# Bitcoin - Eine dezentrale Währung

Peter Uebele

Tübinger Linuxtag

13. Juni 2015

Disclaimer: Keine Anlageberatung!

# Was ist Geld?

- Austauschmedium
- Recheneinheit
- Wertspeicher

**Wichtige Eigenschaften:**

leicht erkennbar, schwer zu fälschen, teilbar, leicht transportierbar, transferierbar, anerkannter Wert, umtauschbar gegen andere Güter

# Was sind Bitcoins?

- Digitales Geld, kryptographisch gesichert
- P2P, ohne Zwischenhändler (Banken)
- Komplett dezentral organisiert
- Endliche Geldmenge (21 Millionen Bitcoins)
- 2008 unter dem Pseudonym „Satoshi Nakamoto“ veröffentlicht, offener Quellcode

# Technischer Hintergrund I

- Geldeinheiten liegen immer bei einer „Adresse“
  ($\approx$ öffentlicher Schlüssel,
  z.B. „1GTEZnF2NRMVYSs7E7xuwAe3yZ5Q7Uqk6v“)
- Ausgeben nur mit zugehörigem privatem Schlüssel möglich!
- Gültigkeit der Transaktionen auch ohne privaten Schlüssel verifizierbar

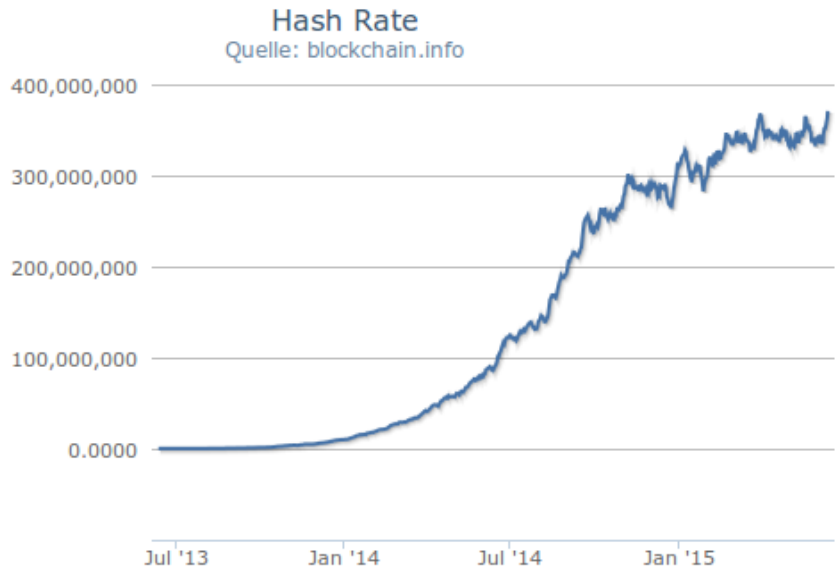
Wer überprüft die Transaktionen?

# Geldentstehung durch „Mining“

- Lösen von mathematischen Rätseln wird durch frisches Geld (+ Transaktionsgebühren) belohnt
- Belohnung (momentan 25 BTC pro Block) wird alle vier Jahre halbiert $\Rightarrow$ Geldmenge endlich
- Schwierigkeit wird dynamisch angepasst, so dass ca. alle 10 Minuten ein Block gefunden wird
- Nebeneffekt: Bestätigung bisher eingegangener Transaktionen

# Technischer Hintergrund II

- Speicherung auf der „Blockchain“:
  Dezentral gelagerte Aufzeichnung aller Transaktionen
- Blockchain jederzeit einsehbar
  $\Rightarrow$ Verhindert „Double Spending“
- Rechenleistung der Miner sichert das Netzwerk



# Vorteile gegenüber konventionellen Währungen I

- Geldtransfer nahezu gebührenlos
  Übliche Transaktionsgebühr beträgt etwa einen Cent
  (für Bitcointransfer in beliebiger Höhe)

  Zum Vergleich: Bei Western Union liegt die Gebühr für einen Geldtransfer von 50 Euro in die USA bei ca. 5 Euro.

Das im Vortrag gezeigte Bild wurde aus Gründen des Urheberrechts entfernt.

# Vorteile gegenüber konventionellen Währungen II

- Schnelle und einfache Bezahlung im Internet
- Micropayments
- Fälschungssicher
- „Multisignatur“-Adressen möglich
- Relativ anonym (pseudonym)
- Bezahlung ohne Übermittlung sensibler Daten
- Kein Fremdzugriff auf das eigene Geld!!

# Mögliche Gegenargumente I

- Börsen können pleite gehen! (siehe Mt.Gox...)
- Sorgsame Verwahrung der privaten Schlüssel erforderlich
- Verlorene Schlüssel können nicht rekonstruiert werden.
- Anonymität auch attraktiv für Kriminelle (wie Bargeld)
- „Mining“ benötigt viel Energie (aber wenig im Vergleich zum gesamten Bankensystem!)
- Akzeptanz bei Händlern noch gering (aber weiter steigend)
- Kein intrinsischer Wert

# Mögliche Gegenargumente II

- Preis sehr volatil!

# Praktische Aspekte I

- Preis bei ca. 200 Euro / BTC
- Teilbar bis auf 8 Dezimalstellen (0,00000001 BTC)
- Tipp zur Aufbewahrung: Nicht auf Börsen! Kleine Beträge auf Computer/Smartphone, größere Beträge auf Paperwallets

# Praktische Aspekte II

- Benutzung erfordert kein technisches Wissen!
- Zum Empfangen genügt es, eine Adresse (evtl. mit QR-code) bereitzustellen
- Auswahl der Software: „Full node“ oder „Lightweight“?
- Aus Gründen der Privatsphäre: Adressen nur einmal verwenden!
- Mining nur noch mit hochspezialisierter Hardware profitabel

# Warum ist der Preis seit Anfang 2014 gesunken?

- Insolvenz der Bitcoin-Börse Mt.Gox
- Schließung des Schwarzmarktes Silk Road (Ende 2013), Versteigerung der beschlagnahmten Bitcoins
- Verkaufsdruck durch professionelles Mining (ca. 3600 BTC pro Tag)
- Verkaufsdruck durch Händler, die Bitcoins akzeptieren und sofort gegen Euro/Dollar umtauschen

# Aktuelle Entwicklungen

- Weltweit ca. 400 Bitcoin Geldautomaten
- Weitere Anwendungen der Blockchain–Technologie (Nasdaq, Landrechte in Honduras, ...)
- Diskussion über Blockgröße und Skalierbarkeit
- OpenBazaar als dezentraler Marktplatz kurz vor Fertigstellung
- „21inc:“ Mining durch elektrische Alltagsgeräte?

# Was könnte den Bitcoin zerstören?

(Bitcoin wurde schon über 70 mal totgesagt, siehe `http://bitcoinobituaries.com/`)

- Staatliche Verbote?
  Ineffektiv gegen eine dezentrale Währung!
- Ein Altcoin, der den Bitcoin ablöst?
  Nicht ausgeschlossen, aber aufgrund des Netzwerkeffekts extrem unwahrscheinlich!
- Quantencomputer?
  Umstellung auf neue Technologie nötig, aktuelle Bitcoins würden aber ihren Wert behalten!
- ??