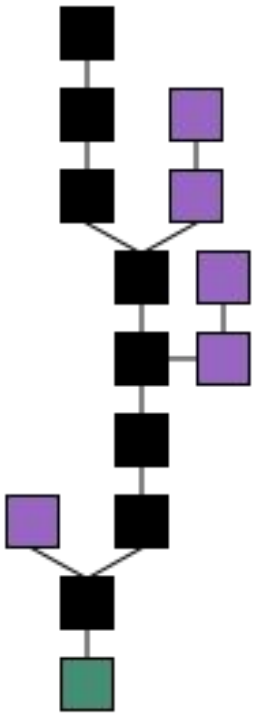
Transparenz im Bitcoin Netzwerk

13.04.2017, Andreas Petersson

Blockchain - Anwendungen heute

- Digitales Cash
- Universelle weltweite Währung
- Gaming
- Setzt neue Standards bei der Sicherheit
- Spekulation
- Basis für andere Finanzprodukte

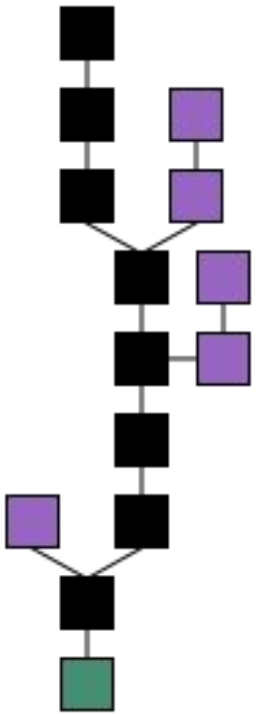
Welches Kernproblem wird gelöst?



Wikipedia,
CC-BY-3.0

- Verteilte weltweite Datenbank
- Viele Teilnehmer → **eine** Wahrheit
- Konsens ohne Vertrauen/Kooperation

Anwendung Bitcoin:
Blockchain als Ledger löst das “Double Spending”–Problem.

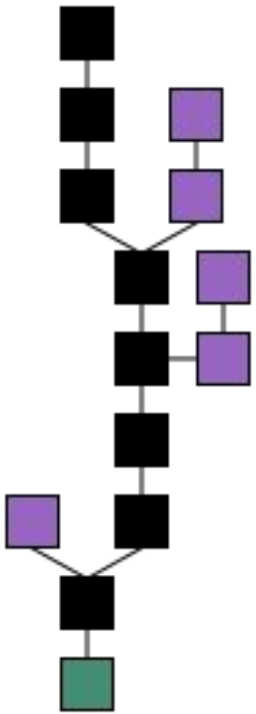


Wikipedia,
CC-BY-3.0

Was ist eine “Blockchain”?

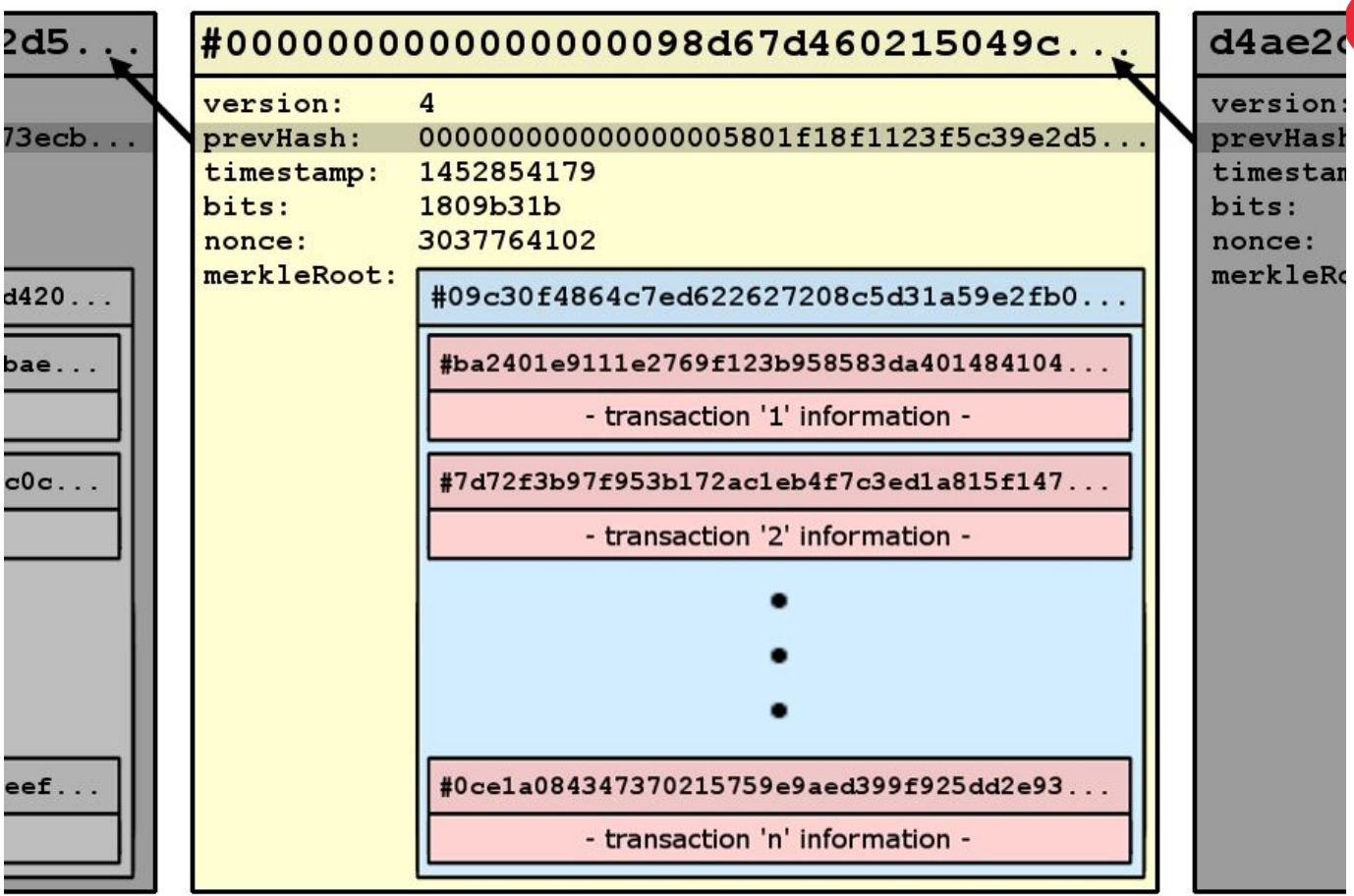
- Jeder Block ist ein unveränderlicher Datensatz (beinhaltet Transaktionen, etc.)
- Referenzierung auf vorhergehenden Block (am Anfang ein “Genesis”-Block)
- Die Blöcke müssen von allen akzeptiert werden
- Mehrere neue Blöcke?
  → Längste Kette ist die “Wahrheit”

Wann spricht man von einer Blockchain?



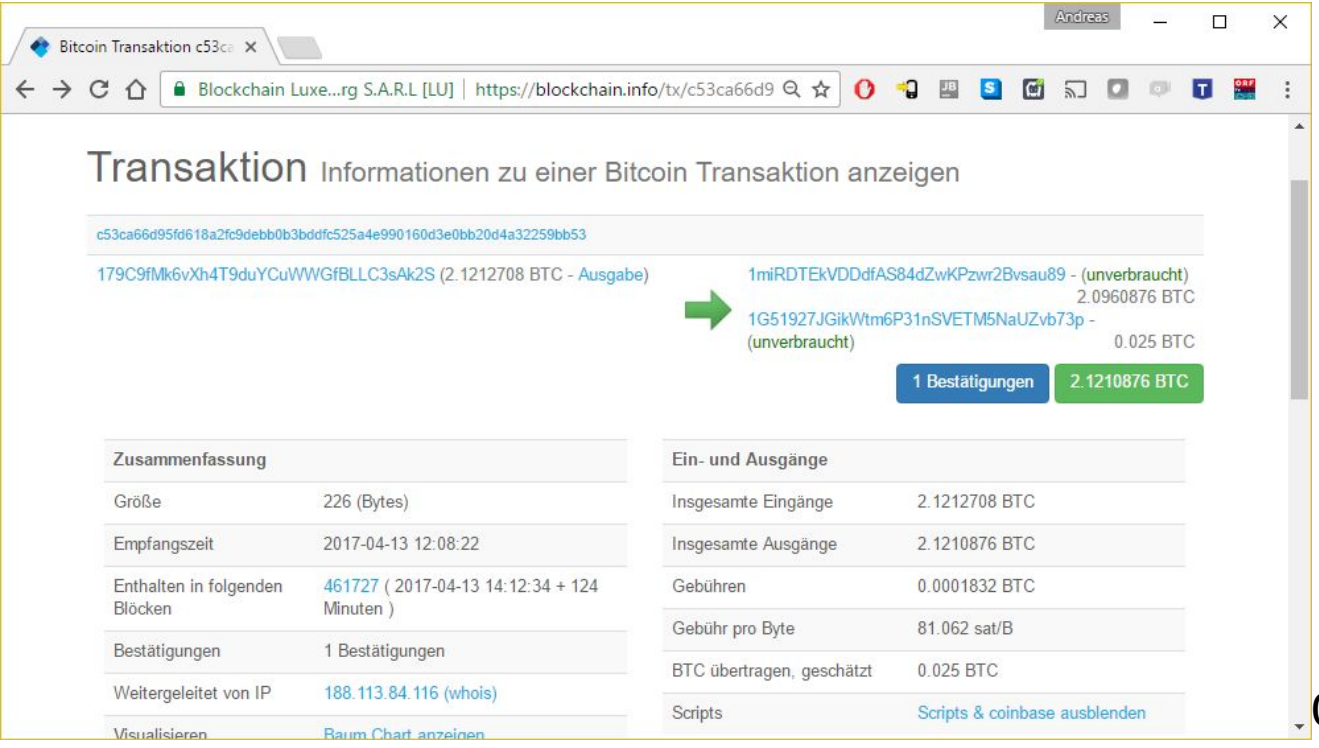
Wikipedia,
CC-BY-3.0

- Die Kernfunktion ist die Anordnung der Transaktionen, sodass keine Konflikte entstehen können
- Welche Blockstruktur, welcher Konsensalgorithmus und welche Interpretation gewählt wird, sind optional

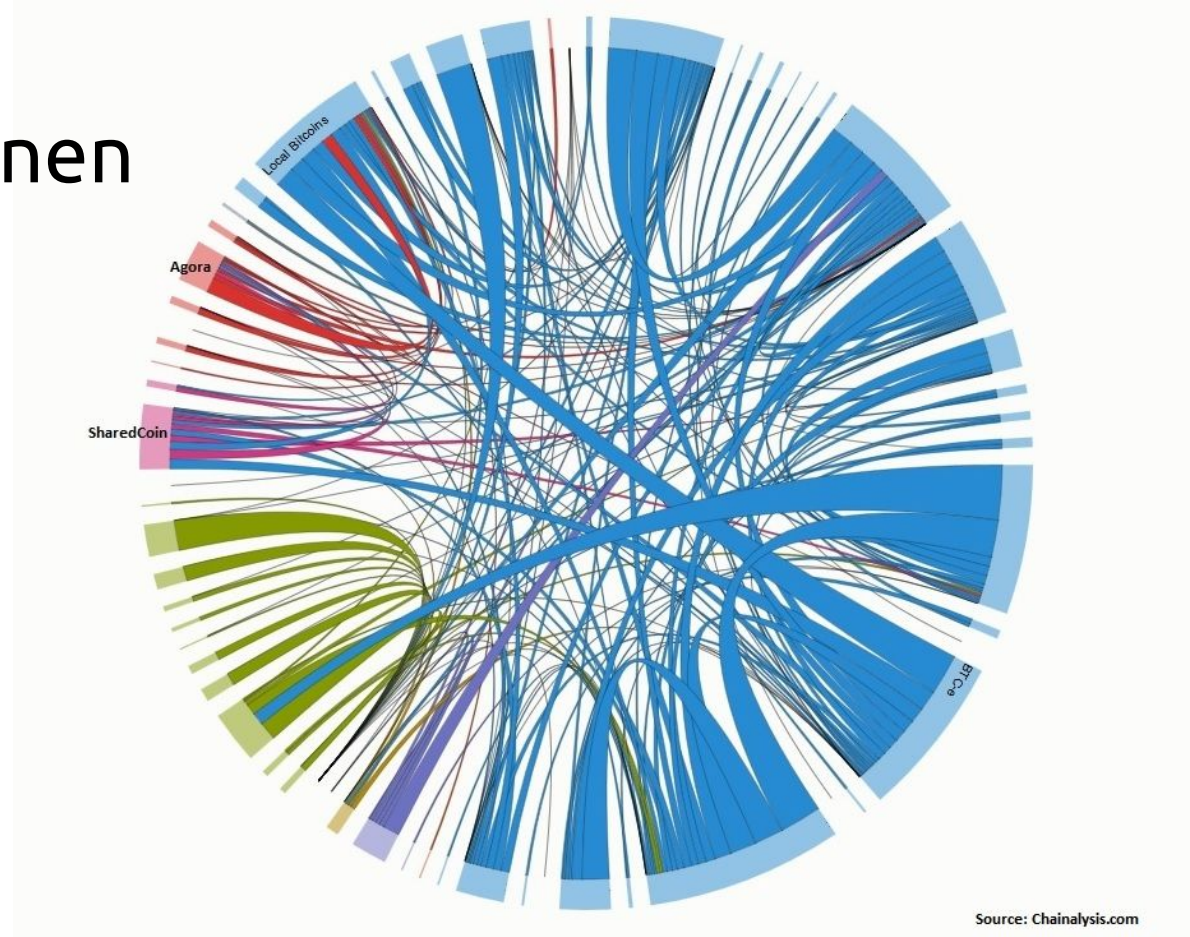


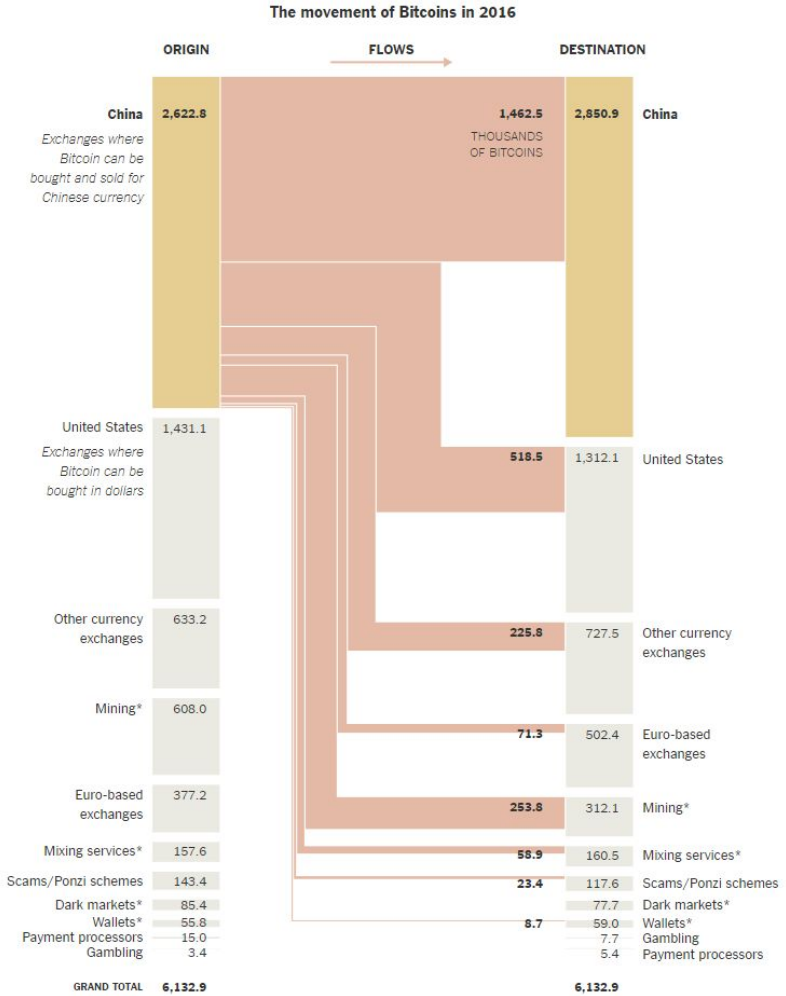
13.04.2017, Andreas Petersson

Beispiel einer Transaktion



Bitcoin Transaktionen 2015





Bitcoin Transaktionen 2016

Quelle: chainalysis.com/
nyt.com

13.04.2017, Andreas Petersson

Eigenschaften als Bezahlsystem

- Gebühren zahlt der Sender
- “Bearer Ecash”
- Irreversibel
- Keine Genehmigungen notwendig
- Nicht anonym
- Währung wird frei gehandelt, schwankt
- Überall verwendbar

Integration von Zahlungsströmen

- Grösstenteils manuelle Anpassungen am IT System notwendig
- Software wie z.b. BitcoinJ bietet eine Grundlage
- Anbieter wie Bitpay automatisieren Vorgänge

Praxis als Bezahlsystem

- Anbieter wie Bitpay, Coinbase übernehmen der Währungsrisiko
- Unabhängigkeit trotzdem möglich
- Großteil der Steuerfragen mittlerweile geklärt

bitcoin austria

Danke für Ihre Aufmerksamkeit!

13.04.2017, Andreas Petersson