, Gold, Waffen, …

Konvention und Gesetz Was muß der Tauschpartner nehmen?

- Weil es das Gesetz vorschreibt: Recht in € / $ zu zahlen
- Deckung: $ als Ersatz für Gold

WAS IST BITCOIN?

The first five times you think you understand it

You don't

(Dan Kaminsky)

Bitcoin (1)

Träger des Geldes

- Bindung an ein Pseudonym ("Bitcoin Adresse")
- Nachweis der Befugnis durch (Public, Private) Key Paar mit ECC
- Bitcoin Adresse ist hash des public key
- Private Key verlieren = Geld verlieren

Identität generieren

- Ohne Bank, Personalausweis, Zentralinstanz
- Freies Generieren eines (Public, Private) Key Paars
- Kollision theoretisch möglich, praktisch nicht – 256 bit randomness

Bitcoin (2)

Übertragen

- Völlig Peer-to-Peer, ohne irgendeine Zentralinstanz
- Jeder Teilnehmer betreibt einen Bitcoin Knoten
- Jeder Knoten speichert Konto-Stände zu allen Adressen
- Transaktionen werden an alle Knoten gesandt
- Berechtigung wird durch Signatur überprüft
- Neue Konto-Stände werden an alle Knoten gesandt

Großes offenes Problem: Inkonsistente Konto-Stände

- Gelöst durch probabilistischen Blockketten-Algorithmus

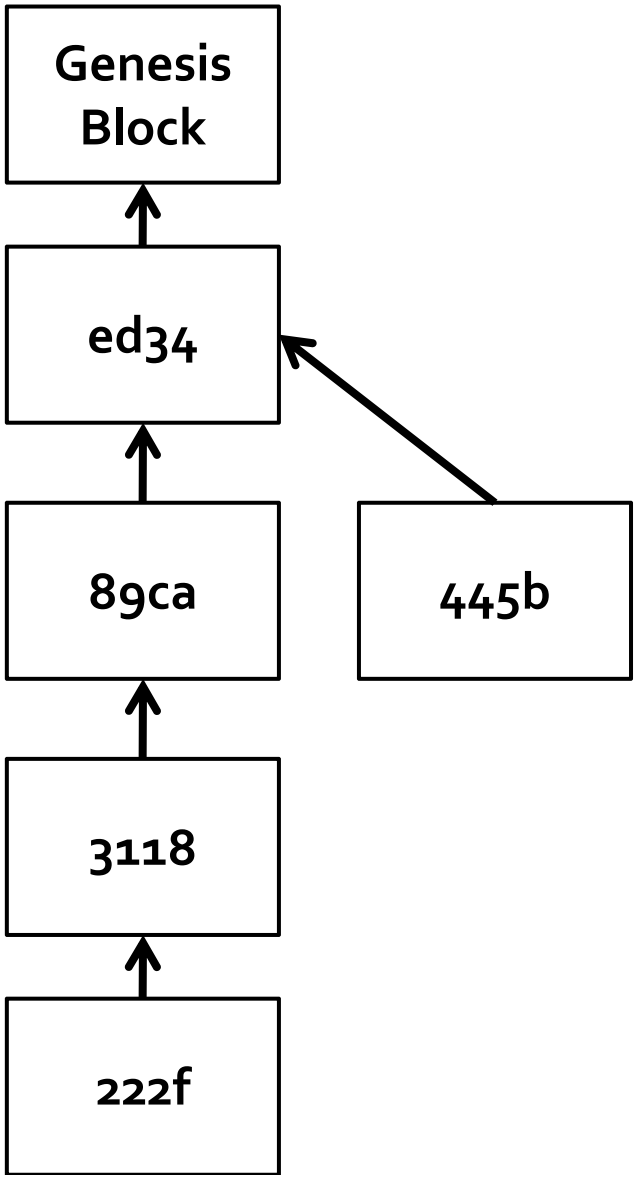
Bitcoin (3)

Wichtigster Aspekt von Bitcoin

Unabhängig vom Hype der Bitcoin Idee

- Hochreplizierte Datenbank
- Wird nach gewisser Zeit global konsistent
- Probabilistischer Konsistenz-Begriff

Blockketten-Algorithmus (1)



Jeder Block

- versiegelt via Hash Funktion eine Welt-Sicht (dh. Kontostände)
- wird durch seinen Hash-Wert addressiert
- verweist via Hash-Wert auf gen. einen Vorgänger

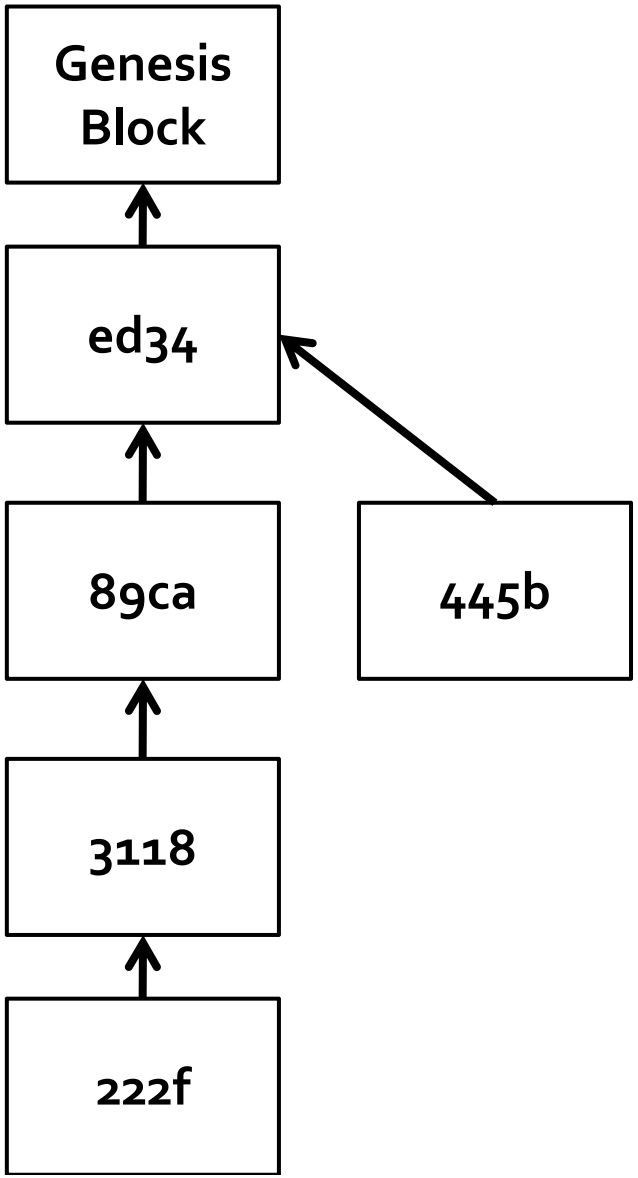
Es gibt einen öff. bek. Genesis-Block als Wurzel

Daraus entsteht ein Baum mit mehreren Ästen

Jeder Teilnehmer kann erhaltene Astinformation

- autonom **ohne Zentralinstanz prüfen** und
- wenn korrekt, in seinen **Baum einbauen**

Blockketten-Algorithmus (2)



Unklar bleibt aber im Fall einer Verzweigung **welche Weltsicht** die richtige ist.

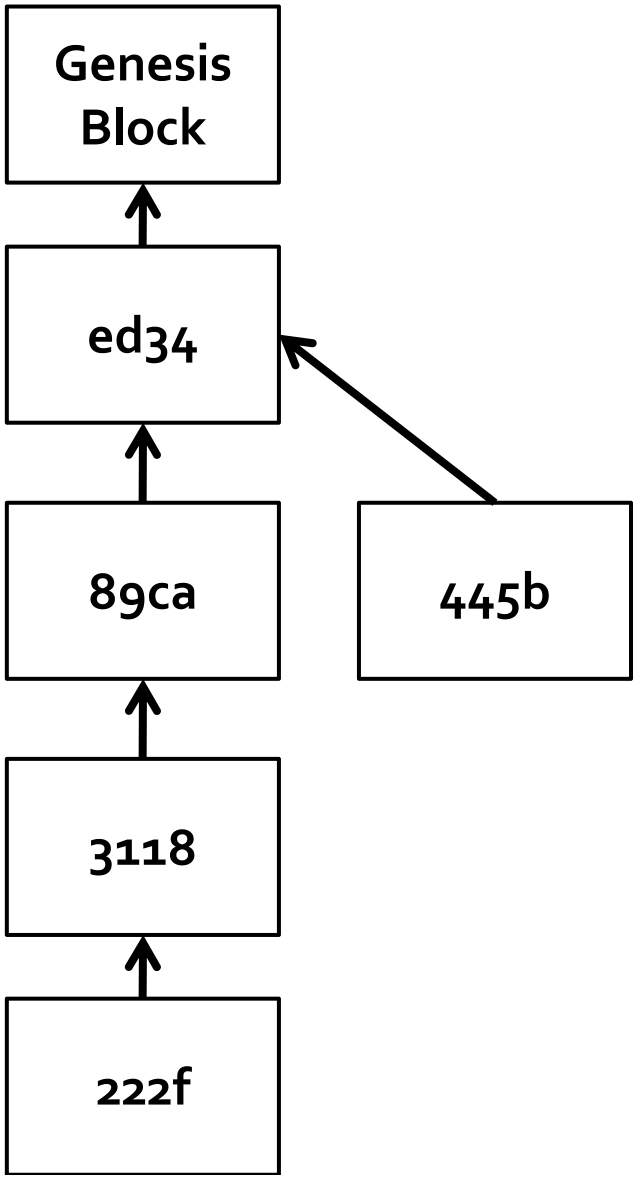
Jeder neue Block muss an frühere ankoppeln und ein Proof of Work enthalten.

hash (block, Zufallszahl) = 00…00 xx xx xx xx

Rate Zufallszahl so, dass hash mit großer Anzahl 0 beginnt – das kostet Rechenzeit.
Je mehr 0en – umso schwieriger.

Wer einen neuen Block findet & verteilt – bekommt 50 BTC (25 BTC, …)

Blockketten-Algorithmus (3)



Als richtig gelten Blöcke mit längstem Pfad.

Genauer: Block mit der meisten Rate-Arbeit

Transaktionen werden per Broadcast versandt

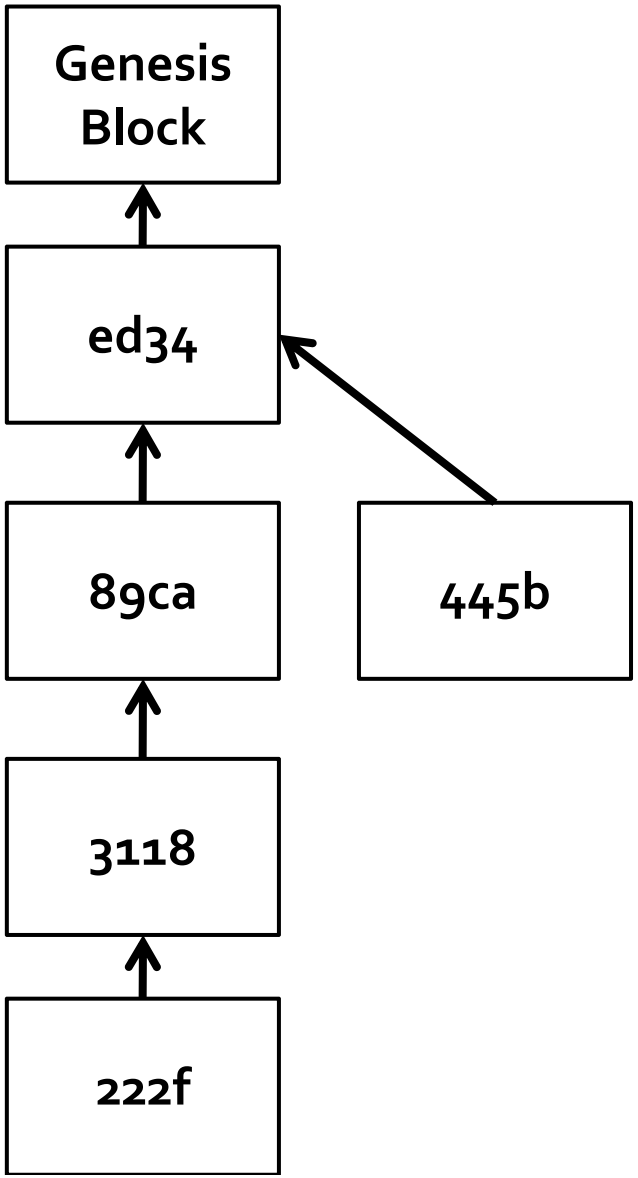
Einige Knoten wollen betrügen

Daher kann es Probleme geben

Wir betrachten hier nur ein Beispiel

Stellvertretend für andere

Blockketten-Algorithmus (4)



Alice sendet ihr ganzes Geld an Bob und an Carol

Und informiert verschiedene Knoten verschieden.

Fazit:

- Manche buchen bei Bob gut.
- Andere buchen bei Carol gut.
- Bob-Blöcke und Carol-Blöcke im Wettstreit
- In der Theorie des Random Walk wird gezeigt
- Wenn eine Mehrheit von Knoten immer den längsten Pfad mit Blöcken verlängern

  und wir lange genug warten
- Dann wird sich eine Weltsicht durchsetzen

  und das ist die korrekte Systemantwort

Bitcoin (3)

Deckung

Durch den Rechenaufwand zum Erraten / Lösen der Proof-of-Work

Bitcoins generieren

- Im Mittel alle 10 Minuten 50 neue BTC für jeden Block
- Parameter 50 wird immer wieder mal reduziert so,
  dass maximale Menge Bitcoins nach oben limitiert ist

Die Antwort auf die Kernfrage

Q: Warum nehme ich 10 BTC ALS Lohn von Alice an?

A: Weil ich weiß, dass bei Bob dafür Brot kaufen kann.

Q: Woher weiß ich, dass ich bei Bob dafür Brot kaufen kann?

A: Weil Bob im System mitmacht und es für ihn am meisten bringt, nach den gültigen Bitcoin Regeln zu handeln.

Q: Warum bringt es für Bob am meisten Vorteile, nach den Regeln zu handeln?

A: Weil es die Mehrheit auch so tut.

Q: Warum tut es die Mehrheit auch so?

A: Weil auch für die Mehrheit die Situation von Bob gültig ist

The first five times you think you understand it

You don't

(Dan Kaminsky)

Hilfreich ist die Diskussion über mögliche Angriffe.

Daher jetzt erst einmal Schluß mit Erklärungen

Und ggf. Zeit für die Diskussion.

Die Mehrheit in Bitcoin

Wird durch die Rechenkapazität zum Lösen der Proof-of-Work bestimmt.

Also demokratisch.

Jedenfalls nicht durch eine Bank oder Institution.

Was ist Bitcoin?

"Das gefährlichste Open Source Projekt aller Zeiten"

(Jason Calacanis)

Nach Open Source Software, Hardware, Büchern, Filmen…

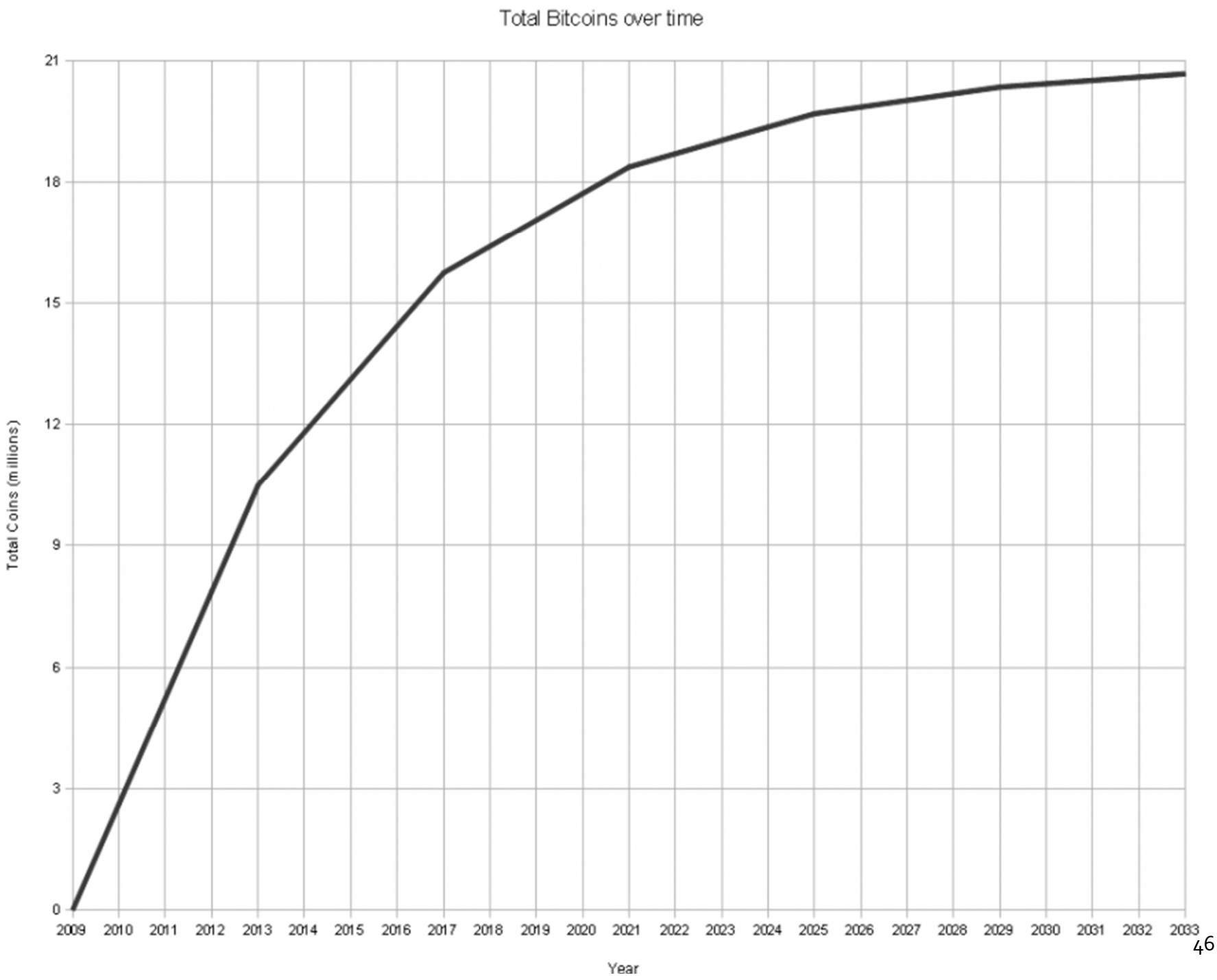
die **erste Open Source Währung, die ohne Bank auskommt.**

Der ökonomische Ansporn

Warum sollten Leute Blöcke versiegeln wollen?

Grund 1: Mining Bounty

- Wer einen Block versiegelt, erhält 50 BTC
- Alle 4 Jahre wird der Wert halbiert
- Asymptotisch: Maximal 21 Millionen BTC hergestellt
- Eingebauter Inflations-Schutz
- Problem: Einstellung: Bitcoin = Mining


Total Bitcoins over time
Total Coins (millions)
0
3
6
9
12
15
18
21
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
Year

Der ökonomische Ansporn

Warum sollten Leute Blöcke versiegeln wollen?

Grund 2: Fees

- Algorithmus sieht vor: Überweisung wird nur durchgeführt, wenn eine kleine Fee gezahlt wird
- Größe der Fee derzeit unklar
- Alternativ: Nur bei "großen" Überweisungen (gorß in Bit, nicht in BTC)
- Ist eine Frage, wie sich die Mehrheit der Knotenbetreiber entscheidet
- Schrittweise Ablöse der Mining Bounty durch die Fees

Der ökonomische Ansporn

Konsequenzen

Wird das Versiegeln ökonomisch unattraktiv

dann versiegeln weniger Leute

dann sinkt die Difficulty

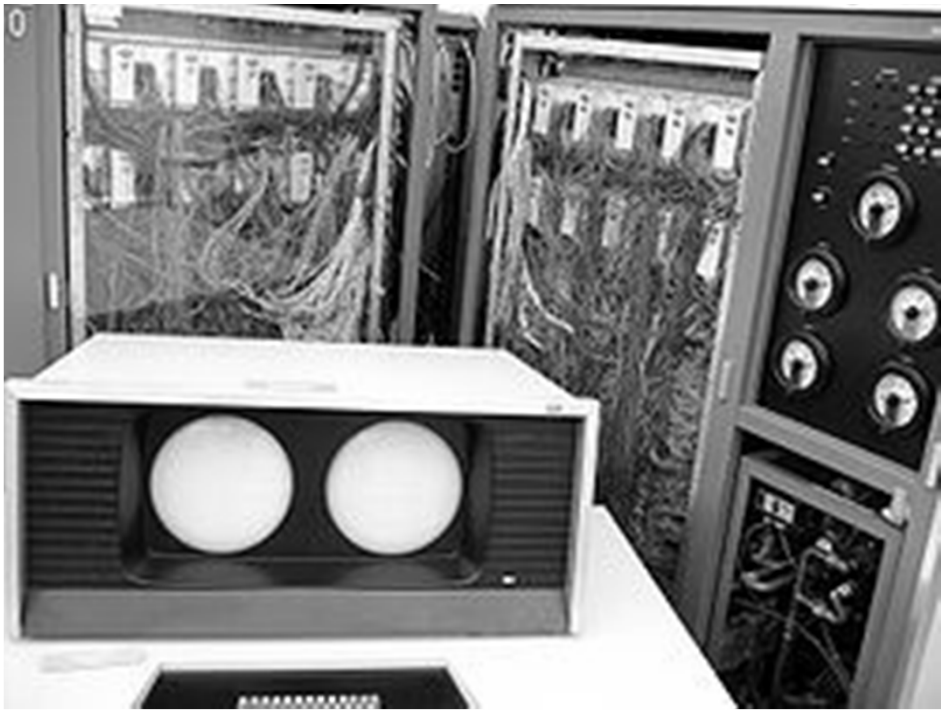
das Versiegeln kostet weniger CPU

und wird dadurch wieder billiger

Stabiles, sich selbst regelndes System

WO STEHT BITCOIN HEUTE?

Wo steht Bitcoin?



Vor 25 Jahren:

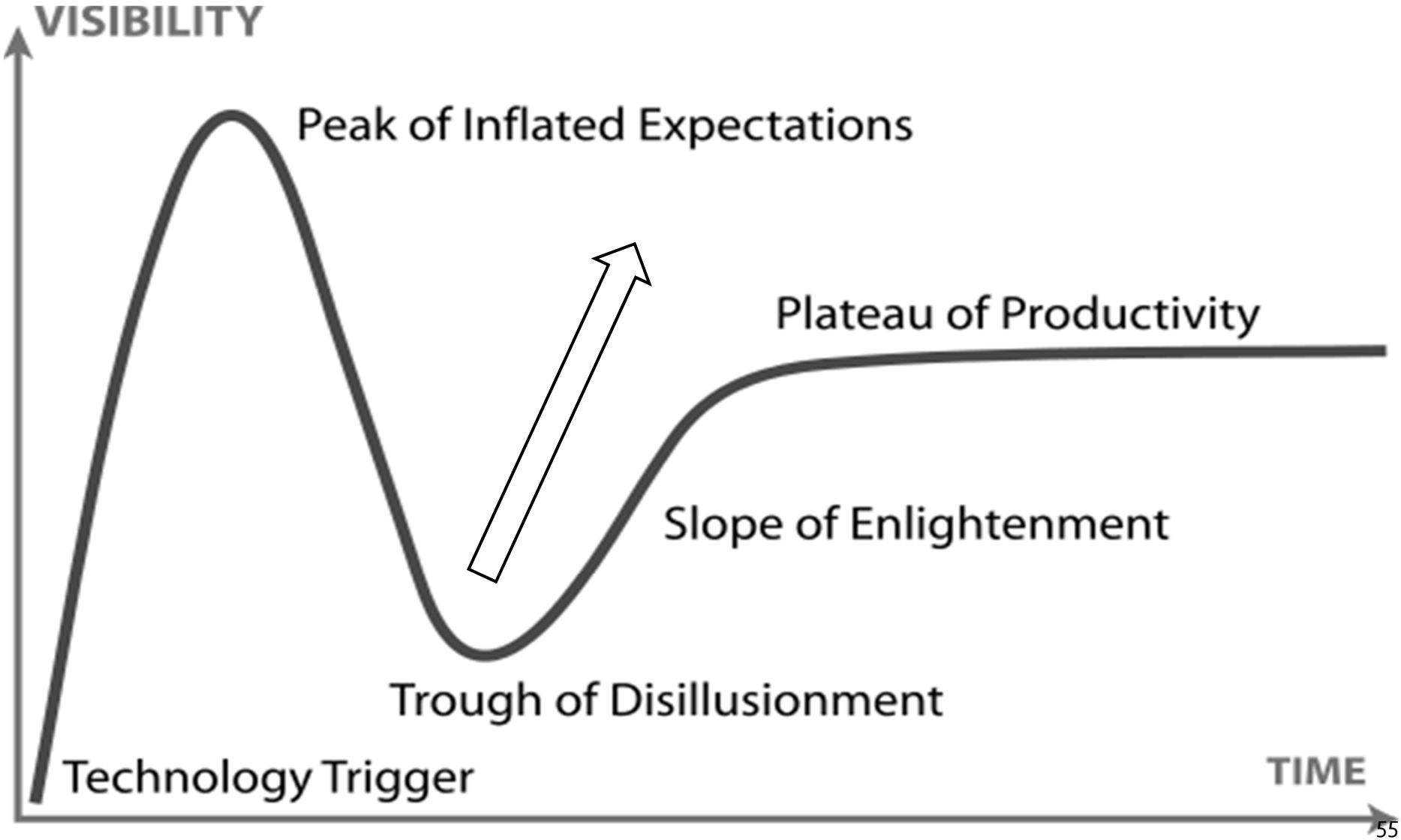
- Große Aufregung: Ich versende meine erste eMail
- Anruf bei Walter Altrichter: "Hast Du meine eMail bekommen".
- "Was habe ich bekommen? … ach so …

  ich schau mal nach und ruf Dich zurück"
- 20 Minuten später: "Ja, hab ich bekommen – hab' Dir auch eine Antwort geschickt"
- "Spannend. ich schau mal nach ob sie angekommen ist und melde mich wieder am Telefon“ … usw …

Heute gibt es auf Youtube Filme
die zelebrieren & zeigen, wie Bitcoins versendet werden

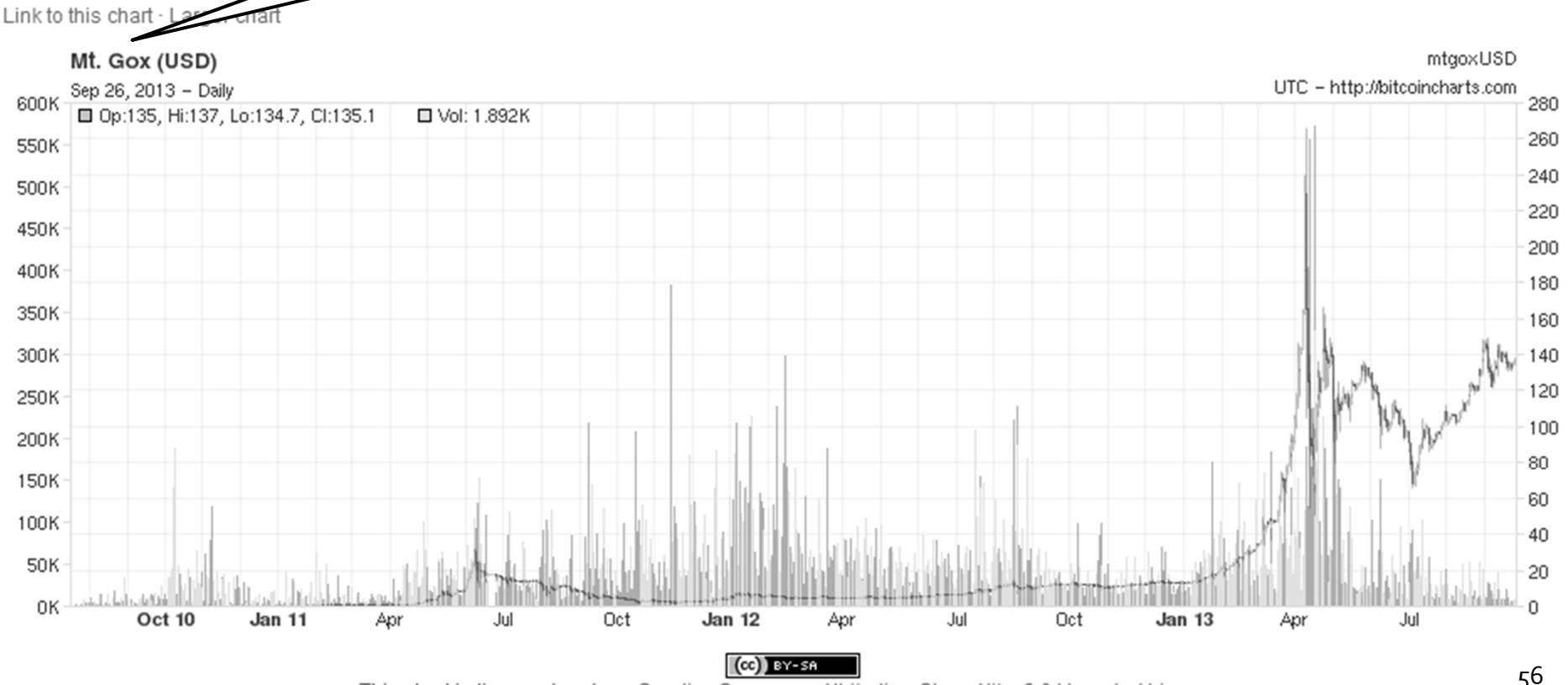

We are learning how to fly !

Gartner Group Entwicklungszyklus neuer Technologien

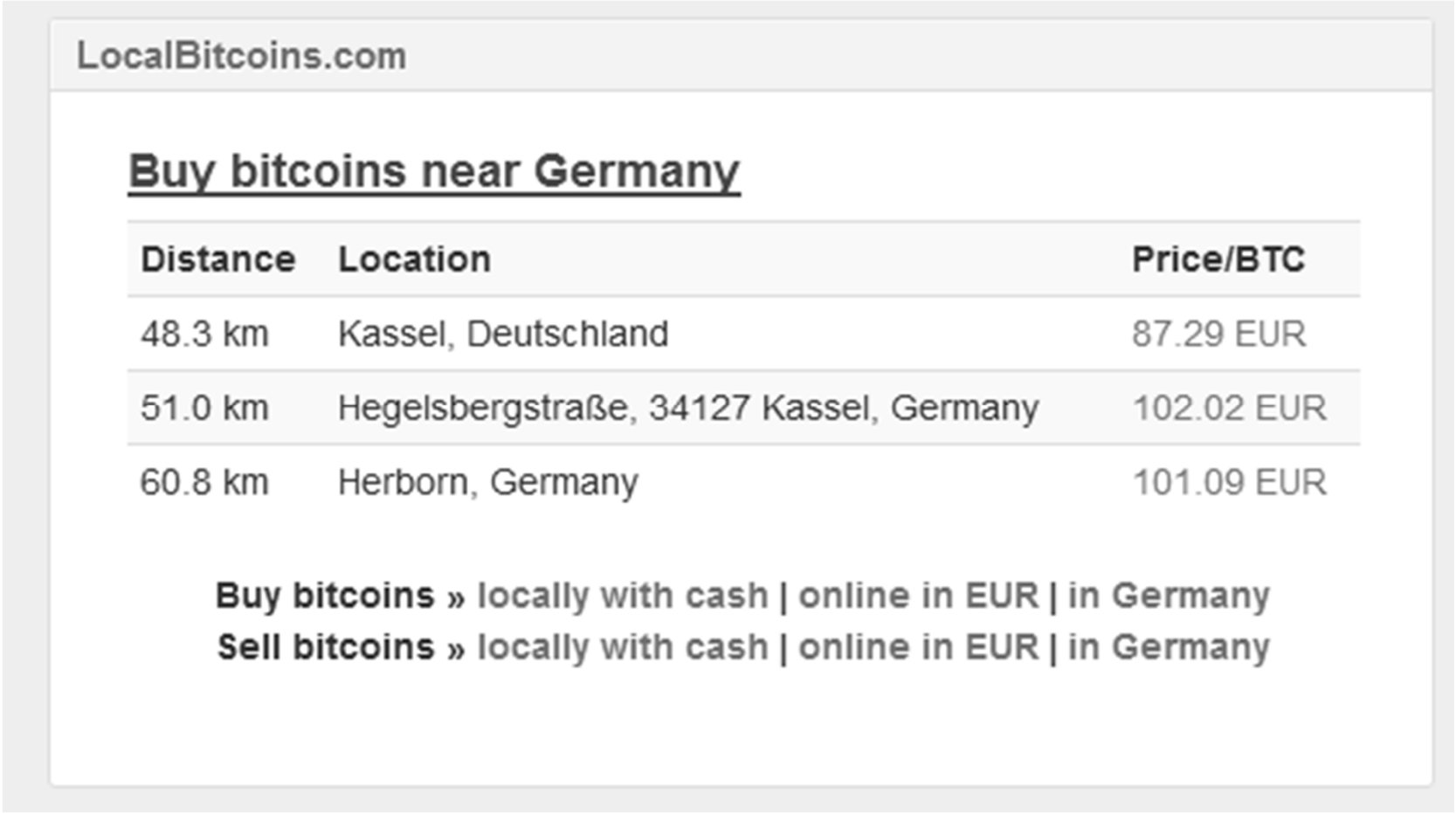


Kursentwicklung & Handelsvolumen 2010 - 2013

März 2014 liquidiert
Kunden geschädigt
Problem: Vertrauen in eine nicht erforderliche intermediäre Instanz



Lokale Handelsplattform


LocalBitcoins.com

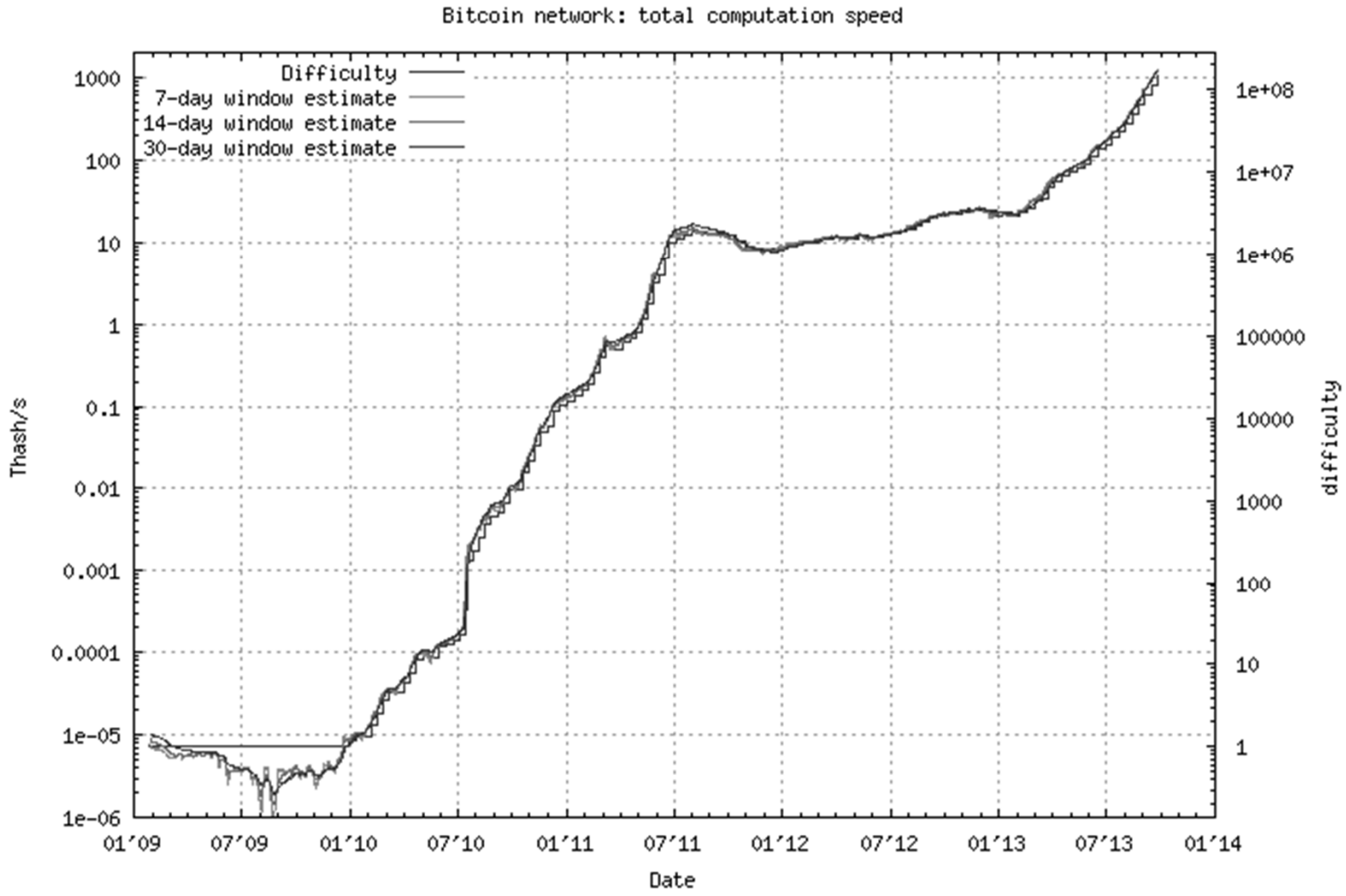
Buy bitcoins near Germany

Distance	Location	Price/BTC
48.3 km	Kassel, Deutschland	87.29 EUR
51.0 km	Hegelsbergstraße, 34127 Kassel, Germany	102.02 EUR
60.8 km	Herborn, Germany	101.09 EUR

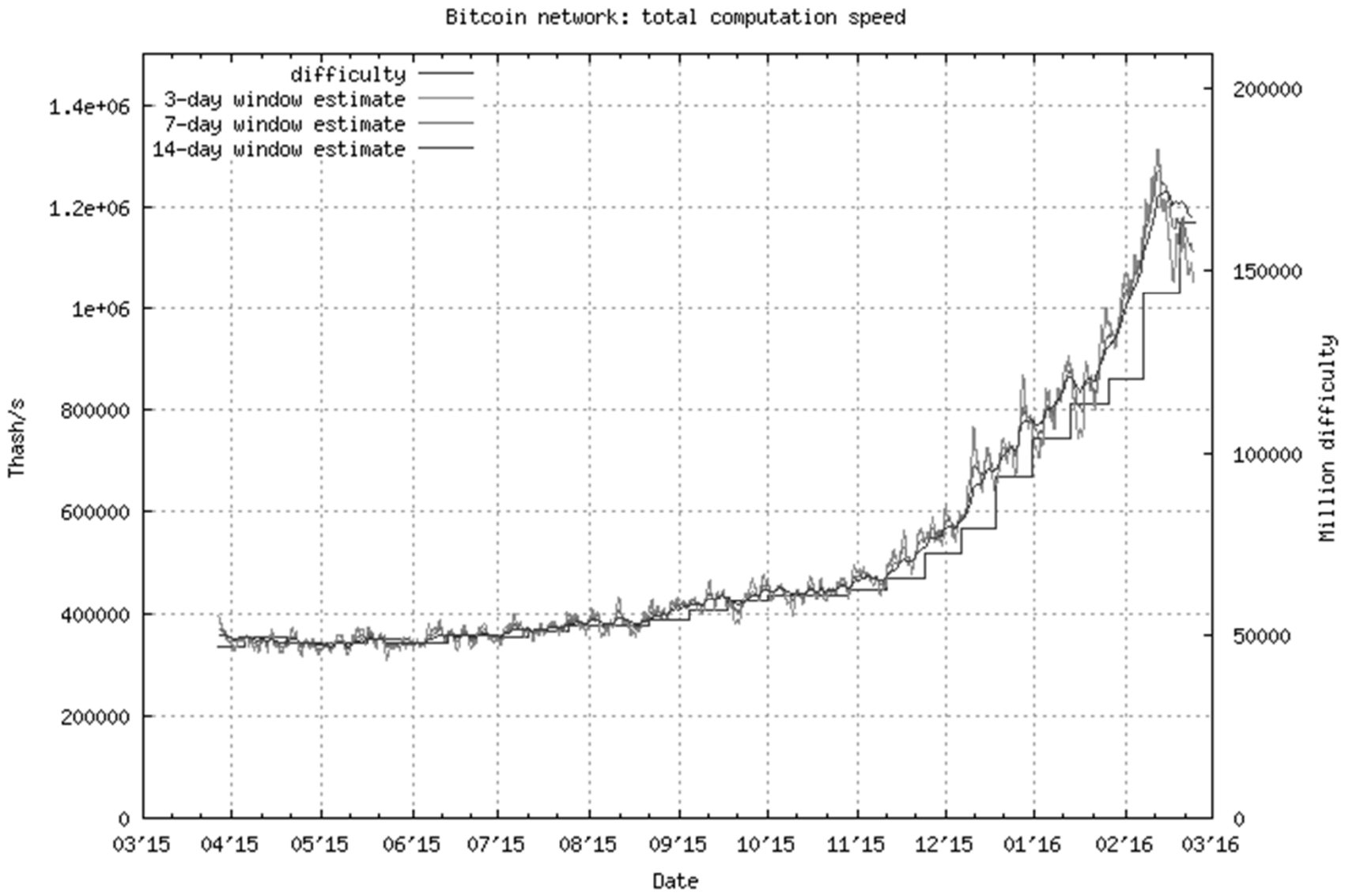
Buy bitcoins » locally with cash | online in EUR | in Germany
Sell bitcoins » locally with cash | online in EUR | in Germany

Network Hash Performance 2009-2014

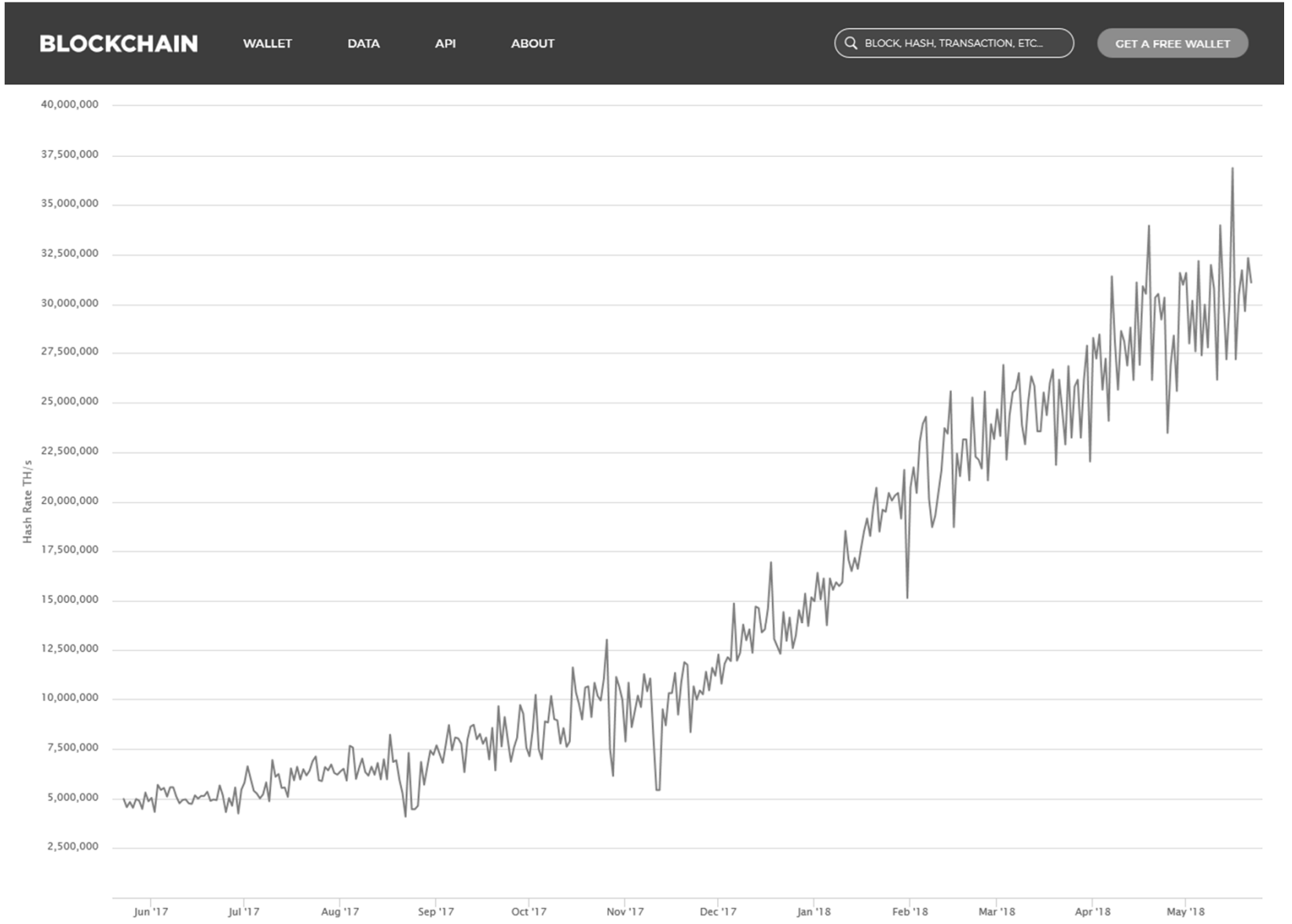
Exponential axis:



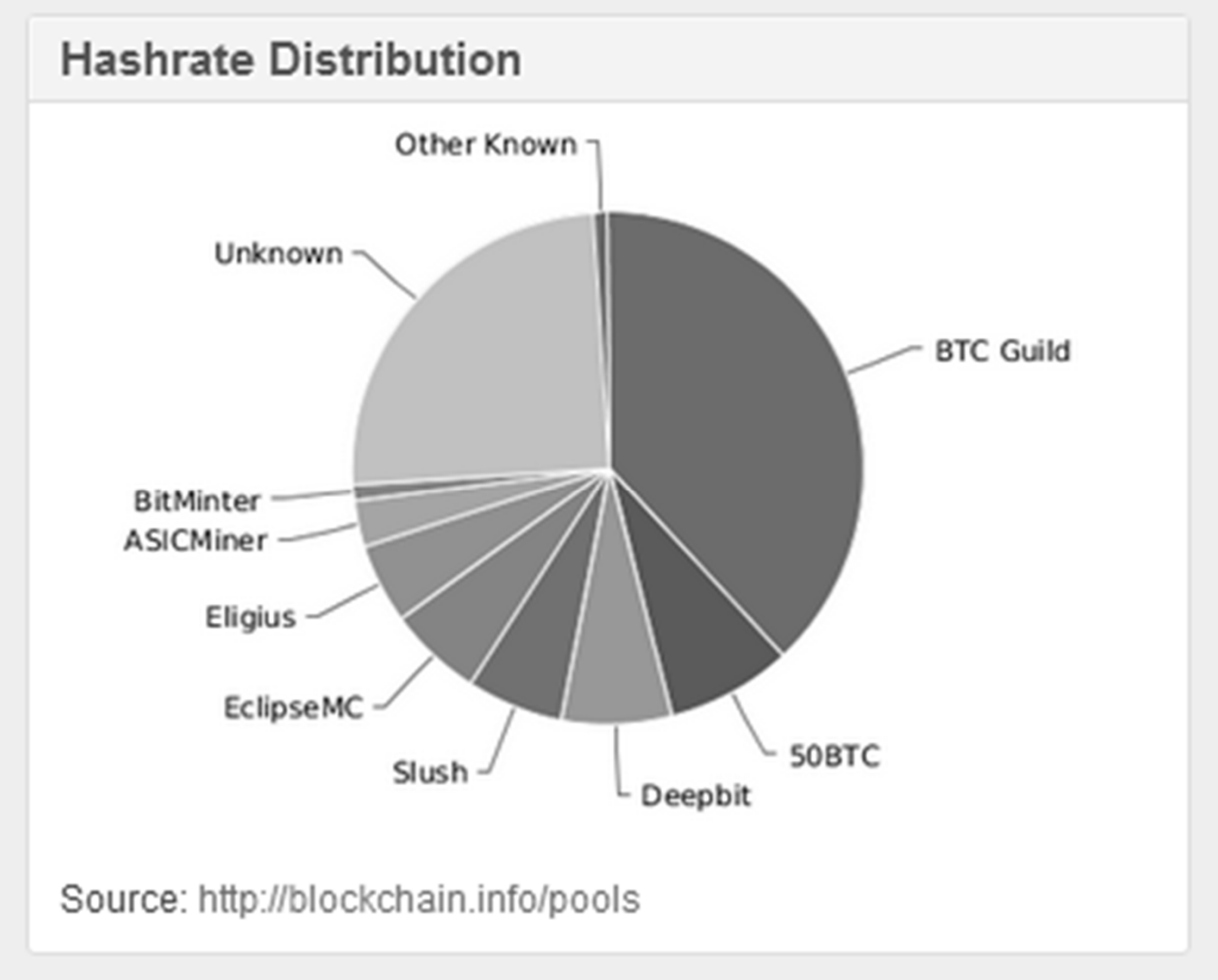
Network Hash Performance 2015-2016



Network Hash Performance komplett



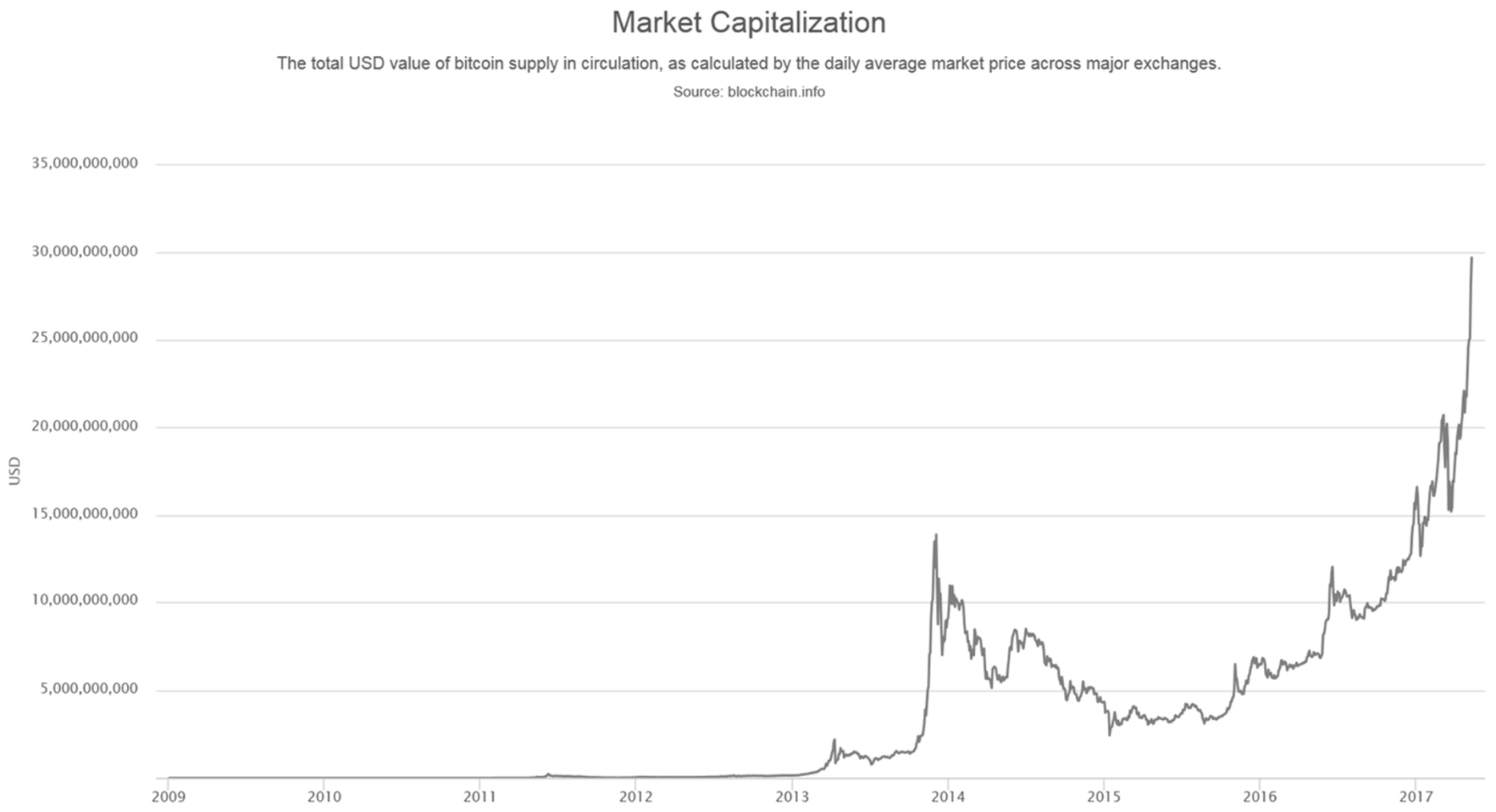
Hashrate Verteilung



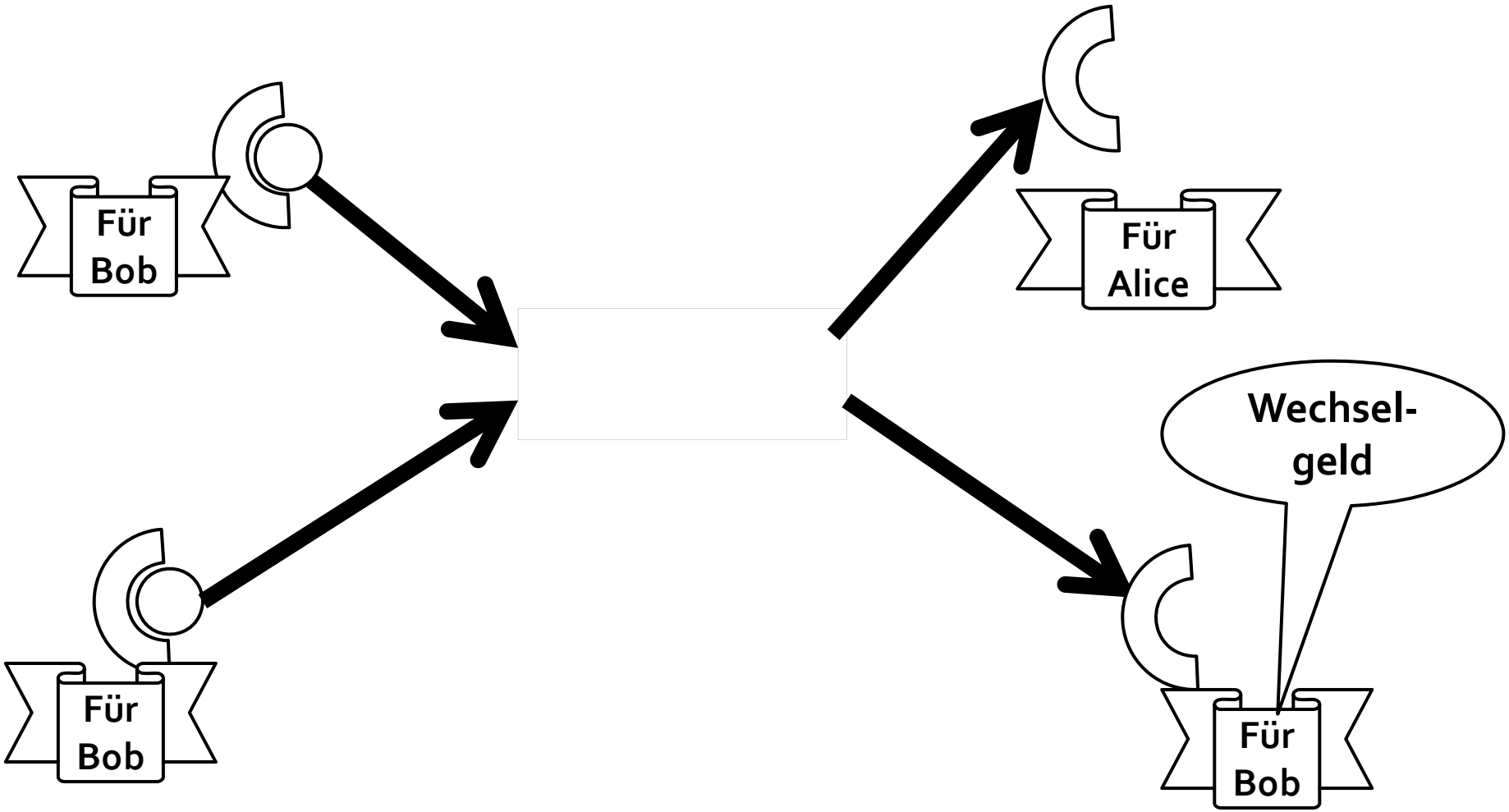
Marktpreis seit Anbeginn

Marktpreis 2017-18

Market Capitalization in USD 2009-2017



Ist Bitcoin anonym?



Ist Bitcoin anonym?

Beispiel:

- Alice an Bob via anonymer Mail

  Sende bitte 10 BTC an Konto 33.
- Bob: Überweist
- Alice: Sieht Überweisung, sendet Ware per anonymer Mail

Aber:

- Wenn Alice an Carol von Konto 33 überweist, dann sieht Bob das
- Daher legt Alice 10 neue Konti an: 20, 56, 88 usw.

  und überweist Geld quer durch die Gegend
- Bob weiß nnun nicht mehr, welche der Konti wirklich Alice gehören
- Bitcoin-Wäsche leicht möglich

Viele Fragen, viele Lösungen

Hit and Run Offences ?

- Bob zahlt, Alice liefert nicht
- Lösung 1: Brauche Escrow Agenturen mit Treuhand Bitcoin Konto
- Lösung 2: Bei digital lieferbaren Gütern gibt es Protokolle

Skalierung ?

- Jeder Knoten speichert jede Adresse
- Lösung 1: Sog. Merkle Tree Konstruktion
- Lösung 2: Light Weight Protocol Variante
- Lösung 3: Expiration Dates für Konti
- Lösung 4: Snapshots in der Blockkette
- Lösung 5: Garbage Collection in der Blockkette

Zahlenwerte zur Skalierung

Bitcoin: 7 Transaktionen / Sekunde

Visa: 2.000 – 10.000 Transaktionen / Sekunde

Paypal: 50 – 100 Transaktinen / Sekunde

Problem: CAP Theorem
Auch: Brewers Theorem nach dem Erfinder

In einem verteilten System bekommt man von

- **C**onsistency: Alle Knoten sehen selbe Daten
- **A**vailability: System bleibt verfügbar bei einzelnen Knoten-Ausfällen
- **P**artition Tolerance: Netz-Partition macht kein Anhalten des Algorithmus erforderlich

maximal 2 Eigenschaften hin.

Formaler Beweis in Modellwelt: 2002 Nancy Lynch.

Bitcoin garantiert … hmm … alle drei.

A und P im strengen Sinne

C aber nur im probabilistischen Sinne.

Was bedeutet "C nur im probablilistischen Sinne" ?

C wird nicht gewährleistet. Punkt.

Also ein inkonsistentes System mit elektronischem Geld ???

:-0

Lösung:

- Gewisse Fehlerwahrscheinlichkeit akzeptieren.
- Diese sinkt exponentiell im Zeitverlauf
- Ein wenig länger warten (30 Minuten – 4 Stunden)
- Schadenserwartungswert damit klein genug machen
- Praktisch C, theoretisch nicht C

Ist Bitcoin sicher?

05.09.2012

Drucken | Senden | Feedback | Merken

Bitfloor

Hacker stehlen 250.000 Dollar in Bitcoins

SPIEGEL ONLINE

Bitfloor-Website am Mittwoch: 24.000 Einheiten der virtuellen Währung sind weg

Ist Bitcoin sicher?

Ja, wenn

- ECC, SHA-256 und RIPEMD sicher sind
- Der private key sicher gespeichert wird

Wer Tausend Euro auf dem Tablett in der Kantine liegen läßt braucht sich nicht wundern wenn sie weg sind.

Wer die private keys seiner Konti unverschlüsselt im Backup hat oder per Virus ins Internet ausposaunt
braucht sich nicht wundern wenn seine Bitcoins weg sind.

Probleme mit Bitcoin

Bezahlung illegaler Transaktionen

Bsp: Drogenhandel auf Silk Road

- Website über Anonymisierungsdienst TOR erreichbar
- Bezahlung über Bitcoin
- Auslieferung über normale Post
- Qualitätssicherung über Reputations-System

Erpressung

Bsp: Vorfall um die Steuererklärung von Mitt Romney

http://pastebin.com/1j1yzQ9S

Dear PricewaterhouseCoopers LLP

Using your Office @ 830 Crescent Centre Drive, Suite 260, Franklin, TN 37067 Telephone: [1] (615) 503-2860 we were able to gain access to your network file servers and copy over the tax documents for one Willard M Romney and Ann D Romney.

We are sure that once you figure out where the security breach was, some people will probably get fired but that is not our concern.

http://pastebin.com/1j1yzQ9S

All major news media outlets are going to be sent an encrypted copy of the most recent tax years

The deal is quite simple. Convert $1,000,000 USD to Bitcoins (Google if if you need a lesson on what Bitcoin is)

Bitcoin Address to Stop Release:

1HeF89wMjC48bWNgWvVo7Wu3RaLW8XVsE8

Bitcoin Address to Promote Full Release:

12AP6iCwRNFQqKLStH3A4b4hw3SL6RaNgB

Who-ever is the winner does not matter to us.

http://pastebin.com/1j1yzQ9S

Reference to avoid Fakes that only you will have.

1. all these considerations did not deter me from the path of duty
2. the moment I understood the will of my Heavenly Father

Vermutlich kann nur Romney erkennen

ob die Drohung ein Fake ist.

Auflösung: Romney hat selber veröffentlicht.

Also Bitcoin verbieten ?

Wie ?

So, wie auch Peer-2-Peer Filesharing von Filmen unter © verboten ist. ☺

Oder Bitcoin nutzen?

Weltweite Überweisung innerhalb von Sekunden

Nach 1 Stunde relativ sicherer Status

Frei von zentralen Instanzen

Kann nicht gesperrt werden

Absolutes "Bank"geheimnis möglich, da keine Bank

Geld im Backup halten

Jeder kann Teil der Infrastruktur sein

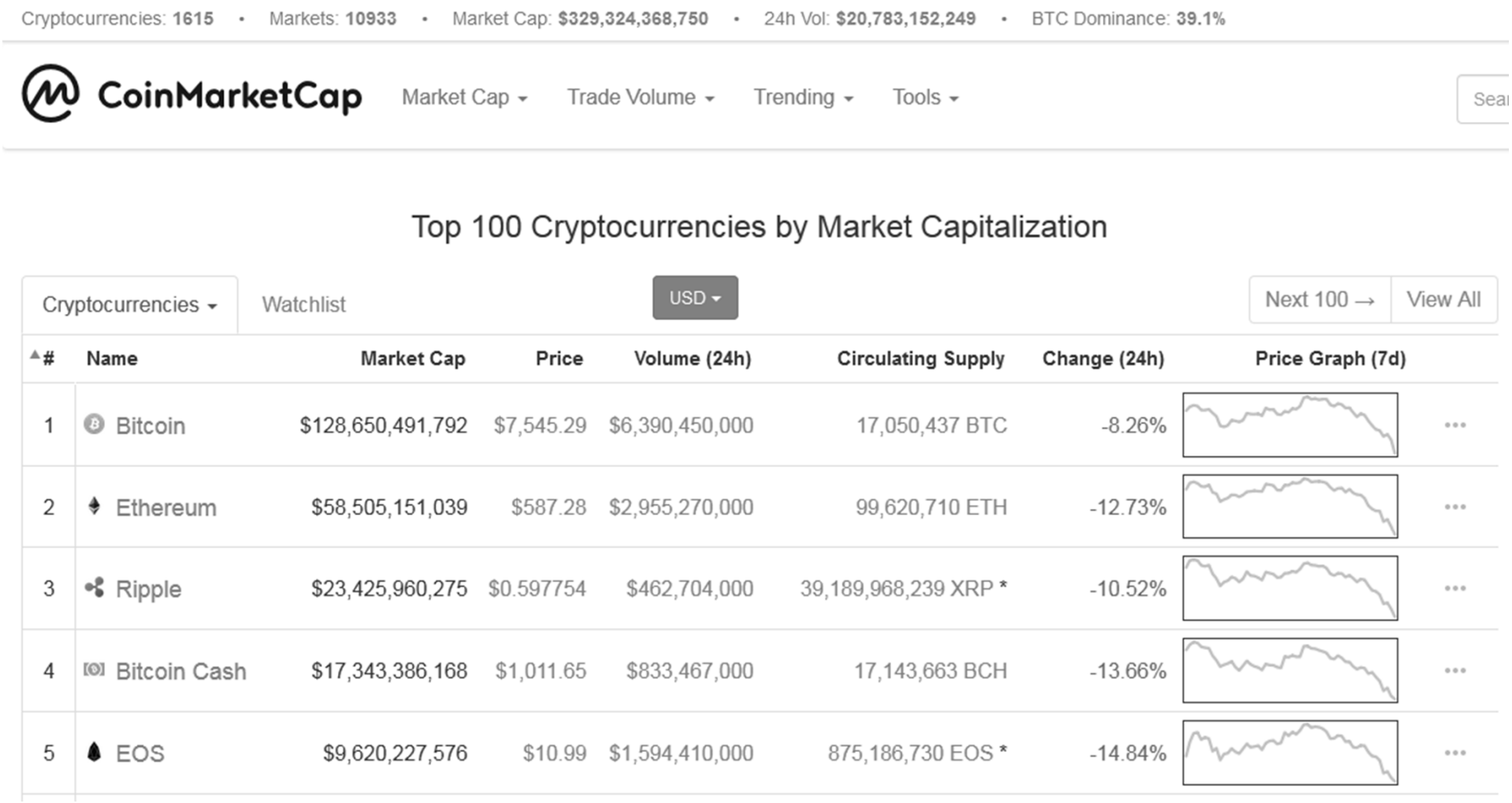
Radikale Konkurrenz bei den Transaktionsgebühren

Immun gegen politische Versuche, Geld zu drucken

Völlig unter der Kontrolle der Mehrheit

Ähnliche Entwicklungen

coinmarketcap.com: 1615 Crypto Currencies



Cryptocurrencies: **1615** • Markets: **10933** • Market Cap: **$329,324,368,750** • 24h Vol: **$20,783,152,249** • BTC Dominance: **39.1%**

CoinMarketCap Market Cap Trade Volume Trending Tools

Top 100 Cryptocurrencies by Market Capitalization

Cryptocurrencies Watchlist USD Next 100 → View All

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	Bitcoin	$128,650,491,792	$7,545.29	$6,390,450,000	17,050,437 BTC	-8.26%	
2	Ethereum	$58,505,151,039	$587.28	$2,955,270,000	99,620,710 ETH	-12.73%	
3	Ripple	$23,425,960,275	$0.597754	$462,704,000	39,189,968,239 XRP *	-10.52%	
4	Bitcoin Cash	$17,343,386,168	$1,011.65	$833,467,000	17,143,663 BCH	-13.66%	
5	EOS	$9,620,227,576	$10.99	$1,594,410,000	875,186,730 EOS *	-14.84%	

Ähnliche Entwicklungen

Namecoin

- **Eine Art Bitcoin & DNS-Datenbank**
- **Nutzt konsistente Replikation für Reservation von Domains**

Ethereum

- **Eine Art Bitcoin 2.0**
- **Derzeit Proof of Concept Phase**
- **Verallgemeinert von "korrekte Kontoführung" auf "beliebige formal definierte Transaktion"**
- **Mehr: Ethereum White Paper http://gavwood.com/Paper.pdf**

Smart Contract

Bitcoin:

Bestimmte Anforderungen an Korrektheit

Summen stimmen...

Signaturen vorhanden und verifizieren...

Difficulty stimmt...

Smart Contract:

Verallgemeinerung dieses Konzepts

Beliebige Bedingungen (Turing vollständig...)

Anbindung an Außenwelt (Ereignisse...)

Weitere Incentives für Miner

Beispiel

Wohnungsmiete

Mieter bekommt Quittung und Zugangsschlüssel

Vermieter bekommt Geld

Bestimmte Zeiten und Übergänge sind vereinbart

Garantien darüber warden eingehalten & überwacht

Blockchain basierte Kontostände passen sich automagisch an

Weitere Beispiele

Altcoins

Crowdfunding Schemata

Prediction Markets

Lotterien

Überwachte Wahlen

Zugangskontrollen

Spiele

Verteilte Organisationen

...

Ethereum

Eigene Programmiersprache für Smart Contracts (Solidity)

Ähnlich wie Javascript; Anbindung an UI und Crypto

Berechnungen einer Transaktion kosten Zeit

Wird in entsprechendes "gas" / Geld umgerechnet

Eigene Blockchain als erweitertes Bitcoin

Anwendung

On top of Ethereum

Funktioniert out of the box

Skalierbarkeit, Sicherheit (viele Miner), Community

Fokus auf eigenen Geschäftsprozess

Kostet gas.

Eigene Blockchain mit Ethereum Technologie

Unabhängigkeit von Schicksal & Entscheidungen bei Ethereum

Eigene Wahl von gas-Preis und weiteren Parametern

Auch private Chain möglich (nur bestimmte, authentisierte Teilnehmer)

Beispiel für Solidity

MINIMUM VIABLE TOKEN

The standard token contract can be quite complex. But in essence a very basic token boils down to this:

```
pragma solidity ^0.4.20;

contract MyToken {
    /* This creates an array with all balances */
    mapping (address => uint256) public balanceOf;

    /* Initializes contract with initial supply tokens to the creator of the contract */
    function MyToken(
        uint256 initialSupply
        ) public {
        balanceOf[msg.sender] = initialSupply;              // Give the creator all initial tokens
    }

    /* Send coins */
    function transfer(address _to, uint256 _value) public {
        require(balanceOf[msg.sender] >= _value);           // Check if the sender has enough
        require(balanceOf[_to] + _value >= balanceOf[_to]); // Check for overflows
        balanceOf[msg.sender] -= _value;                    // Subtract from the sender
        balanceOf[_to] += _value;                           // Add the same to the recipient
    }
}
```

Proof of Work

Mechanismus:

Validator ist, wer ein PoW lost

PoW ist ein Hash Rätsel, das nur durch Probieren gelöst werden kann

Probieren braucht Zeit oder Performanz

Wer das Rätsel als erster löst hat statistisch die besten Chancen,
dass sein Block in der globalen Blockchain verbleibt
und damit sein Eigentum an der Bounty wahr bleibt/wird

Probleme:

Stromverbrauch, CO2 Footprint

51% Attacke, hop-on-hop-off Attacke von Minern

Absicherbar durch private Blockchain

Zeitbedarf

Proof of Stake

Mechanismus

Validator wird, wer einen hohen Stake nachweisen kann

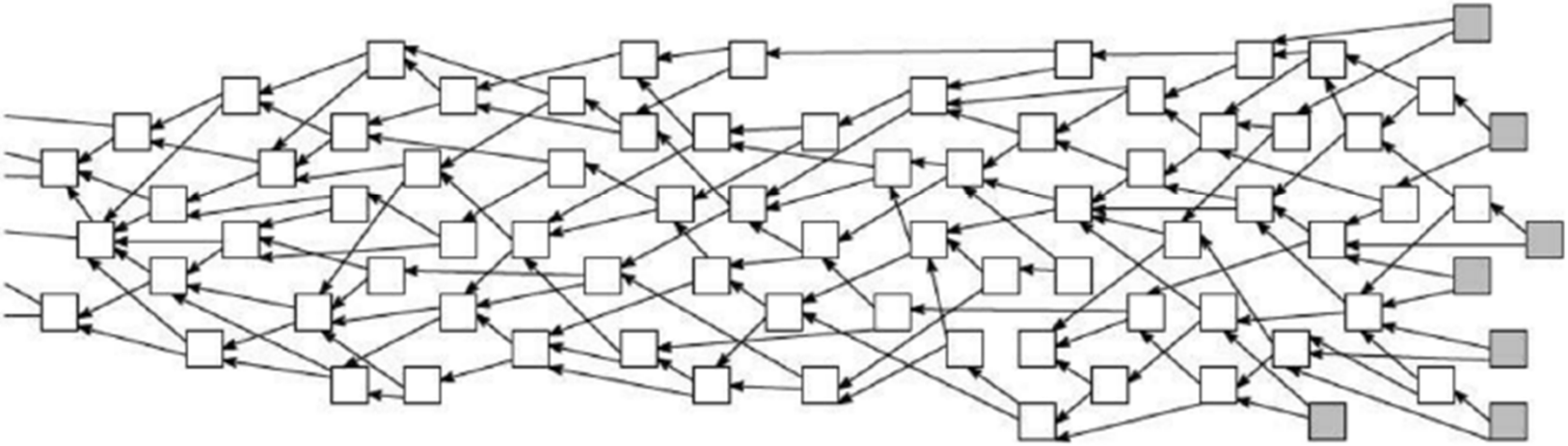
Stake: Einsatz, ev. auch in Tokens

Auswahl durch Zufallsmechanismus

Wahrscheinlichkeit der Auswahl steigt mit Stake

Validator, der sich nicht an Regeln halt, verliert später Stake u/o Bounty

DAG Verifikation
Am Bsp: IOTA Tangle



DAG Verifikation
Am Bsp: IOTA Tangle

Mechanismus:

Wer Ledger nutzen will muss auch validieren

Validator unterschreibt mit private Key

Jeweils 2 vorangegangene Blöcke einbinden

Auswahl der nächsten 2 Kandidaten nach Random Walk

Kleine PoW als Spam und Sybil Schutz

Bewertung:

Skaliert besser, leichtgewichtig

Keine Fees nötig sondern eigene Mitarbeit

Auch offline Transaktionen

Für IoT Anwendungen gut geeignet