Einführung in die Bitcoin-Technology

Sep 2017

Agenda

- Einführung
- Virtuelle Währung
- Technology
  - Transaktion
  - Blockchain
  - Netzwerk
  - Mining
  - Wallet
  - Gefahren für BTC

Einführung - 1

- Bitcoin (BTC) ist eine digitale Währung, die elektronisch geschaffen (gemined) und verwahrt wird.
  Mit Bitcoins können Güter und Dienstleistungen erworben sowie Finanzmarktgeschäfte durchgeführt werden
- Der Bitcoin ermöglicht Transaktionen zwischen Sender und Empfänger, ohne dass dazu ein Dritter im Spiel ist, dem man vertrauen muss.
- Bitcoins werden nicht wie der Euro physisch gedruckt, sondern von vielen Menschen weltweit mit Computer errechnet
- Niemand kontrolliert die Währung. Das Netzwerk steuert sich selbst
- Bitcoins werden digital gespeichert
- BTC ist die bekannteste digitale Währung (auf Blockchain Prinzipien beruhen u. a. Ethereum, Monero, Litecoin, Dash, ...)
- Erfinder: Satoshi Nakamoto
  „Bitcoin: A Peer-to-Peer Electronic Cash System“ (31.10.2008)
  (Referenz: https://bitcoin.org/bitcoin.pdf)
  - Identität unbekannt
    (https://en.wikipedia.org/wiki/Satoshi_Nakamoto#Candidates)

Einführung - 2

- Wichtigste Eigenschaften
  - Dezentralität
  - Keine Kontrollinstanz (jeder kann Konto eröffnen)
  - Anonymität
  - Geringe Transaktionskosten
  - Geschwindigkeit
  - Weltweite Verfügbarkeit, weltweite Reichweite
  - Volle Eigenverantwortung
- Stand Jul 2017
  - viele Online Händler akzeptieren Bitcoins
  - >15.000.000 User
  - >7.700 Bitcoin-Nodes überwachen das Netz
  - Viele Börsen, e.g. https://localbitcoins.com

Einführung - 3

- Warum dieser Vortrag? Mich haben folgende Fragen interessiert:
  - BTC werden bei einer Börse mit richtigem Geld gekauft. Warum spricht man dann bei Bitcoins von Anonymität?
  - Woher kommen neue Bitcoins?
  - Wieso ist die Menge an BTC beschränkt?
  - Ein data mit gleichem Hash ist schwer zu finden… Wie schafft man es dann, dass alle 10 Minuten ein neuer Block gefunden wird?
  - Wieso klappt das, wenn die Rechnerleistung immer weiter steigt?
  - Je mehr TAs getätigt werden, um so länger muss es dauern zu überprüfen ob ein Eigentümer von BTC diese wirklich noch hat ???
  - ...

Einführung - 3

- Warum dieser Vortrag? Mich haben folgende Fragen interessiert:
  - BTC werden bei einer Börse mit richtigem Geld gekauft. Warum spricht man dann bei Bitcoins von Anonymität?
  - Woher kommen neue Bitcoins?
  - Wieso ist die Menge an BTC beschränkt?
  - Ein data mit gleichem Hash ist schwer zu finden… Wie schafft man es dann, dass alle 10 Minuten ein neuer Block gefunden wird?
  - Wieso klappt das, wenn die Rechnerleistung immer weiter steigt?
  - ...
- Antworten: siehe

Virtuelle Währung

- Was macht BTC interessant?
  - Interessante Eigenschaften (s. Einführung)
  - Glaube an seinen Wert
    (50 € Schein ist auch nur bedrucktes Papier)
  - Knappes Gut (wie Gold)
    - Mai 2017: 16,36 Millionen BTC
    - 2030: 21 Millionen BTC (max)
    - Ca. alle 10 Minuten werden (heute) 12.5 BTC neu „geschürft“

Virtuelle Währung - 2

- 2010: 1 Pizza: 5.000 BTC
- 2011: 1 BTC = 0,1 €
- 30.06.17: 1 BTC = 2235 €
- 06.09.17: 1 BTC = 3755 €

Transaktion

- BTC: Transaktions-Arten
  - Transfer
  - Generierung
- Elemente einer TA
  - Wer
  - An wen
  - Wie viel
  - Digitale Signatur

Transaktion

- BTC: Transaktions-Arten
  - Transfer
  - Generierung
- Elemente einer TA
  - Wer
  - An wen
  - Wie viel
  - Digitale Signatur

Transkationsliste

Ausgangspunkt: A hat 10 BTC

A: 4 BTC --> B
B: 2 BTC --> C
A: 4 BTC --> C
C: 3 BTC --> D
B: 1 BTC --> D
...

Zwischenstand:

A: 2
B: 3
C: 1
D: 4

Transaktion - 2

- Adressen anstelle von Namen
- Fortsetzung Beispiel

Zwischenstand:

X5kSZfA11mRUmTTkevl97Ycnex2gfL42dy/fey8UsF+3: 2

H0H+ki9q9pShywXPRS2vzx1SUQOo/TaafewLufwlcy: 3

Uchsu+fdsfsfd/kl3adfUj84js3KGkLCnewN37/fs+2dFd: 1

4FkV9jCldcnjqpsaKfLxbMn3md+dsj3jDjk6KH1hsadnB: 4

Transaktion - 2

- Adressen anstelle von Namen
- Fortsetzung Beispiel

Zwischenstand:

X5kSZfA11mRUmTTkevl97Ycnex2gfL42dy/fey8UsF+3: 2

H0H+ki9q9pShywXPRS2vzx1SUQOo/TaafewLufwlcy: 3

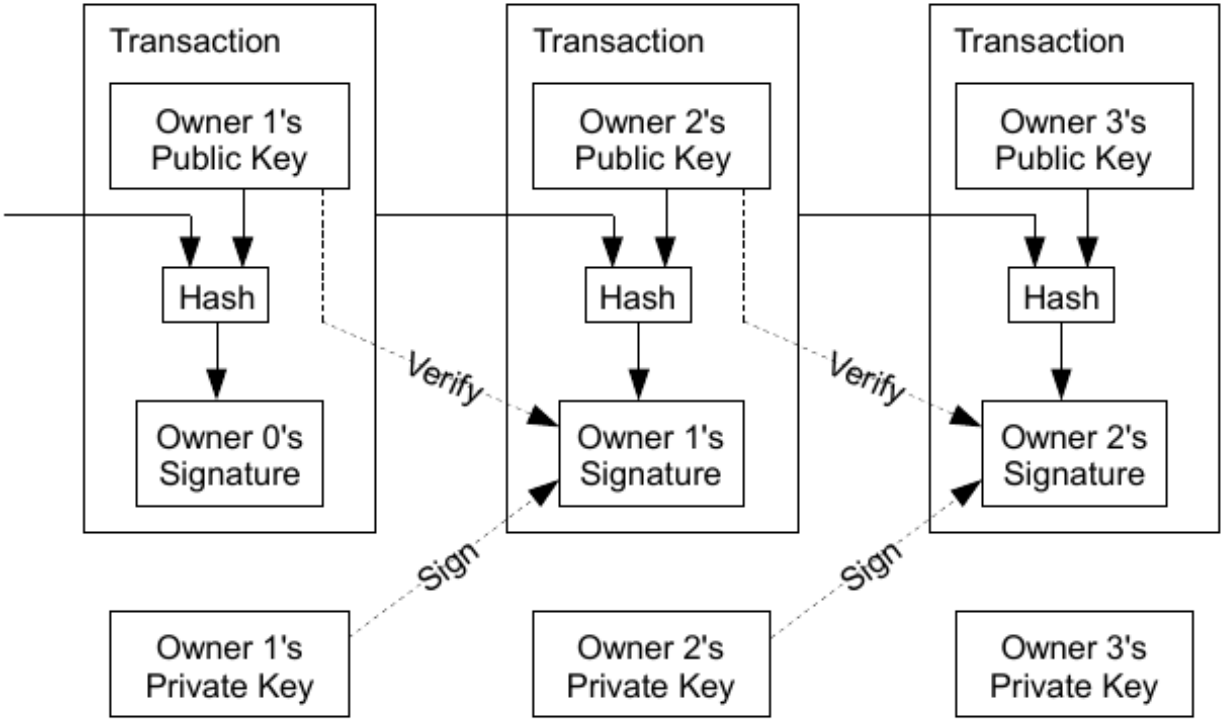
Uchsu+fdsfsfd/kl3adfUj84js3KGkLCnewN37/fs+2dFd: 1

4FkV9jCldcnjqpsaKfLxbMn3md+dsj3jDjk6KH1hsadnB: 4

- Adresse
  - Öffentlicher Schlüssel (Punkt auf elliptischer Kurve)
  - Kurve: Sec256k1 von SECG (Standards for Efficient Cryptographic Group)
  - Codierung: Base58 encoded string über Version + Hash of public key + Checksum

Idee einer Digitalen „Coin“

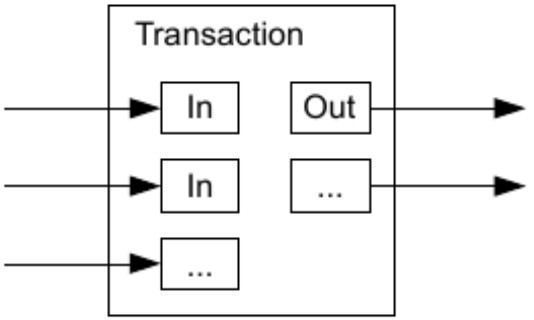
(Quelle: https://bitcoin.org/bitcoin.pdf)



- Coins können nur vom Eigentümer weitergereicht werden
- Bild Mitte: nach Unterschrift von Owner-1 gehört der Coin Owner-2

Transaktion - 3

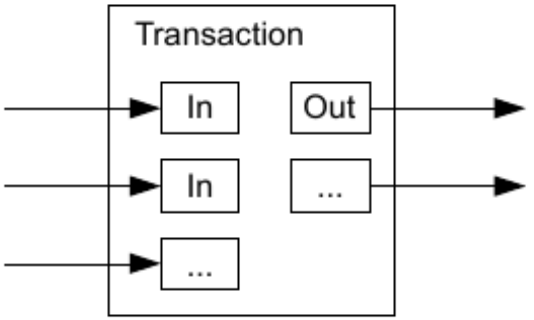
- Coins werden nicht einzeln weitergereicht
- Eine TA kann mehrere „Inputs“ und 1 oder 2 „Outputs“ enthalten
- Input:
  - 1 Input von einer früheren TA - oder
  - Kombination kleinerer Beträge von früheren TAs



Bildquelle:
https://bitcoin.org/bitcoin.pdf

Transaktion - 3

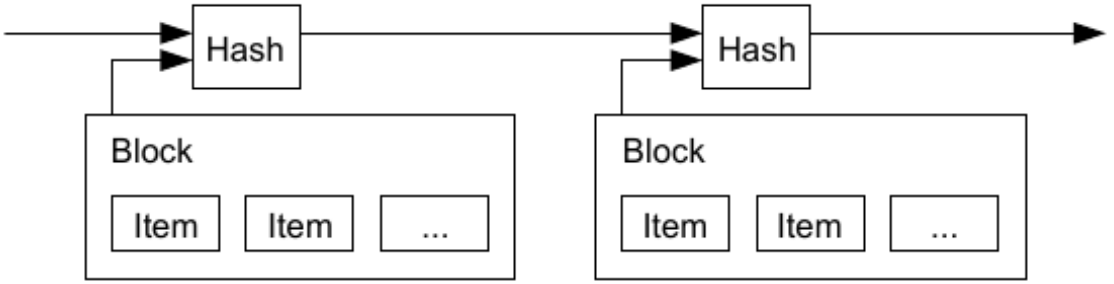
- Coins werden nicht einzeln weitergereicht
- Eine TA kann mehrere „Inputs“ und 1 oder 2 „Outputs“ enthalten
- Input:
  - 1 Input von einer früheren TA - oder
  - Kombination kleinerer Beträge von früheren TAs
- Ouput:
  - 1 Output für den Empfänger
  - Optional: 2. Output mit dem Restbetrag (der beim Sender verbleibt) an sich selbst
- → Nur die letzte TA einer „Kette“ enthält den Betrag, der dem Owner des public key gehört !



Bildquelle:
https://bitcoin.org/bitcoin.pdf

Blockchain

- Prinzip einer Blockchain

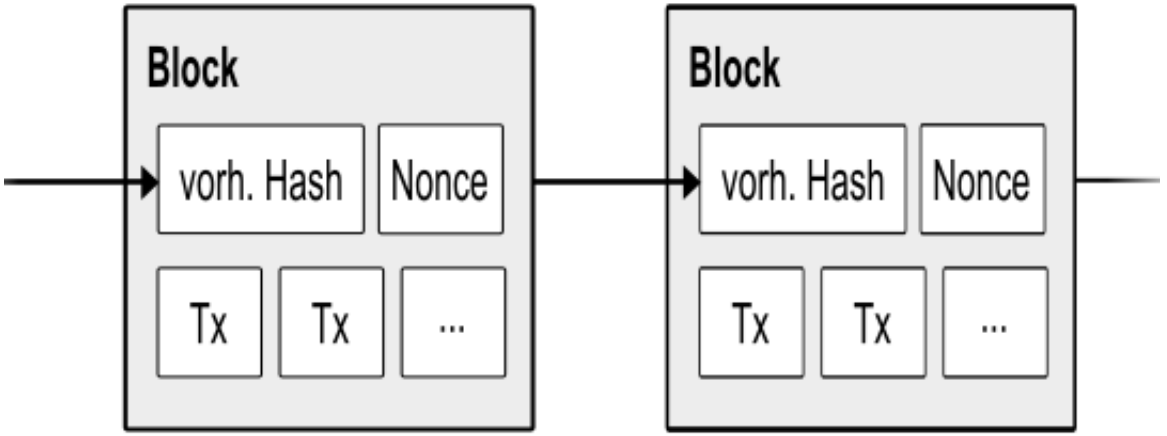


Bildquelle:
https://bitcoin.org/bitcoin.pdf

- Kann für viel mehr als nur virtuelles Geld genutzt werden
  - Interesse / Tests von Versicherungen, Autoverleihern, Energieversorgern, …
  - Projekt SeCoDE: Ziel Ladeinfrastruktur für E-Mobilität aufzubauen, die auf Blockchain Technologie beruht

Blockchain - 2

- BTC-Transaktionen werden in Blöcken gespeichert
- Ein neuer Block wird ca. alle 10 Minuten erzeugt
- Einen neuen gültigen Block „erzeugt“ der Client, der **zuerst** eine passende Nonce (beliebige Zahl) findet, die eine mathem. Aufgabe löst (dazu später mehr)
- Blöcke sind miteinander verlinkt
  → Vertrauenskette



Bildquelle:
https://bitcoin.org/bitcoin.pdf

Blockchain - 3

- Die Blockchain bildet ein digitales Transaktionsbuch
  - Enthält alle jemals gemachten TAs
  - Wird dezentral gespeichert (auf jedem full client im Bitcoin Netzwerk)
  - Die Blockchain ist „fälschungssicher“ (je länger, desto sicherer)
  - Größe Anfang Juli 2017: 120 GB

Netzwerk - 1

- Jeder node hat die gleiche (open source) Software (July 2017: > 7.700 nodes)

  Notation im folgenden: node meint „full node“

- Neue Nodes
  - Einige „DNS seeds“ sind hardcoded
  - Damit werden weitere Nodes gefunden

Netzwerk - 2

- Jede Transaktion wird publiziert, d.h. an alle nodes geschickt
- Jeder node kontrolliert jede publizierte TA
  - Ist die Signatur korrekt?
  - Ist die Ausgabe „gedeckt“?
- Eine gemachte TA kann niemals rückgängig gemacht werden

Netzwerk - 3

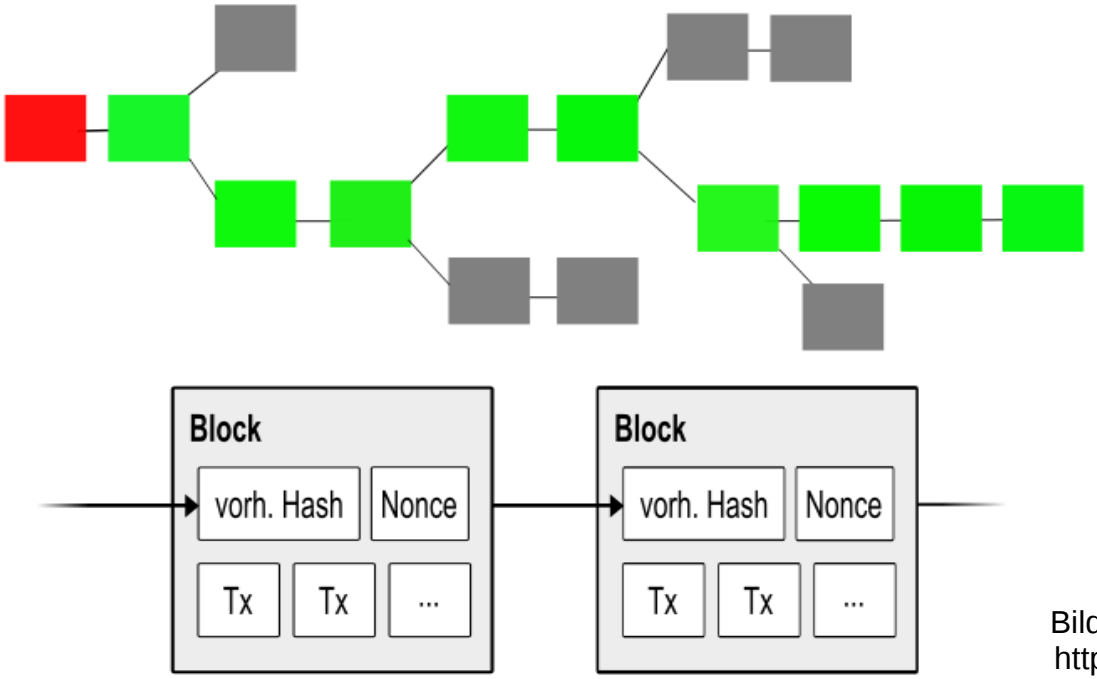
- Jeder node kontrolliert jeden publizierten Block
- Nach der Publikation einen Blocks fangen alle nodes mit den übrigen (und neuen) TAs einen neuen Block an

Detail (from Satoshi Nakamotos white paper)

- The problem of course is the payee can't verify that one of the owners did not double-spend the coin. A common solution is to introduce a trusted central authority, …
- We need a way for the payee to know that the previous owners did not sign any earlier transactions. For our purposes, the earliest transaction is the one that counts, so we don't care about later attempts to double-spend. The only way to confirm the absence of a transaction is to be aware of all transactions.
- To accomplish this without a trusted party, transactions must be publicly announced, and we need a system for participants to agree on a single history of the order in which they were received.
- The payee needs proof that at the time of each transaction, the majority of nodes agreed it was the first received.

Blockchain - 4

- Wenn ein neuer Block quasi gleichzeitig gefunden wird gewinnt die längste Kette (grün)
- Das System gilt als sicher, wenn die Mehrheit der benutzen Rechenpower ehrlichen nodes gehört
- Um zu fälschen müsste man alle nachfolgenden Blöcke „nach-erzeugen“



Bildquelle:
https://bitcoin.org/bitcoin.pdf

Detail (from Satoshi Nakamotos white paper)

- „… Proof-of-work is essentially **one-CPU-one-vote**. The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it. If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains...“

Zusammenfassung

- Jede Transaktion (TA) wird per broadcast an alle Clients verteilt
- Jeder Client sammelt mehrere neue TAs in einem neuen Block
- Jeder Client sucht dann eine passende „Nonce“
- Wenn gefunden, wird der neue Block an alle Clients geschickt
- Jeder Client kontrolliert alle TAs in dem neuen Block. Der neue Block wird nur akzeptiert, wenn alle TAs gültig sind (e.g. korrekte Unterschriften, Coins nicht bereits früher ausgegeben, ...)
- Clients beginnen dann mit einem neuen Block (und verwenden den Hash des gerade geprüften Blocks im neuen Block)

Note: Wenn 2 Clients „gleichzeitig“ einen neuen Block verteilen, verwenden sie den zuerst erhaltenen Block. Der andere wird für den Fall gespeichert, dass dieser in einer Kette verwendet wird, die danach länger wird. Falls ja, wird die längere Kette weiter verwendet.

Mining

- Warum stellen Benutzer ihre Rechenleistung zur Verfügung?
  - Als Belohnung bekommt der Client für jeden gefundenen neuen Block neue BTC (Generierung), die sie anschließend auf Marktplätzen verkaufen
  - Die erste Transaktion in einem Block ist eine „Generation Transaction“ (Generierung von neuen BTC)
    - Analogie zum „Gold **Mining**“
    - Ausgabe für 100 Blocks lang gesperrt

Mining

- Warum stellen Benutzer ihre Rechenleistung zur Verfügung?
  - Als Belohnung bekommt der Client für jeden gefundenen neuen Block neue BTC (Generierung), die sie anschließend auf Marktplätzen verkaufen
  - Die erste Transaktion in einem Block ist eine „Generation Transaction“ (Generierung von neuen BTC)
    - Analogie zum „Gold **Mining**“
    - Ausgabe für 100 Blocks lang gesperrt

  - Ausschüttung wird alle 4 Jahre halbiert (50, 25, 12.5, 6.25, …)
  - Gesamte Menge jemals erzeugte Bitcoins
    - Alle 10 Minuten ein neuer Block →

      6 * 24 * 365 * 4 * (50 * (1+ ½ + ¼ + **1/8** + …) =

      6 * 24 * 365 * 4 * 100 =

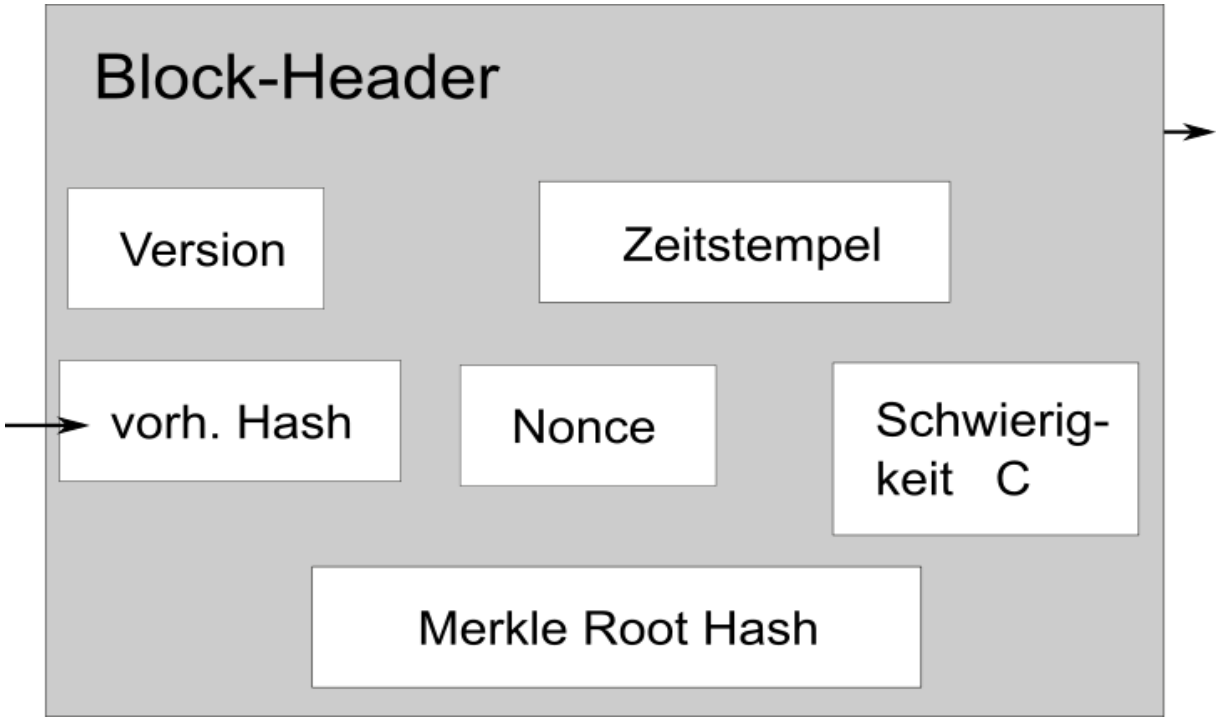
      21.024.000

Mining - 2

- Transaktions-Gebühr
  - Wird vom Bezahlenden angeboten
  - Wird vom Betrag der Bezahlung einbehalten
  - Wird dem Block-Erzeuger gutgeschrieben und 100 Blöcke lang gesperrt
  - Stand heute: wenige Cent je TA
- TA-Gebühr bietet weiteren Anreiz für
  - Miner
  - Bezahlender, damit seine TA schnell in einen gültigen Block kommt

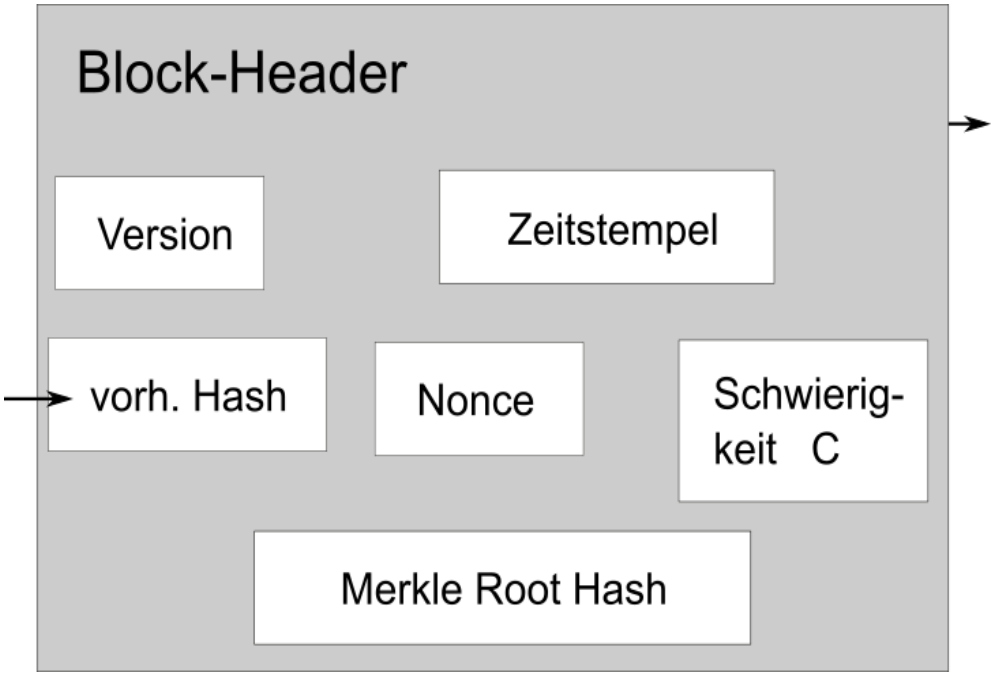
Mining - 3

- Ziel: im Mittel soll alle 10 Minuten ein neuer Block erzeugt werden, der die bis dahin neu aufgetretenen Transaktionen enthalten soll
- Aufgabe: Finde eine „Nonce“ (Bestandteil des Block-Headers) so dass ein gültiger Hash entsteht (SHA-256)



Mining - 3

- Ziel: im Mittel soll alle 10 Minuten ein neuer Block erzeugt werden, der die bis dahin neu aufgetretenen Transaktionen enthalten soll
- Aufgabe: Finde eine „Nonce“ (Bestandteil des Block-Headers) so dass ein gültiger Hash entsteht (SHA-256)
- Was ist ein gültiger Hash?
  Aufgabe:
  Hash des Blocks-Headers < C



- Beispiel: C=1024
  → Die ersten 247 Bit des Hash müssen 0 sein

Mining - 4

- Durch dynamisch anpassbare Vorgabe von C (target threshold) wird das Ziel „10 Minuten“ erreicht
- C ist ein 256-bit unsigned integer, der nach 2016 gefundenen Blöcken angepasst wird

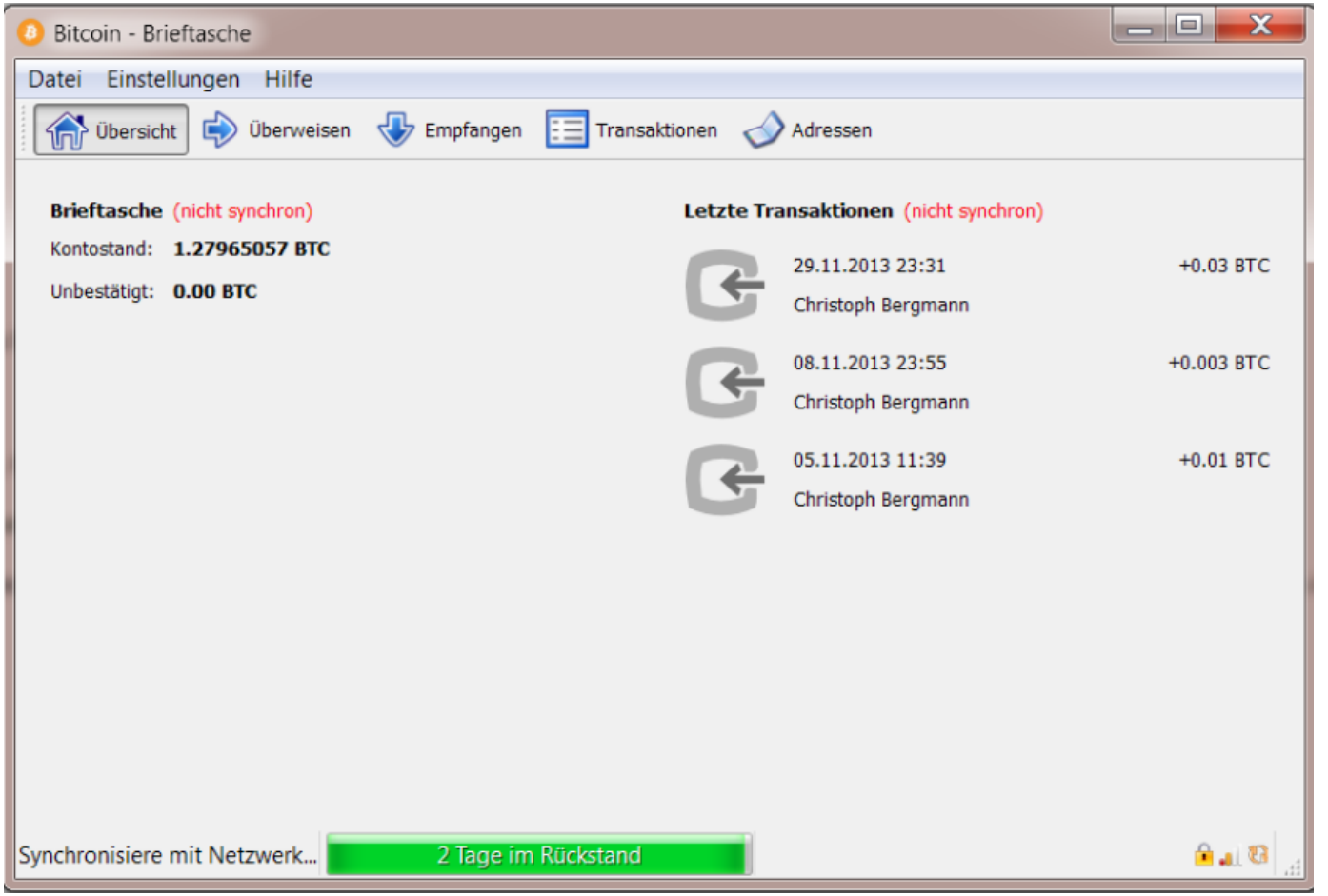
  (ca. 14 Tage: 6 * 24 * 14 = 2016)

Entwicklung des Minings

- Entwicklung des Mining
  - PC
  - Graphikkarten
  - Spezialhardware (ASIC)
  - Mining Pools
- Heute vor allem in China
- Wer heute seinen Computer minen lässt, bekommt weniger in Bitcoin, als er Strom verbraucht
- Für Privatleute eignet sich daher nur Cloudmining
  - Anteile auf Mining-Hardware kaufen
  - Anbieter des Cloudmining kauft und betreibt diese Hardware
  - Vertrauen nötig

Wallet - 1

- Zum Kaufen / Verkaufen braucht man eine Wallet
  - Reiche Auswahl, auch für PC and Smartphone
  - i.d.R. Thin Client
- Bitcoin-QT
  - Original
  - Open source
- Full client/node notwendig für Mining



Wallet - 2

- Funktionen einer Wallet
  - Bitcoins senden (Bezahlung)
  - Adressen als Zeichenfolge oder QR-Code anzeigen (Empfang von Bitcoins)
  - Eine Bezahlung signieren
  - Die Wallet mit einem Passwort verschlüsseln
  - Mehrere Schlüssel verwalten
  - Sicherung von privaten Schlüsseln
    !! Wer einen priv. Key kennt, kann die BTC dieser Adresse ausgeben !!
  - Neue Schlüssel generieren
- Sonderfunktionen einiger Wallets
  - Private keys und Signieren auf „offline“ Gerät
    - Anderer PC or Spezialhardware

Wallet - 3

- Privacy
  - Nach Kauf von BTC bei einem Broker ist Privacy nicht gegeben
  - Jeder kann neue public/private keys generieren
  - (Teilweiser) Transfer des eigenen Guthabens zu einem eigenen anderen public key stellt die privacy her
  - Ein Adresse (pub key) sollte nur für eine TA verwendet werden

Gefahren für BTC

- Währungsschwankungen
- Spekulation
- Schrumpfender Gewinn der Miner
  - Ohne Miner wird das System unsicher
    (TA-Gebühren gleichen dies aus)
- Skalierbarkeit (→Bitcoin-Fork August ´17 → Bitcoin Cash)
- Regulierung
  - EU Commisision: Anti-Geldwäsche Regeln
  - Auch Wallets sollen den Geldwäsche-Regularien unterstehen
  - Bitcoin Startups verlassen die EU
- *Eingeschränkt: Quantencomputer*
  - *Transaktion-ID enthält nur Hash des Public key*
  - *Erst beim Bezahlen taucht der public key sichtbar auf*
  - *→ wenn key nur 1x verwendet wird, könnte Quantencomputer nur agieren bevor TA in einem Block ist*

Literatur

- https://bitcoin.org/en/developer-reference
- https://bitcoin.org/en/developer-documentation
- White Paper: https://bitcoin.org/bitcoin.pdf
- https://bitcoin.org/de/waehlen-sie-ihre-wallet
- Suche nach Block-Hash or TA or Adresse:
  https://blockchain.info (Suche)
  https://blockchain.info/de/charts (Charts)
- Crypto Currency Market Capitalisations:
  https://coinmarketcap.com
- Mining Pool:
  e.g. https://cryptogold.com/
- http://www.finanzen.net/nachricht/devisen/nach-bitcoin-split-das-sind-die-unterschiede-zwischen-bitcoin-und-bitcoin-cash-5635958

Backup

Hash Function - 1

- Eine Hash Function ist eine Abbildung eines beliebig langen Datenblocks (z. B. Softwarepaket, Datei, String, Nachricht, …) auf einen Bytestring einer festen Länge
  - Bekannte Hash Funktionen:
    - MD5: 16 Byte (veraltet, gilt als unsicher)
    - SHA1: 20 Byte (nicht mehr empfohlen)
    - SHA256: 32 Byte (für Bitcoin verwendet)
- Beispiele
  - echo „123“ | shasum → a8fdc205a9f19cc1.c7507a60c4f01b13d11d7fd0
  - echo „124“ | shasum → c62fb32eadd5a0fc.ceb1ddf2697e2345c604f451
  - echo „123“ | sha256sum → 181210f8f9c779c2.6da1d9b2075bde01.27302ee0e3fca38c.9a83f5b1dd8e5d3b
  - echo „124“ | sha256sum → ca2ebdf97d746949.6b1f4b78958f9dc8.447efdcb623953fe.e7b6996b762f6fff

Hash Function - 2

- Eigenschaften
  - Einwegfunktion, nicht umkehrbar (mathem.: nicht bijektiv)
  - Abbildungsmenge ist „gleichmäßig verteilt“
  - Ein Hash kann schnell berechnet werden
  - Umkehrung sehr schwierig/rechenintensiv (anderen input string mit gleichem Hash zu finden)
- Anwendungsfälle
  - Prüfsummen (z. B. bei ausgelieferter Software)
  - Im Umfeld von digitalen Signature wird der Hash einer Nachricht signiert (anstelle der Nachricht selber)
- Literatur

  https://en.wikipedia.org/wiki/Comparison_of_cryptographic_hash_functions