Bitcoin

blueling und Deaddy

Einführung

Bitcoins aus Usersicht

Technik hinter Bitcoin

Mining

Ökonomie

Zwischenfälle und Angriff-szenarien

Bitcoin - eine kryptographische P2P-Währung

blueling und Deaddy

2011-07-09

Outline

1 Einführung

2 Bitcoins aus Usersicht

3 Technik hinter Bitcoin

4 Mining

5 Ökonomie

6 Zwischenfälle und Angriffszenarien

Überblick über Bitcoin

Bitcoin

blueling und Deaddy

Einführung

Bitcoins aus Usersicht

Technik hinter Bitcoin

Mining

Ökonomie

Zwischenfälle und Angriff-szenarien

- erste **dezentrale** digitale Währung
- 8 Seiten Paper 2008 unter Pseudonym 'Satoshi Nakamoto' veröffentlicht
- Wurzeln in der Cypherpunk-Bewegung (z.B. Wai Dai, b-money (1998))
- 2009 erste Implementation von Satoshi released
- community driven open source Projekt (http://bitcoin.org (Wiki, Forum), #bitcoin auf freenode)

Problem?

Bitcoin

blueling und Deaddy

Einführung

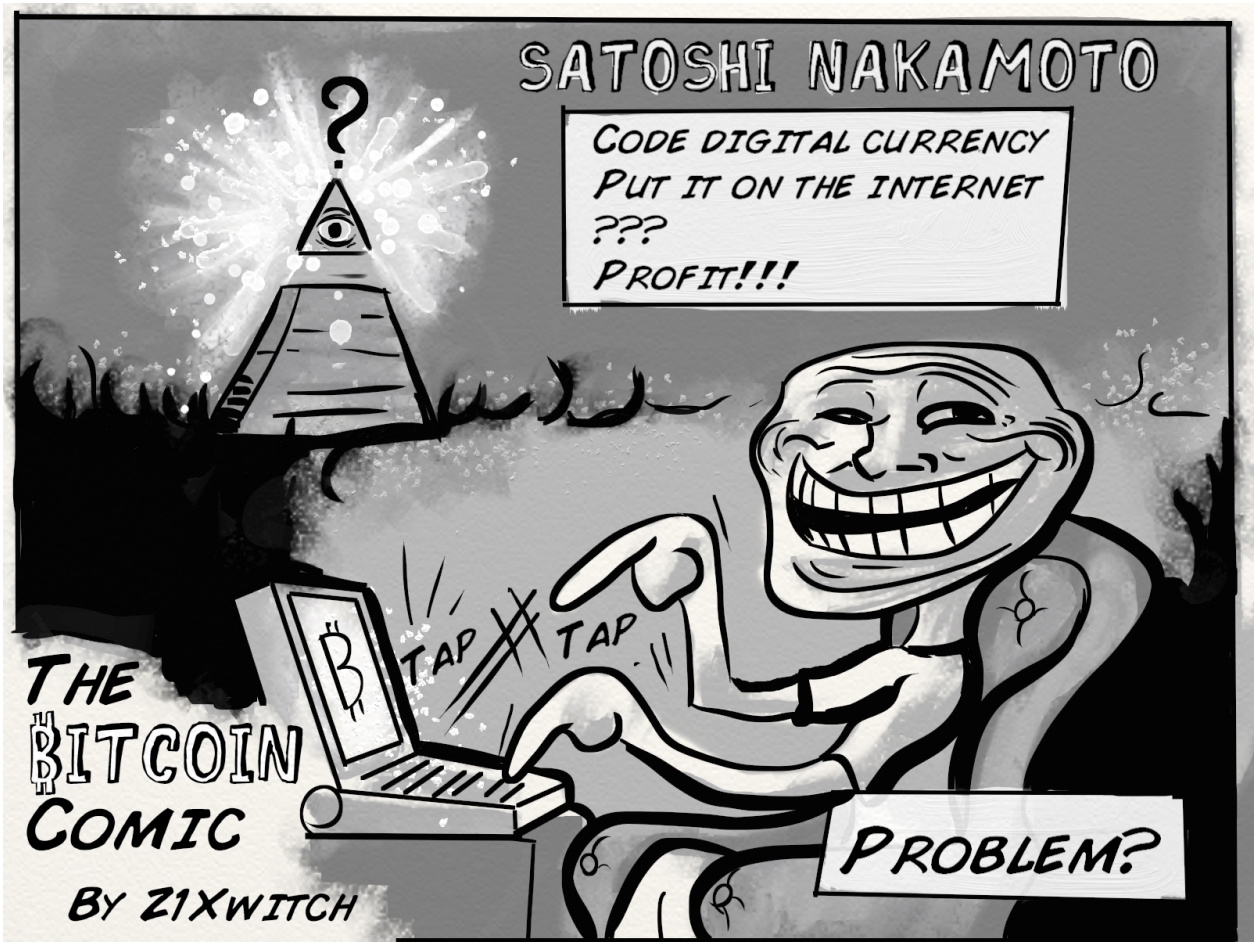
Bitcoins aus Usersicht

Technik hinter Bitcoin

Mining

Ökonomie

Zwischenfälle und Angriff-szenarien



Features

Bitcoin

blueling und Deaddy

Einführung

Bitcoins aus Usersicht

Technik hinter Bitcoin

Mining

Ökonomie

Zwischenfälle und Angriff-szenarien

- (bedingt) anonym
- grenzüberschreitend
- schnell
- dezentral
- kostengünstig
- fälschungssicher
- staatsunabhängig
- viral

Outline

1 Einführung

2 Bitcoins aus Usersicht

3 Technik hinter Bitcoin

4 Mining

5 Ökonomie

6 Zwischenfälle und Angriffszenarien

Bitcoins aus Usersicht

Bitcoin

blueling und Deaddy

Einführung

Bitcoins aus Usersicht

Technik hinter Bitcoin

Mining

Ökonomie

Zwischenfälle und Angriff-szenarien

- bitcoin-client für Windows/Linux/Mac unter MIT-Lizenz (GUI und CLI)
- für Überweisungen benötigt man nur die Empfängeradresse (Zeichenkette wie 13rigybYMphatCxAhKksDeozbWE1s6sP6L)
- beliebig viele eigene Empfängeradressen für Anonymität
- jede Adresse beliebig lange verwendbar

Bitcoin Client unter Windows

Bitcoin

blueling und Deaddy

Einführung

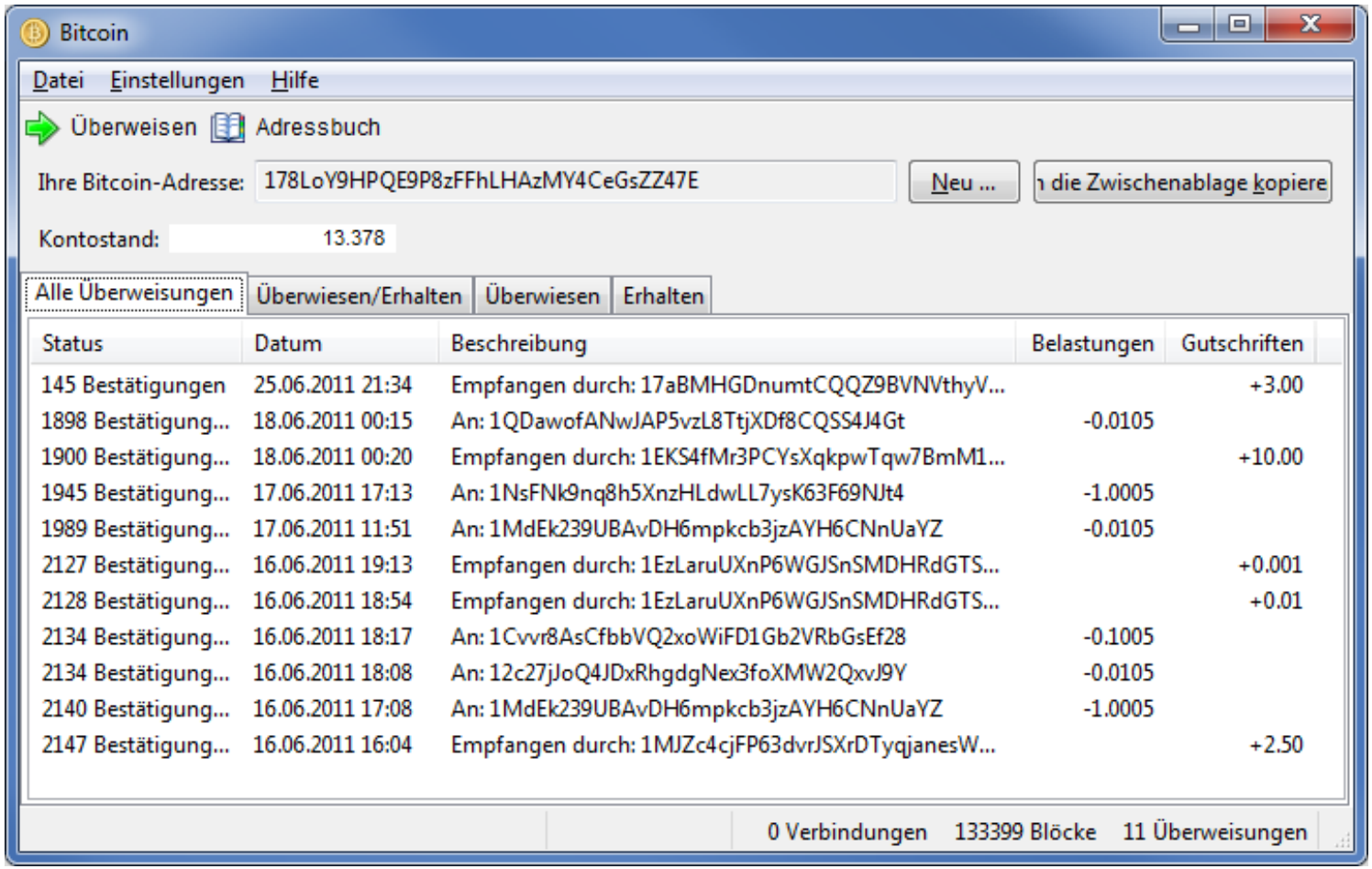
Bitcoins aus Usersicht

Technik hinter Bitcoin

Mining

Ökonomie

Zwischenfälle und Angriff-szenarien



Durchführen einer Überweisung

Bitcoin

blueling und Deaddy

Einführung

Bitcoins aus Usersicht

Technik hinter Bitcoin

Mining

Ökonomie

Zwischenfälle und Angriff-szenarien

- Empfängeradresse, Betrag (+ evtl. Transaktionskosten) eingeben und absenden
- gültige Transaktion wird binnen ca. 10 Minuten das erste mal bestätigt; der Empfänger sieht die unbestätigte Transaktion gewöhnlich bereits nach wenigen Sekunden
- 6 Blöcke (etwa 1h) später wird die Transaktion als offiziell bestätigt angezeigt
- Bitcoins können erst nach Bestätigung ausgegeben werden

Einheiten

Bitcoin

blueling und Deaddy

Einführung

Bitcoins aus Usersicht

Technik hinter Bitcoin

Mining

Ökonomie

Zwischenfälle und Angriff-szenarien

- BTC als Währungsabkürzung in Anlehnung an ISO-4217
- ฿ inoffizielles Währungssymbol (von der thailändischen Währung Baht)
- jeder Bitcoin auf bis 8 Nachkommastellen teilbar, kleinste Einheit 1 Satoshi, also ein μ฿= 100 Satoshi

Outline

1 Einführung

2 Bitcoins aus Usersicht

3 Technik hinter Bitcoin

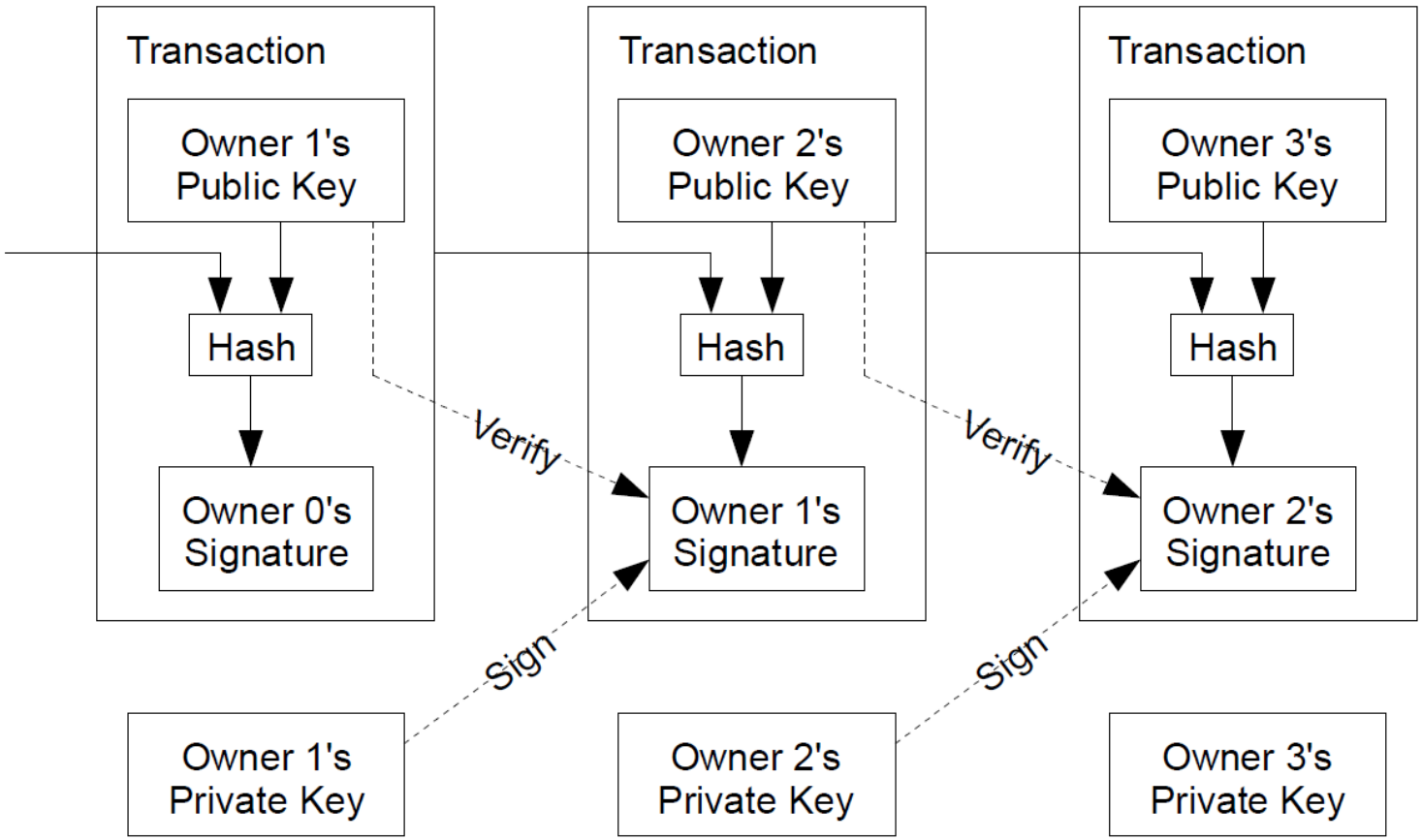
4 Mining

5 Ökonomie

6 Zwischenfälle und Angriffszenarien

Transaktionen

Transaktionen basieren auf asymmetrischer Verschlüsselung



wallet.dat

Bitcoin

blueling und Deaddy

Einführung

Bitcoins aus Usersicht

Technik hinter Bitcoin

Mining

Ökonomie

Zwischenfälle und Angriff-szenarien

- Keyring für die eigenen Adressen und Transaktionen
- bei Verlust ist das Geld unwiderruflich verloren
- (noch) keine built-in Verschlüsselungs- oder Backupmechanismen
- Viren und Metasploitmodule sind im Umlauf

Probleme bei digitalen Transaktionen

Bitcoin

blueling und Deaddy

Einführung

Bitcoins aus Usersicht

Technik hinter Bitcoin

Mining

Ökonomie

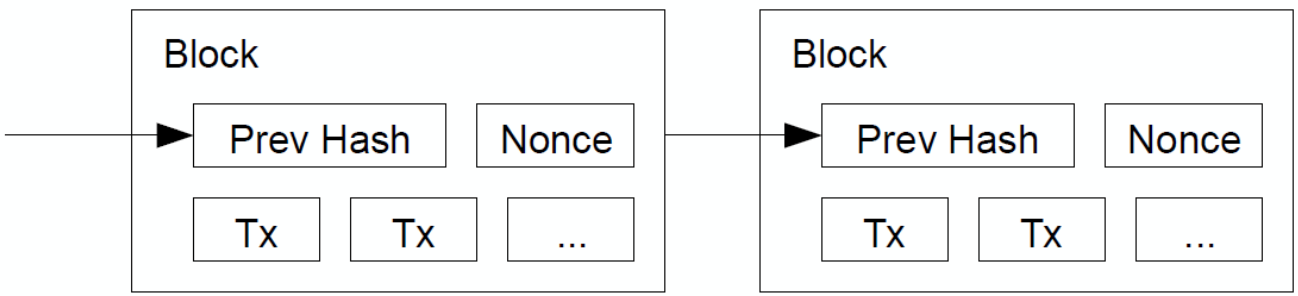
Zwischenfälle und Angriff-szenarien

- „double-spending“ verhindern erfordert Klärung der chronologischen Abfolge von Transaktionen
- vor Bitcoins setzte dies eine vertrauenswürdige Zentralinstanz voraus

Wie löst man das dezentral?

Lösung: Distributed timestamp server

- Transaktionen werden über Flooding-Algorithmus in das Netz gebroadcastet
- Transaktionen werden in Blöcken zusammengefasst und signiert, dabei enthält jeder Block den Hash des vorherigen Blocks
- es entsteht die sogenannte „Blockchain“



Bestätigung eines Blocks

Bitcoin

blueling und Deaddy

Einführung

Bitcoins aus Usersicht

Technik hinter Bitcoin

Mining

Ökonomie

Zwischenfälle und Angriff-szenarien

- zur Bestätigung eines Blocks muss mit einer Nonce ein SHA-256-Hash gefunden werden, der kleiner als das aktuelle Target ist (anschaulich Anzahl der 0-bits am Anfang des Hashes)
- der Schwierigkeitsgrad wird protokollseitig über einen gleitenden Durchschnitt alle 2016 Blöcke (ca. 2 Wochen) so angepasst, dass im Schnitt alle 10 Minuten ein Block berechnet wird

Blockchain

Bitcoin

blueling und Deaddy

Einführung

Bitcoins aus Usersicht

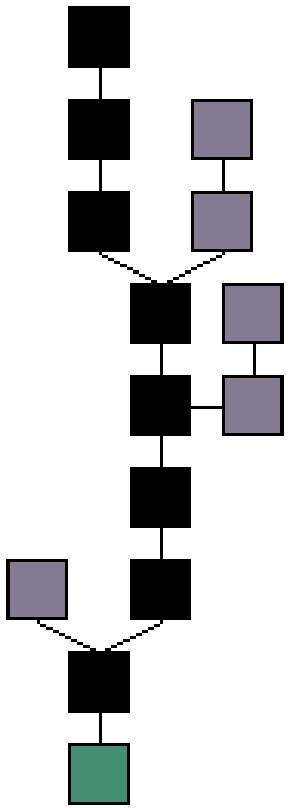
Technik hinter Bitcoin

Mining

Ökonomie

Zwischenfälle und Angriff-szenarien

- längste Kette ist offiziell und wird als Grundlage für den nächsten Block genommen
- „Länge“ ist die Gesamtschwierigkeit für die Blockchain
- gibt es zwei gleichlange Ketten, rechnet die Node nur an der zuerst erhaltenen und verwirft diese, falls die andere früher erweitert wird



Wer berechnet die Blockchain?

Bitcoin

blueling und Deaddy

Einführung

Bitcoins aus Usersicht

Technik hinter Bitcoin

Mining

Ökonomie

Zwischenfälle und Angriff-szenarien

- jeder kann sich an der Hashberechnung beteiligen
- um die Blockchain durch eine manipulierte zu ersetzen (z.B. für double-spending) muss man die Kette ab dem zu ändernden Block neu Berechnen (mit einer Difficulty $\geq$ der originalen Chain)
- mit $> 50\%$ der Rechenleistung bestimmt man das Netzwerk

Sicherheit der Blockchain

Bitcoin

blueling und Deaddy

Einführung

Bitcoins aus Usersicht

Technik hinter Bitcoin

Mining

Ökonomie

Zwischenfälle und Angriff-szenarien

Angriff auf die Blockchain ist ein binomialer Random-Walk und analog zum Gambler's Ruin problem: ein Spieler mit unendlichem Kredit startet mit einem Defizit und spielt eine möglicherweise unendliche Anzahl Spiele um dieses auszugleichen. Die Wahrscheinlichkeit q_z, dass er mit z Blöcken Rückstand wieder aufholt ist

$$q_z = \begin{cases} 1, & \text{falls } p \leq q \\ (q/p)^z, & \text{sonst} \end{cases}$$

wobei p = Wahrscheinlichkeit, dass eine ehrliche Node den nächsten Block findet und q = Wahrscheinlichkeit, dass der Angreifer den nächsten Block findet
Besitzt der Angreifer $\geq 50\%$ der Rechenleistung, entspricht dies dem Fall $q \geq p$

Outline

1 Einführung

2 Bitcoins aus Usersicht

3 Technik hinter Bitcoin

4 Mining

5 Ökonomie

6 Zwischenfälle und Angriffszenarien

Mining

Bitcoin

blueling und Deaddy

Einführung

Bitcoins aus Usersicht

Technik hinter Bitcoin

Mining

Ökonomie

Zwischenfälle und Angriff-szenarien

- Blockchain-Berechnung ist rechenintensiv
- es gibt als Belohnung für die Erstellung eines Blocks anfangs 50BTC (halbiert sich alle 210k Blöcke/4 Jahre)
- zusätzlich erhält der Blockersteller etwaige (freiwillig zahlbare) Transaktionsgebühren
- der Miner bestimmt welche Transaktionen er aufnimmt (z.B. nur welche mit Transaktionsgebühren)

Mining

Bitcoin

blueling und Deaddy

Einführung

Bitcoins aus Usersicht

Technik hinter Bitcoin

Mining

Ökonomie

Zwischenfälle und Angriff-szenarien

- die Belohnung für das Finden von Block-Hashes ist die einzige Geldschöpfung
- hierdurch wird das Gesamtvolumen auf etwa 21 Millionen BTC (etwa 2031 erreicht) begrenzt, bei der derzeitigen Aufteilung gibt es maximal $2,1 \cdot 10^{15}$ diskrete Einheiten
- derzeit befinden sich etwa 6.765.550 BTC im Umlauf (Stand: 08. Juli 16 Uhr)

Entwicklung der Bitcoinmenge

Bitcoin

blueling und Deaddy

Einführung

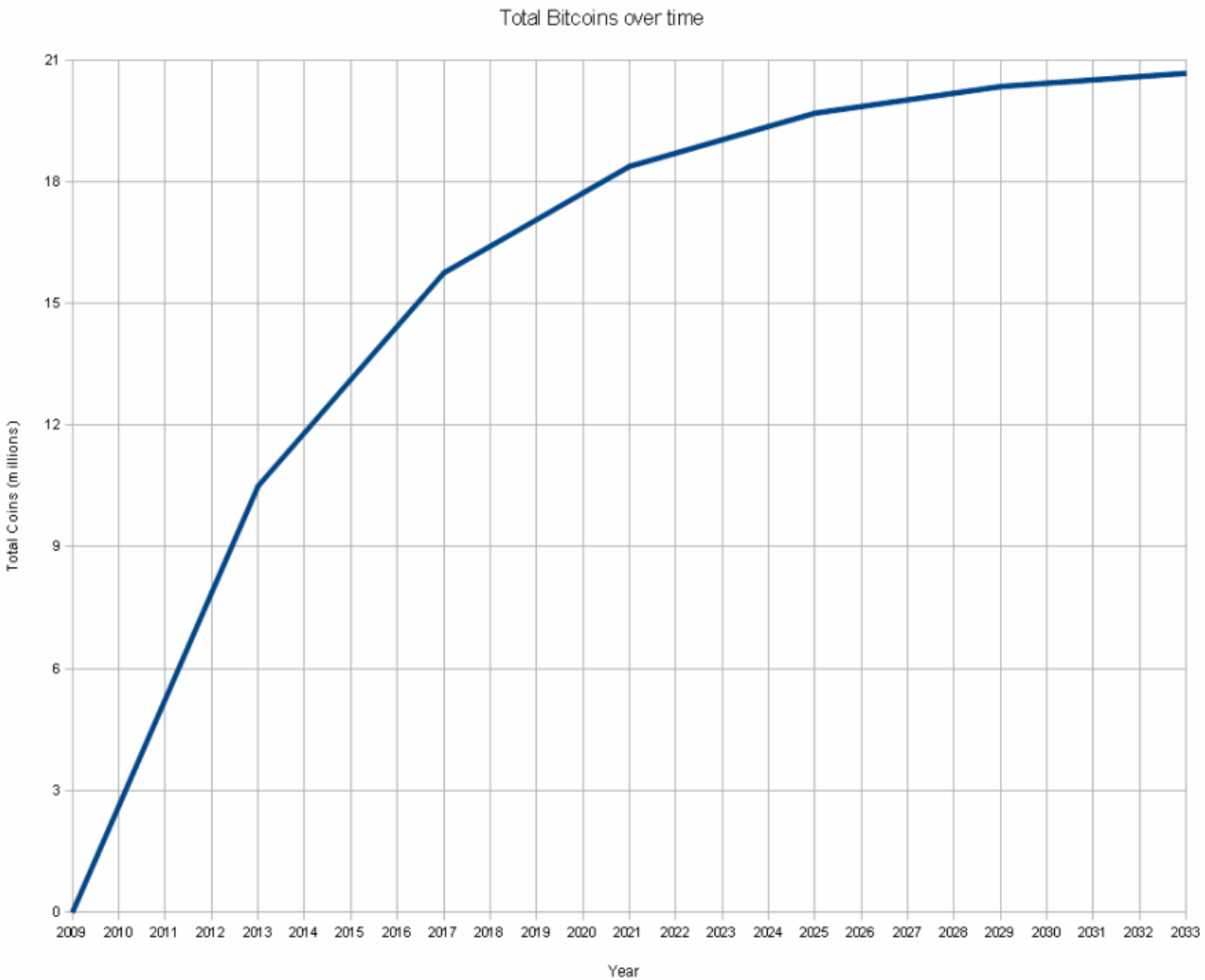
Bitcoins aus Usersicht

Technik hinter Bitcoin

Mining

Ökonomie

Zwischenfälle und Angriff-szenarien



Rechenaufwand beim Minen

Bitcoin

blueling und Deaddy

Einführung

Bitcoins aus Usersicht

Technik hinter Bitcoin

Mining

Ökonomie

Zwischenfälle und Angriff-szenarien

- mit steigender Rechenleistung des Gesamtnetzes erhöht sich langfristig nicht die Anzahl der generierten Coins ($6 \cdot 50 BTC/h$)
- Grenzkosten für die Profitabilität liegen bei den Energiekosten (bei aktuellem Kurs von etwa \$15 pro BTC bleibt Mining bis \$108k Energiekosten für das gesamte Netz profitabel)
- derzeit verwenden Miner hauptsächlich GPUs
- wegen Energieffizienz demnächst vermutlich hauptsächlich über dedizierte ASICs oder FPGAs

Typisches Mining-Rig

Bitcoin

blueling und Deaddy

Einführung

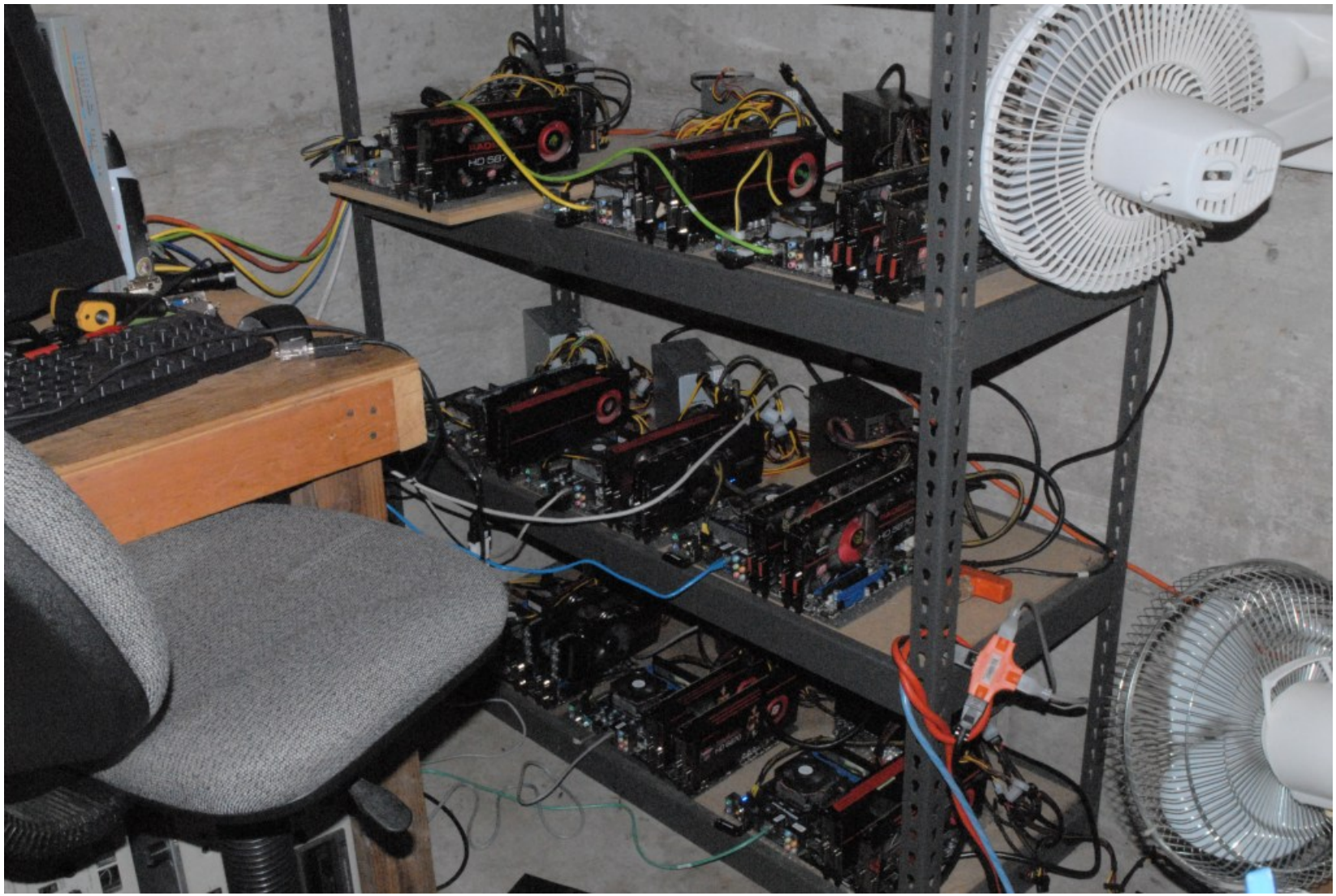
Bitcoins aus Usersicht

Technik hinter Bitcoin

Mining

Ökonomie

Zwischenfälle und Angriff-szenarien



Weniger wirtschaftliches Mining-Rig

Bitcoin

blueling und Deaddy

Einführung

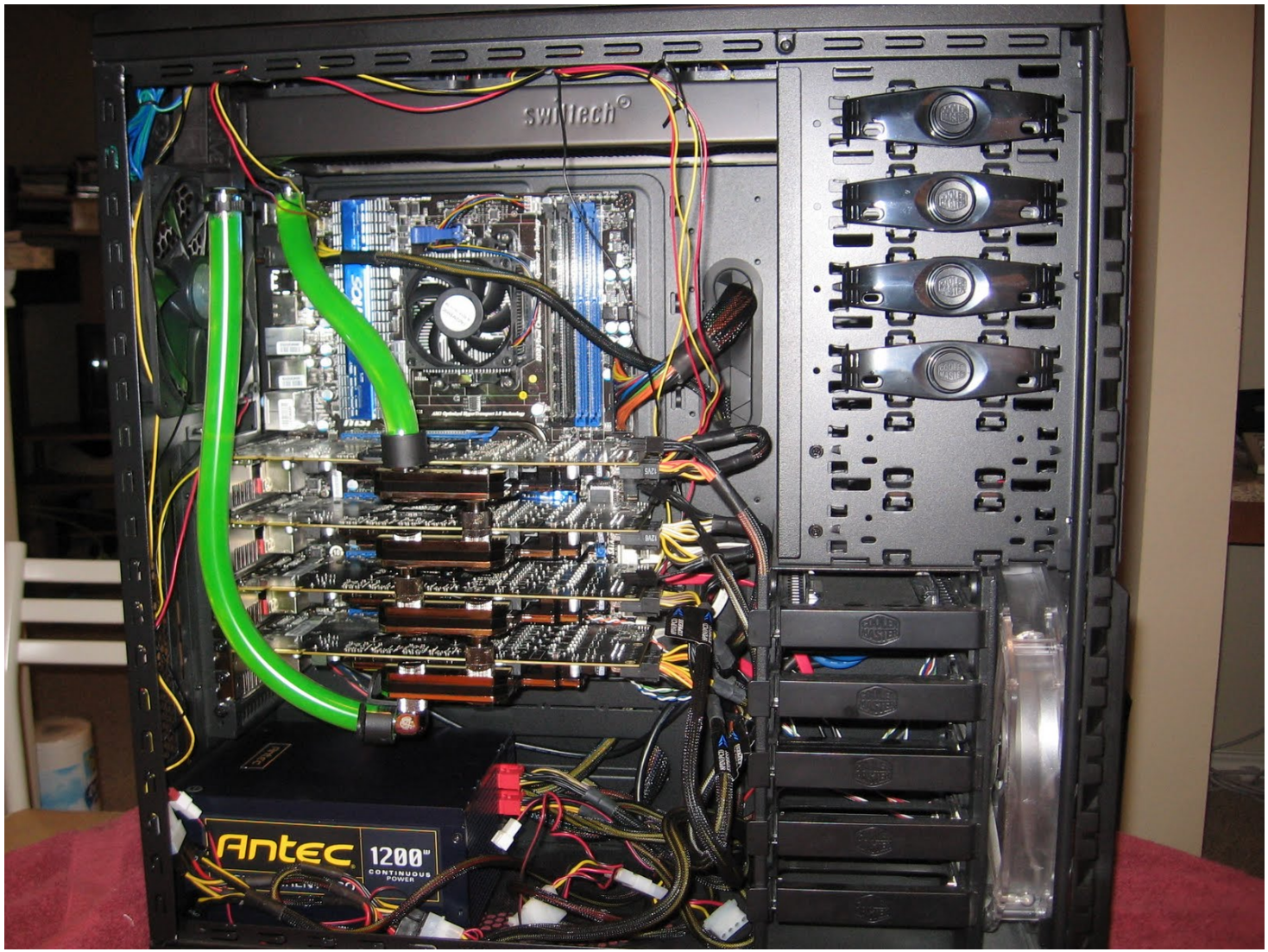
Bitcoins aus Usersicht

Technik hinter Bitcoin

Mining

Ökonomie

Zwischenfälle und Angriff-szenarien



Preis-Leistungs-Sieger (Rackmount)

Bitcoin

blueling und Deaddy

Einführung

Bitcoins aus Usersicht

Technik hinter Bitcoin

Mining

Ökonomie

Zwischenfälle und Angriff-szenarien

Kooperatives Minen im Pool

Bitcoin

blueling und Deaddy

Einführung

Bitcoins aus Usersicht

Technik hinter Bitcoin

Mining

Ökonomie

Zwischenfälle und Angriff-szenarien

- je größer das Netzwerk, desto schwieriger wird es für den einzelnen einen Block zu finden
  $\Rightarrow$ Zusammenschluss in Mining-Pools
- findet ein Teilnehmer einen Block, werden alle Poolteilnehmer proportional zur eingebrachten Rechenleistung entlohnt; es fällt ggf. eine Poolgebühr im einstelligen Prozentbereich an
- unabhängig von Pool- oder Solomining ist der durchschnittliche
  $Ertrag/h \approx \frac{eigeneHashleistung}{gesamteHashleistungdesNetzes} \cdot 6 \cdot 50BTC/h$
- mit steigender Poolgröße wird die Varianz des Ertrags reduziert, auf lange Sicht wird der Gesamtertrag aber kaum geändert (nur Poolgebühren und evtl. Grenzeffekte wenn die generierten Coins gegen 0 gehen)

Hashrate-Verteilung

Bitcoin

blueling und Deaddy

Einführung

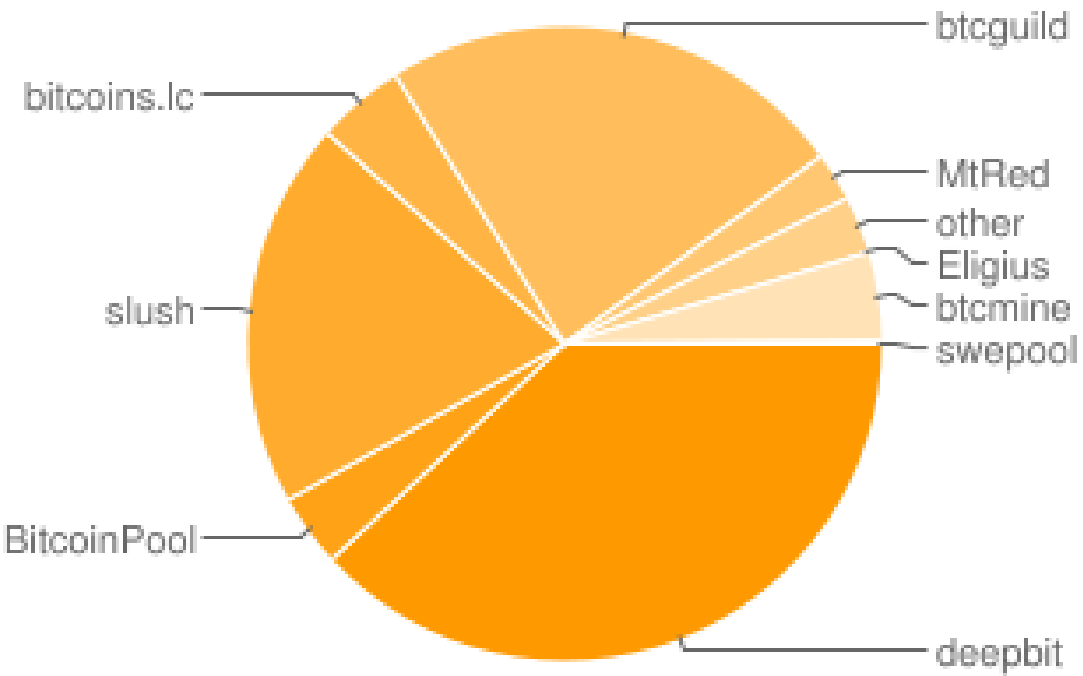
Bitcoins aus Usersicht

Technik hinter Bitcoin

Mining

Ökonomie

Zwischenfälle und Angriff-szenarien



Kann man mit Mining reich werden?

Bitcoin

blueling und Deaddy

Einführung

Bitcoins aus Usersicht

Technik hinter Bitcoin

Mining

Ökonomie

Zwischenfälle und Angriff-szenarien

Kann man mit Mining reich werden?

Bitcoin

blueling und Deaddy

Einführung

Bitcoins aus Usersicht

Technik hinter Bitcoin

Mining

Ökonomie

Zwischenfälle und Angriff-szenarien

- Early Adopters haben definitiv profitiert; risikoreich für Neueinsteiger
- Energiekosten drücken den Gewinn
- Beispiel-Miner mit 2 HD 5850 hat etwa tägliche Stromkosten von 1,50 EUR, generiert derzeit 0.35 BTC pro Tag, das entspricht etwa 3,50 EUR, es bleiben also nur 2€ Gewinn pro Tag (Stand 08. Juli)
- aktueller Mining-Tagesertrag lässt sich nicht extrapolieren: Preis treibt Difficulty

Entwicklung der Mining-Leistung

Bitcoin

blueling und Deaddy

Einführung

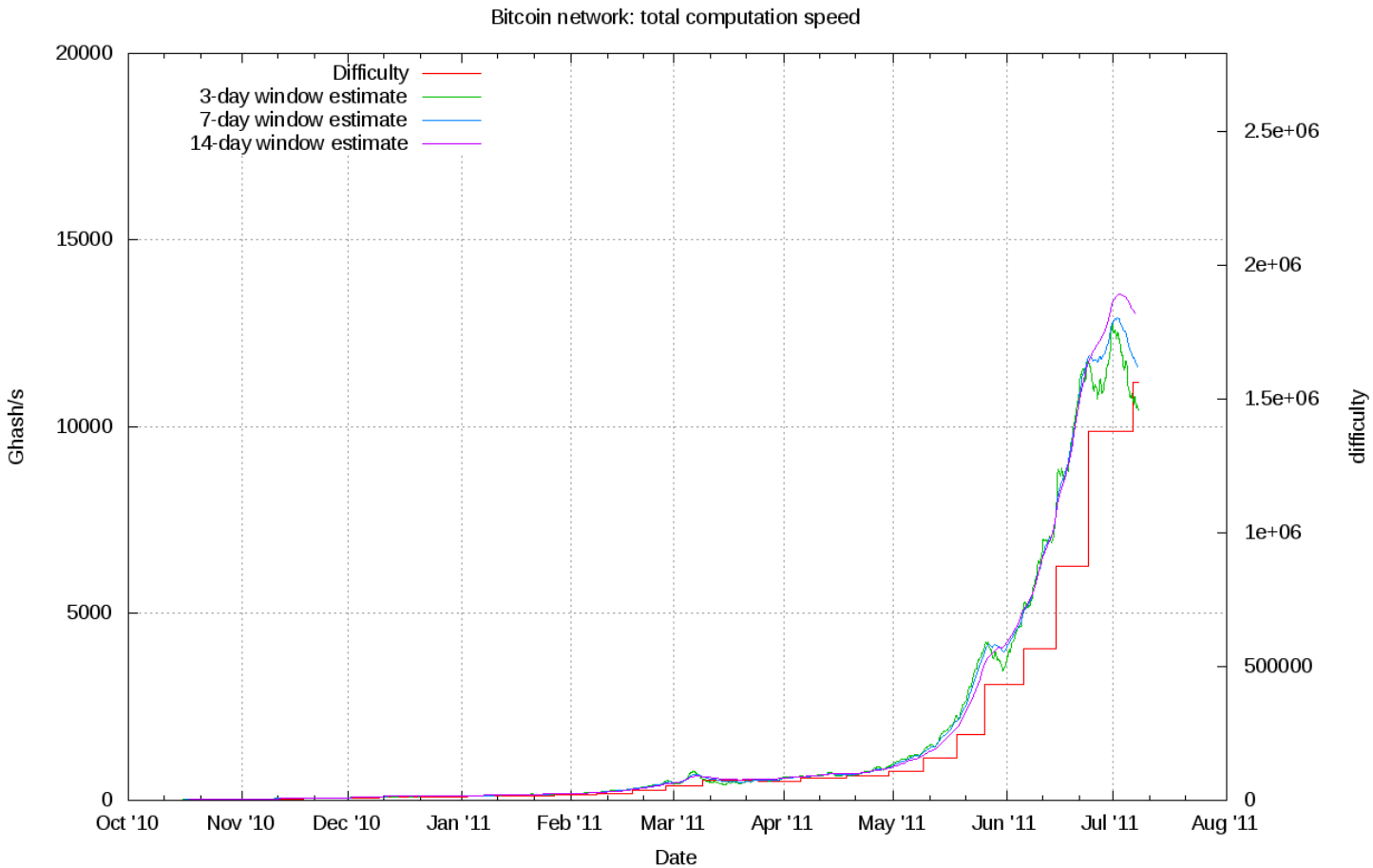
Bitcoins aus Usersicht

Technik hinter Bitcoin

Mining

Ökonomie

Zwischenfälle und Angriff-szenarien



Kann man mit Mining reich werden?

Bitcoin

blueling und Deaddy

Einführung

Bitcoins aus Usersicht

Technik hinter Bitcoin

Mining

Ökonomie

Zwischenfälle und Angriff-szenarien

- dedizierte FPGA/ASIC-Miner-Boards in Aussicht
- GPU vs. CPU Energieeffizienz liegt bei 10:1
  ASIC vs. GPU vermutlich auch
- wer auf steigende Preise hofft, kann BTCs besser kaufen als sie selbst zu minen
- Mining aus Spaß an der Freude (vgl. Folding@Home, SETI@home) ist natürlich immer möglich

Erste Aussteiger

Bitcoin

blueling und Deaddy

Einführung

Bitcoins aus Usersicht

Technik hinter Bitcoin

Mining

Ökonomie

Zwischenfälle und Angriff-szenarien

- Mining-Rig-Verkäufe nehmen zu

Outline

1 Einführung

2 Bitcoins aus Usersicht

3 Technik hinter Bitcoin

4 Mining

5 Ökonomie

6 Zwischenfälle und Angriffszenarien

Währungsentwicklung - eine Blase?

Bitcoin

blueling und Deaddy

Einführung

Bitcoins aus Usersicht

Technik hinter Bitcoin

Mining

Ökonomie

Zwischenfälle und Angriff-szenarien

Währungsentwicklung in Zahlen

Bitcoin

blueling und Deaddy

Einführung

Bitcoins aus Usersicht

Technik hinter Bitcoin

Mining

Ökonomie

Zwischenfälle und Angriff-szenarien

Zeitraum	Preis in USD
2010/10	0,06
2010/11–2011/01	0,2–0,5
2011/01–2011/04	0,5–1
2011/04–2011/06	1–30
8. Juni	31.5 (All-Time-High)
10.–11. Juni	Crash von 30 auf 15
2011/07	15

Grundlagen der Ökonomie

Bitcoin

blueling und Deaddy

Einführung

Bitcoins aus Usersicht

Technik hinter Bitcoin

Mining

Ökonomie

Zwischenfälle und Angriff-szenarien

- BTC sind ein limitiertes Gut, welches nicht nach Belieben erzeugt werden kann
- BTC lassen sich **echt übertragen**, sie werden nicht einfach nur kopiert
  $\Rightarrow$ sie eignen sich als digitales Tauschmittel
- BTC eignen sich für grenzüberschreitende Bezahlvorgänge
- Teilnahme am System für jedermann möglich

Startschwierigkeiten

Bitcoin

blueling und Deaddy

Einführung

Bitcoins aus Usersicht

Technik hinter Bitcoin

Mining

Ökonomie

Zwischenfälle und Angriff-szenarien

- Währungsfunktion hängt von anhaltender Bereitschaft „offizielles“ Geld in BTC zu tauschen ab
- Kreislauf: Kunde tauscht lokale Währung in BTC, bezahlt Gut/Dienstleistung in BTC, Händler/Anbieter tauscht BTC in lokale Währung und deckt seine Kosten
- es existieren kaum Angebote mit fixen BTC-Preisen, Bezugsgröße sind Preise in USD, EUR etc.

Essen für BTC

Bitcoin

blueling und Deaddy

Einführung

Bitcoins aus Usersicht

Technik hinter Bitcoin

Mining

Ökonomie

Zwischenfälle und Angriff-szenarien

Hardware für BTC

Bitcoin

blueling und Deaddy

Einführung

Bitcoins aus Usersicht

Technik hinter Bitcoin

Mining

Ökonomie

Zwischenfälle und Angriff-szenarien

Exchanges

Bitcoin

blueling und Deaddy

Einführung

Bitcoins aus Usersicht

Technik hinter Bitcoin

Mining

Ökonomie

Zwischenfälle und Angriff-szenarien

- Online-Händelsplätze mit Verrechnungskonto bei denen ähnlich wie bei Wertpapier-Online-Brokern gehandelt wird, z.B. Mt. Gox, tradeHill, bitcoin7
- Escrow-Handelsplattformen bei denen ein Orderbook, aber kein Währungskonto geführt wird, BTC-Betrag wird treuhänderisch verwaltet (Geldtransfer läuft außerhalb bspw. über Überweisungen),
  z.B. bitmarket.eu

Handel außerhalb von Exchanges

Bitcoin

blueling und Deaddy

Einführung

Bitcoins aus Usersicht

Technik hinter Bitcoin

Mining

Ökonomie

Zwischenfälle und Angriff-szenarien

- neben Überweisungen sind anonyme Barzahlungen oder Bargeld-Versand per Brief gängig
- OTC Handel per IRC-Channel #bitcoin-otc-foyer auf freenode.net
- Vereinzelt existieren BTC-Meetups/User groups/Stammtische
- Hacker/Geeks Deines Vertrauens

Beispiel: Mt. Gox

Bitcoin

blueling und Deaddy

Einführung

Bitcoins aus Usersicht

Technik hinter Bitcoin

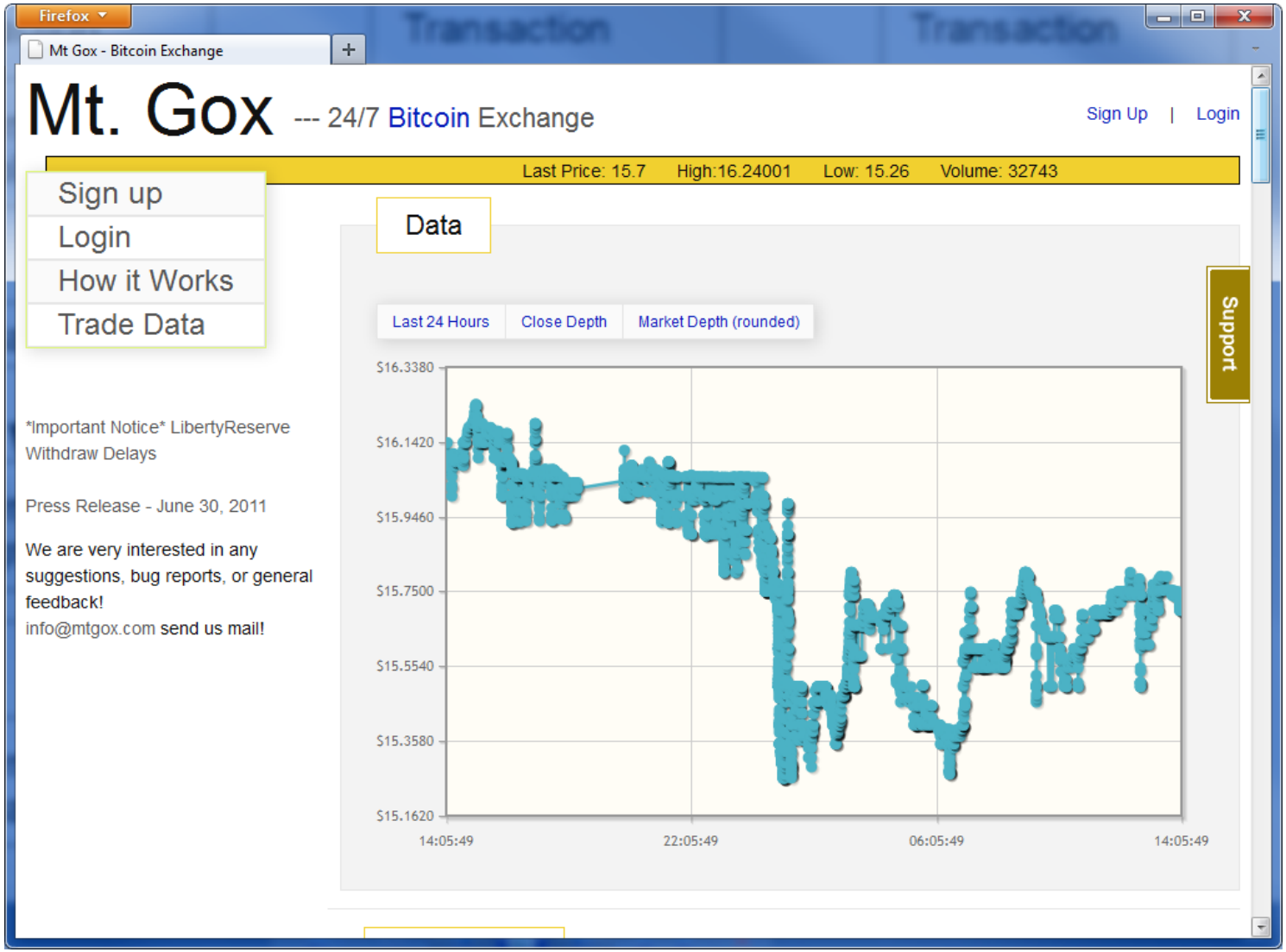
Mining

Ökonomie

Zwischenfälle und Angriff-szenarien

- Mt. Gox wird von Tibanne Co. Ltd. (Japan) betrieben, EUR SEPA Überweisungen laufen aber von/zu einem Konto in Frankreich und werden zum EZB-Kurs in USD getauscht
- teils wird eine API (RESTful) für eigene automatische Handelssysteme angeboten
- Angebot soll für Trader ausgeweitet werden: Margin- und Optionshandel, Leerverkäufe etc.; derzeit hauptsächlich nur primitive Limit-Orders möglich
- keine Verträge oder Sicherheiten

Mt. Gox Webseite



Deflation

Bitcoin

blueling und Deaddy

Einführung

Bitcoins aus Usersicht

Technik hinter Bitcoin

Mining

Ökonomie

Zwischenfälle und Angriff-szenarien

- Bitcoins sind ein Gegensatz zu gängigen Fiat-Währungen, die vom Staat per Beschluss erzeugt und gewollt inflationiert werden
- inflationäre Fiat-Währungen (unser Weltwährungssystem) sind wegen des exponentiellen Wachstums nicht aufrechtzuerhalten

USD-Geldmenge

Bitcoin

blueling und Deaddy

Einführung

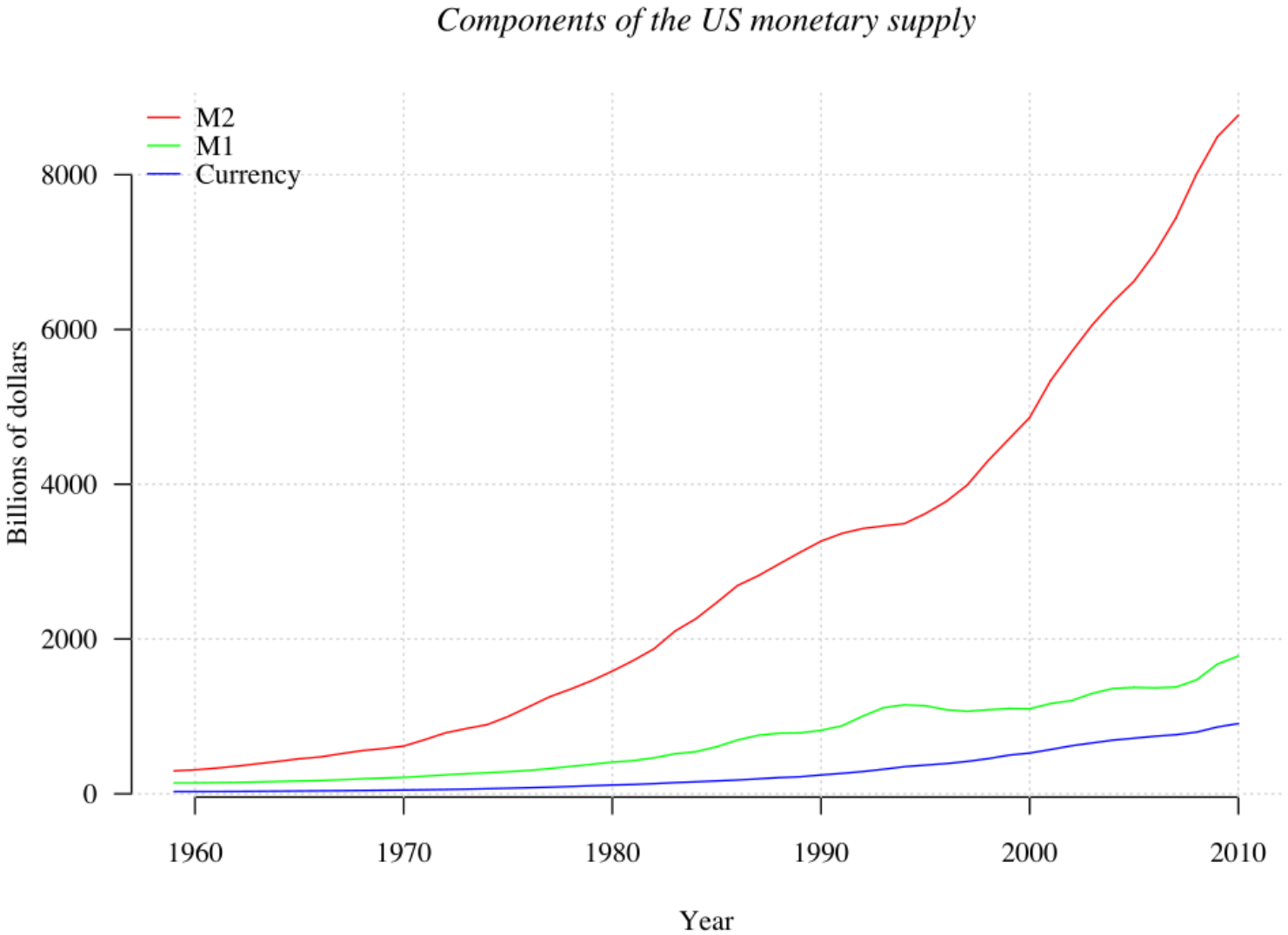
Bitcoins aus Usersicht

Technik hinter Bitcoin

Mining

Ökonomie

Zwischenfälle und Angriff-szenarien



Wirtschaftliche Kritik an BTC

Bitcoin

blueling und Deaddy

Einführung

Bitcoins aus Usersicht

Technik hinter Bitcoin

Mining

Ökonomie

Zwischenfälle und Angriff-szenarien

- BTC-Geldmenge kann nicht durch zentrale Instanz angepasst werden (vgl. rohstoffgedeckte Währung)
- Deflationsspirale befürchtet: bei steigender Kaufkraft der Währung leiden Schuldner
- Folgen: Horten von BTC als Wertaufbewahrungs- oder Spekulationsobjekt, Kaufzurückhaltung
- Kreditvergabe und Fractional Banking auch mit BTC möglich

Rechtslage

Bitcoin

blueling und Deaddy

Einführung

Bitcoins aus Usersicht

Technik hinter Bitcoin

Mining

Ökonomie

Zwischenfälle und Angriff-szenarien

- kein staatlich anerkanntes oder verbindliches Zahlungsmittel
- noch keine Präzedenzfälle bekannt
- Stress mit dem Finanzamt vorprogrammiert
- steuerlich vermutlich keine Währung, sondern Ware
  $\Rightarrow$ MwSt. muss abgeführt werden

Legalität

Bitcoin

blueling und Deaddy

Einführung

Bitcoins aus Usersicht

Technik hinter Bitcoin

Mining

Ökonomie

Zwischenfälle und Angriff-szenarien

- im privaten Bereich ist der gelegentliche Handel vmtl. bis 600 €/Jahr steuerfrei (§23 EStG)
- fraglich: ist der Handel mit BTC aktive Teilnahme an organisierter Geldwäsche?
- Interessenlage des Staates bzgl. BTC dürfte klar sein

Outline

1 Einführung

2 Bitcoins aus Usersicht

3 Technik hinter Bitcoin

4 Mining

5 Ökonomie

6 Zwischenfälle und Angriffszenarien

Overflow Bug (15. August 2010)

Bitcoin

blueling und Deaddy

Einführung

Bitcoins aus Usersicht

Technik hinter Bitcoin

Mining

Ökonomie

Zwischenfälle und Angriff-szenarien

- Block 74638 enthielt eine TX, die für zwei Adressen insgesamt 184 Milliarden BTC erzeugte
- Blockchain musste geforked werden
- trotz einiger ungepatchter Nodes überholte die neue Chain schließlich die mit der Fehlbuchung

Mt. Gox-Hack (25. Juni 2011)

Bitcoin

blueling und Deaddy

Einführung

Bitcoins aus Usersicht

Technik hinter Bitcoin

Mining

Ökonomie

Zwischenfälle und Angriff-szenarien

- BTC-Kurs fiel innerhalb weniger Minuten von USD 17,5 auf USD 0,01
- offizielle Ursache: Konto mit administrativem Zugriff (von jemandem der als externer Audits durchführt) wurde kompromittiert und ermöglichte die Ausschüttung sehr vieler, nur in der Datenbank von Mt. Gox existierender Bitcoins
- kurz darauf war eine .csv-Datei mit allen Mt. Gox-Accounts für jeden herunterladbar

Folgen des MT. Gox-Hacks

Bitcoin

blueling und Deaddy

Einführung

Bitcoins aus Usersicht

Technik hinter Bitcoin

Mining

Ökonomie

Zwischenfälle und Angriff-szenarien

- Handel wurde eine Woche eingestellt, es wurde ein Rollback der Transaktionen durchgeführt, Mt. Gox ersetzte die 1000 BTC die vom Angreifer ausgezahlt werden konnten aus eigener Tasche
- Handel startete erstaunlich ruhig wieder; Trading-API erst einige Tage später wieder voll funktionstüchtig
- „goxed“ bürgerte sich als Meme in der Bitcoin-Community ein

Kurs/Volumen während des Hacks

Bitcoin

blueling und Deaddy

Einführung

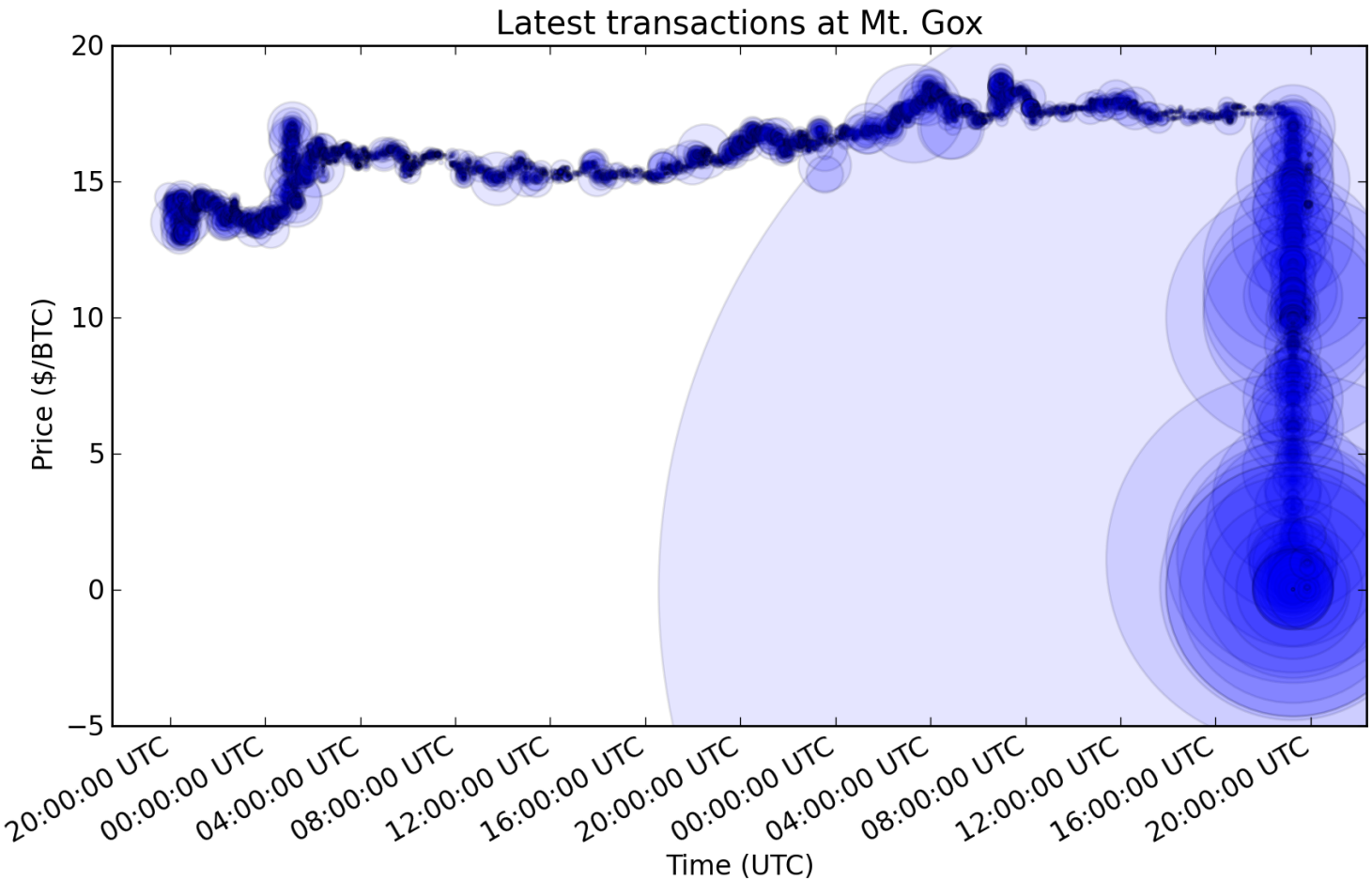
Bitcoins aus Usersicht

Technik hinter Bitcoin

Mining

Ökonomie

Zwischenfälle und Angriff-szenarien



Huch

Bitcoin

blueling und Deaddy

Einführung

Bitcoins aus Usersicht

Technik hinter Bitcoin

Mining

Ökonomie

Zwischenfälle und Angriff-szenarien

accounts.csv - OpenOffice.org Calc

Datei Bearbeiten Ansicht Einfügen Format Extras Daten Fenster Hilfe

Arial 10

A32825:AMJ32825 Deaddy

	A	B	C	D
32813	32809	FrankLucas		1a9bOf6Y1$fRtc6kfBcjnTA94g.zy3d1
32814	32810	coinforeal	bob1111777@yahoo.com	1tk9c8buG$4UvqWR7nyFI.LEa7h0KSd.
32815	32811	drknexus	drknexus+mtgox@gmail.com	1TFhJeBSH$g.ahuuR.6uGDncxPRoa/e.
32816	32812	ppbay		1/kjjt25H$NweZfp4A0JNVYvGUs1UST/
32817	32813	newcoin4411	bob1111777@yahoo.com	1.GIkBbQP$w9Hu8wty/NAf30aOQZ1Zc0
32818	32814	k65onyx	k65onyx@gmail.com	1RvahwEap$rQtovJ3JCq6ltlClk432p1
32819	32815	springcoin	bob1111777@yahoo.com	1ftUo4HBK$mlot9hPo/9wp2lLsp.ncX0
32820	32816	springcoin7711	bob1111777@yahoo.com	1a1laclJu$8eg0SVUS.z2SKxCtBm.1f1
32821	32817	Peter1969		1XKBVjn6G$SvlN5VHD.NYGH1cC7LR8z1
32822	32818	barfoo411	barfoo411@gmail.com	1ay0FFBPs$srunZ.gOjYyZiJoEbFdP9.
32823	32819	Peter1969_		1NiMq7x6W$lMCmu7XW6lxkDM49m4Kdj.
32824	32820	EscapingYou	software@thunold.no	1gbLeK4GQ$zdL3kW0jAssruikJs3KLu/
32825	32821	Deaddy	koksvernichter@googlemail.com	1m/Q1cUVV$Lv.UPrufKxKzeZN7ZnAsl0
32826	32822	Nephelim	fischl@gmx.de	1nfWFT8xM$OYhOXnV3mj40ioWxWpJyL.
32827	32823	cergmu	cergmu@gmail.com	1hhHdilOz$DPb7Dnw1dRURMM72gRM23.
32828	32824	michoo	m.wolniak@gmail.com	1MoZKtc6Z$VAJf.Lu/gHYIRHHTYOcc71
32829	32825	gelraen	gelraen.ua@gmail.com	1AihQ/Nhl$QUY0lRfoUyS2kZcl04NT41
32830	32826	pwnz		1Hn5rpCmq$znj.3tOr.pttAR86KvNI31
32831	32827	hajons	hajons@gmail.com	1PE25jjwb$SPvXDQlWOm7dlkj7Lcjs4.
32832	32828	lpc13	paomic@gmail.com	1di8/xAZR$Ri/Ys1ux5yzC6v47ILdWn.
32833	32829	globexminer	feech@mail.ru	1sFbddB9D$1QWsjBJ6VdDQBKy1QHF0t.
32834	32830	jestlluka	jestlluka@gmail.com	$1$9lM6lq4l$693tW51SNAJeQR3/6lLH1/
32835	32831	duy1124	hardin_pham@yahoo.com	1hbvWEX5g$zkaOSdfwxCmgPlyGAopn.
32836	32832	mattacis1010	zanpmatt@gmail.com	1WPKZECJ8$sAbxNVHEFauf.zuoVxH4E.
32837	32833	vinky1	woutervinkenborg@gmail.com	1cosFSpfu$2mFKml/9fko3YnHgCWwCG0

Tabelle1

Tabelle 1 / 1 Standard STD * Summe=32821 100%

Weitere Angriffszenarien

Bitcoin

blueling und Deaddy

Einführung

Bitcoins aus Usersicht

Technik hinter Bitcoin

Mining

Ökonomie

Zwischenfälle und Angriff-szenarien

- Timejacking: durch das Einhashen einer falschen Netzwerkzeit (eine Node verwirft Blöcke erst ab 2h Diskrepanz zur eigenen Zeit) kann man ggf. einzelne Nodes mit einer falschen Blockchain isolieren und falls man es schafft, dem Client 6 falsche Blöcke zu senden, würden Transaktionen als bestätigt erscheinen
- Cancer Nodes: mit sehr vielen IPs die sich in den höchsten 16 Bits unterscheiden kann man im IRC-Bootstrap-Channel ein Netzwerk aus bösen Clients aufbauen, mit welchem man zumindest störende Aktionen fahren kann

Quellen und Links

Bitcoin

blueling und Deaddy

Einführung

Bitcoins aus Usersicht

Technik hinter Bitcoin

Mining

Ökonomie

Zwischenfälle und Angriff-szenarien

- `http://www.bitcoin.org/` – Hauptseite des Projekts: Infos, Wiki, Forum
- `http://blockexplorer.com/` – Überweisungen tracken etc.
- `http://www.weusecoins.com/` – Erklärung von Bitcoin für Non-Geeks
- `http://bitcoin.sipa.be/` – Bitcoin Network Charts
- `http://bitcoincharts.com/` – Marktübersicht