



Bitcoin, technische Grundlagen



Zuerst gab es Wert

- Eine Sache hat Wert
- Eine Erwartungshaltung der zukünftigen Nützlichkeit
- Niemals absolut über die Zeit



Dann gab es Geld.

Seltenheit

Haltbarkeit

Teilbarkeit

Verifizierbarkeit

Transportfähigkeit

Austauschbarkeit



Bitcoins Genesis

- 18. August 2008 Name reserviert
- Publiziert Anfang 2009.
- Kein Wert
- Hobbyprojekt und “unmöglich”



Bitcoins Eigenschaften als Geld

Seltenheit 😊

Haltbarkeit 😊/☐

Teilbarkeit 😊

Verifizierbarkeit ☐

Transportfähigkeit 😊

Austauschbarkeit ☐



Endgeräte, welche Bitcoin benutzen

- Handy
- Laptop/Desktop
- Server
- Hosted “Wallet”, Browser Lösungen



Wie bekomme ich eine Adresse?

Es gibt keine künstlichen Zutrittsbarrieren

Eine Bitcoin Adresse wird von einem geheimen “**Private Key**” abgeleitet.

Jeder kann so einen Schlüssel erzeugen: es gibt **keine Registrierung**, es braucht **keine Erlaubnis** eingeholt werden, **kein Name**, **keine Emailadresse**, **kein Passwort**, **kein Ausweis**, **kein Foto**, **keine Behörde**, **keine Bank**, niemand!



Wert von Bitcoin

- 5 .October 2009: Erster Bitcoin Broker
\$1.00 USD=1,309.03 BTC 10/05/2009
- 22. May 2010 - Berühmte Bitcoin Pizza um 10,000 BTC - erste “echt-welt” transaktion
- 12 July 2010 - Erste “Bitcoin Bubble” mit 10x Wachstum



Blockchain - Anwendungen heute

- Digitales Cash
- Universelle weltweite Währung
- Setzt neue Standards bei der Sicherheit
- Spekulation
- Basis für andere Finanzprodukte
- Grundlage für Smart “Contracts”

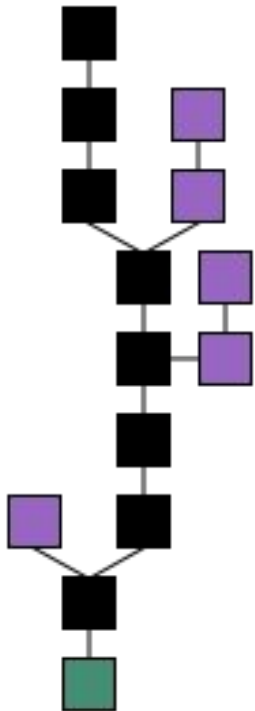


Welches Kernproblem wird gelöst?

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

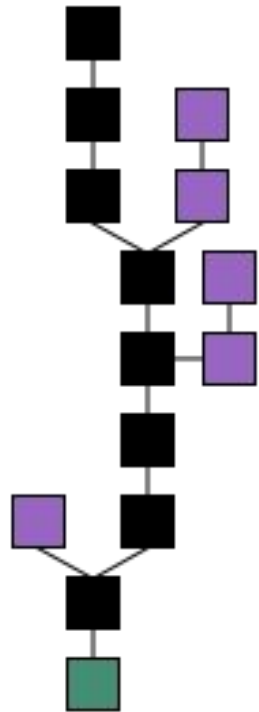
Anwendung Bitcoin:

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





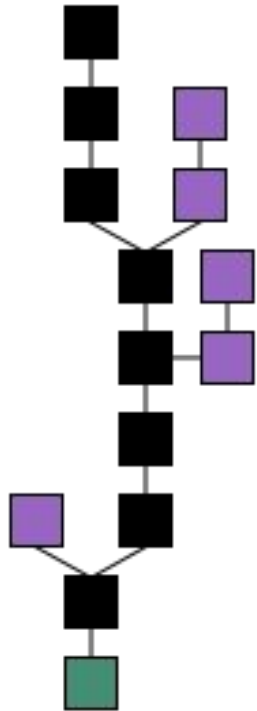
Was ist eine “Blockchain”?



- 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”



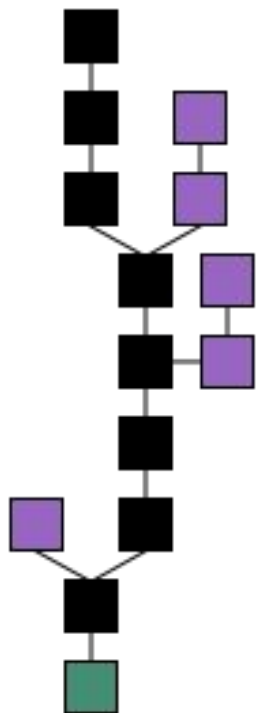
Wann spricht man von einer Blockchain?



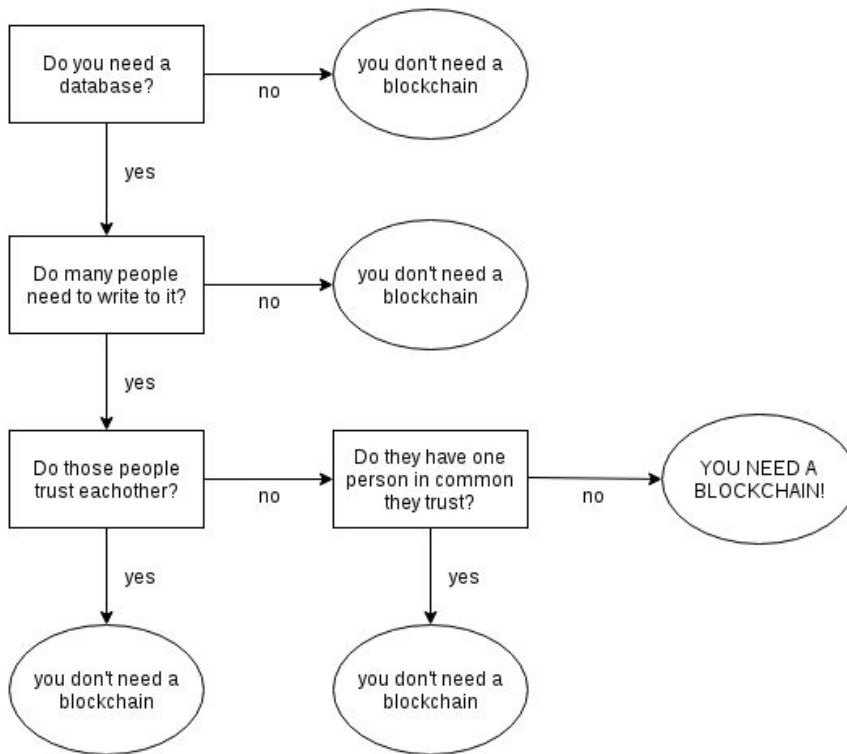
- Die Kernfunktion ist die Anordnung der Transaktionen, sodass keine Konflikte entstehen können
- Welche Blockstruktur, welcher Konsensalgorithmus und welche Interpretation gewählt wird, sind optional



Wann braucht man eine Blockchain?



Wikipedia,
CC-BY-3.0





Beispiel einer Transaktion

The screenshot shows a web browser window displaying a Bitcoin transaction on the blockchain.info website. The browser's address bar shows 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 `179C9fMk6vXh4T9duYCuVWVGfBLLC3sAk2S` (2.1212708 BTC - Ausgabe) and two outputs: `1miRDTEkVDDdfAS84dZwKPzwr2Bvsau89` (2.0960876 BTC, unverb. verbraucht) and `1G51927JGikWtm6P31nSVETM5NaUZvb73p` (0.025 BTC, unverb. verbraucht). A green arrow points from the input to the outputs. Summary statistics include "1 Bestätigungen" and a total value of "2.1210876 BTC". Below the main content are two tables: "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 |



Thanks for your attention

CC-BY 4.0 // 2017