



Transparenz im Bitcoin Netzwerk



Blockchain - Anwendungen heute

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

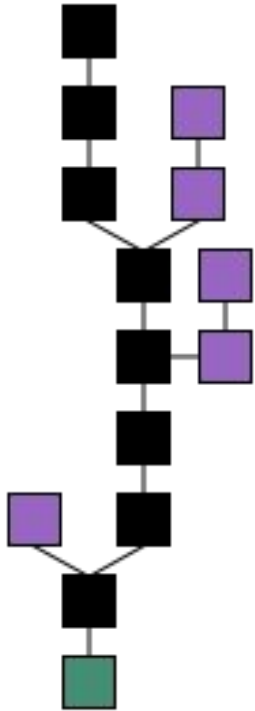


Welches Kernproblem wird gelöst?

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

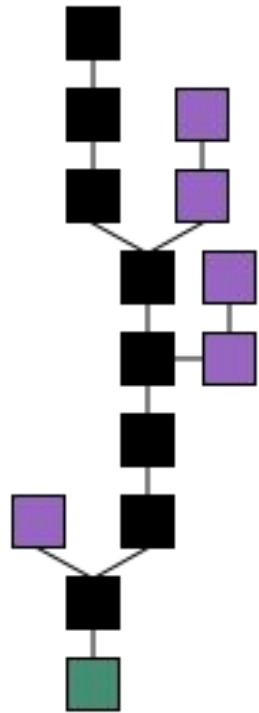
Anwendung Bitcoin:

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





Was ist eine “Blockchain”?

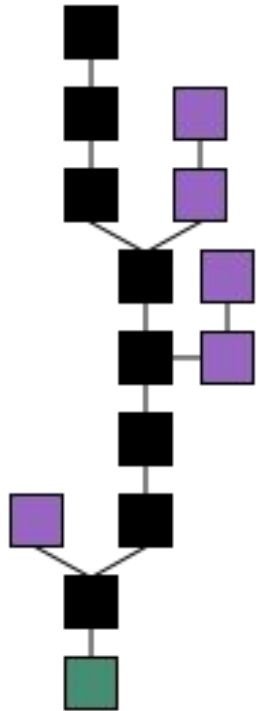


- Jeder Block ist ein unveränderlicher Datensatz (beinhaltet Transaktionen, etc.)
- Referenzierung auf vorhergehenden Block (am Anfang ein “Genesis”-Block)
- Die Blöcke müssen von allen akzeptiert werden
- Mehrere neue Blöcke?
→ Längste Kette ist die “Wahrheit”

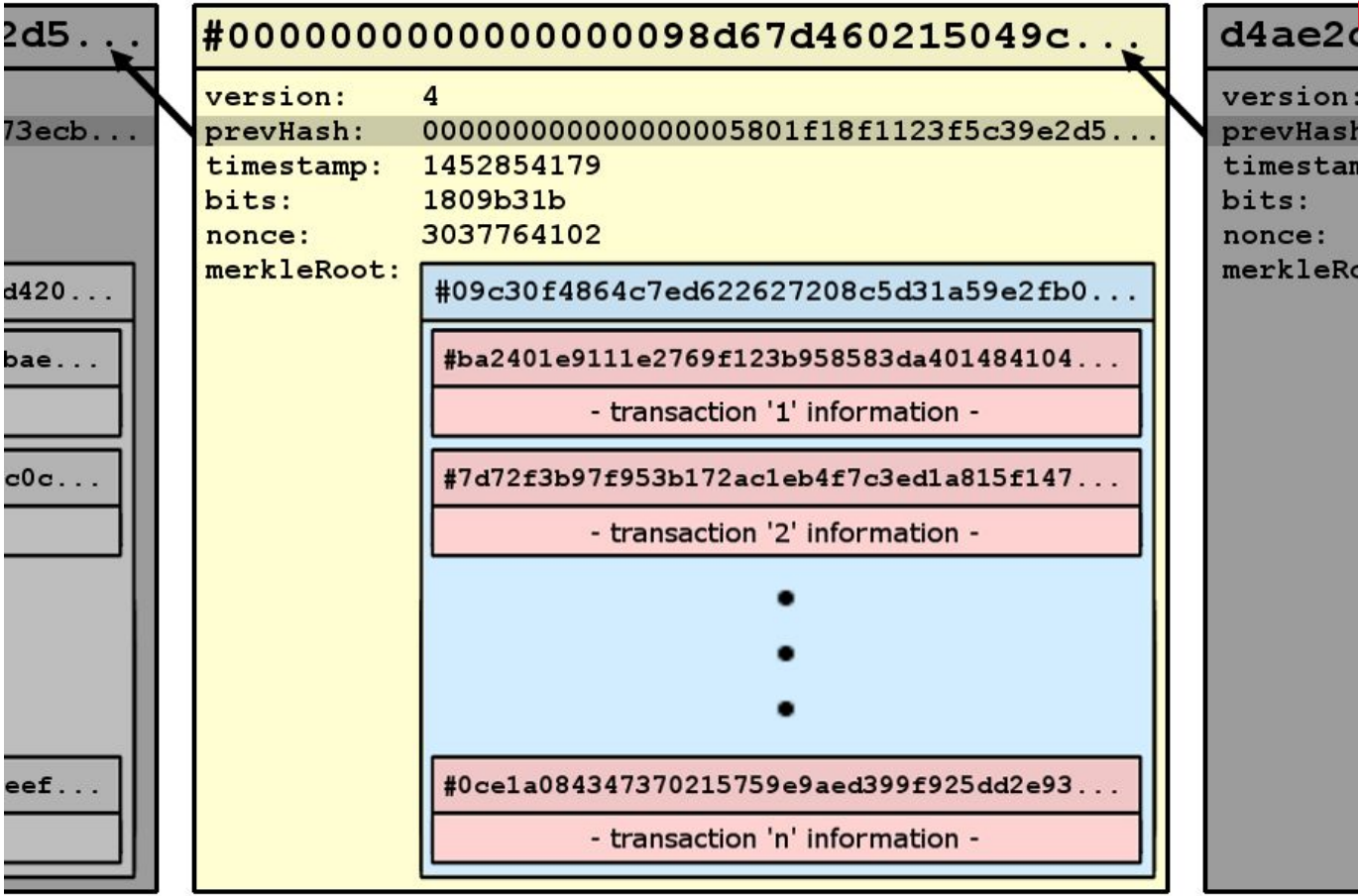
Wikipedia,
CC-BY-3.0



Wann spricht man von einer Blockchain?



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





Beispiel einer Transaktion

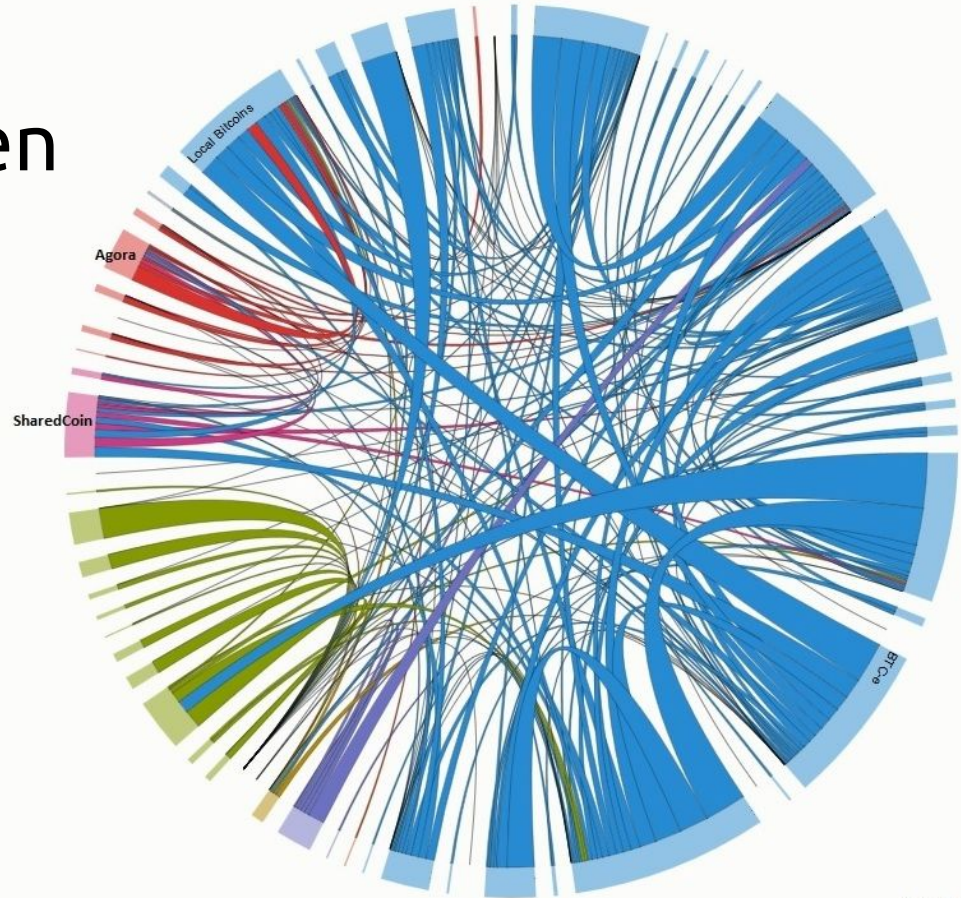
The screenshot shows a web browser window with the URL <https://blockchain.info/tx/c53ca66d9>. The page title is "Transaktion Informationen zu einer Bitcoin Transaktion anzeigen". The transaction ID is `c53ca66d95fd618a2fc9debb0b3bddfc525a4e990160d3e0bb20d4a32259bb53`. The transaction details show an input of `179C9fMk6vXh4T9duYCuWWGfBLLC3sAk2S` (2.1212708 BTC - Ausgabe) and two outputs: `1miRDTEkVDDdfAS84dZwKPzwr2Bvsau89` (2.0960876 BTC, unbraucht) and `1G51927JGikWtm6P31nSVETM5NaUZvb73p` (0.025 BTC, unbraucht). A green arrow points from the input to the second output. Summary statistics include 1 confirmation and a total value of 2.1210876 BTC. Two tables provide further details: "Zusammenfassung" and "Ein- und Ausgänge".

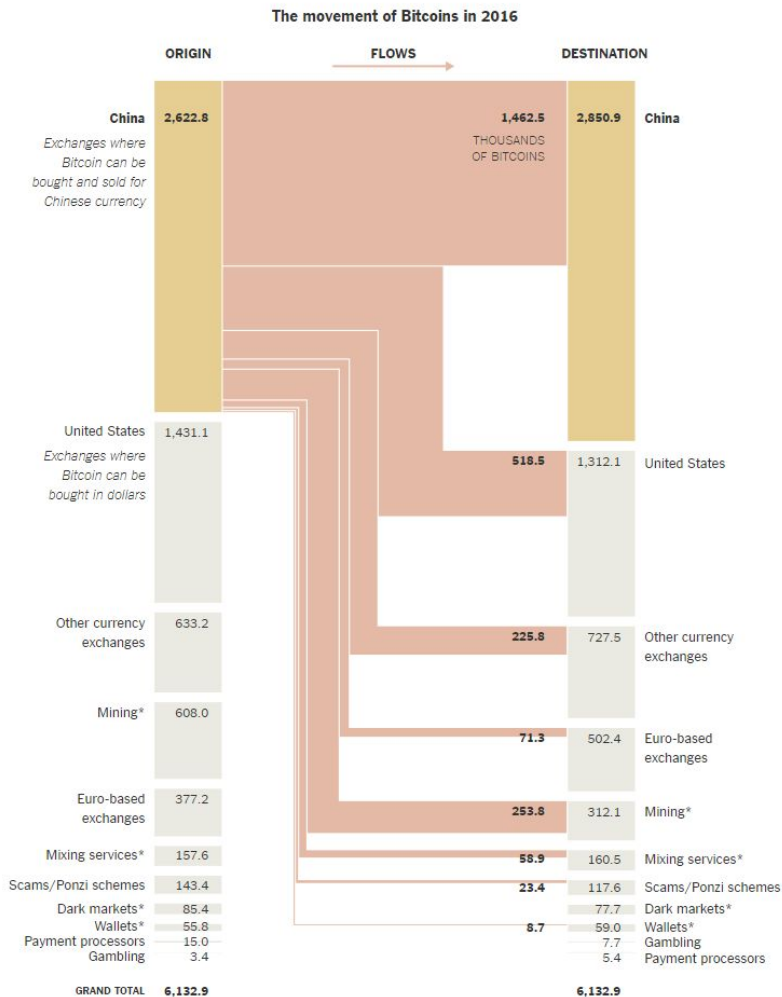
Zusammenfassung	
Größe	226 (Bytes)
Empfangszeit	2017-04-13 12:08:22
Enthalten in folgenden Blöcken	461727 (2017-04-13 14:12:34 + 124 Minuten)
Bestätigungen	1 Bestätigungen
Weitergeleitet von IP	188.113.84.116 (whois)
Visualisieren	Baum Chart anzeigen

Ein- und Ausgänge	
Insgesamte Eingänge	2.1212708 BTC
Insgesamte Ausgänge	2.1210876 BTC
Gebühren	0.0001832 BTC
Gebühr pro Byte	81.062 sat/B
BTC übertragen, geschätzt	0.025 BTC
Scripts	Scripts & coinbase ausblenden



Bitcoin Transaktionen 2015





Bitcoin Transaktionen 2016

Quelle: chainalysis.com/
nyt.com



Eigenschaften als Bezahlungssystem

- 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 Bezahlungssystem

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



Danke für Ihre Aufmerksamkeit!

CC-BY 4.0 // 2016