Cryptos – Technik und Benutzung

Axel Wachtler

axel@uracoli.de

Chemnitzer Linuxtage 2018

Fahrplan

- Funktion einer Crypto-Währung
  - Das Netzwerkprotokoll im Schnelldurchlauf
- Die Crypto-Währung aus Benutzersicht / Beispielüberweisung
  - Software / Einstieg / Funktion der Komponenten
  - Spaziergang im Abenteuerland
- Ausblick

Rückblick: 2. Chemnitzer Linux Tag, 12.3.2000
Lutz Donnerhacke:

Das ewige Logfile
Anonymes vorbezahltes elektronisches Geld

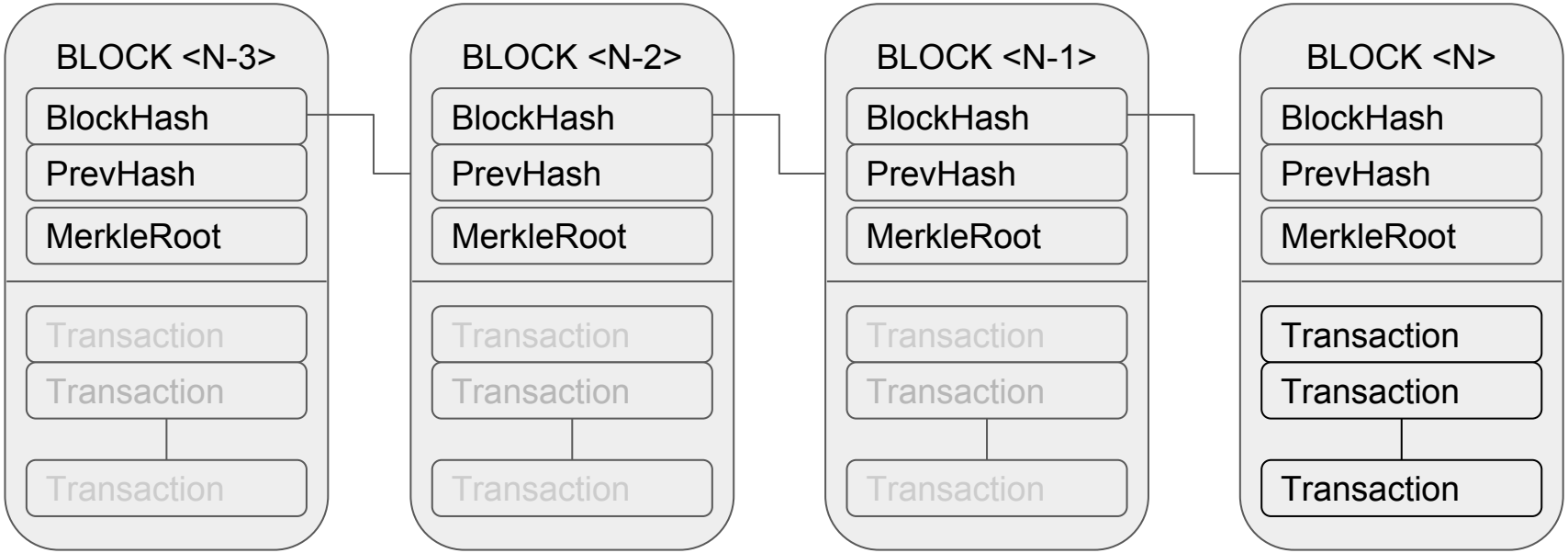
http://altlasten.lutz.donnerhacke.de/mitarb/lutz/vortrag/

Funktion einer Crypto-Währung

- Netzwerk von unabhängigen Knoten verwaltet eine verteilte Datenbank (BlockChain/Ledger) .
- In der BlockChain werden einzelne Transaktionen chronologisch und fälschungssicher gespeichert.
- Eine Transaktion beschreibt den Übertrag von Coins/Token von einer Coin-Adresse (Konto) auf ein anderes Konto.
- Benutzer senden Transaktionen an das Netzwerk.
- Die Netzwerkknoten überprüfen die Gültigkeit der Transaktionen und schreiben die Blockchain fort.
- Die Integrität der Blockchain wird über die Verkettung von Hash-Werten sichergestellt.

Die Blockchain

- Verkettete Liste von Blöcken (Verkettung über Hash des vorherigen Blockes)
- Jeder Block fasst mehrere Transaktionen zusammen.



Konsens unter den Knoten

- Das Hashen von Daten ergibt quasi-zufällige Zahlen,
  die als 256-Bit-Integer-Werte aufgefasst werden.

- Ist der ermittelte Hashwert kleiner als ein Target-Wert
  dann wird ein Block als gültig angesehen und die BlockChain aufgenommen
  (Suche nach dem Target macht das Erzeugen der Blöcke schwierig).

- Der Hashwert ist einfach nachzuprüfen.

- Der Target-Wert wird regelmäßig im Netzwerkprotokoll adaptiert.

Proof of Work (PoW)

Die Miner modifizieren solange einen Nonce Wert, bis sie einen Blockhash finden, der kleiner als der Target-Wert ist.

Grundlegender Ablauf der PoW Berechnung (Pseudo-Code):

```
while(true){
  Nonce ++
  blockHash = hash(Nonce, prevBlockHash, merkleRoot, blockTime, …)
  if(blockHash =< powTarget)
    createNewBlock()
}
```

Proof of Stake (PoS V3.0)

Erzeugung des Blockes auf Basis einer “Unspend Transaction” (utxo), gesuchter Hash errechnet sich aus der Zeit und den utxo-Parametern.

Pseudo-Code:

```
while(true){
  foreach(utxo in wallet){
    blockTime = currentTime - currentTime  % 16
    prevStakeModifier = hash(params(utxo))
    krnlhash = hash(prevStakeModifier , utxo.time, utxo.hash, utxo.n,
blockTime)
    if(krnlhash/utxo.value  =< posTarget)
      createNewBlock()
  }
  wait(16s) // wait until the block time can be changed
}
```

Siehe auch: http://earlz.net/view/2017/07/27/1904/the-missing-explanation-of-proof-of-stake-version

PoW vs. PoS

- Für PoW benötigt man bei derzeit populären Währungen “teures Equipment” und “billige Energie”.
  - massiver Vorschuss an Kapital erforderlich.
  - System zentralisiert sich in den Händen weniger Miner / Mining Pools
  - leistungsarm und abgas-stark: hoher Energieverbrauch bei geringer Transaktionsleistung: https://digiconomist.net/bitcoin-energy-consumption

- Für PoS benötigt man Token der jeweiligen Währung und einen Kleinrechner
  - Erforderliches Equipment: z.B. RaspberryPI-3
  - Kauf einer handvoll Coins
  - Entsperren des Wallets zum Staking

9.3.18 BTC-Parameter:

- 768 kWh / TX
- *Kühlschrank: 60-170kWh/Jahr*
- Ca. 7 - 10 TX/s
- *Visa: 25k TX/s*
- 26 ExaHash/s
- 386 kg CO_2 / TX

Benutzung einer Crypto-Währung - BlackCoin

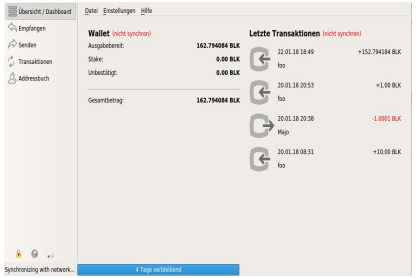
Warum BlackCoin?

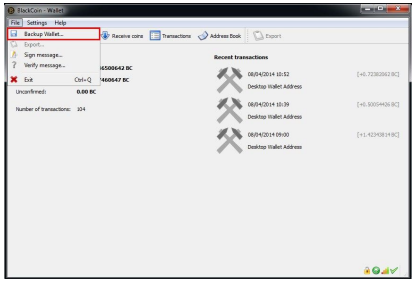
- Basis “Proof of Stake” V 3.0
  - Umweltverträglich
- Derzeit relativ geringer Token-Wert
  - ca . 0,30€/BLK
- Schnelle Transaktionsabwicklung
  - geringe Netzlast, ca. aller 1 - 2 Min. ein Block
- Freundliche und hilfsbereite Community
  - Gitter: https://gitter.im/BlackCoin_Hub
  - Reddit: https://www.reddit.com/r/blackcoin/
- Wird seit 2014 entwickelt.
  Basiert auf Bitcoin-Core-Funktionen
  - Fehlende Dokumentation? siehe https://en.bitcoin.it

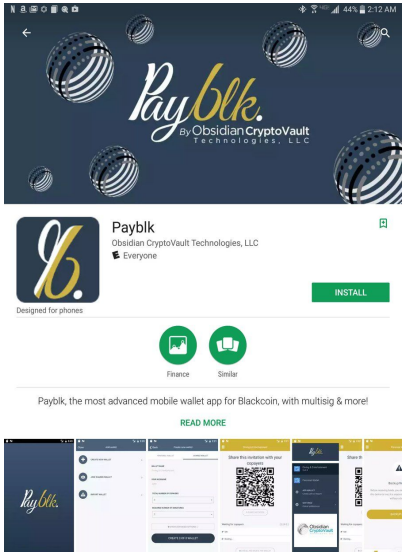
… Jede Menge Software für BlackCoin

Lore, Blackcoin-qt, PayBlk, NightTrader, BlackHalo, Iris …. ????

```
2018-02-28 05:43:40 Bitcoin version v2.12.1.0-335b89e
2018-02-28 05:43:40 InitParameterInteraction: parameter interaction: -whitelistforcerelay=1 -> setting -whitelistrelay=1
2018-02-28 05:43:40 Default data directory /home/pi/.lore
2018-02-28 05:43:40 Using data directory /home/pi/.lore
2018-02-28 05:43:40 Using config file /home/pi/.lore/lore.conf
2018-02-28 05:43:40 Using at most 125 connections (65536 file descriptors available)
2018-02-28 05:43:40 Using 4 threads for script verification
2018-02-28 05:43:40 scheduler thread start
2018-02-28 05:43:40 HTTP: creating work queue of depth 16
2018-02-28 05:43:40 No rpcpassword set - using random cookie authentication
2018-02-28 05:43:40 Generated RPC authentication cookie /home/pi/.lore/.cookie
2018-02-28 05:43:40 HTTP: starting 4 worker threads
2018-02-28 05:43:40 Using BerkeleyDB version Berkeley DB 6.2.32: (April  5, 2017)
2018-02-28 05:43:40 Using wallet wallet.dat
2018-02-28 05:43:40 init message: Verifying wallet...
2018-02-28 05:43:40 CDBEnv::Open: LogDir=/home/pi/.lore/database ErrorFile=/home/pi/.lore/db.log
2018-02-28 05:43:40 Bound to [::]:15714
2018-02-28 05:43:40 Bound to 0.0.0.0:15714
2018-02-28 05:43:40 Block index database configuration:
2018-02-28 05:43:40 * Using 1000 max open files
2018-02-28 05:43:40 * Compression is enabled
2018-02-28 05:43:40 Cache configuration:
2018-02-28 05:43:40 * Max cache setting possible 1024MiB
2018-02-28 05:43:40 * Using 12.5MiB for block index database
2018-02-28 05:43:40 * Using 29.9MiB for chain state database
2018-02-28 05:43:40 * Using 57.6MiB for in-memory UTXO set
2018-02-28 05:43:40 init message: Loading block index...
2018-02-28 05:43:40 Opening LevelDB in /home/pi/.lore/blocks/index
2018-02-28 05:43:41 Opened LevelDB successfully
2018-02-28 05:43:41 Using obfuscation key for /home/pi/.lore/blocks/index: 0000000000000000
2018-02-28 05:43:41 Opening LevelDB in /home/pi/.lore/chainstate
2018-02-28 05:43:42 Opened LevelDB successfully
2018-02-28 05:43:42 Using obfuscation key for /home/pi/.lore/chainstate: 85da10a5032221f7
```





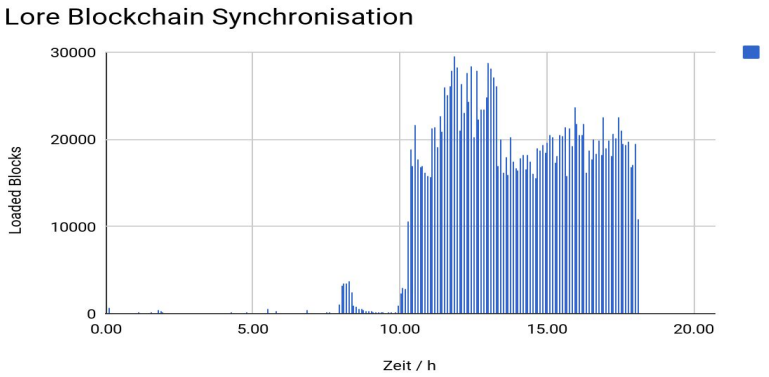


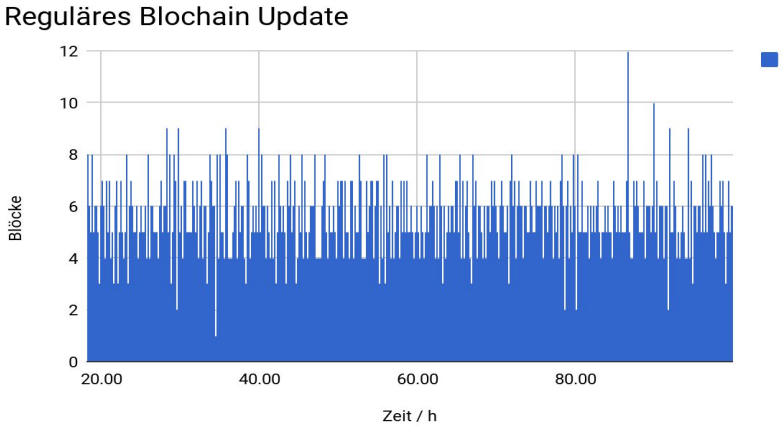
Klassifizierung der Coin-Software

- Core Software (blackcoind, lored) / CLI Software (blackcoind, lore-cli)
  - Headless / Kommandozeilen-Tool
  - Stellt Basis-Funktionalität des Netzwerkes bereit
  - Funktionen sind über API (intern) und RPC (extern) nutzbar
  - RPC wird per default nur auf lokalem Netzwerk bereitgestellt
- GUI Software (blackcoin-qt, lore-qt)
  - graphisches Frontend, das an den Core-Daemon compiliert ist
  - Stellt auf Basis der API User Level Funktionen bereit (Kontostände, Transaktions-Historie,...)
- Web Applikationen (PayBlk)
  - Software die sich mit einem Server (trust!) verbindet und den dort laufenden Daemon nutzt.
- Spezial Applikationen
  - Für Smart-Contracts and Colored Coins

Installation

1. Software selbst kompilieren
   - Richtiges Repository finden
   - Qt5 Pakete für GUI erforderlich
   - Auf Raspi 3 ~~Raspi 2~~ dauert Build ca. 8h
2. Startup-Scripte für Dämon schreiben
   - Keine Integration ins Paket-Managment
3. Download der Blockchain
   - Derzeit (5.2.2018) ca. 2.6 GByte
   - Synchronisation mit Lore auf Raspi3 in ca. 10 - 18h
   - Alternativ Snapshot von installieren, http://cryptochainer.com/ - trust?





Erzeugung der Schlüssel und Adressen

- Privat-Key - Public Key - Coin-Adresse
  - Privater Schlüssel:
    256 Bit (32 Byte) Zahl zwischen 1 und 0xFF..FE
  - Öffentlicher Schlüssel:
    Abgeleitet per secp256k1 - ECDSA Funktion
  - Bitcoin-Adresse:
    160 Bit Hash des öffentlichen Schlüssels
- Schlüsselgenerierung / Wallet-Struktur
  - Einzelne Key-Paare aus Zufallszahlen
    Backup des Wallets nach jedem neu erzeugtem Key
  - Ableitung der Adressen aus einem Master-Seed mit Key-Derivation-Funktion
    Masterkey ermöglicht Rekonstruktion aller aktuellen und künftigen Adressen
  - *Details siehe BIP0032: https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki*

Speicherung von Wallets

- Wallet.dat
  - Datei im jeweiligen Coin-SW-Directory, z.B. ~/.lore/wallet.dat
  - binäre Datei-Formate, sind nicht untereinander kompatibel
- Hardware Wallet
  - USB Devices, z.B. Ledger Nano S, Trezor, Jaxx,
    ... leider keiner mit BlackCoin-Support
- Paper Wallet
  - Ausdruck des Privaten und öffentlichen Schlüssels, z.B.
  - https://bitbucket.org/awachtler/monedero
- Brain Wallet
  - Ausdenken einer Passphrase und Ableitung eines Schlüsselpaares über Hash/Key-Derivation Funktion - der menschliche Geist ist ein schlechter Zufallsgenerator.

Erzeugung eines Paper-Wallet

Für BlackCoin-Addresse:

`BCzGtKHjYPAMpJCwqbZxrgEhcK9VtHucCT`

```
./mk_wallet.py -o clt_test_pwallet.pdf -w clt_test
```

Erzeugt verschlüsseltes PDF-File

Source Code:
https://bitbucket.org/awachtler/monedero

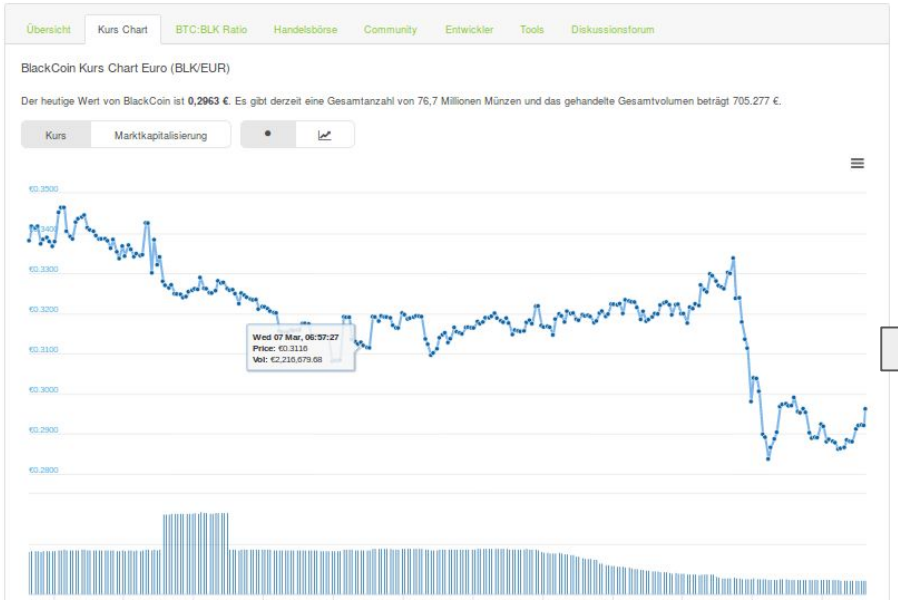
Example-Key, do not use!

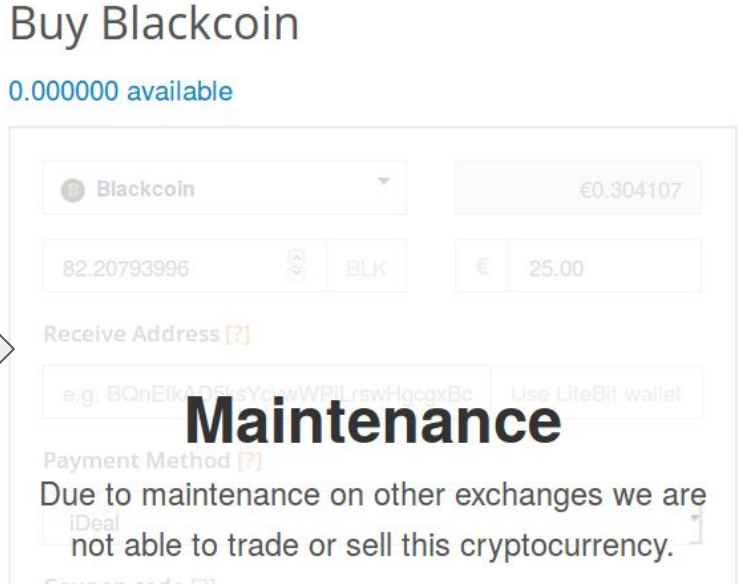
Wo bekommt man BlackCoin?

- Internet-Wechselstube (Börse) z.B. anycoindirect.eu, litebit.eu
  - Unterschiedliche Zahlungsarten werden unterstützt
  - Tw. willkürliche und spontane Regeländerung
  - Finanzierung über Spreadings und Gebühren
- Vor dem Kauf anmelden
  - Verifikationsprozess erfordert Zeit
  - Zahlungsflüsse in beide Richtungen testen.
- Am Fiat-Gateway
  - entsteht Wohlstand/Armut - Wissen was man tut!
  - Gewinne sind steuerpflichtig - Buchführung nicht vergessen (FIFO)
  - Börsen sind Ziel von Hackern - Coins zügig auf eigene Adresse überweisen

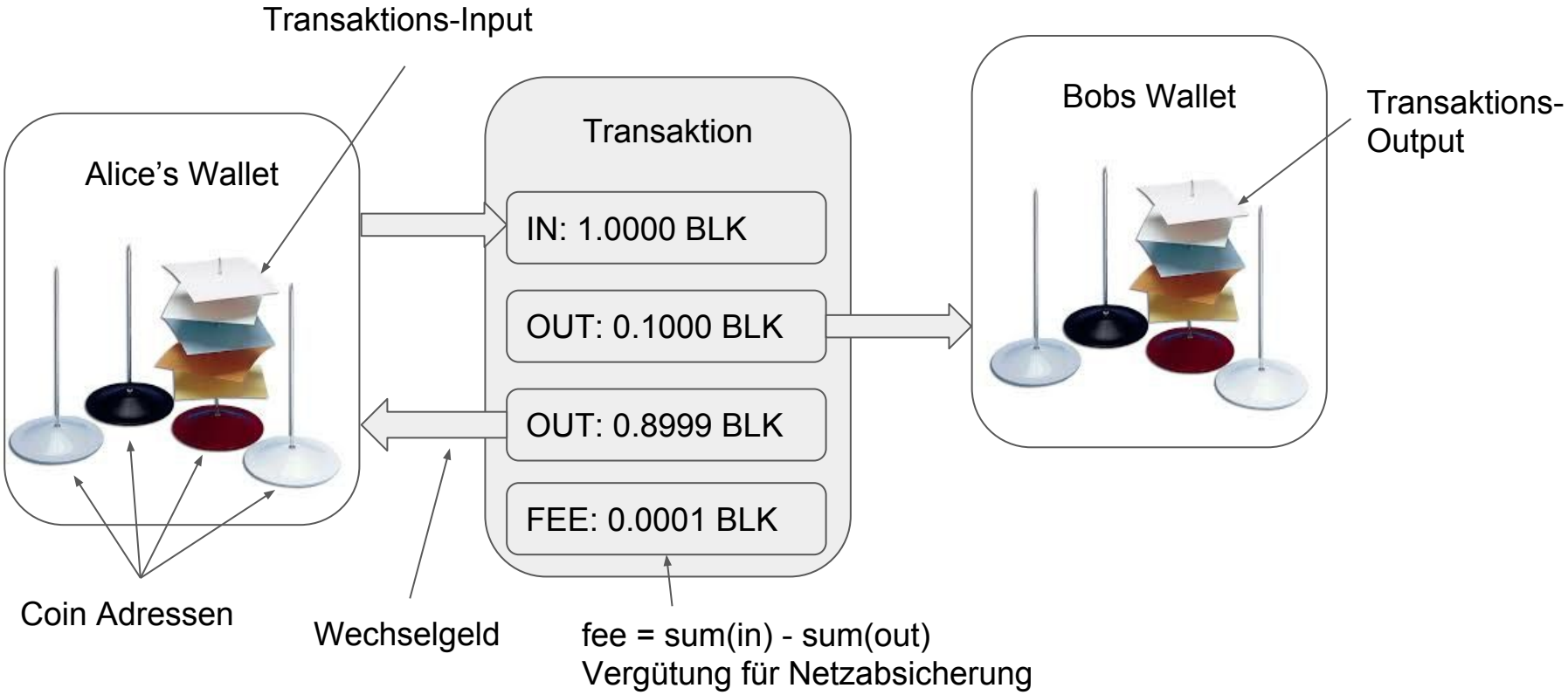
Noch zum Thema Börsen ….

Wer glaubt da noch an Zufall …

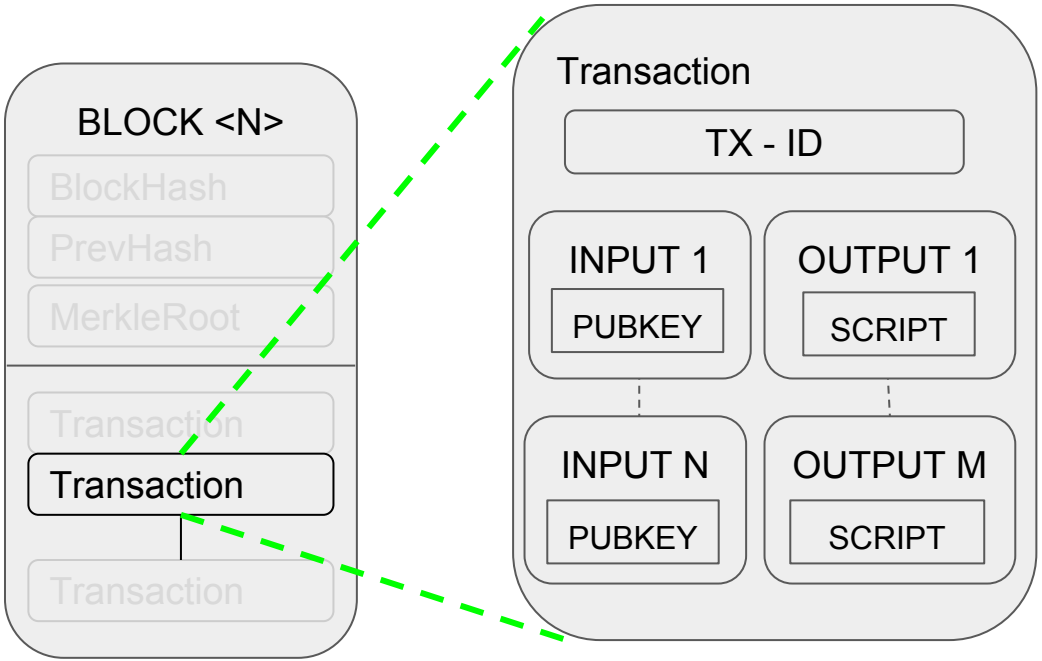




Analogie zur realen Welt



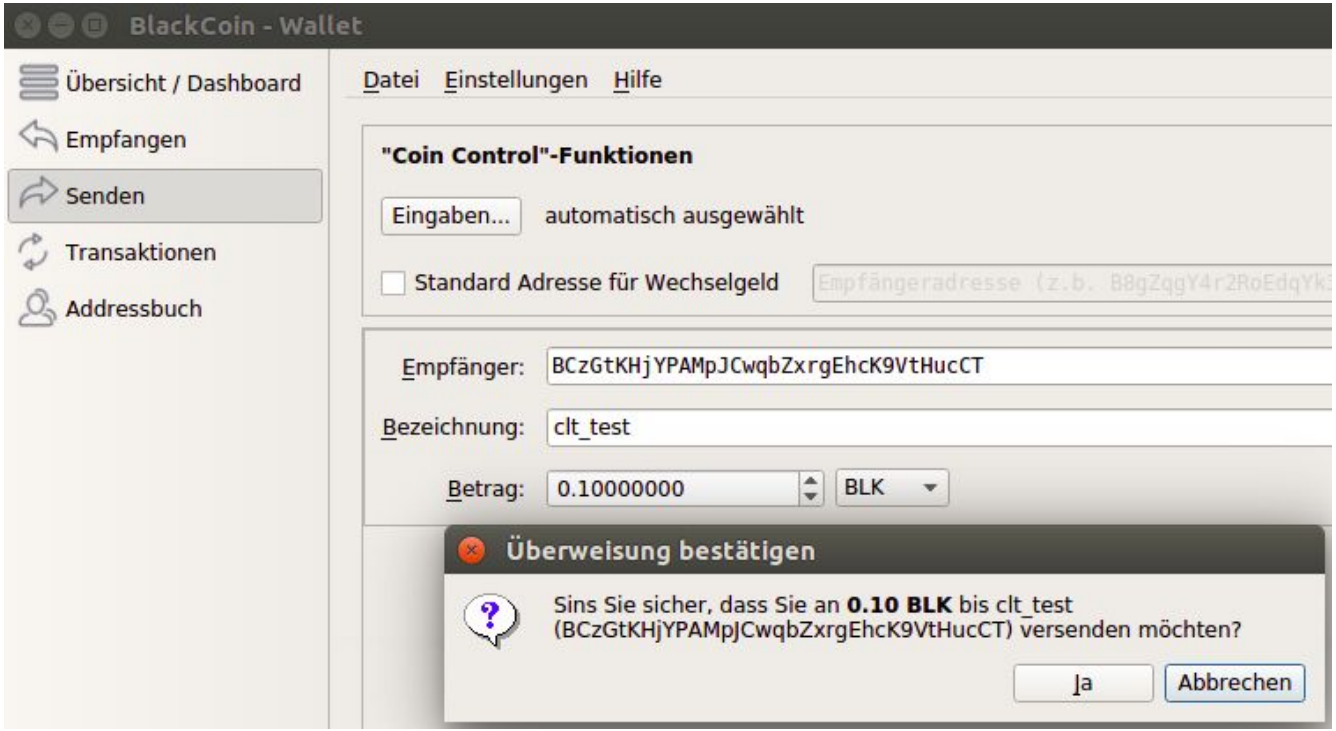
Transaktionen



- TX-ID
  eindeutige Nummer der Transaktion
- INPUT [1 … N]
  Referenz zu einer vorangegangen Überweisung
  + Öffentlichen Schlüssel (PUBKEY)
- OUTPUT [1 … M]
  Bitcoin-Adresse Empfänger
  + Betrag
- SCRIPT
  Programm zur Verifikation der Transaktion, normalerweise Signatur-Prüfung

Eine Beispielüberweisung

clicker-di-click … money go away!



Beispielüberweisung

Status: 0/unbestätigt, über 9 Knoten übertragen
Datum: 04.03.18 08:41
Belastung: -0.9999 BLK
Gutschrift: 0.9999 BLK
Transaktionsgebühr: -0.0001 BLK
Nettobetrag: -0.0001 BLK
Transaktions-ID:
cf1c3a41090eed159365359f36fffceeaf11c6a1d0219044862cd0724988dd41-000


```
Signatur Check Programm (FORTH Dialekt):
Vin:
     304402207c4b2512025b6… # sig for vout 0
     037df11ee96de189d8939…#  sig for vout 1
Vout:
     OP_DUP
     OP_HASH160
     685ec41781b916b2da56a4a80228b31875073baa
     OP_EQUALVERIFY
     OP_CHECKSIG
```

Rückverfolgung - Blockchain-Explorer

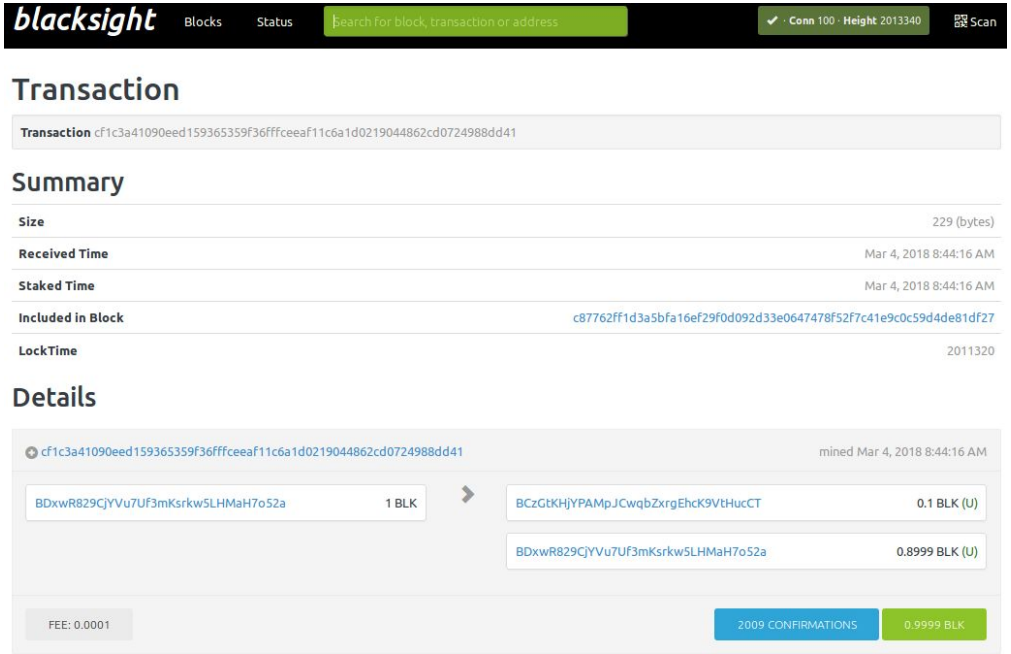
Anzeige des Blockchain-Inhaltes in menschenlesbarer Form.

BlackSight: Blockchain Explorer von BlackCoin

- https://node.blackcoin.io/insight

Cryptoid: Generischer Explorer für verschiedene Cryptos

- https://chainz.cryptoid.info/blk/



Staking

- Dient Absicherung des Netzwerkes und Generierung neuer Blöcke

- Voraussetzung:
  - Blackcoind/lored läuft permanent
  - Wallet ist zu Staking entsperrt (auf Applikationsebene, nur Selbstüberweisung möglich)

- Für einen neuen Block wird derzeit 1,5BLK ausgeschüttet + Fees der Transaktionen des Blockes.

Ausblick: Weitere Anwendungen

BlackHalo

- Software zur Erstellung von SmartContracts
- http://blackhalo.info/

IRIS

- Erstellung von Colored Coins & Multisignature Wallet
- https://iris.blackcoin.io/

Danke für die Aufmerksamkeit.

Gibt es noch Fragen ?

⇒ siehe Q&A auf den folgenden Slides.

Q&A #1

Q: *Stromverbrauch: Es fehlt die Gegenüberstellung mit kW/TX kosten bei anderen Dienstleistern wie VISA bzw. normalen Banküberweisungen, gibt es dazu Daten?*

A: Auf https://digiconomist.net/bitcoin-energy-consumption gibts dazu Antworten im Abschnitt “Comparing Bitcoin’s energy consumption to other payment systems”.

Der Hrsg. schränkt jedoch ein, dass die Daten z.B. von Visa nicht vollständig sind, z.B. der Office-Bedarf nicht enthalten ist.

Q&A #2

Anmerkung:

Nicht nur ewiges Logfile, auch Askemos.org a.k.a. "blockchain für smart contracts" gab es 2001 http://sf.net/projects/askemos

E**rgänzung:**

Leider hab ich die Vortraege in 2001 nicht gefunden, vielleicht wars ja auch ein anderes Jahr. https://chemnitzer.linux-tage.de/2001/vortraege/

Allenfalls ist es aber gut zu wissen, das die alten Programme erhalten geblieben sind.

Q&A #3

Q: Warum braucht man mehrere Wallets?

A: Leider kann ich nicht mehr nachfragen, ob Wallet oder Coin-Adresse gemeint war?

Mehrere Wallets sind an sich nicht erforderlich, man ist dann in der Verantwortung die per Backup akkurat zu sichern. Es ergibt sich aber zwangsläufig, wenn man z.B. die SW wechselt (z.B. BlackCoin-qt => lore-qt). In dem Fall sollte man alles vom alten auf das neue Wallet überweisen.

Mehere CoinAdressen sind eine “Sicherheit”, wenn ein PrivKey bekannt wird, sind nicht alle Coins weg.

Q&A #4

Ohne Gewähr!

Q: Was ist mit Bitcoin und Steuern?

A: Wenn das Finanzamt bemerkt das man einem Fiat-Gateway (sprich Coin-Börse) war, wird man Einnahmen und Ausgaben erklären müssen. Aufgrund der Eigenschaften der BlockChain kann es das auch viel später bemerken. Hier zwei Links als Apetizer, jedoch ohne Gewähr auf Korrektheit.

https://www.heise.de/newsticker/meldung/Richtig-versteuern-Kryptogeld-Millionaer-was-nun-3971930.html?seite=all

https://www.finanzgefluester.de/besteuerung-von-kryptowaehrungen/

Auf alle Fälle gilt: Alles Aufschreiben/Protokollieren und mit Steuerfachleuten die entsprechenden Anlagen ausfüllen.

Q&A: 5

Anmerkung:

Energie pro Transaktionen: mit dem Lightening Network wird die Kapazität dramatisch steigen und der Ressourcenverbrauch nur noch ein Bruchteil sein.

Anmerkung zur Anmerkung:

Mit dieser Technik habe ich mich noch nicht befasst, aber vielleicht gibts ja im nächsten Jahr ein Update zum Vortrag :-)

Q&A 6

Q: Proof of Stake = noch mehr Zentralisierung als PoW - da die Teilnehmer mit großen Kontoständen die Block-Rewards verdienen und tendenziell das Netzwerk kontrollieren.

A: Diese Frage ist interessant und veranlasste mich dann dochmal zu schauen, wie es in der Praxis aussieht. Wie bei PoW ist es auch bei PoS so, dass die Jungs mit den dicken Brieftaschen einen Vorteil haben. Ein 51% Angriff ist bei PoS und PoW Systemen gleichermassen unwahrscheinlich. Wer viel Geld in ein System steckt, wird es nicht “schrotten”. Auf der nächsten Folie habe ich mal die “Staker” der letzten 10000 BlackCoin Blöcke analysiert. (siehe Script staker.py im Monedero Repo).

Zu Q&A 6

```
BLRfF5SVxzBbmt7YKCAXH6fA4K6ia4M8o8 {'cnt': 582, 'sum': 2437.8505}
BEy8zHSbZ17XrhMCGVKqvwjN9adFXdNkCD {'cnt': 524, 'sum': 160.85}
BGpPm3hP7aHTwn6UjkZ5z1Df5dgZQhnVmk {'cnt': 505, 'sum': 833.8405}
BTJij8jAFrw6rYTctG1VqxFh3Tub6a7kz4 {'cnt': 430, 'sum': 103.7501}
B5N4XL1t23ic2EWqBYbiGbYyrUTeAVoaiL {'cnt': 309, 'sum': 208.98}
BCfkpRt5bG2ttYrza7BQGdVzdtVnzbQhs8 {'cnt': 272, 'sum': 159.32}
BTAWwhGxGqTs3kHb4nfYjbPQLyLamBqV4w {'cnt': 234, 'sum': 131.2501}
BDBzUazqFFasQQvxZgJER94XYtazKX813M {'cnt': 224, 'sum': 169.7063}
BMkPquNz3zzjCift68Y96Npp4U2YwnSN8y {'cnt': 221, 'sum':
609.36490939}
BPzYwAWmZGrorQ4u28qQsDi9iUpn82mcrx {'cnt': 212, 'sum': 740.8503}
BCRaeowCXGtrp9ZWt5kBmRvUWEKgmHt68j {'cnt': 209, 'sum': 252.81}
BDwjyPQ8Pe8QVgMPLLPcQeS2HwYMEW5eeR {'cnt': 198, 'sum': 4696.1}
BMt5fvB1v4aJMEaaFnJGotzhWYz98V9L1Y {'cnt': 188, 'sum': 127.9501}
BDAvWspRGDUW1JzqaRB3iuG8S62hUTmFbn {'cnt': 164, 'sum': 369.55}
BPUFi2KhB46RW1CujphivqZ7oXPWngRbTZ {'cnt': 185, 'sum': 199.36}
BBfyMah59Bq61YzPKGimW4YDNQd72NZm7t {'cnt': 152, 'sum': 192.69}
BLK88898Cxz6QhbUbckwRfN347F4tQWZj2 {'cnt': 149, 'sum': 170.77}
```

Untersucht wurden 10000 Blöcke, cnt ist die Block-Anzahl, die die Addr. erzeugt hat.

Diese 10000 Blöcke wurden durch 663 Adressen erzeugt.

In der Tat ist es so, dass die Top-Adresse in Summe 613909BLK an UTXOs hat und auf Platz 20 der “Rhich-List” rangiert.

Nummer 2 ist auf Platz 16 und hat sogar mehr BLK an UTXOs als Nr. 1.

Der letzte der Besten ist Nr. 61 und hat 221770 BLK an UTXOs.

Was man nicht weiss, wieviele Knoten im Netzwerk tatsächlich “staken”, die Anzahl aktiver Knoten gabs mal auf bitinfocharts.com, ist aber nicht mehr da.

Zu Q&A 6 - Zusammenfassend sei gesagt

1. “Ja, wer mehr BLK hat, staked auch öfter”. Die Division durch utxo.value (siehe Slide 7) ist die Ursache.
2. Es kommt auch darauf an, viele Lose im Topf zu haben (siehe for-Schleife auf Slide 7).
3. Jedoch macht man es sich schwerer, wenn man einen kleinen Betrag auf vielen UTXOs hat (siehe Division in Slide 7).
4. Diese Kurzuntersuchung ist nur eine Schlüssel-Loch-Statistik, aber vielleicht findet sich an einer Uni jemand, der das Thema mal gründlich aufs Korn nimmt.
5. Die Anzahl der aktiv “stakenden” Coins sieht man hier: https://chainz.cryptoid.info/blk/#!extraction

Q&A: 7

Q: Die weitaus meisten BTC Miner stehen auf Island und werden mit Geothermie betrieben (und vom Wind gekühlt) - also keine Angst um die Eisbären :-)

A: Ob dem tatsächlich so ist, vermag ich nicht zu sagen. Ein großer Teil der Miner ist sicher auch in China installiert (https://steemit.com/bitmain/@kenshishido/visit-to-bitmain-s-mining-facility-in-china-1-2). und dort geht man mit der Umwelt nicht unbedingt zimperlich um.

Demnächst soll das Mining in Island genauso viel Energie benötigen, wie die Einwohner des Landes. Das Argument mit der Geothermie ist nur ein Aspekt. Die “verhashte” Energie geht in Form von Wärme ungebremst durch die Decke des Rechenzentrums in die Umwelt. D.h. es entstehen Wärme-Einträge in Gegenden, in den es sonst eigentlich kalt sein sollte.