

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

Warpzone

2011-07-09

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

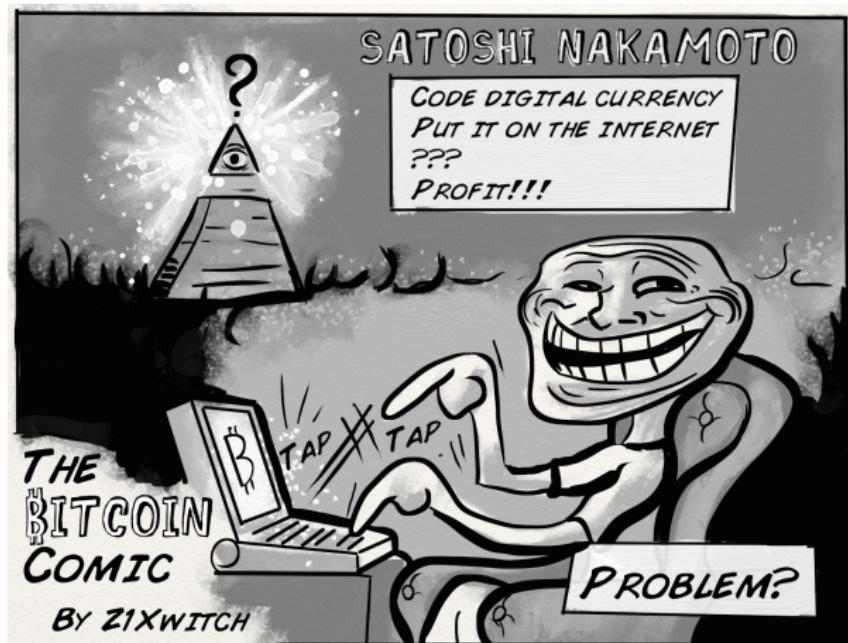
Bitcoins aus
Usersicht

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

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

The screenshot shows the Bitcoin client interface on a Windows operating system. The window title is "Bitcoin". The menu bar includes "Datei", "Einstellungen", and "Hilfe". Below the menu is a toolbar with icons for "Überweisen" (Send), "Adressbuch" (Address Book), and other functions. A status bar at the bottom displays "0 Verbindungen", "133399 Blöcke", and "11 Überweisungen".

The main area contains the following information:

- Ihr Bitcoin-Adresse: 178LoY9HPQE9P8zFFhLHAzMY4CeGsZZ47E
- Kontostand: 13.378
- Buttons: "Neu ...", "in die Zwischenablage kopiere"
- Tab navigation: "Alle Überweisungen" (selected), "Überwiesen/Erhalten", "Überwiesen", "Erhalten".
- Table of transactions:

Status	Datum	Beschreibung	Belastungen	Gutschriften
145 Bestätigungen	25.06.2011 21:34	Empfangen durch: 17aBMHGDnumtCQQZ9BVNVthyV...	+3.00	
1898 Bestätigung...	18.06.2011 00:15	An: 1QDawofANwJAP5vzl8TjtXdf8CQSS4J4Gt	-0.0105	
1900 Bestätigung...	18.06.2011 00:20	Empfangen durch: 1EKS4fMr3PCYsXqkpwTqw7BmM1...	+10.00	
1945 Bestätigung...	17.06.2011 17:13	An: 1NsFNk9nq8h5XnzHLdwLL7ysK63F69NJt4	-1.0005	
1989 Bestätigung...	17.06.2011 11:51	An: 1MdEk239UBAvDH6mpkcb3jzAYH6CNnUaYZ	-0.0105	
2127 Bestätigung...	16.06.2011 19:13	Empfangen durch: 1EzLaruUXnP6WGJSnSMDHRdGTS...	+0.001	
2128 Bestätigung...	16.06.2011 18:54	Empfangen durch: 1EzLaruUXnP6WGJSnSMDHRdGTS...	+0.01	
2134 Bestätigung...	16.06.2011 18:17	An: 1Cvr8AsCfbvBQ2xoWiFD1Gb2VrbGsEf28	-0.1005	
2134 Bestätigung...	16.06.2011 18:08	An: 12c27jloQ4JdxRhgdgNex3foXMW2QxvJ9Y	-0.0105	
2140 Bestätigung...	16.06.2011 17:08	An: 1MdEk239UBAvDH6mpkcb3jzAYH6CNnUaYZ	-1.0005	
2147 Bestätigung...	16.06.2011 16:04	Empfangen durch: 1MJZc4cjFP63dvrJSxrDTyqjanew...	+2.50	

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 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 $\mu\text{₿} = 100 \text{ Satoshi}$

Transaktionen

Bitcoin

blueling und
Deaddy

Einführung

Bitcoins aus
Usersicht

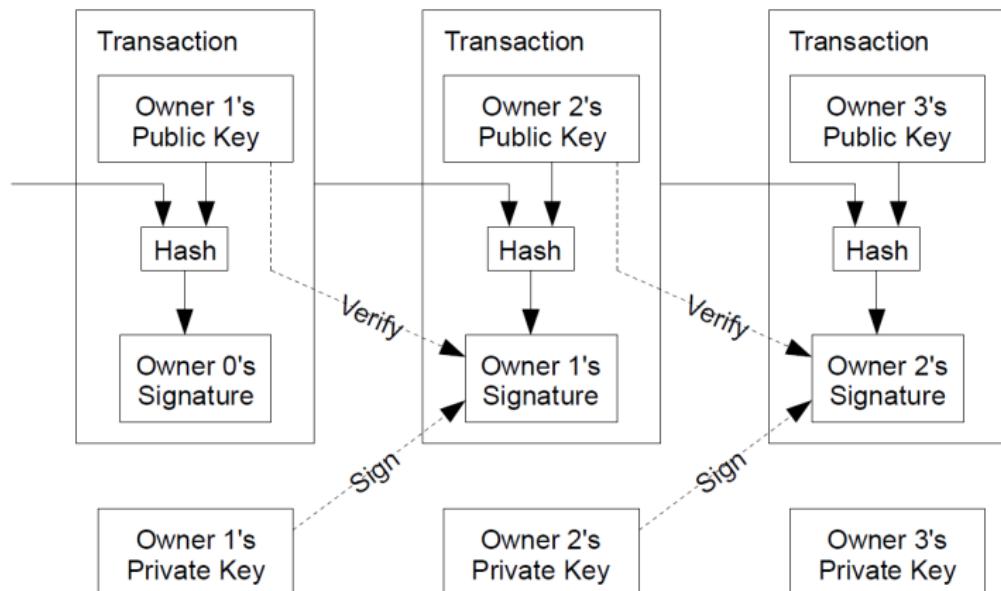
Technik hinter
Bitcoin

Mining

Ökonomie

Zwischenfälle
und Angriffs-
szenarien

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“ verhindert erfordert Klärung der chronologischen Abfolge von Transaktionen
- vor Bitcoins setzte dies eine vertrauenswürdige Zentralinstanz voraus

Wie löst man das dezentral?

Lösung: Distributed timestamp server

Bitcoin

blueling und
Deaddy

Einführung

Bitcoins aus
Usersicht

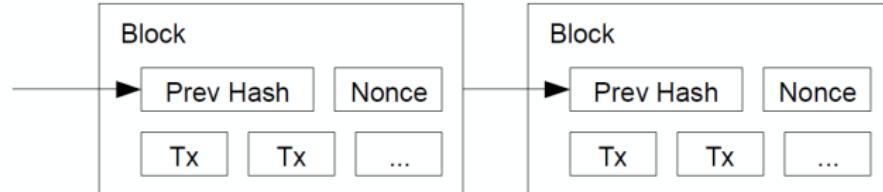
Technik hinter
Bitcoin

Mining

Ökonomie

Zwischenfälle
und Angriff-
szenarien

- 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 einerNonce 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

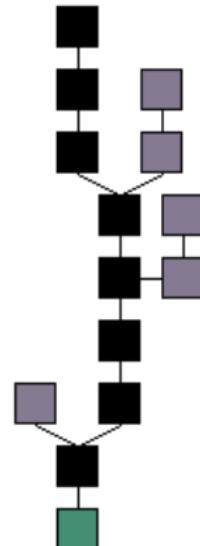
Technik hinter
Bitcoin

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 $q \geq p$

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

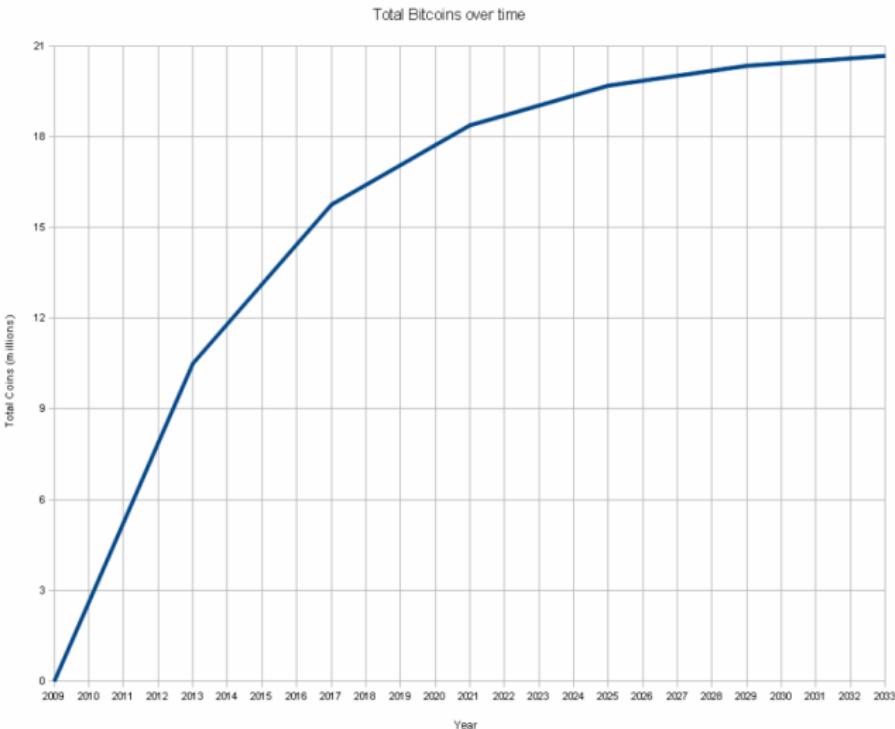
Bitcoins aus
Usersicht

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 ($6 \cdot 50BTC/h$)
- 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 Energieeffizienz demnächst vermutlich hauptsächlich über dedizierte ASICs oder FPGAs

Typisches Mining-Rig

Bitcoin

blueling und
Deaddy

Einführung

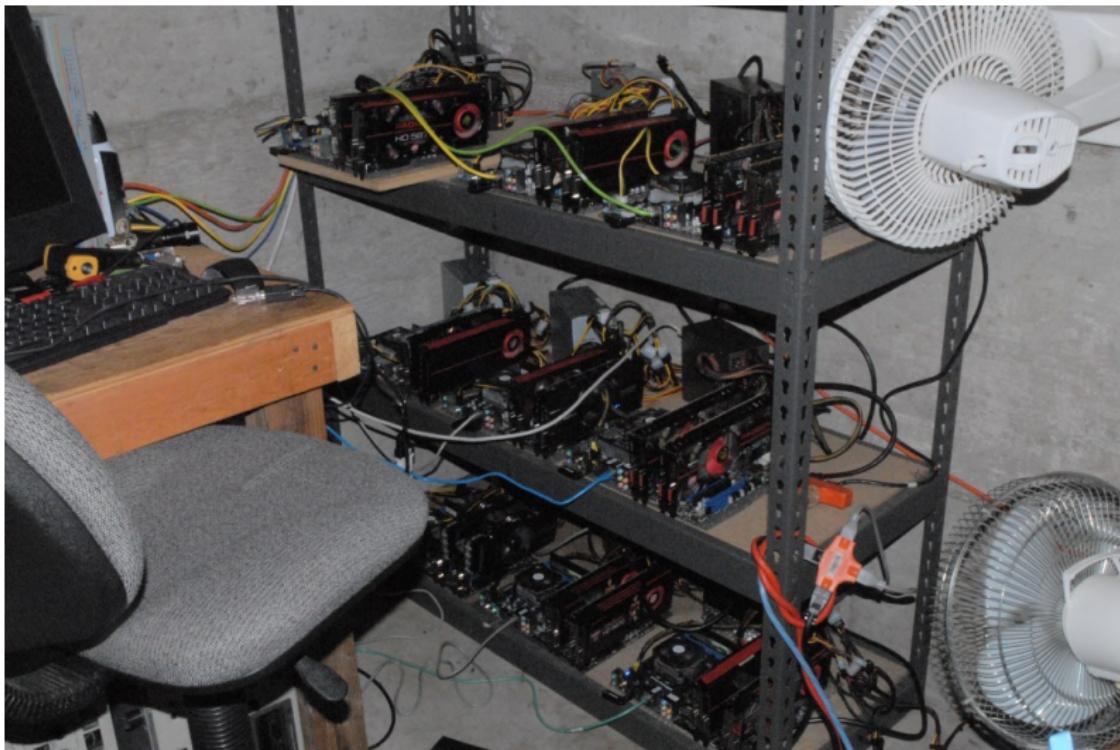
Bitcoins aus
Usersicht

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

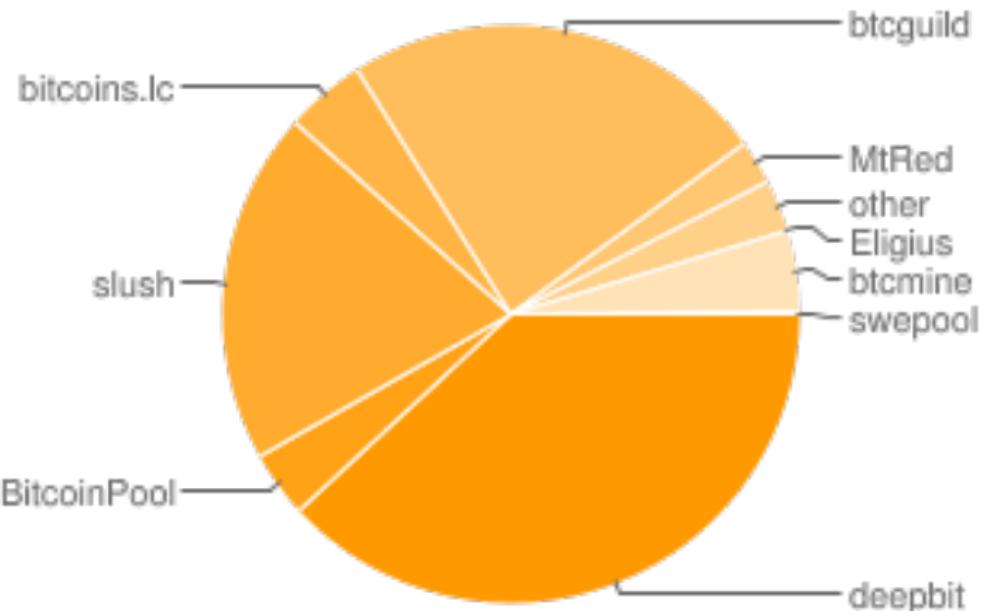
Mining

Ökonomie

Zwischenfälle
und Angriff-
szenarien

- je größer das Netzwerk, desto schwieriger wird es für den einzelnen einen Block zu finden
⇒ 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
$$\text{Ertrag}/h \approx \frac{\text{eigeneHashleistung}}{\text{gesamteHashleistungdesNetzes}} \cdot 6 \cdot 50\text{BTC}/h$$
- 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 reichen 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 extrapoliieren: Preis treibt Difficulty

Entwicklung der Mining-Leistung

Bitcoin

blueling und
Deaddy

Einführung

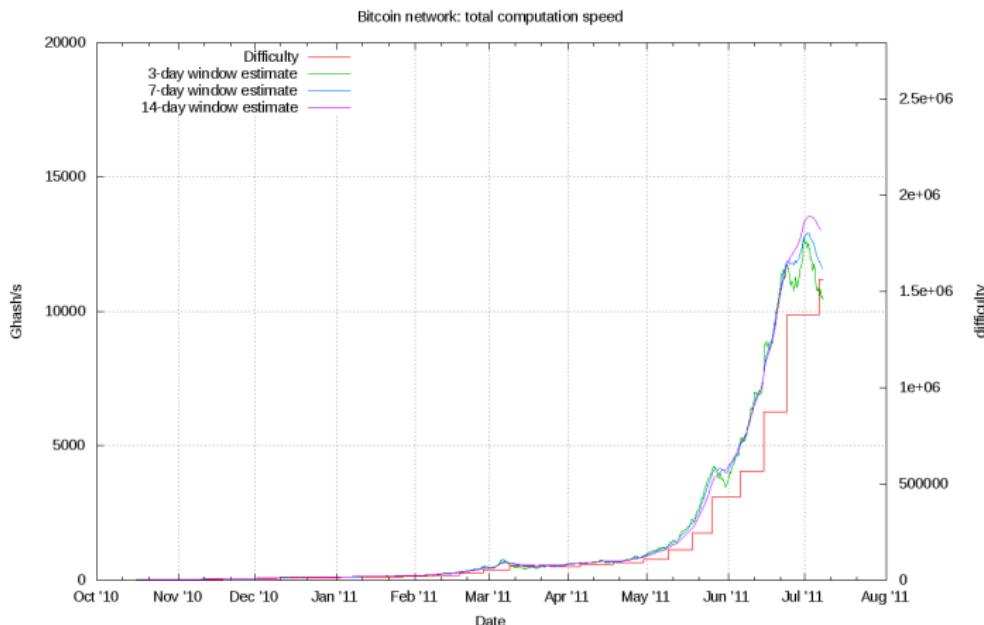
Bitcoins aus
Usersicht

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



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
⇒ es eignet sich als Tauschmittel
- BTC eignen sich für grenzüberschreitende Bezahlvorgänge
- Teilnahme am System erfordert nur Internetzugriff

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

Firefox bitmunchies

BitMunchies

Welcome to BitMunchies!

Welcome Guest! Would you like to [log yourself in?](#) Or would you prefer to [create an account?](#)

Bitmunchies is intended to provide access to goods unavailable elsewhere in the bitcoin economy. We are always looking for new products and distributors. Tell us your favorite snack, and we will find a way to get it for you!

bitmunchies.com now accepts international orders! Check out as you normally would, and you will be given international shipping options.

New Products For July

 Men's Eco Power™ Quarter Top Socks - 10 pair 1.187BTC	 Men's Eco Power® Quarter Top Socks - 10 pairs 1.187BTC	 Orville Redenbacher's Movie Theater Butter - 1 bag 0.050BTC
 Orville Redenbacher's Smart Pop! Butter - 1 bag 0.050BTC	 Welch's® Squeeze Grape Jelly - 22oz 0.164BTC	 Jif® Creamy Peanut Butter - 40 oz 0.329BTC

Categories

- Food > (189)
- Beverages > (31)
- Clothing (4)
- Medicine Cabinet > (57)
- Pipe and Smoke (1)

Manufacturers

Please Select

Quick Find

Use keywords to find the product you are looking for.
[Advanced Search](#)

What's New?

 Men's Eco Power™ Quarter Top Socks - 10 pair 1.187BTC

Information

[Shipping & Returns](#)
[Privacy Notice](#)
[About Bitcoins](#)

Cart Contents

0 items

Bestsellers

1. Freeze Dried Fruit Chips - Apple
2. Jif® Creamy Peanut Butter - 40 oz
3. Men's Eco Power™ Quarter Top Socks - 10 pair
4. Raspberry fizzy drink mix
5. Zig Zag King Size - Orange
6. Crest Extras Whitening Toothpaste
7. Nutella
8. ACT II® Butter Lovers Microwave Popcorn - 1 bag
9. Progresso® Chicken Noodle Soup
10. Chef Boyardee® Beef Ravioli

Specials

 Madras Lentils
--

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 bspw. 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

Bitcoin

blueling und
Deaddy

Einführung

Bitcoins aus
Usersicht

Technik hinter
Bitcoin

Mining

Ökonomie

Zwischenfälle
und Angriff-
szenarien

The screenshot shows the Mt. Gox Bitcoin Exchange homepage. At the top, there's a navigation bar with "Sign Up" and "Login" buttons. Below the header, a yellow bar displays the current price information: Last Price: 15.7, High: 16.24001, Low: 15.26, and Volume: 32743. A sidebar on the left contains links for "Sign up", "Login", "How it Works", and "Trade Data". The main content area features a large, interactive candlestick-style price chart titled "Data". The chart tracks the price of Bitcoin over the last 24 hours, with major ticks at \$16,3380, \$16,1420, \$15,9460, \$15,7500, \$15,5540, \$15,3580, and \$15,1620. The x-axis shows time points from 14:05:49 to 14:05:49 the next day. The chart shows significant volatility, with prices fluctuating between approximately \$15.26 and \$16.24. A "Support" button is located on the right side of the chart area.

Deflation

Bitcoin

blueling und
Deaddy

Einführung

Bitcoins aus
Usersicht

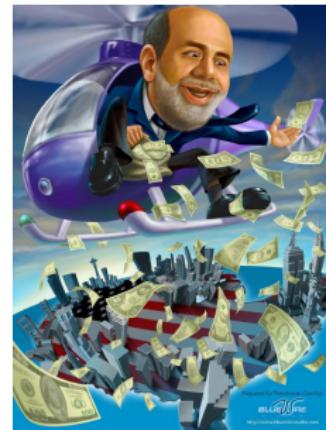
Technik hinter
Bitcoin

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

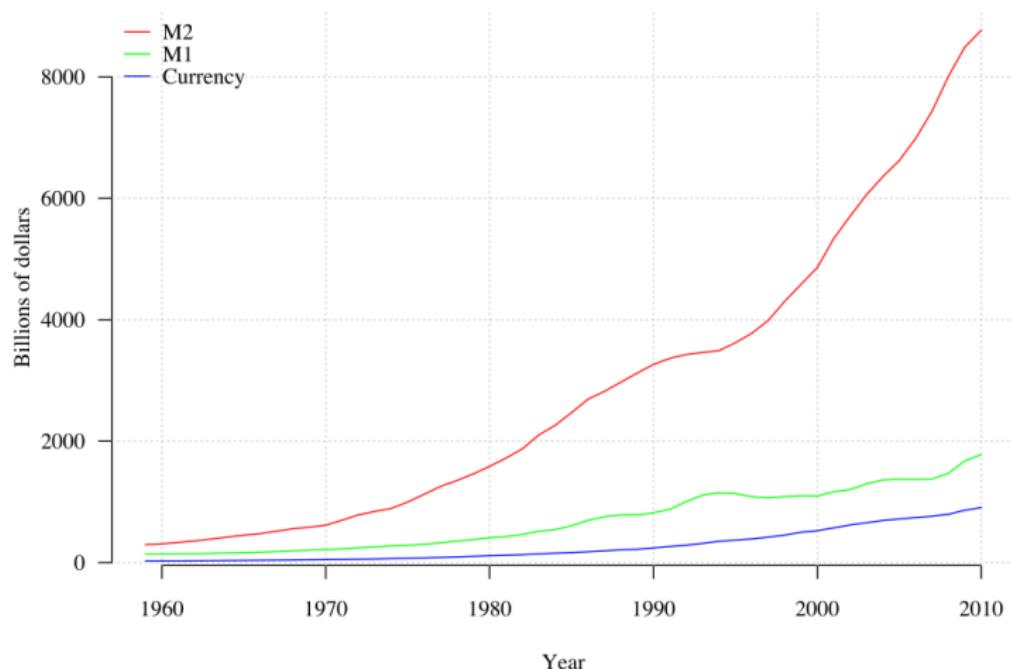
Technik hinter
Bitcoin

Mining

Ökonomie

Zwischenfälle
und Angriff-
szenarien

Components of the US monetary supply



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
⇒ 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 EUR/Jahr steuerfrei
- fraglich: ist der Handel mit BTC aktive Teilnahme an organisierter Geldwäsche?
- Interessenlage des Staates bzgl. BTC dürfte klar sein

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

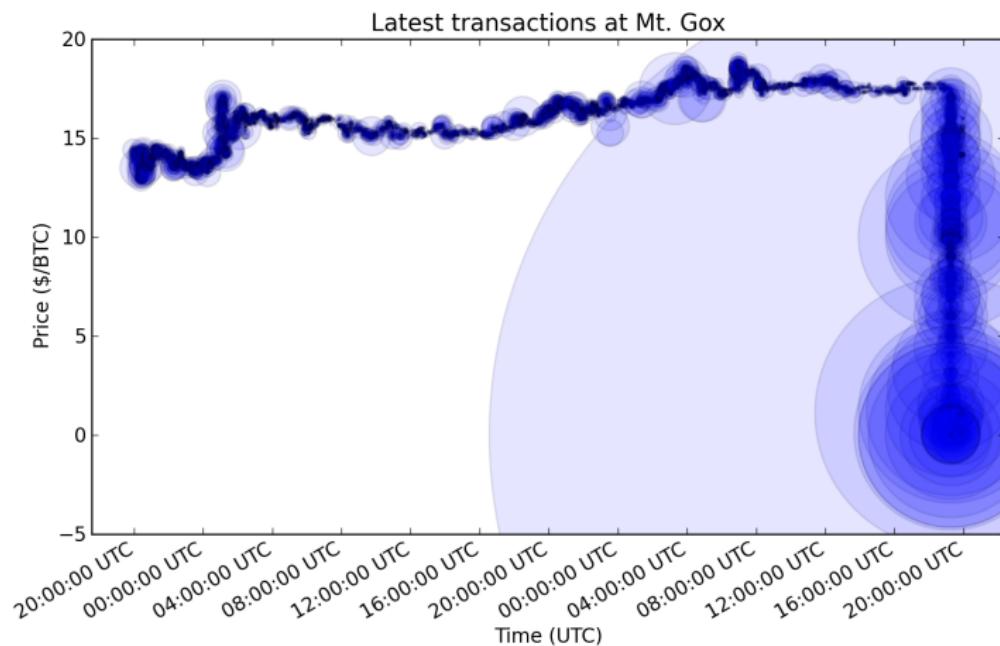
Bitcoins aus
Usersicht

Technik hinter
Bitcoin

Mining

Ökonomie

Zwischenfälle
und Angriff-
szenarien



Huch

Bitcoin

Ökonomie

Zwischenfälle und Angriff- szenarien

A	B	C	D
32813	32809 FrankLucas	bob1111777@yahoo.com	\$1\$9bOf6Y1\$Rtc6hBcjnTA94g zy3d1
32814	32810 coinform		\$1\$tk9cbuG34uvQWryFILea90Ksd.
32815	32811 drknexus	drknexus+mtnox@gmail.com	\$1\$TFhjeBSH5g ahuvR_6uGDcaRRe/e.
32816	32812 pbbay		\$1\$kj25h1SwZp2fAUjNvVYGuS1UST/
32817	32813 newcoin4411	bob1111777@yahoo.com	\$1\$GkBbQP5w9Hu8wtyNAf30a0QzC12c0
32818	32814 k65onyx	k65onyx@gmail.com	\$1\$RvhawPcap9tQovJ3Cg9nIClk432p1
32819	32815 springon	bob1111777@yahoo.com	\$1\$tuJo4Pb6n9t9hPw9y2Lsp.ncX0
32820	32816 springon7711	bob1111777@yahoo.com	\$1\$aa1acJluS8epGSUZ25KuicBm.1f1
32821	32817 Peter1969		\$1\$XKBVjnGSwINSvHD.NYGH1cCTLR8z1
32822	32818 barfoo411	barfoo411@gmail.com	\$1\$ayOFFPBp+s5un2_gOjYyZloEbfpd9
32823	32819 Peter1969		\$1\$NiMq7x6WSIMCrw7XW6lxkDM49m4Kdj.
32824	32820 EscapingYou	software@thunold.no	\$1\$gbLeK4GQSzd.3kW0\$AssruJ3sKLw
32825	32821 Deaddy	koksvemichter@googlemail.com	\$1\$mrQ1UV5Vsl_UPrufKxxzeT7NzAsI0
32826	32822 Nephelim	fischl@mx.de	\$1\$nfWT8xMoSYOhXnm3j40wVxWpJyl.
32827	32823 cermu	cermu@gmail.com	\$1\$hhHdZiQ2Dpb7Dnw1rURRM727R2M3
32828	32824 michoo	m.wolniak@gmail.com	\$1\$MoZkt623sVAjfLuJghYHRHTYOcc71
32829	32825 gerlaen	gerlaen.ua@gmail.com	\$1\$AihiQ7nh5QU10R6UyS2zL2n0T414
32830	32826 pnzw		\$1\$Hm5pnMcq5ng_3tOr ptA86K6MhI31
32831	32827 hajons	hajons@gmail.com	\$1\$PE25jwbPSw\$QDViW0m7dIjLcs4.
32832	32828 pc13	paomic@gmail.com	\$1\$di9yA2RSRyYs1ux5yzC6w47LdWn
32833	32829 globexminer	feech@mail.ru	\$1\$afbdd9S051QWsjB6U6DQBkY1QHF0.
32834	32830 jestiluka	jestiluka@gmail.com	\$1\$9lM6lqI5693tW151NAjeQR3/61LH/
32835	32831 duy1124	hardin.pham@yahoo.com	\$1\$hbWEX5g5kaSdfwXcmgPlVgAopn.
32836	32832 mattacris1010	zanpmatt@gmail.com	\$1\$WPkFCEJB83sAbxtVHEauf.zuo1xh4E.
32837	32833 woutervenkenborg@gmail.com	woutervenkenborg@gmail.com	\$1\$cosfSpuf5mFKml/9fk3yNgVwgCwG0
32838	32834 p002100		\$1\$2D7M...OGC1...7V9...11CMh...8D0

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