# Das BitCoin-System

Matthias Brüstle

Nürnberg 2016-11-20

# Wie funktioniert BitCoin?

Überlegt Euch mal kurz für Euch selbst:

- Wie entsteht eine BitCoin?
- Was für eine Form hat eine BitCoin?
- Wie funktioniert eine BitCoin?

# BitCoin – digitales Fiat-Geld

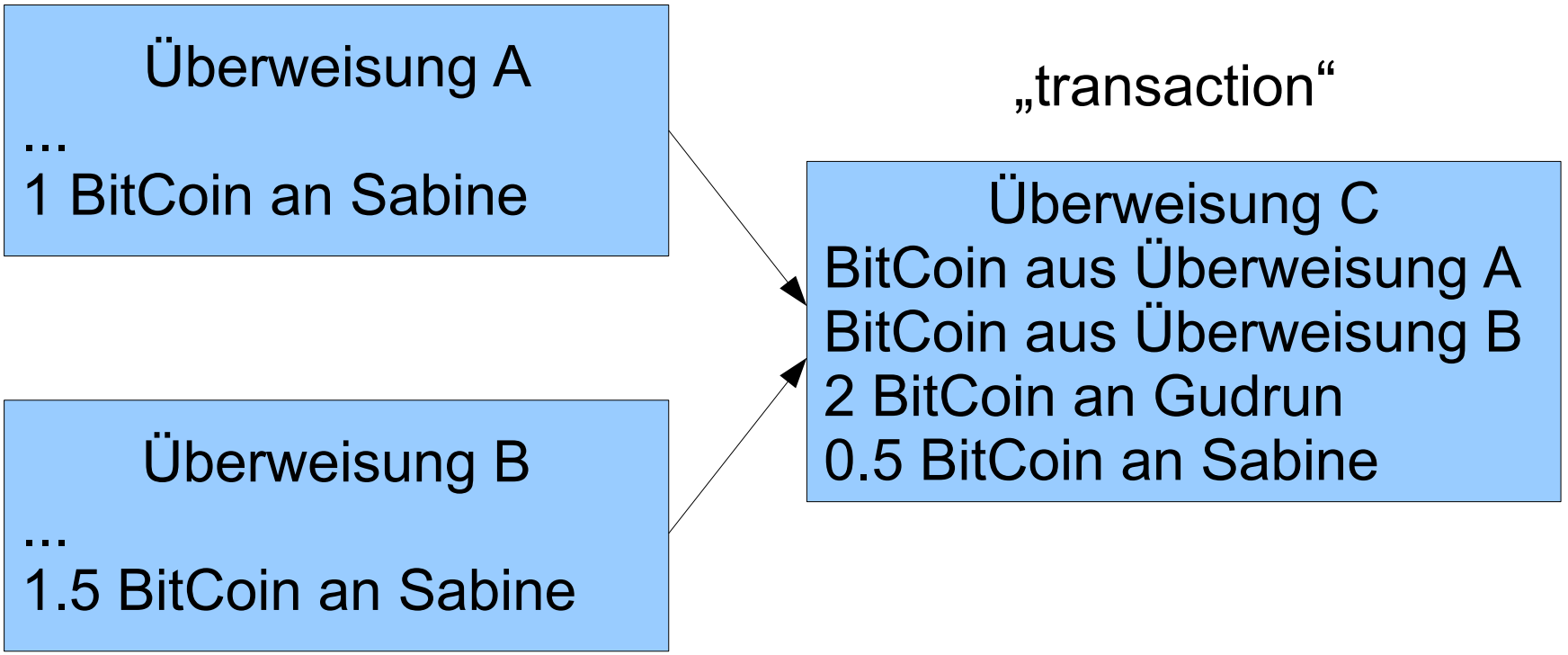
- Am Anfang war das Wort Satoshi Nakamotos, der die Funktionsweise von BitCoin definiert hat
- Seitdem hat sich die Idee einer allgemeinen Übereinkunft zur Funktionsweise (Regeln) etabliert („Consent“)
- Der Consent kann sich auch ändern

(Fiat: lateinische, „es sei!“)

# Wie funktioniert BitCoin?
# Die Block Chain

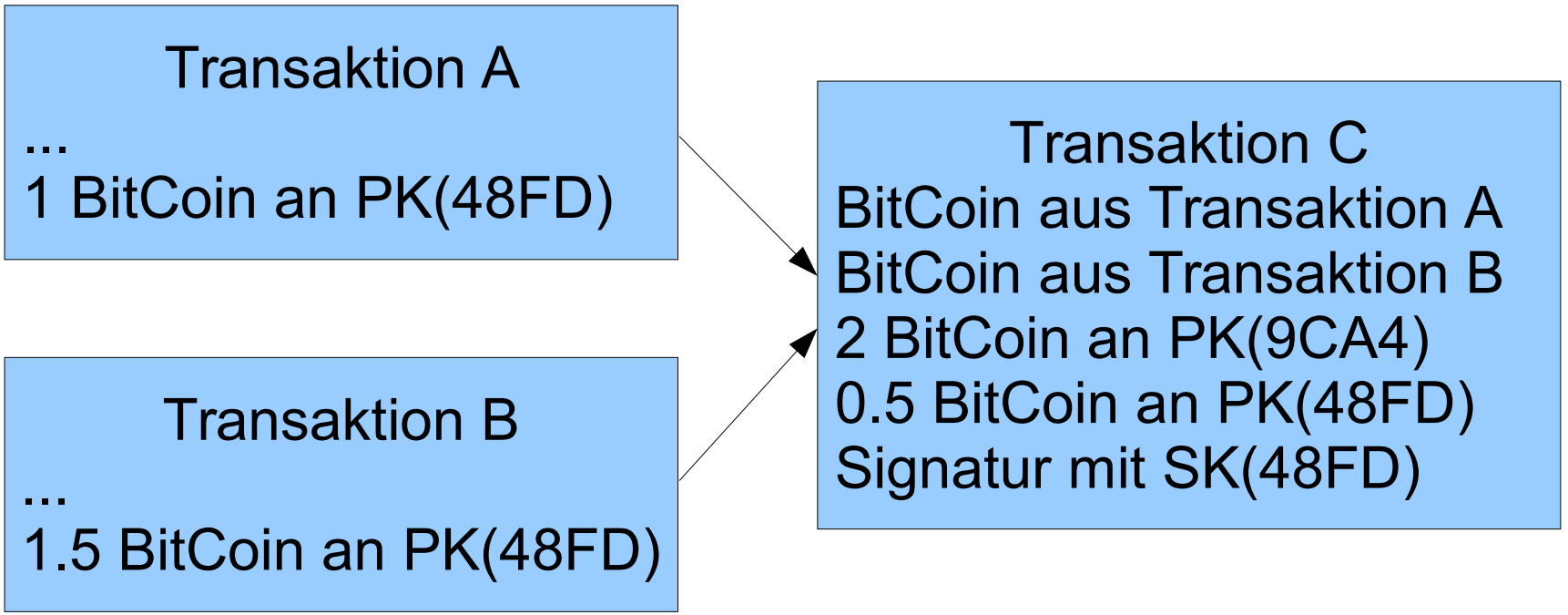
- Basiert auf einem dezentralen, öffentlichen Kassenbuch in der alle Buchungen stehen
- Die Buchungen sind in Blöcken zusammengefasst
- Die Blöcke sind kryptographisch über Hash-Werte verkettet => Block Chain
- Der Startblock (Block 0) wird in der BitCoin-Software als Ankerpunkt mitgeliefert

# Wie funktioniert BitCoin?
# Eine Buchung (1)



# Wie funktioniert BitCoin? Eine Buchung (2)

- Keine Namen sondern asymmetrische Krypto (private + öffentliche Schlüssel, Signaturen)




Adresse: **1**GH474yPCgxqkEsZqESs99W3Z89scFuQHk
Privater Schlüssel: L445cN3MQY8skQVGJPfzb3yngwte8Nj1rRYi21X4szhh1HsNeiVG

# Wie funktioniert BitCoin? Problem: Wie hält man ein dezentrales Kassenbuch konsistent?

Das *Problem der byzantinischen Generäle* (räumliche Distanz, Signallaufzeiten, Verräter)

Problem: BitCoins mehrmals ausgeben

Lösung bei BitCoin:

- Um einen Block verteilen zu dürfen muß man eine rechenintensive Aufgabe erfüllt haben (Hash-Wert < x, Proof of Work/PoW)
- Die längste regelkonforme Blockkette wird weitergeführt

# Wie funktioniert BitCoin?
# Wo das Geld herkommt

Satoshi hat beim BitCoin-Start festgelegt, dass:

- man zur Motivation für das Berechnen des Block-Hash-Wertes mit neu herbeidefinierten BitCoin belohnt wird („Miner“, „BitCoin Mining“)
- die Belohnung in regelmäßigen Abständen halbiert wird (aktuell 12.5 BitCoins pro Block)

und außerdem:

- bei einer Buchung zur Motivation eine Gebühr („Fee“) an den Miner bezahlt werden kann (z.Z. 0.5 – 1.0 BitCoins pro Block)

# Was kostet eine Transaktion?

- 1 Block enthält im Durchschnitt etwa 1500 Transaktionen
- Belohnung pro Block: 12.5 BitCoin = 7500 Euro (Kurs 600 EUR/XBT im Oktober)
- Gebühren pro Block: 0.75 BitCoin = 450 Euro
- Mittlere effektive Kosten pro Transaktion:
  - Gebühren: 0.30 Euro
  - Insgesamt: **5.30 Euro**

# Konsequenzen aus PoW und Belohnung?

- Belohnung pro Tag 1.15 Mio. Euro (600 EUR/XBT, 1 Block alle 10 Minuten)
- Es werden so viele mitrechnen, dass es für die effizientesten mit billigstem Strom noch profitabel ist
- Jährlich können 415 Mio. Euro für Hardware, Strom, Strom und Strom ausgegeben werden
- Geschätzer Stromverbrauch: **250 MW** = ca. 500 000 Haushalte
  - Aktuell eff. Hardware S9: 100 W pro TH/s
  - Aktuell gesamte Hash-Rate: 2 EH/s
- Profit-Rechner: https://tradeblock.com/bitcoin/mining/

# Alternativen zu BitCoin?

- Massig! Über 500 „AltCoins“ https://coinmarketcap.com/
- Spielwiese für neue Technologieen
  - Proof of Stake: Bestätigung von Blöcken vor allem davon abhängig, wieviel Coins man hat
- Versuche schnell Geld zu verdienen („Scam“)
  - Vorab erzeugte Coins
  - Business-Pläne
- Ethereum, Ripple, LiteCoin, Ethereum Classic

# Vorteile von BitCoin

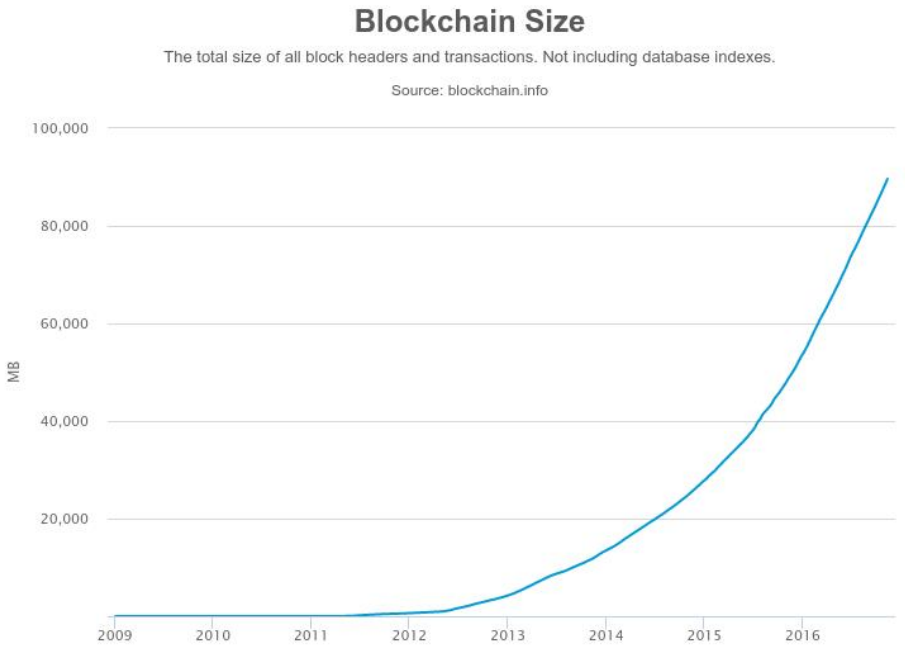
- „Direkter“, weltweiter Transfer für jeden ohne Kartenterminals und dazwischen abkassierender Firma
- Mobiles bezahlen per Barcode
- Komplexere Bedingungen für eine Buchung möglich, z.B. 4-Augen-Prinzip
- Spekulationsgewinne
- Pseudonymer Bezahlungsvorgang

# Nachteile von BitCoin

- Man muß EUR -> XBT -> EUR tauschen
- Man sollte das System etwas verstehen, z.B. Miner's Fee
- Wenn der private Schlüssel zerstört wird ist die BitCoin unwiederbringlich weg (Festplattencrash, unverstandene Software)
- Wenn der private Schlüssel geklaut wird ist die BitCoin unwiederbringlich beim Dieb
- Kursrisiken
- Auswertung der öffentlichen Blockchain

# Nachteile von BitCoin (2)

- Gigantischer Stromverbrauch
- Immer wachsende Blockchain (aktuell 90GB)
- Aktuell Transaktions-Limit von ca. 300000 Transaktionen / Tag
- Gefahr durch cryptografische Angriffe
- Dangerous Satoshi (1 Mio. XBT, 6.5%)
- Der Erfolg bremst die Weiterentwicklung der Crypto-Währungen

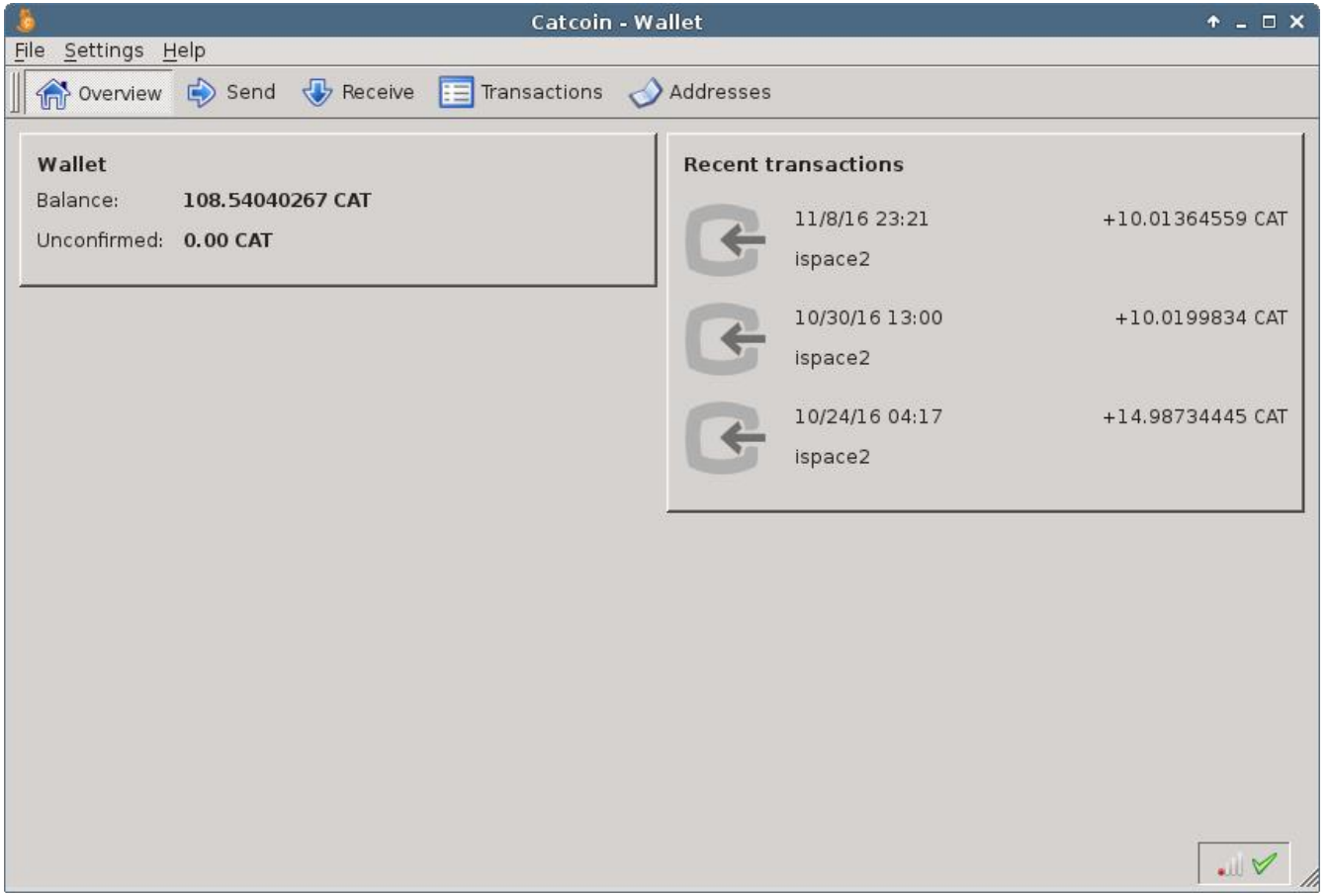


# Wallet / Geldbörse

- Paper-Wallet
  - https://www.bitaddress.org (auch offline verwendbar)

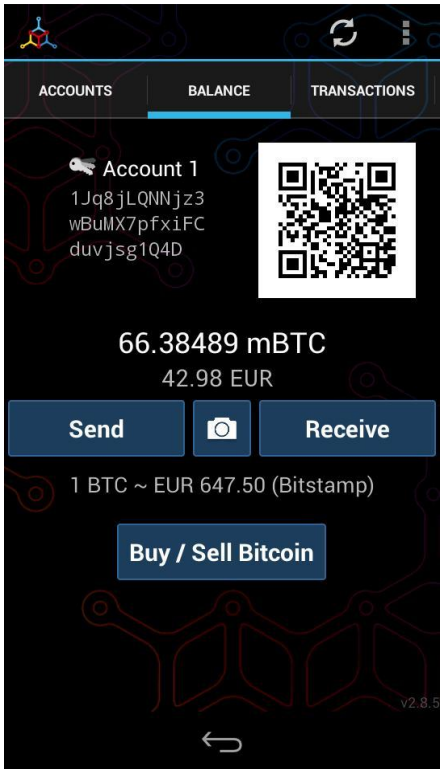
# Wallet / Geldbörse (2)

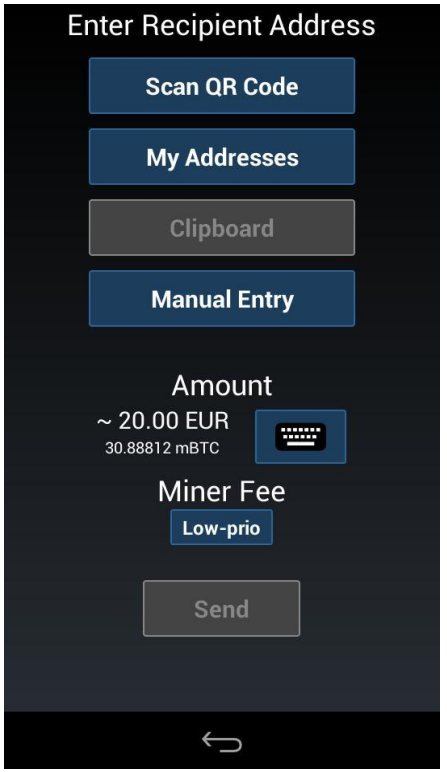
- offizielle BitCoin-Wallet (speichert die komplette Blockchain)

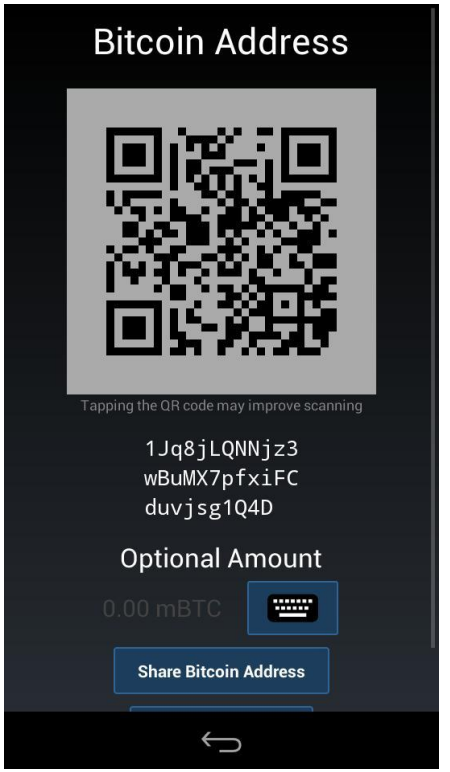


# Wallet / Geldbörse (3)

- diverse BitCoin-Wallets ohne Blockchain
  - HD-Wallets erleichtern Backups
  - z.B. Mycelium für das Smart-Phone:



# Wallets / Geldbörse (4)

- Spezial-Hardware zur Speicherung und Verwendung des privaten Schlüssels
- Schützt vor Viren, Trojaner, Dieben
- z.B. Trezor, Ledger

# Links

- BitCoin Forum: https://bitcointalk.org
- Satoshi Nakamoto; Bitcoin: A Peer-to-Peer Electronic Cash System: https://bitcoin.org/bitcoin.pdf
- Satoshi Nakamoto Institute Literaturliste: http://nakamotoinstitute.org/literature/
- Princeton Bitcoin Book (Entwurf, Vorlesung): http://bitcoinbook.cs.princeton.edu/
- BitCoin zuschauen: https://tradeblock.com/bitcoin

# Saenks!

Matthias Brüstle

Nürnberg 2016-11-20