Überblick - Anonymität (- ZeroCoin)

Seminar: Electronic Identity
Dozent: Dr. Wolf Müller
Vortragende: Björn G. , Markus Waas

13.12.2013

BITCOIN OWNERS

What my friends think I do

What my mom thinks I do

What society thinks I do

What Politicians think I do

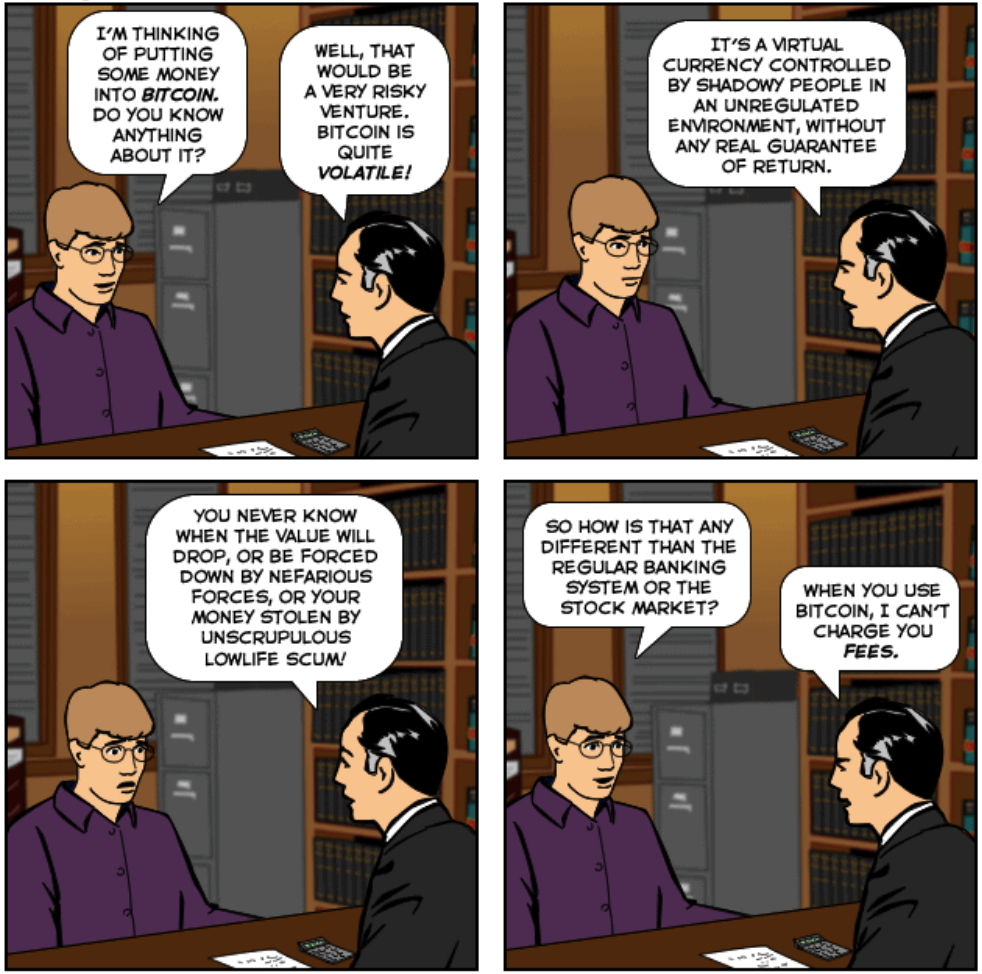
What I think I do

What I really do

What is Bitcoin?

Geld

“**Geld** ist jedes allgemein anerkannte Tausch- und Zahlungsmittel.”



Motivation

- Kosten
- Langsam
- Anonymität
- indirekte Tranksaktionen
- Abhängigkeit von zentraler Entität
- Limits/Beschränkungen

Geschichte

1998: Vorgänger “bit gold”

Nov 2008: bitcoin.org/bitcoin.pdf - Satoshi Nakamoto

9. Jan 2009: Bitcoin v0.1

12. Jan 2009: erste Transaktion

2009: Niedrigster Preisstand für Bitcoins mit Verkauf von 15.000BTC für 0.03$

Geschichte

Mai 2010: erste 10.000BTC Pizza

Jul 2010: Mtgox Tauschbörse

Aug 2010: erster und einziger kritischer Sicherheitsbug bisher

Apr 2011: TIME Bitcoin-Artikel

Nov 2012: Halbierung des Block-Rewards auf 25BTC

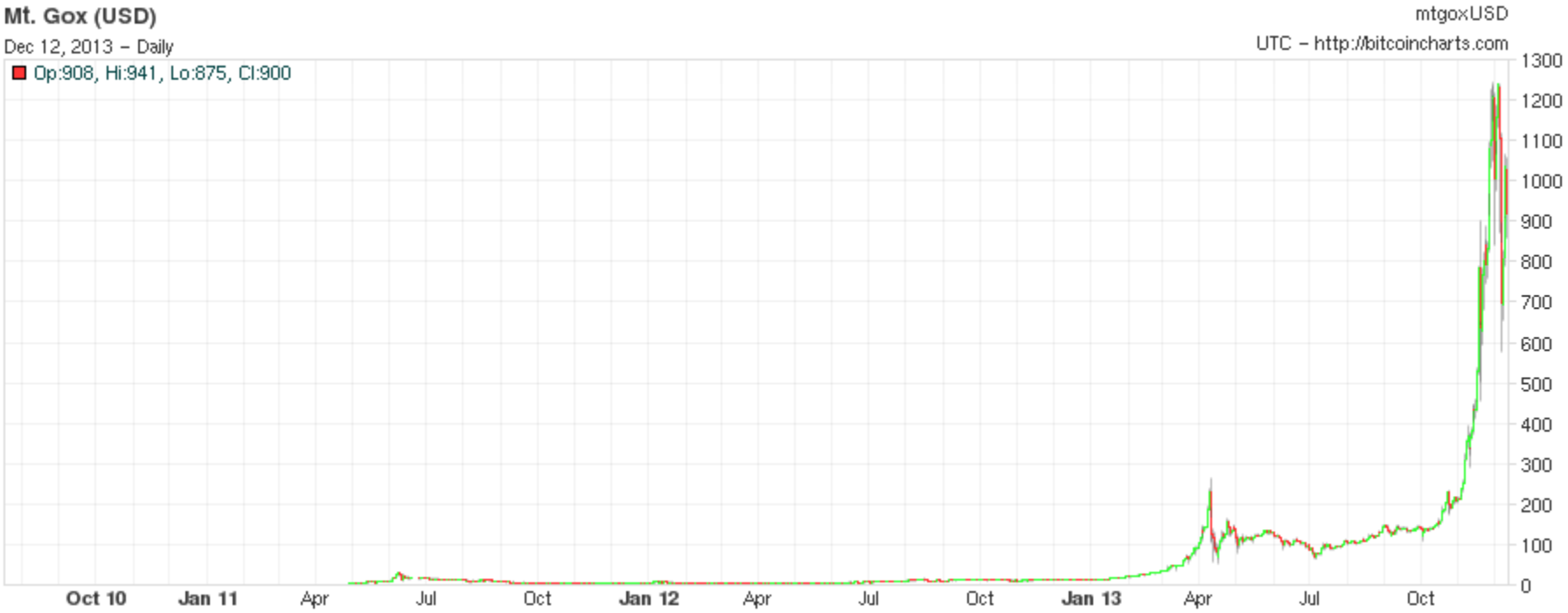
Geschichte

Oct 2013: Beschlagnahmung von 26.000BTC durch FBI (Silk Road)

Nov 2013: Gesamte Bitcoin-Rechenleistung höher als alle Top 500 Supercomputer vereint

Dez 2013: 40.000BTC Sheep Market Scam

Kursverlauf



Satoshi?

´Return of Satoshi´

http://tinyurl.com/satoshireturn

Mining

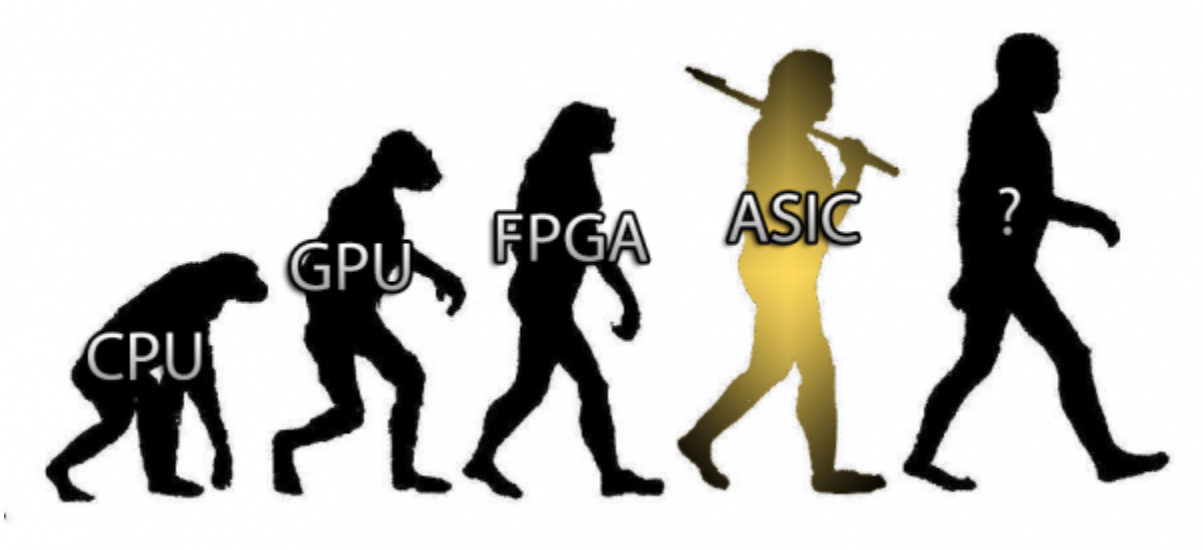
Woher kommen die Bitcoins?

Mining

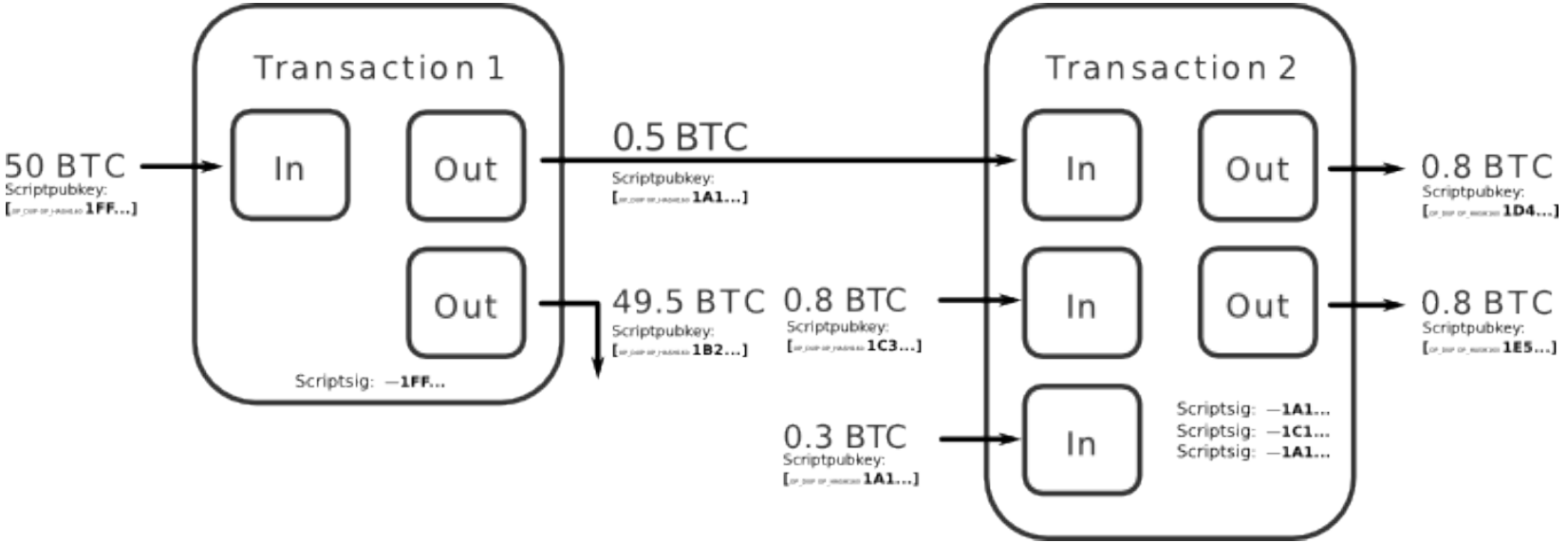
Proof of work

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

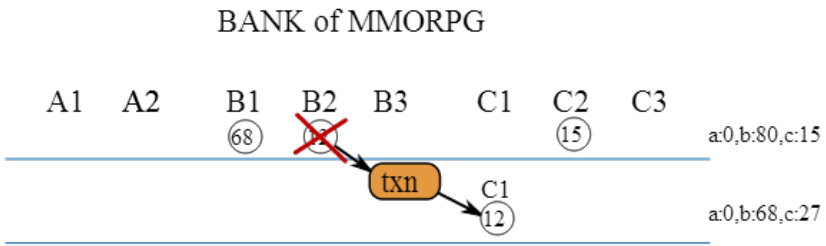
Mining



Transaktionen

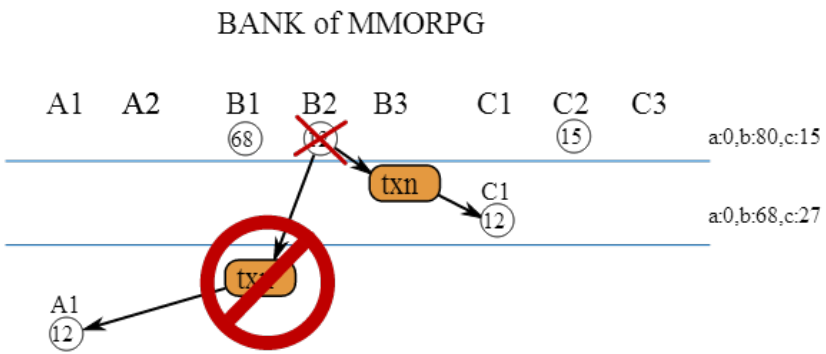


Transaktionen

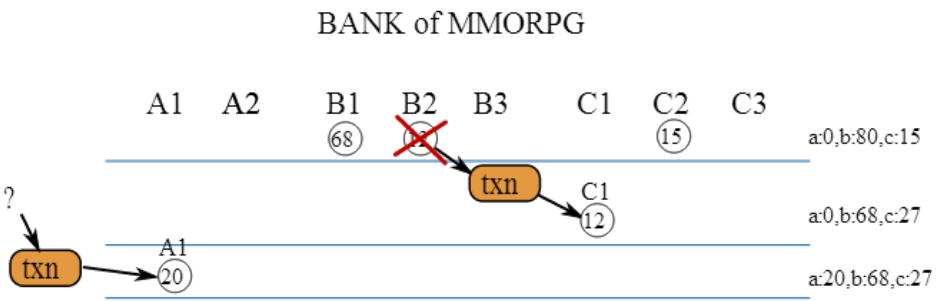


http://people.mozilla.org/~bwarner/bitcoin/slides.html

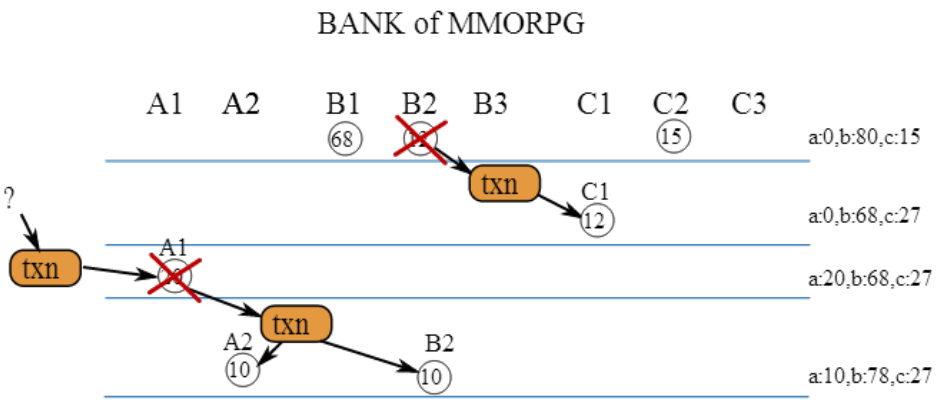
Transaktionen



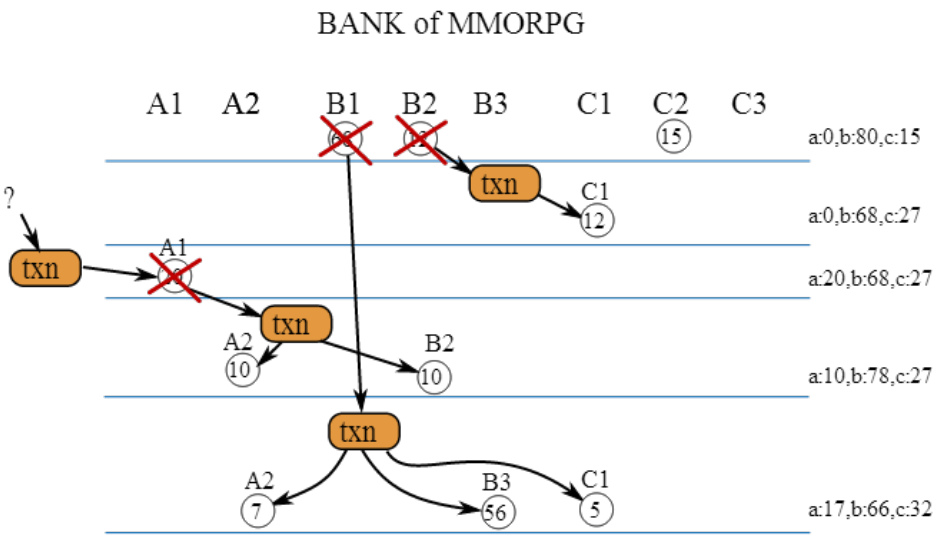
Transaktionen



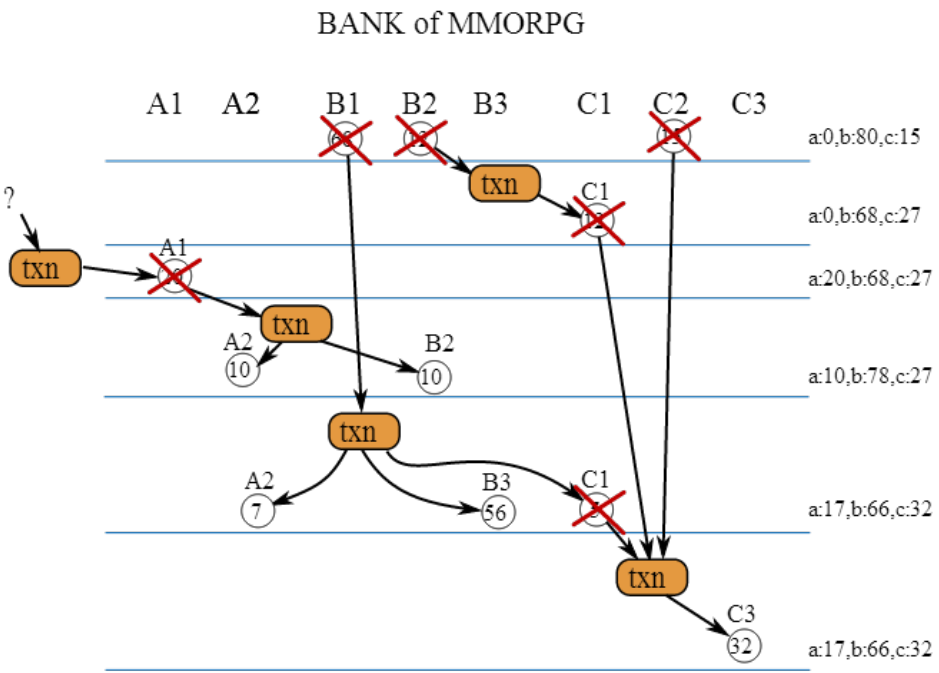
Transaktionen



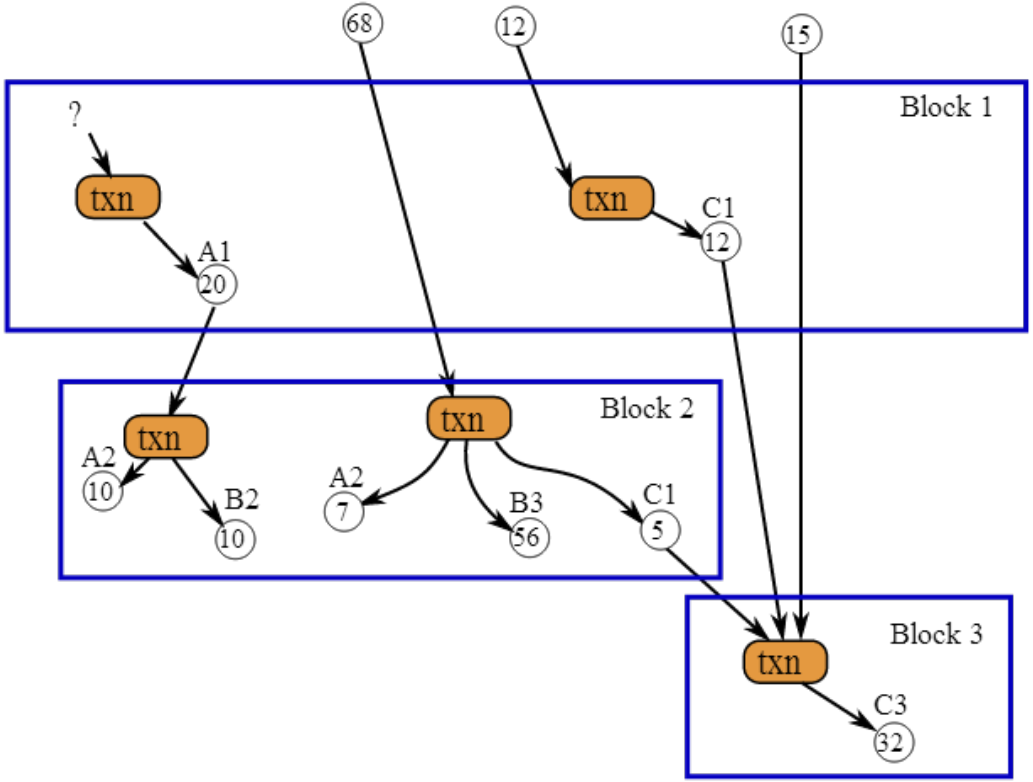
Transaktionen



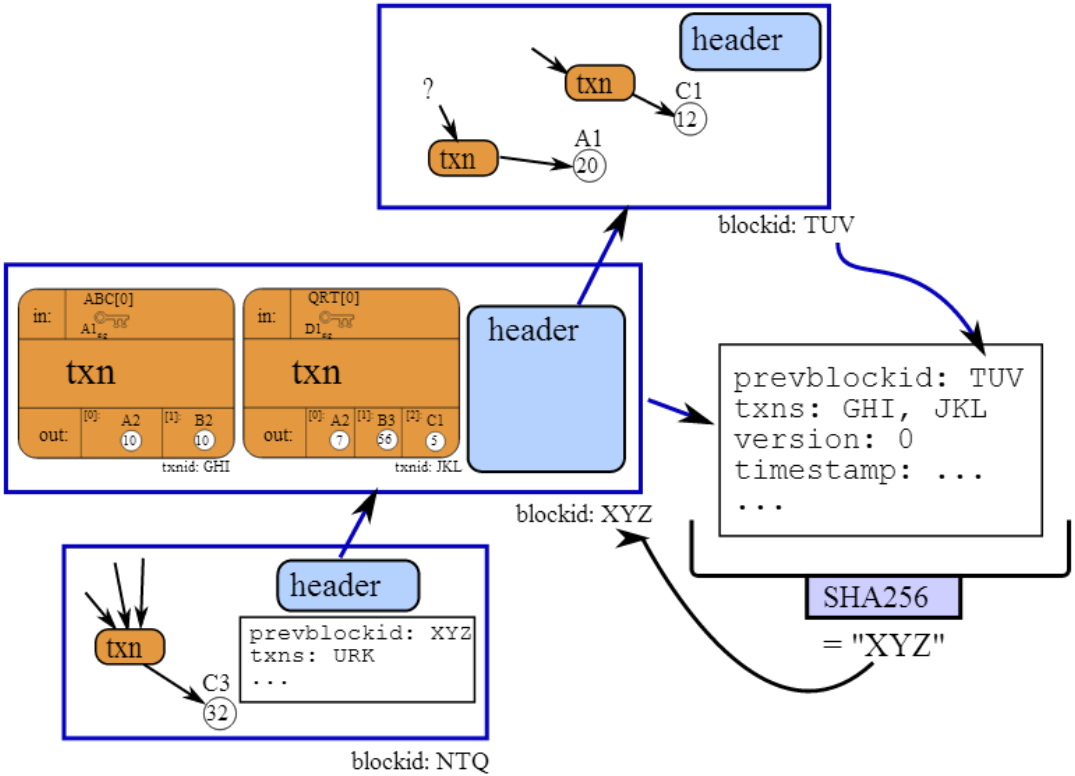
Transaktionen



Blöcke


68
12
15
Block 1
?
txn
A1
20
txn
C1
12
Block 2
txn
A2
10
B2
10
txn
A2
7
B3
56
C1
5
Block 3
txn
C3
32

Die Block Chain



Adressenerzeugung

ECDSA Private + Public Key (Kurvenparameter secp256k1)

Private: 18E14A7B6A307F426A94F8114701E7C8E774E7F9A47E2C2035DB29A206321725

Public: 0450863AD64A87AE8A2FE83C1AF1A8403CB53F53E486D8511DAD8A04887E5B23522CD470243453A299FA9E77237716103ABC11A1DF38855ED6F2EE187E9C582BA6

X = SHA-256 + RIPEMD-160 auf Public Key

010966776006953D5567439E5E39F86A0D273BEE

Y = Netzwerk-ID-Byte vorne an X einfügen (0x00 für Haupt-Netzwerk)

00010966776006953D5567439E5E39F86A0D273BEE

Z = SHA-256^2 (Y)

D61967F63C7DD183914A4AE452C9F6AD5D462CE3D277798075B107615C1A8A30

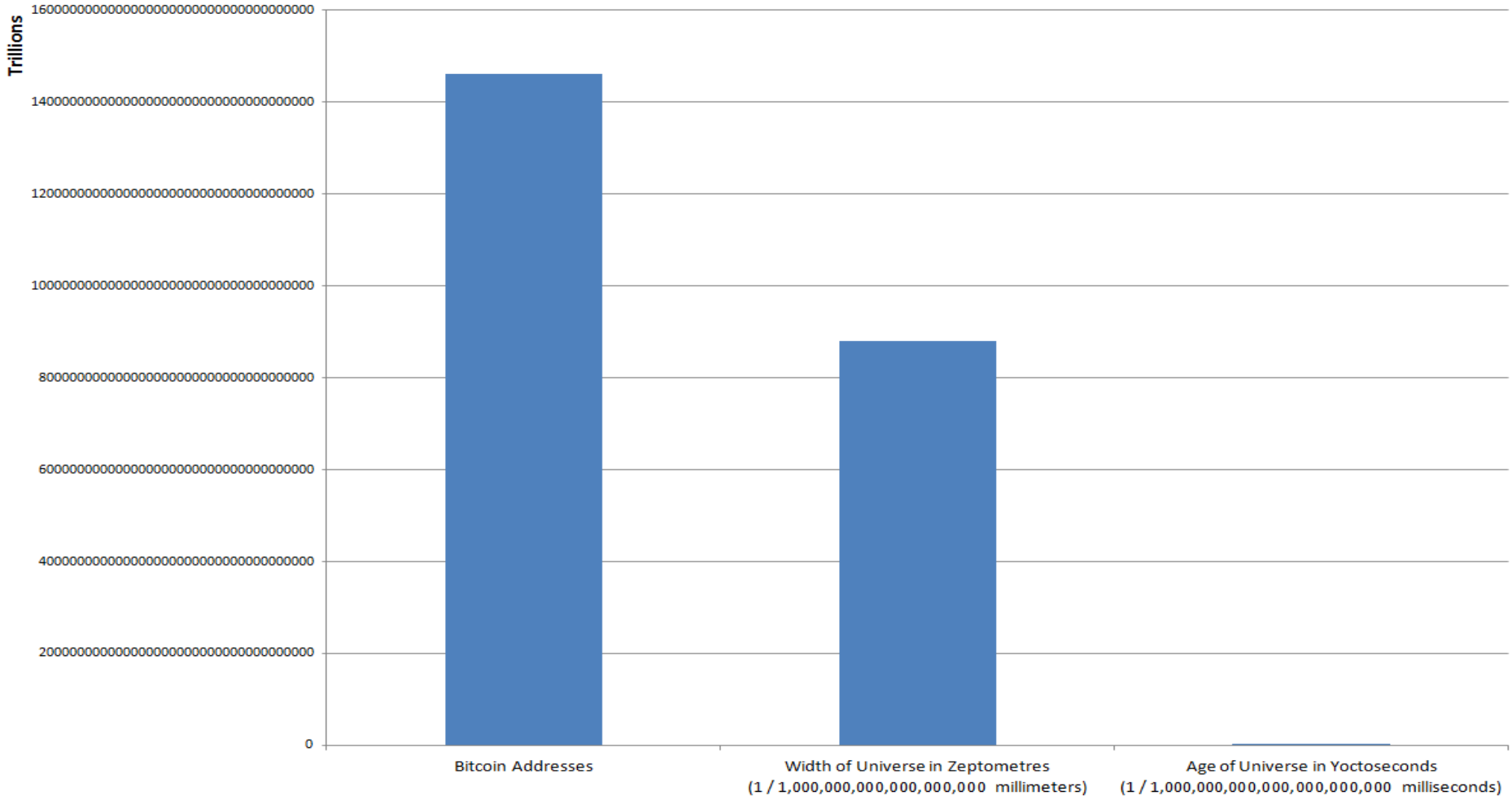
Checksumme (erste 4 Bytes) an X anhängen

00010966776006953D5567439E5E39F86A0D273BEED**61967F6**

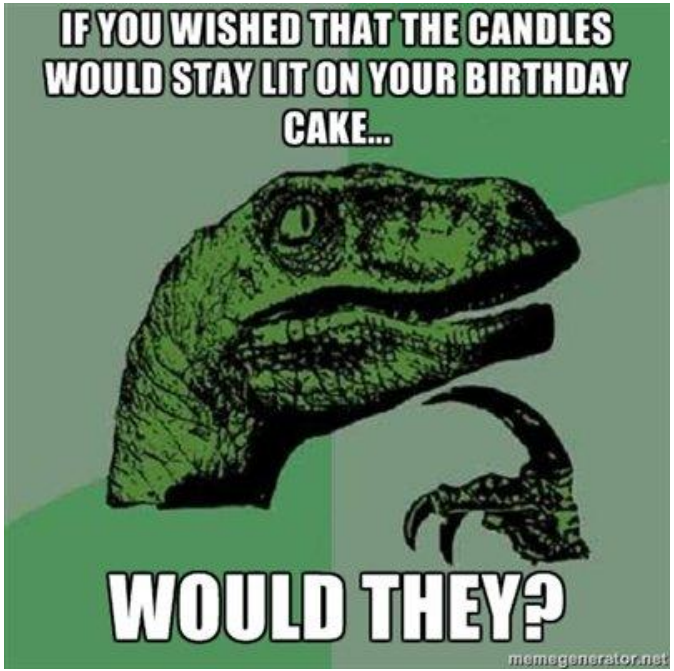
Base58-Kodierung

16UwLL9Risc3QfPqBUvKofHmBQ7wMtjvM

How many Bitcoin addresses are there?



Geburtstagsparadoxon



Geburtstagsparadoxon

0.1% Wahrscheinlichkeit einer Kollision

benötigt 5.4 x 10^22 Adressen

komplette Bitcoin-Rechenleistung würde allein zum Generieren von so vielen Adressen 127.000 Jahre brauchen

Anonymität

Anonyme Bitcoins?

Anonyme Bitcoins?

Jede Transaktion wird in der Blockchain veröffentlicht und ist jederzeit und für jeden einsehbar

Anonyme Bitcoins?

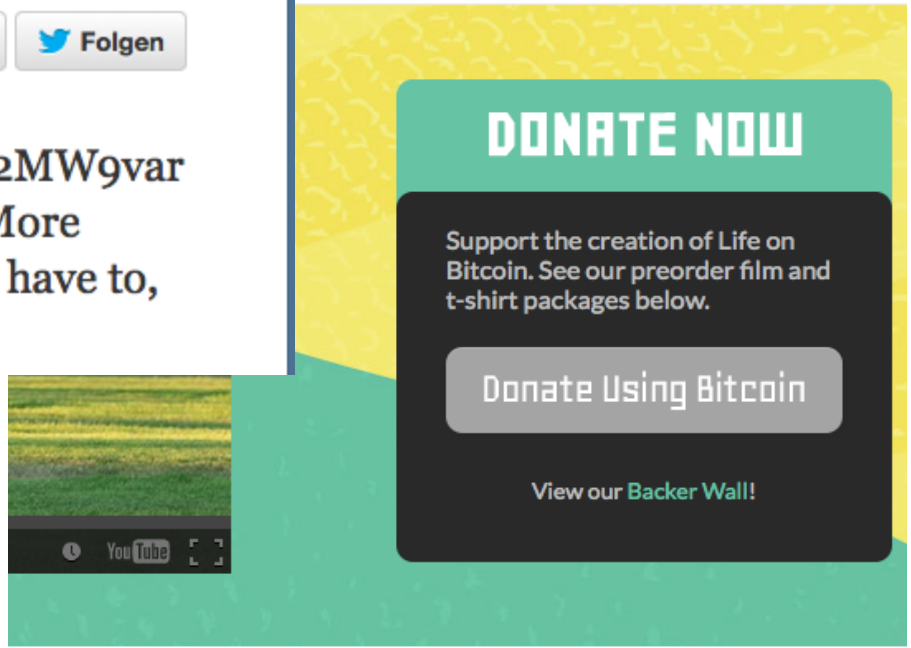
… und damit auch jederzeit, wann wie viele Bitcoins in welcher Wallet waren!

SatoshiDICE 48%

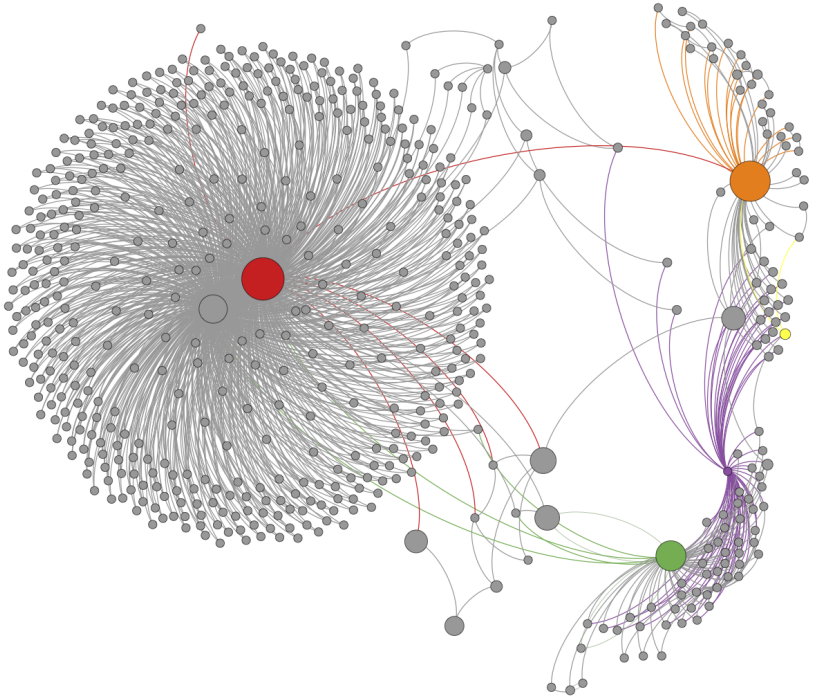
Zusammenfassung	
Adresse	1dice8EMZmqKvrGE4Qc9bUFf9PX3xaYDp
Hash 160	06f1b66ffe49df7fce684df16c62f59dc9adbd3f
Tools	Taint Analyse - Kennzeichnungen - Unverbrauchten Ausgänge

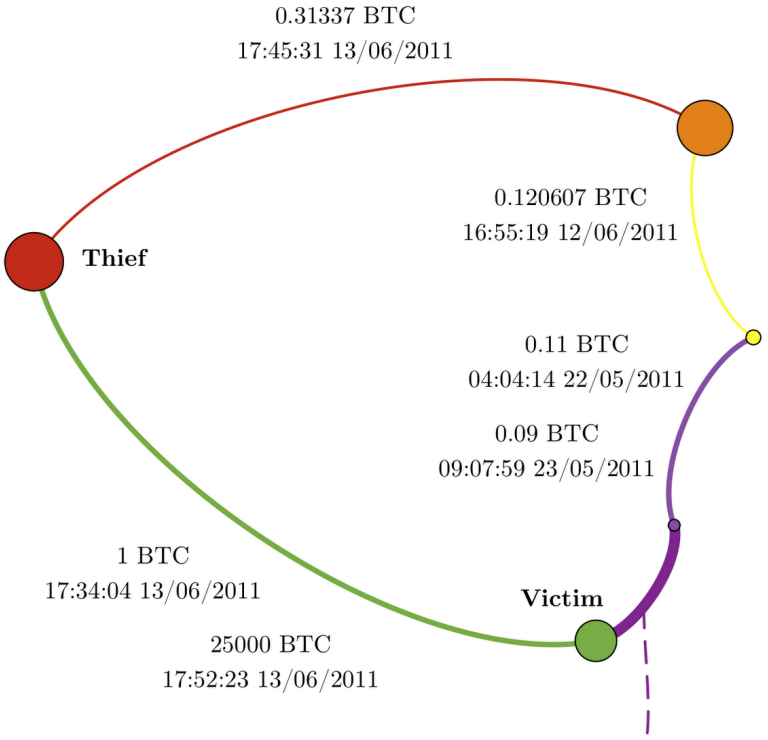
Transaktionen		
Anzahl der Transaktionen	3108447	
Insgesamt empfangen	1,014,372.27709027 BTC	
Schlussbilanz	0.87345313 BTC	

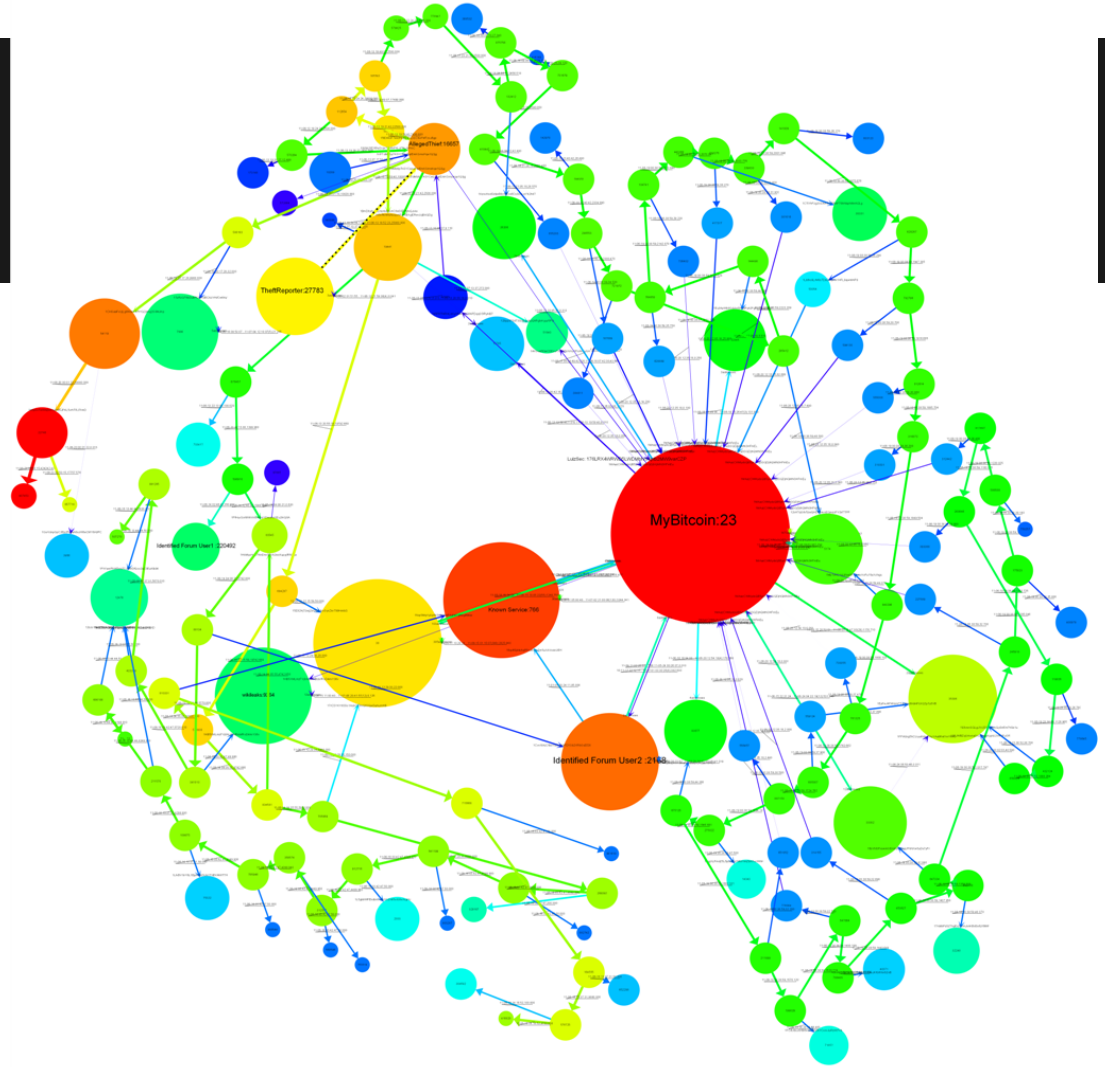
Anonyme Bitcoins?



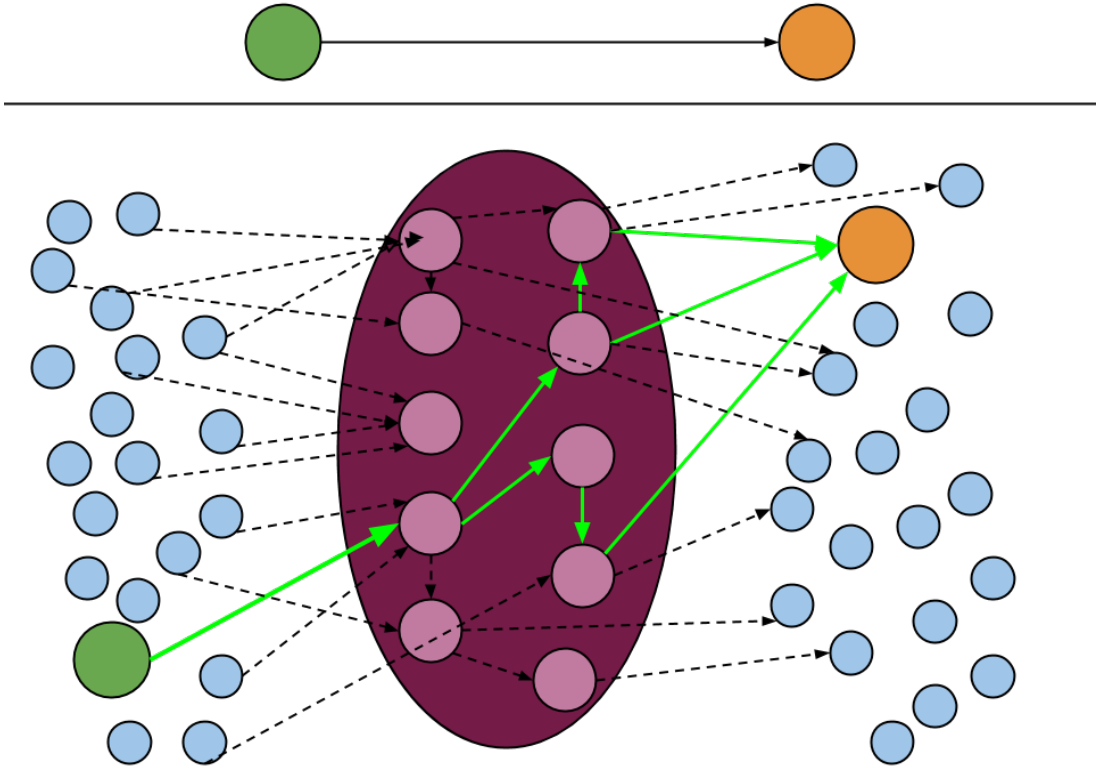
Verfolgung




0.31337 BTC
17:45:31 13/06/2011
0.120607 BTC
16:55:19 12/06/2011
Thief
0.11 BTC
04:04:14 22/05/2011
0.09 BTC
09:07:59 23/05/2011
1 BTC
17:34:04 13/06/2011
Victim
25000 BTC
17:52:23 13/06/2011


MyBitcoin:23
Known Service:766
Identified Forum User2 :2183
TheftReporter:27783

Laundry, Mixer & Tumbler



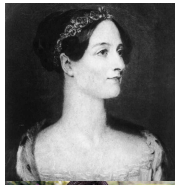
Laundry, Mixer & Tumbler

We may share your personal information with:
Law enforcement, government officials, or other third parties when:

- *We are compelled to do so by a subpoena, court order or similar legal procedure; or*

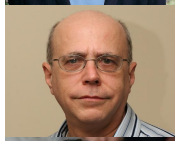
- *We believe in good faith that the disclosure of personal information is necessary to prevent physical harm or financial loss, to report suspected illegal activity or to investigate violations of our User Agreement.*

ZeroCoin



1 Lovelace = 1 Bitcoin

1 Goldwasser = 10 Bitcoin

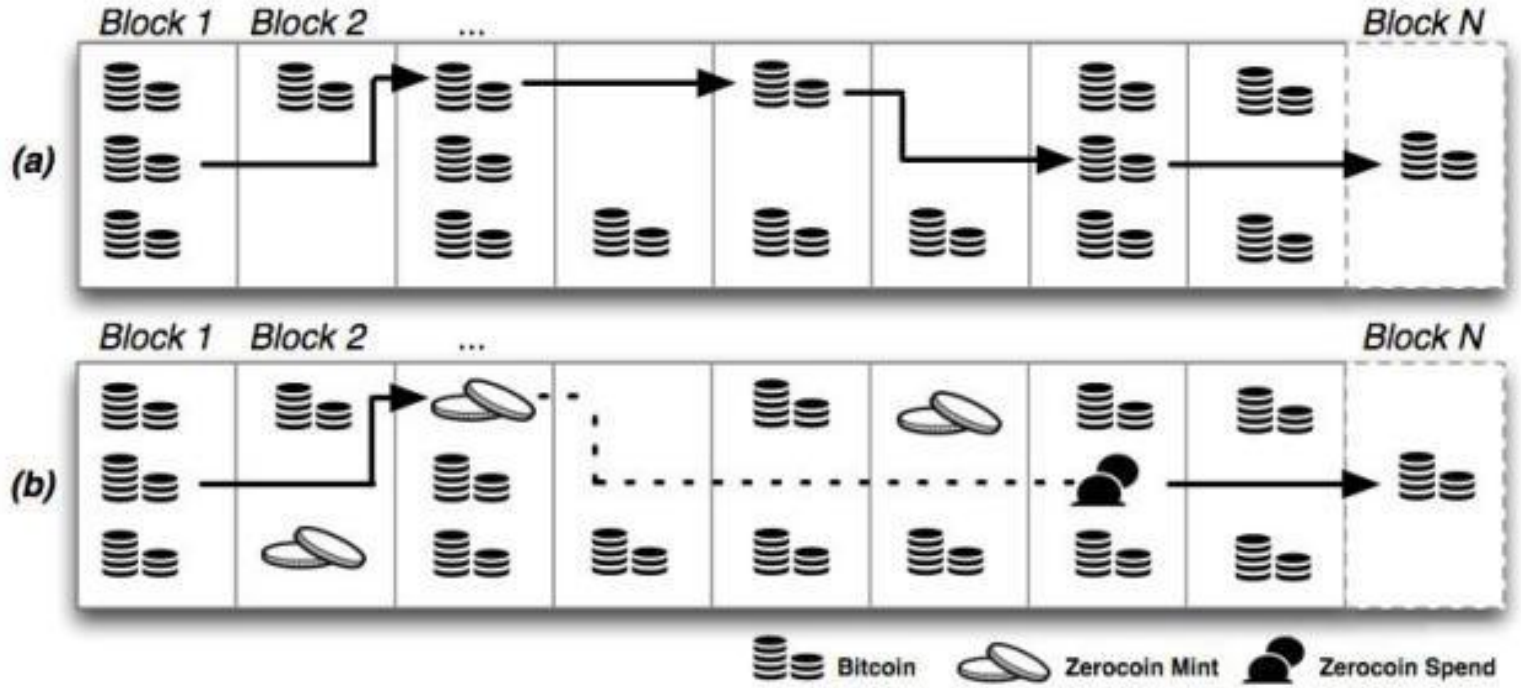


1 Rackoff = 25 Bitcoin

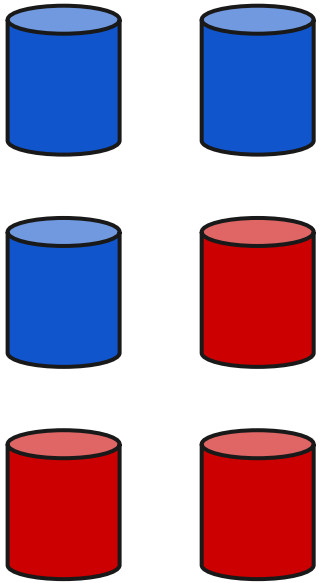
1 Pedersen = 50 Bitcoin

1 Williamson = 100 Bitcoin

ZeroCoin


Block 1
Block 2
...
Block N
(a)
Block 1
Block 2
...
Block N
(b)
Bitcoin
Zerocoin Mint
Zerocoin Spend

Zero-Knowledge-Proof



Spend A ZeroCoin

* Serial (PrivatCoin) des eigenen Coins

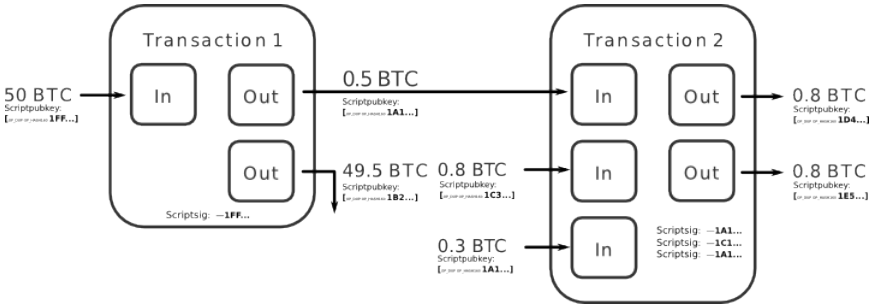
* Set aus unverbrauchten Zerocoins, das den eigenen enthält

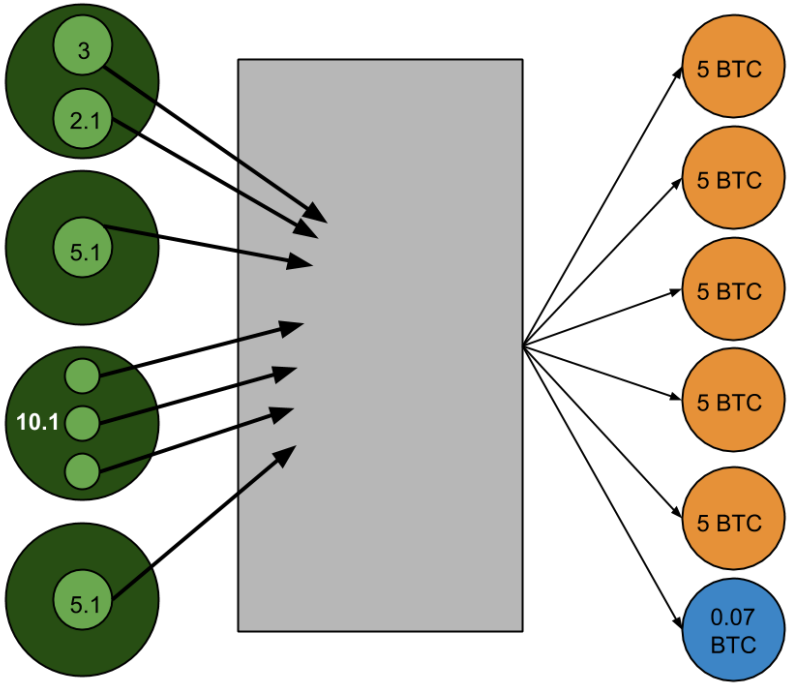
* zufälliger Coin aus Set

* Ziel-Adresse für Bitcoin

* Coin-Signatur

CoinJoin


Transaction 1
50 BTC
Scriptpubkey:
In
Out
Out
0.5 BTC
Scriptpubkey:
49.5 BTC
Scriptpubkey:
Scriptsig: —1FF...
Transaction 2
In
Out
In
Out
In
0.8 BTC
Scriptpubkey:
0.8 BTC
Scriptpubkey:
0.8 BTC
Scriptpubkey:
0.3 BTC
Scriptpubkey:
Scriptsig: —1A1...
Scriptsig: —1C1...
Scriptsig: —1A1...


3
2.1
5.1
10.1
5.1
5 BTC
5 BTC
5 BTC
5 BTC
5 BTC
0.07 BTC

Weitere Probleme

Diebstahl

Dos Attacken

Illegaler Inhalt in der Block-Chain

Sicherheitbugs

Energieverbrauch

instabiler Preis und Deflationsspirale

Wahrscheinlich keine Probleme

Kryptographie wird gebrochen

Skalierbarkeit

Zerstörung aller Coins

Alternative CryptoCoins

Litecoin LTC 

Namecoin NMC 

AnonCoin ANC 

PPcoin PPC 

PrimeCoin XPM 

.. unzählige weitere

MAJOR:
(big market, high security)

-**BTC Bitcoin-** - first, strongest, most accepted, most mined, high volume market, a true currency
-**LTC Litecoin-** second only to BTC , faster than BTC, ASIC-hostile GPU SCRYPT mining.
-**NMC Namecoin-** merged mined with BTC, used for alternative p2p domain system
-**PPC PPcoin-** Proof Of Stake [very innovative, low energy]

MINOR:
(established, but small)

-**XPM PrimeCoin-** mining PrimeCoin helps looking for prime numbers, instead of wasting energy. for now cpu-only.
-**NVC NovaCoin-** scrypt hashing[like LTC], proof of stake [like PPC]
-**FTC FeatherCoin-** LTC clone with 4x more coins. starting diff 0
-**TRC Terracoin-** BTC clone, many diff algo updates, still abused.
-**DVC Devcoin-** merged mined with BTC, 90% of generation goes to foundation, 10% to miners

CANDIDATES:
(not stable yet, with some community support)

-**MEC Megacoin-** based on 8.2 code. 0 starting diff.
-**CGB CryptogenicBullion-** 0.94% Premined NVC Clone
-**MNC Mincoin-** LTC clone, started with no binaries and 25000% reward blocks. 0 starting diff
-**DGC DigitalCoin-** LTC clone. 20 sec blocks. 0 starting diff + progresive reward.
-**ANC Anoncoin-** a coin with I2P support
-**WDC Worldcoin-** LTC clone. 15 sec blocks. 0 starting diff.
-**FRC Freicoin-** 4.89% anual demurrage. for the first 3 years 80% block subsidy goes to foundation, 20% to miners.
-**IXC IxCoin-** merged mined with BTC, BTC clone.
-**IFC Infinitecoin-** LTC clone with huge reward of 524288 and extreme fast reward drop.

THE PURGATORY:
(many new clones)

-**BTB BitBar-** scarce, PoW + PoS[like PPC] scrypt. 0 starting diff + quick adjustment.
-**BQC BBQCoin-** forgotten , now revived and active. faster version of LTC.
-**ZET Zetacoin-** BTC clone, sha256.
-**GLD Goldcoin-** LTC clone. 0 starting diff, 2000% superblocks at start [3.2% instamine]
-**PXC PhenixCoin-** LTC clone. 1'000'000 coins premine
-**PyBC Coin-** An example coin to show new "Python Blockchain" Library capabilities.
-**YAC YACoin-** Yet Another altCoin. NovaCoin fork, with modified scrypt hashing
-**FRK Franko-** LTC clone. fast blocks. 0 starting diff. scarce.
-**BTE Bytecoin-** the 1:1 bitcoin copy
-**CAP Bottlecaps-** NVC clone, with a 0.25 diff start and quick 9 years inflation
-**NBL nibble-** LTC clone. progresive starting reward.
-**FLO Florin coin-** a coin with trasaction comments
-**GME Gamecoin-** unfinished FTC clone , killed on launch. failed to revive once, and now finaly revived.
-**CNC CHNCoin-** LTC clone, announced on chinese forum first.0 starting diff
-**HBN HoboNickels-** Fast NVC clone. Extreme, over 100% ROI. 0 starting diff.
-**JKC JKC-** LTC clone. 0 starting diff with superblocks, random superblocks.
-**FST Fastcoin-** LTC clone. 12 sec blocks. 0 starting diff.
-**KGC krugercoin-** LTC clone. 15 sec blocks. 0 starting diff.
-**QRK Quark-** Sifcoin clone. CPU only.
-**BTG bitgem-** NVC scarce clone. 0 starting diff
-**I0C I0coin-** ixcoin without the premine. died 3 times. After very long time revived again.

-**ZCC ZcCoin-** Yacoin clone.
-**FEC FreeCoin-** Yacoin clone.
-**MemoryCoin-** SHA512 + modified scrypt coin with grands.
-**PHS Philosopherstone-** NVC Clone with random blocks and in-blockchain messages.
-**AMC Americancoin-** premined LTC clone with 6.5k-14k blocks giving zero reward
-**SPC supercoin-** JunkCoin clone. 0 starting diff
-**doubloons-** LTC clone. 0 starting diff
-**LKY LuckyCoin-** superblocks at start, random superblocks [JunkCoin clone].
-**SPT Spots-** smallchange clone, 0 starting diff.
-**MEM MEMEcoin-** premined LTC clone. 10 sec blocks. 0 starting diff + superblocks.
-**EZC EzCoin-** LTC clone. 0 starting diff and superblocks
-**CMC CosmosCoin-** NVC fork with no fees and transaction comments
-**DMD Diamond-** Scarce NVC clone with random reward.
-**ARG Argentum-** premined LTC clone
-**StableCoin-** 0 starting diff, died and revived.
-**SIC Sifcoin-** Uses new hashing, series of SHA-3 candidates, CPU only.
-**Ybc Ybcoin-** YAC Clone.
-**GLX Galaxycoin-** Fast NVC clone with constant reward for 8 years.
-**NUG Nuggets -** premined LTC clone with random superblocks and constant base reward.
-**LBW Lebowskis-** NVC clone.
-**CSC CasinoCoin-** LTC clone. 0 starting diff, superblocks at start.
-**EGC EagleCoin-** LTC clone. 0 starting diff.
-**ZTC ZenithCoin-**Freicoin based -demurrage +Scrypt. 50% tax for developer.
-**ONC Onecoin-** a coin that has total supply of 1, Scrypt-jane
-**ELP ElephantCoin-** LTC Clone with random blocks and in-blockchain messages.0.4% premined.
-**GLC GlobalCoin-** LTC clone
-**CDC Cloudcoin-** 1000000 premined NVC clone with random blocks.
-**GDC Grand coin-** JKC clone
-**PYC Paycoin -** CosmosCoin clone.

-**CENT Pennies-** Hidden launch Yacoin clone.
-**NEC Neocoin-** NVC-like, with messages. Multiple failed relaunches until finaly ok.
-**JPC Jupitercoin-** Scarce LTC Clone. 0 starting difficulty, 0.27% premined.
-**CRM Crimecoin-** A little (0.03%) premined LTC clone.
-**VLC ValueCoin-** 0,75% premined LTC clone
-**GRW Growthcoin-** Super quickly mined NVC clone, halving every 3 months + 100% RoI! Exponential inflation.
-**SYC Skycoin-** premined LTC clone
-**SXC Sexcoin-** JunkCoin clone, overtaken.
-**CL Copperlark-** Uses new hashing, SHA-3. CPU only. Massively premined
-**RYC RoyalCoin-** starting superblocks LTC clone
-**DNC Dragoncoin-** smallchange clone, 0 starting diff.
-**Emerald-** LTC clone. progresive starting reward. scarce.
-**NAN NanoTokens-** premined LTC clone
-**MST MasterCoin-** premined LTC clone
-**USC UScoin-** premined LTC clone
-**FEC FerretCoin-** LTC clone. 0 starting diff.
-**Noirbits-** LTC clone
-**GIL-** premined LTC clone with random reward.
-**CDC Cloudcoin-** 1000000 premined NVC clone with random blocks.
-**RCH RichCoin-** premined LTC clone
-**XNC XenCoin-** premined LTC clone
-**REC RealCoin-** premined LTC clone
-**ALF Alphacoin-** LTC clone with 1000000 premined and starting superblocks.
-**RED Redcoin-** 1000000 premine, random reward, transaction messages.
-**One last Coin-** premined LTC clone
-**ORB Orbitcoin-** The most(66%) premined coin since MMMcoin . 0 starting diff.
-**Quantumcoin-** dead and relaunched clone

DEAD / DYING :

-**TDC TradeCoin-** 100% premine LTC clone experiment. Dying.
-**NUC NuCoin-** premined LTC clone. officially dead.
-**6CN 6coin-** LTC clone. Never really picked up.
-**PWC Powercoin-**] LTC clone. 30 sec blocks. killed by 51%
-**SRC sunrisecoin-** LTC clone. 0 starting diff. Dying because of no prime node from the start.

Ausblick

Bildquellen

http://depot2.de/blog/wp-content/Dickies-People-4-1024x601.jpg

https://twitter.com/wikileaks/status/80774521350668288

http://blockchain.info/de/

http://lifeonbitcoin.com

http://anonymity-in-bitcoin.blogspot.de/2011/07/bitcoin-is-not-anonymous.html

http://commons.wikimedia.org/wiki/File:Shafi_Goldwasser.JPG

http://media.npr.org/assets/artslife/arts/2009/12/lovelace_custom-62179d4aea6d0e31fe0f01b8d41ca246e154e20c-s6-c30.jpg

http://www.iacr.org/fellows/2011/Rackoff.jpg

http://www.egovplus.dk/nyhedsbrev/april09/P4223974_1.jpg

http://www.livinginternet.com/g/williamson_malcolm1.JPG