bitcoin austria

Bitcoin, technische Grundlagen

18.10.2017, Andreas Petersson

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.

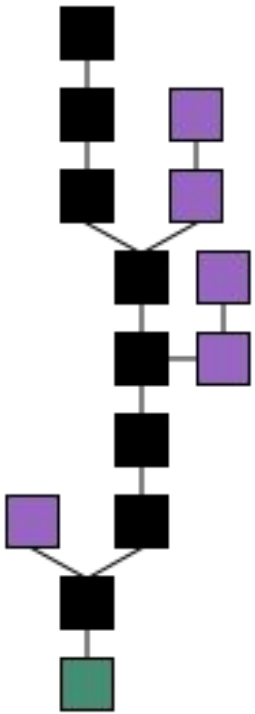
Jeder kann so einen Schlüssel erzeugen: es gibt **keine Registrierung**, es braucht **keine Erlaubnis** eingeholt werden, **kein Name**, **keine Emailadresse**, **kein Passwort**, **kein Ausweis**, **kein Foto**, **keine Behörde**, **keine Bank**, niemand!

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”

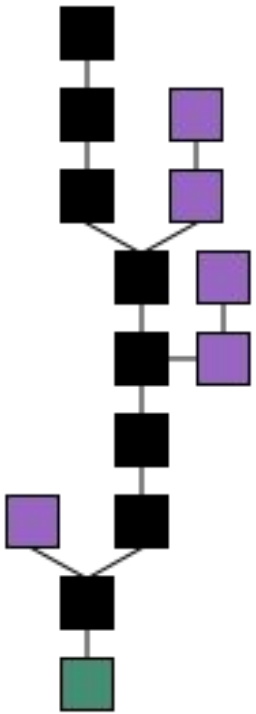


Wikipedia,
CC-BY-3.0

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.



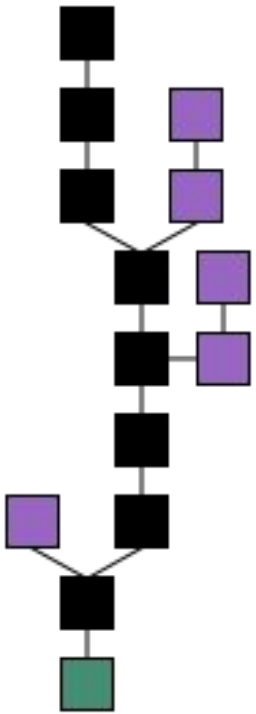
Wikipedia,
CC-BY-3.0

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”

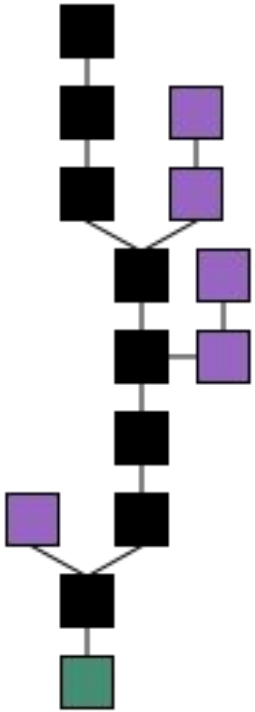
Wann spricht man von einer Blockchain?



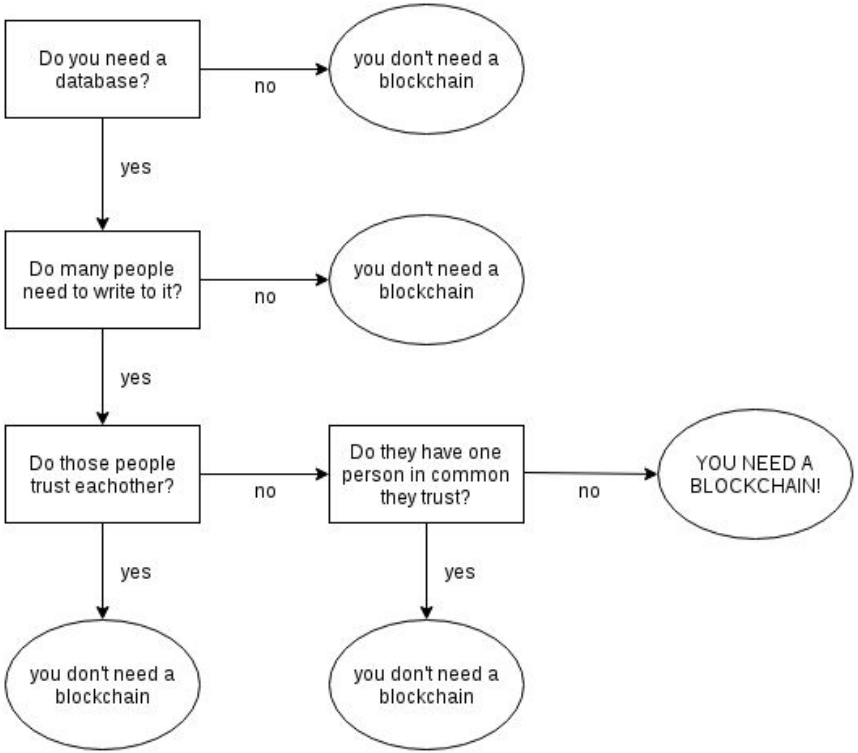
Wikipedia,
CC-BY-3.0

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

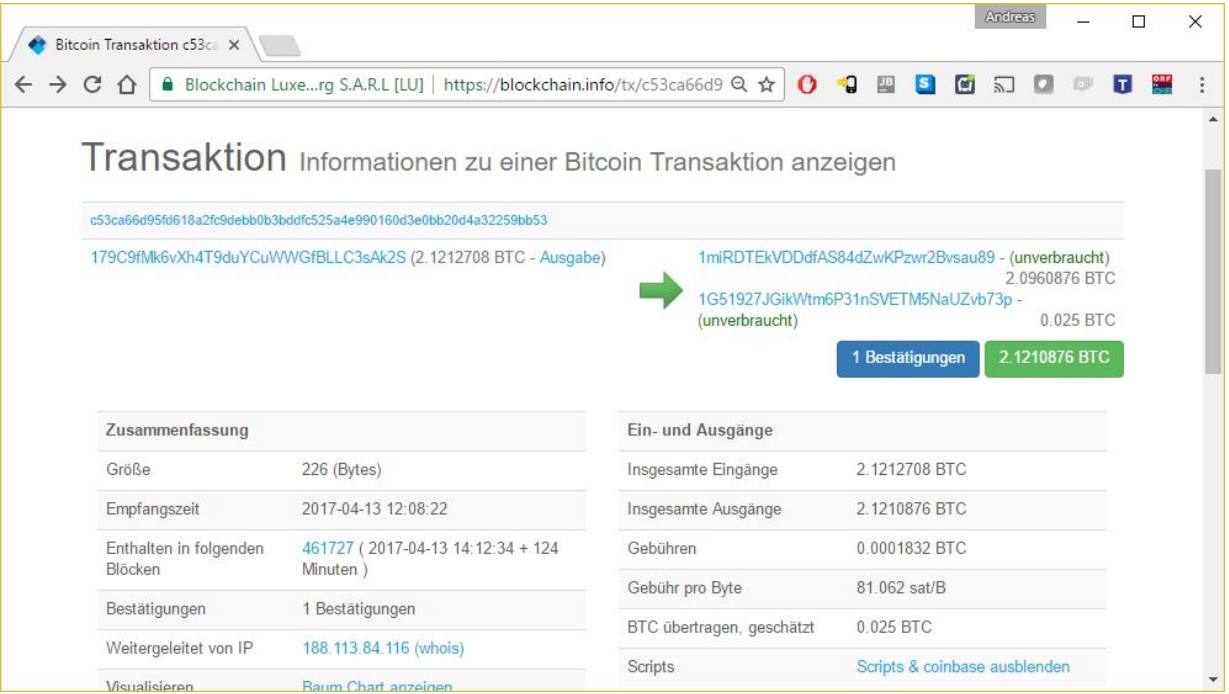
Wann braucht man eine Blockchain?



Wikipedia,
CC-BY-3.0



Beispiel einer Transaktion



bitcoin austria

Thanks for your attention

18.10.2017, Andreas Petersson