Bitcoin

Die Technologie, und warum sie cool ist

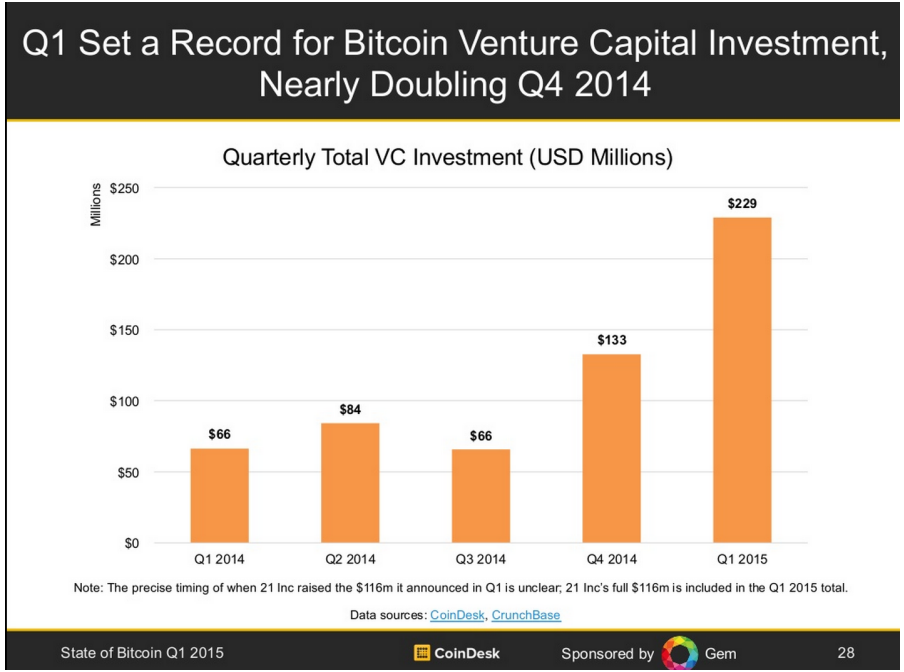
3. Technologieplauscherl, 16.4.2015

Inhalt

- Was ist Bitcoin?
  - Wer ist Satoshi Nakamoto?
  - Demo
- So funktioniert’s
  - Kryptographie
  - Transaktionen
  - Blockchain
- Selber verwenden
  - Wallets
  - kaufen & ausgeben
- Ausblick

Was ist Bitcoin?

- **Digitale Währung - Cryptocurrency**
  - 2009 von Satoshi Nakamoto
  - Mischung aus Gold & TCP/IP
- **Software-basiertes Zahlungssystem**
  - Peer-to-peer Netzwerk
  - Viel Kryptographie - aber nichts ist verschlüsselt!
- **Kommt ohne Banken aus**

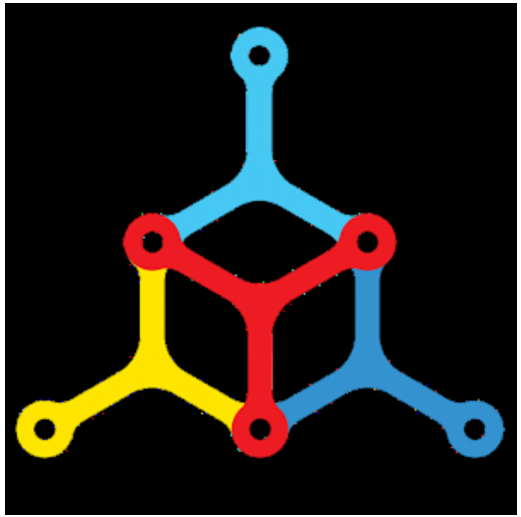


Wer ist Satoshi Nakamoto?

- 2008: Bitcoin paper
- bis 2010: Satoshi entwickelt
- April 2011: “moved on to other things”
- Satoshi ist Kein Kryptographieexperte
  - Aber: doppel-SHA256, spezielle elliptic curve, RIPEMD+SHA
- guter Hacker

Demo!

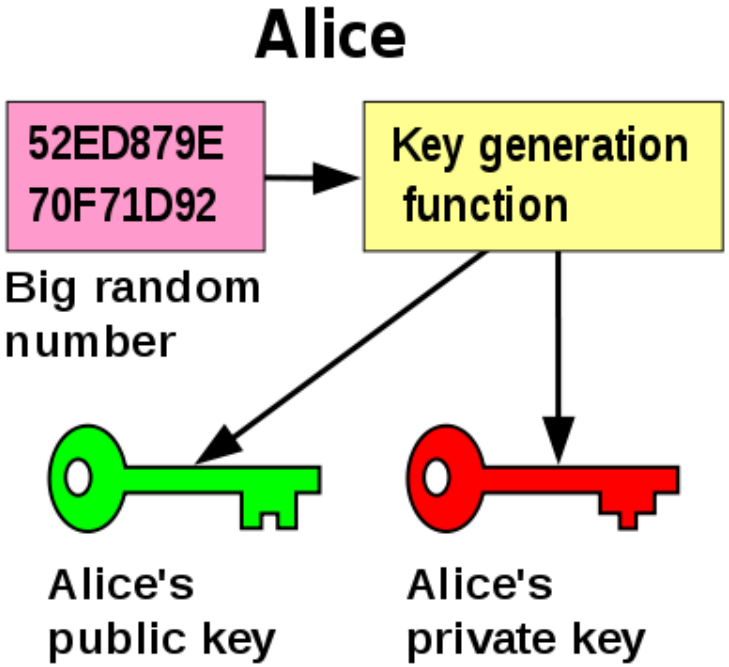
- Google Play: “Mycelium”
- Online Wallet: https://greenaddress.it/

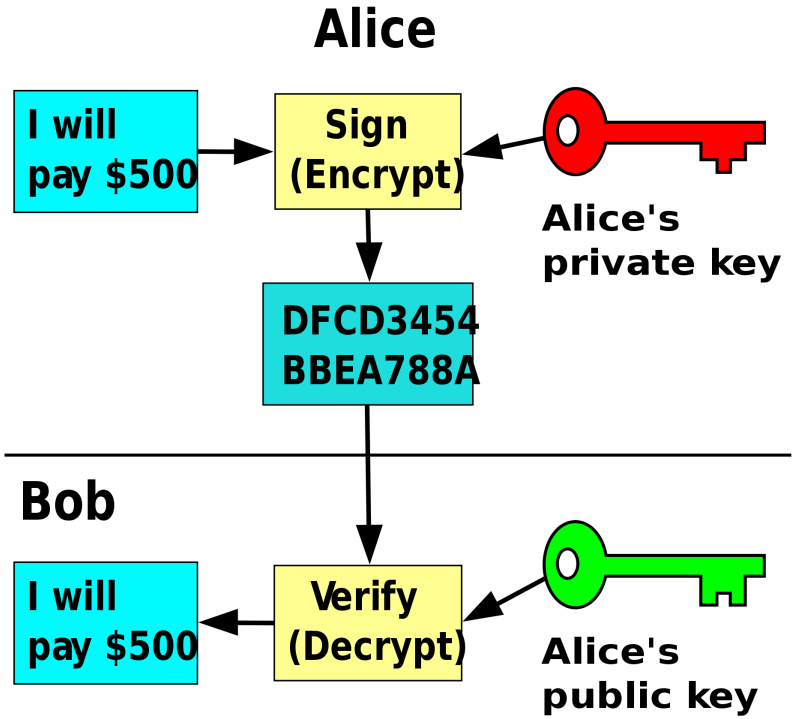


Wichtige Kryptographie

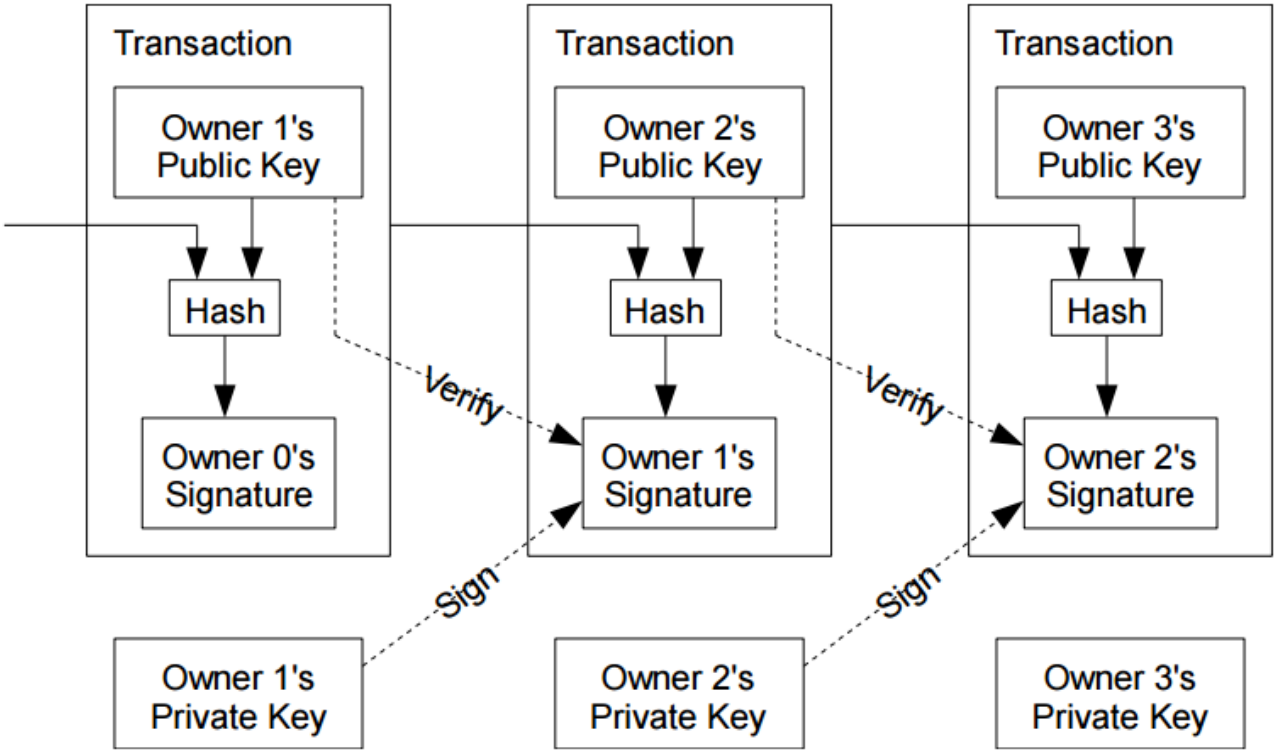
- Hashing: $y = h(x)$
  - von y auf x zu kommen ist praktisch unmöglich.
  - x zu finden für bestimmtes y ist auch unmöglich
  - nur “durchprobieren” möglich.
- Signaturen
  - Um Authentizität zu demonstrieren
  - Z.B: Alice prüft ob Nachricht von Bob kommt.
  - Coin = Kette von digitalen Signaturen
- Public & Private Key

Public & Private Key



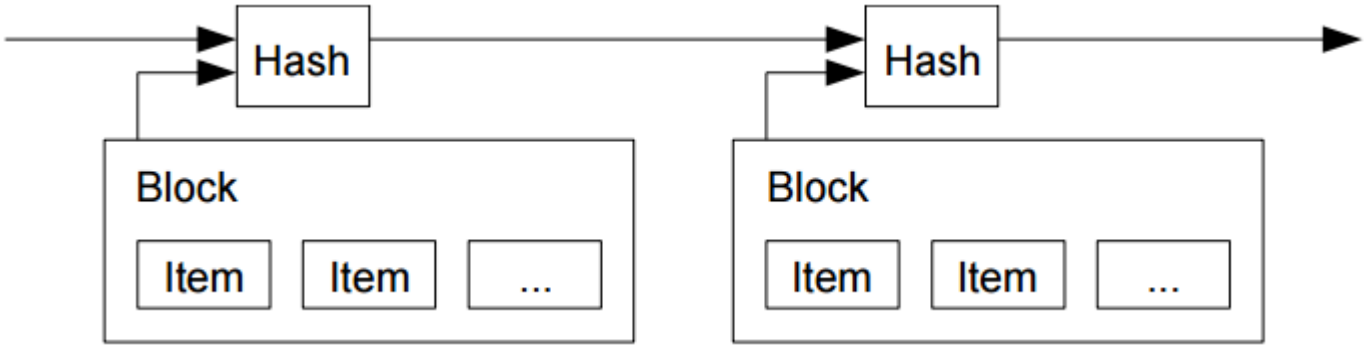


Transaktionen



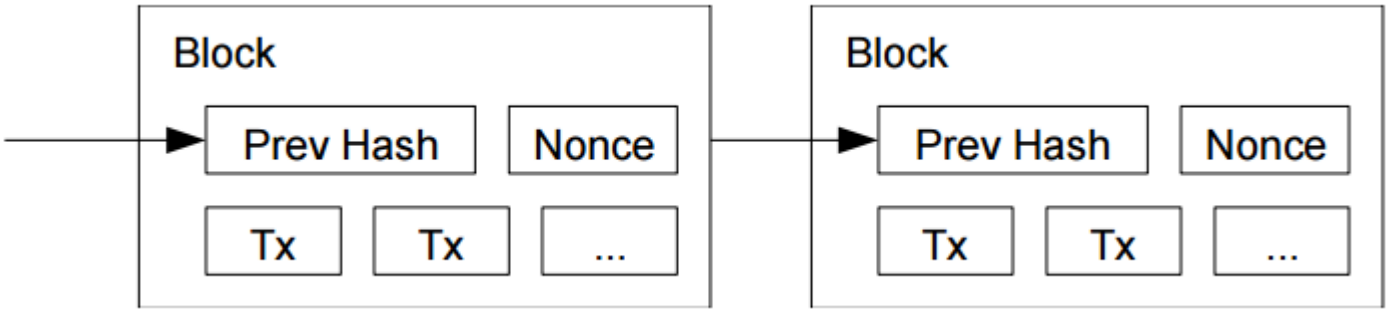
Timestamping

- Garantierte Ordnung: Hash von voriger Nachricht & aktuelle Nachricht
- Problem: Wie Peer-to-Peer lösen?
  - Wer garantiert die richtige Reihenfolge?
  - Problem “Double Spending”!



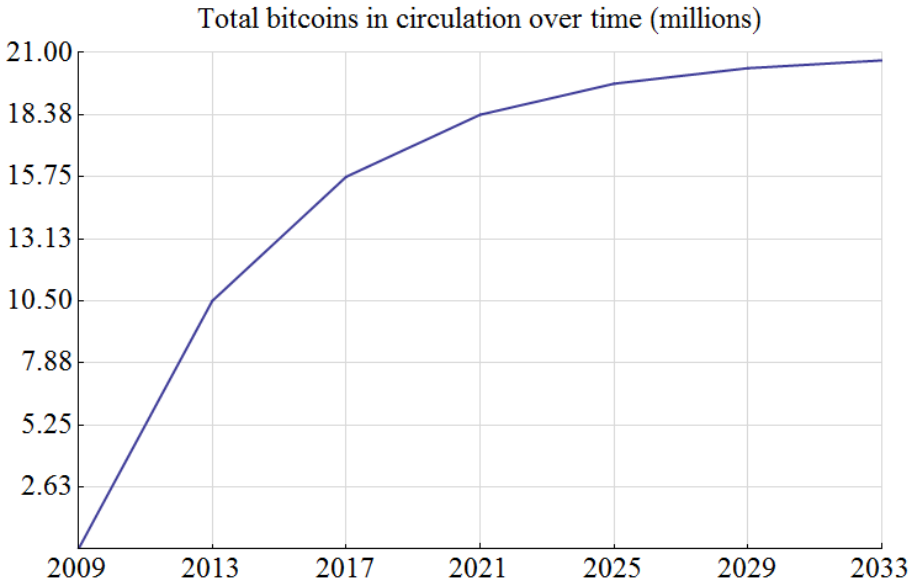
Von Timestamping zur Blockchain

- Proof of Work: “Mining”
  - Der erste Peer der eine schwierige Aufgabe löst, bestimmt das nächste Element in der Kette.
  - Schwierigkeit passt sich automatisch an
  - Alle 10 Minuten ein neuer Block



Motivation zum Mining

- Block reward: 25BTC + Fees
  - 25 * 210€ = 5.250€ pro Block
  - 6 * 24 = 144 Blöcke pro Tag
  - 5.250€ * 144 = 756.000€ pro Tag
- Halbierung alle 210000 Blöcke (ca 4 Jahre)
- Lohnt sich praktisch nicht
  - Außer mit ASIC-Farm
  - und wenig Stromkosten



Wallets

- **Man ist selbst für seine Sicherheit verantwortlich!**
  - “Hierarchically deterministic Wallets” verwenden
  - Seed aufschreiben, an 2+ Plätzen aufbewahren
- **“hot wallet”, vgl. Geldbörse**
  - Android: z.B. Mycelium
  - Greenaddress, ...
- **“cold wallet”, vgl. Bankkontos**
  - z.B. Electrum z.B. auf https://tails.boum.org/
- **“deep cold wallet”, vgl. Gold im Safe.**
  - 2-of-3 paper wallet

Bitcoins kaufen

- Handelsbörse https://www.kraken.com/
- LocalBitcoins https://localbitcoins.com/
- Bitcoinbon https://www.bitcoinbon.at/
- Mycelium Trader
- Wer mag, von mir :-)

Bitcoins ausgeben

- Angebot in Österreich noch sehr begrenzt :-(
- http://www.lieferservice.at/
- http://coinmap.org/
- International
  - Dell, Microsoft, … (derzeit nur US)
  - https://www.humblebundle.com/ PC Spiele
  - http://overstock.com/ (wie Amazon, auch nach AT)

Aktuelle Entwicklungen

- **Entwicklung geht rasend schnell**
- **Smart Contracts**
  - P2SH: “Pay to Script Hash”
  - 2-of-3 Wallets
  - Treuhanddienst: Käufer, Verkäufer, Mittelmann.
  - Time-locked deposit
  - ...
- **Colored Coins**
  - Bitcoins mit realem Verknüpfen: ein Satoshi repräsentiert Eigentum

Links

- Tech
  - https://bitcoin.org/bitcoin.pdf
  - https://bitcoin.org/en/developer-guide
- News
  - http://www.reddit.com/r/bitcoin
  - http://www.coindesk.com/
  - https://bitcointalk.org/

Typische Gegenargumente

- **“Bitcoins ist nur was für Geeks!”**
  - vgl. Internet 1995
- **“Bitcoin hat keinen inherenten Wert!”**
  - Was ist der inherente Wert von Bargeld? Papier & farbe.
- **“Jeder kann selbst eine digitale Währung machen!”**
  - Stimmt. Aber: Network effect. Vgl. Facebook
- **“Niemand sichert/garantiert den Wert!”**
  - Vertrauen in Banken/Regierungen?
  - Vertrauen in Mathematik