Bitcoin in Theorie und Praxis

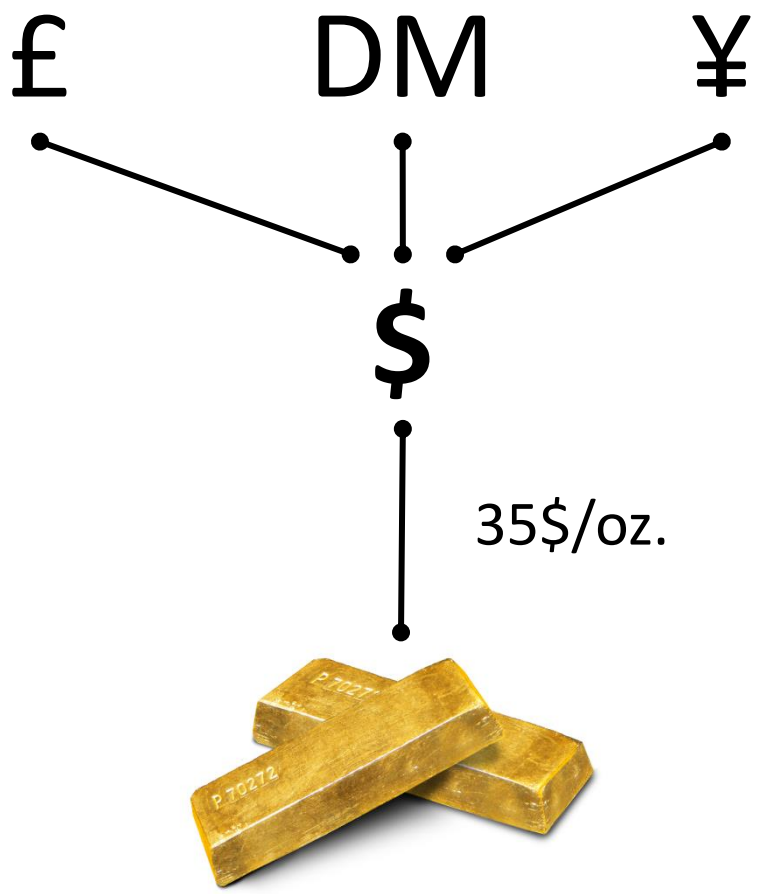
Gerold Lechner
gerold.lechner@aquila-ic.com

Salzburg, den 11.01.2018

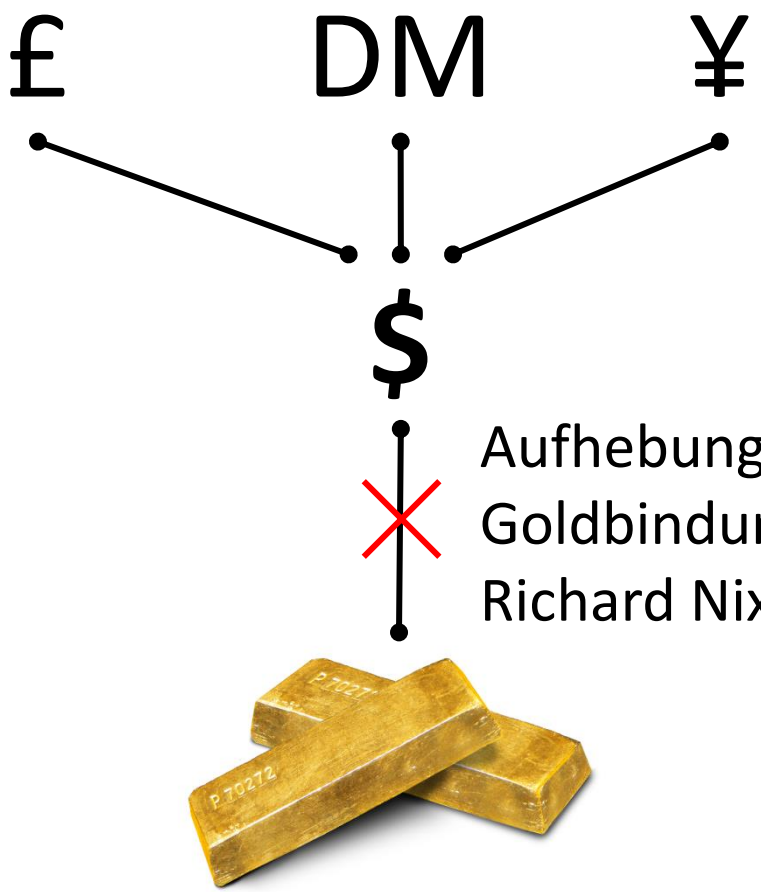
AQUILA
INDUSTRIE & CAPITAL GMBH

US Dollar, 1928

Bretton-Woods-System, 1944



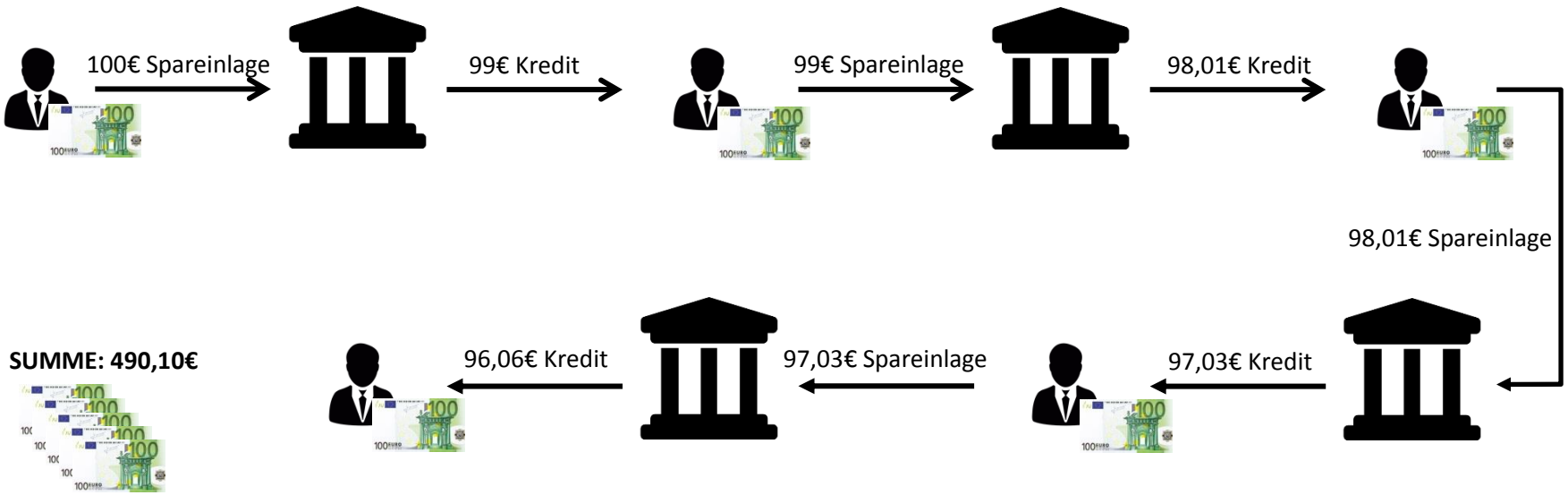
Aufhebung Goldbindung, 1971



Mindestreserve-System

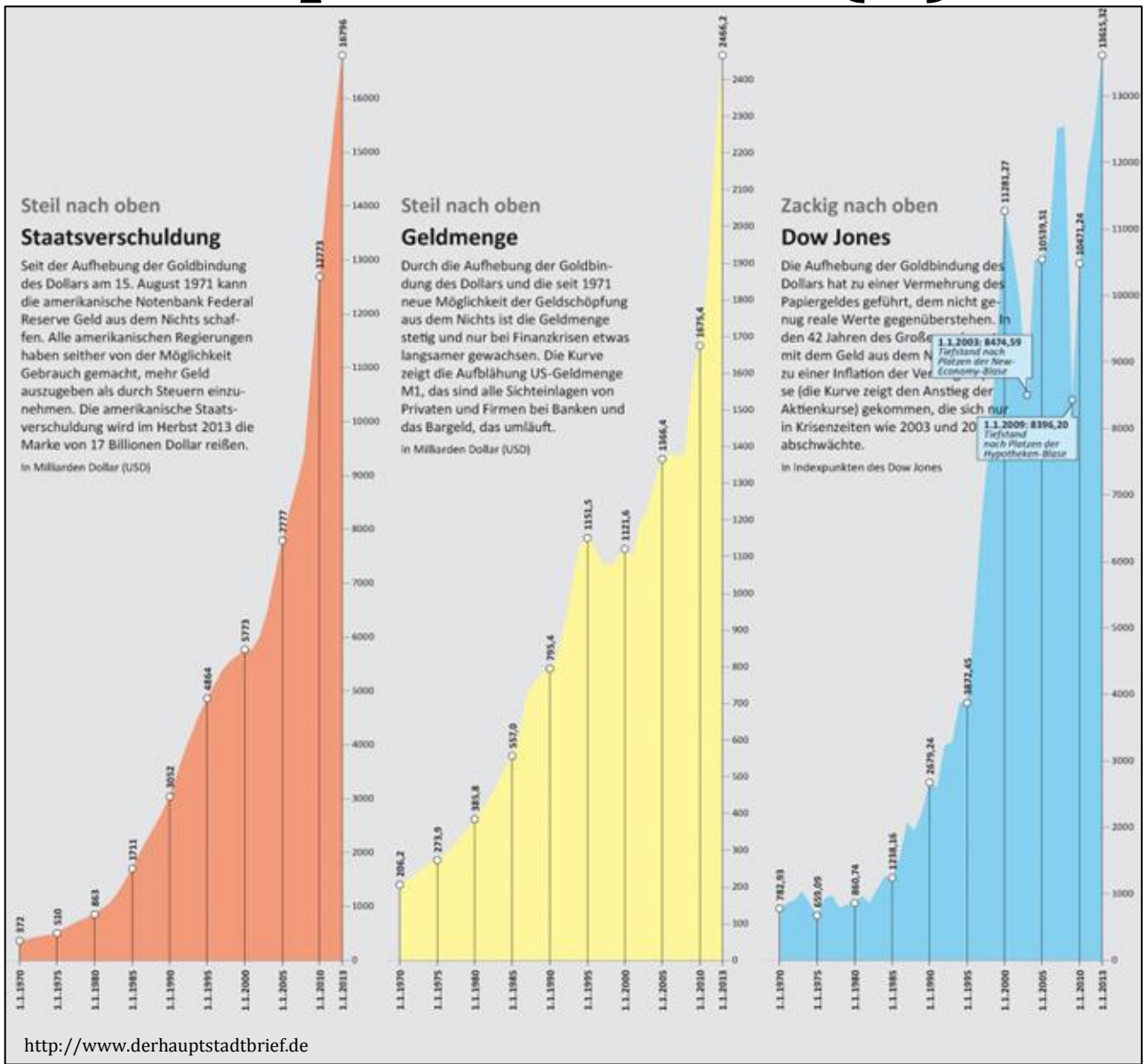
(engl. „fractional-reserve banking“)

- Geldschöpfung durch Geschäftsbanken
- Aktuelle Mindestreserve: 1%*



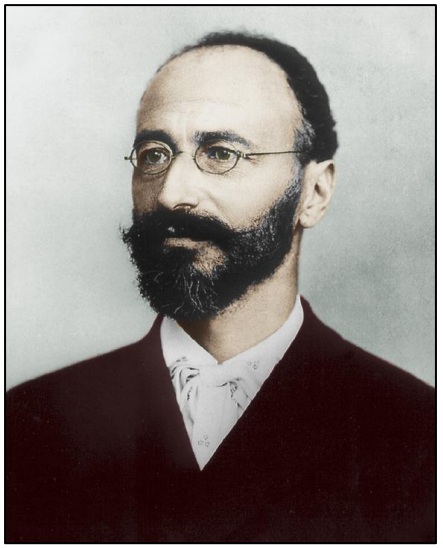
* http://bundesbank.de (30.10.2017)

Implikationen (1)



http://www.derhauptstadtbrief.de

Eugen von Böhm-Bawerk



- Mitbegründer der Österreichischen Schule
- Finanzminister 1895-1904
- Ziele
  - Ausgeglichener Staatshaushalt
  - Strikte Einhaltung der Golddeckung
- Buch: Kapital und Kapitalzins, 1884

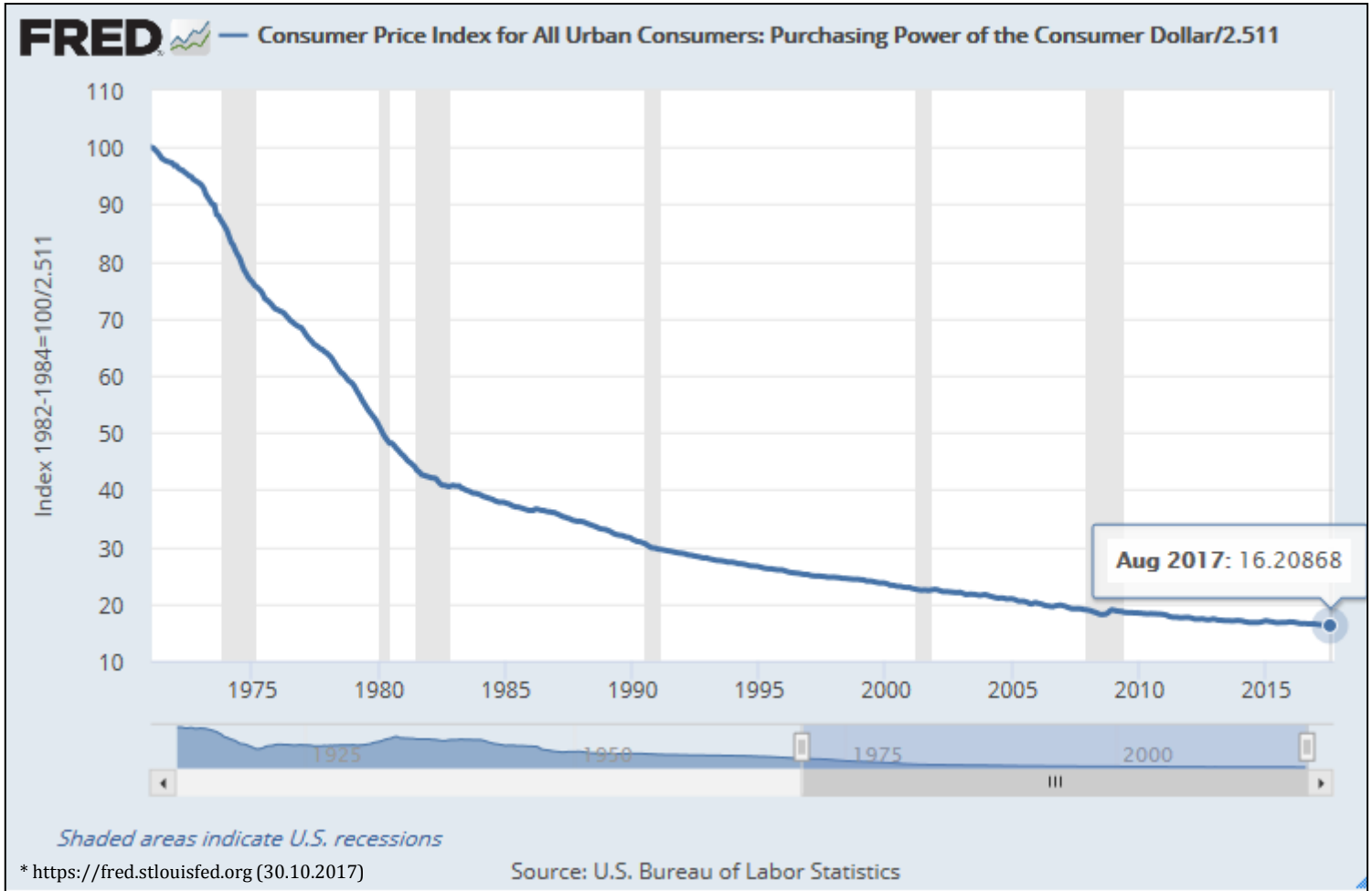
Vergleich Schilling/Euro

100-Schilling-Schein
Abbildung: Eugen von Böhm-Bawerk

100-Euro-Schein
Abbildung: Fiktive Brücke

Implikationen (2)

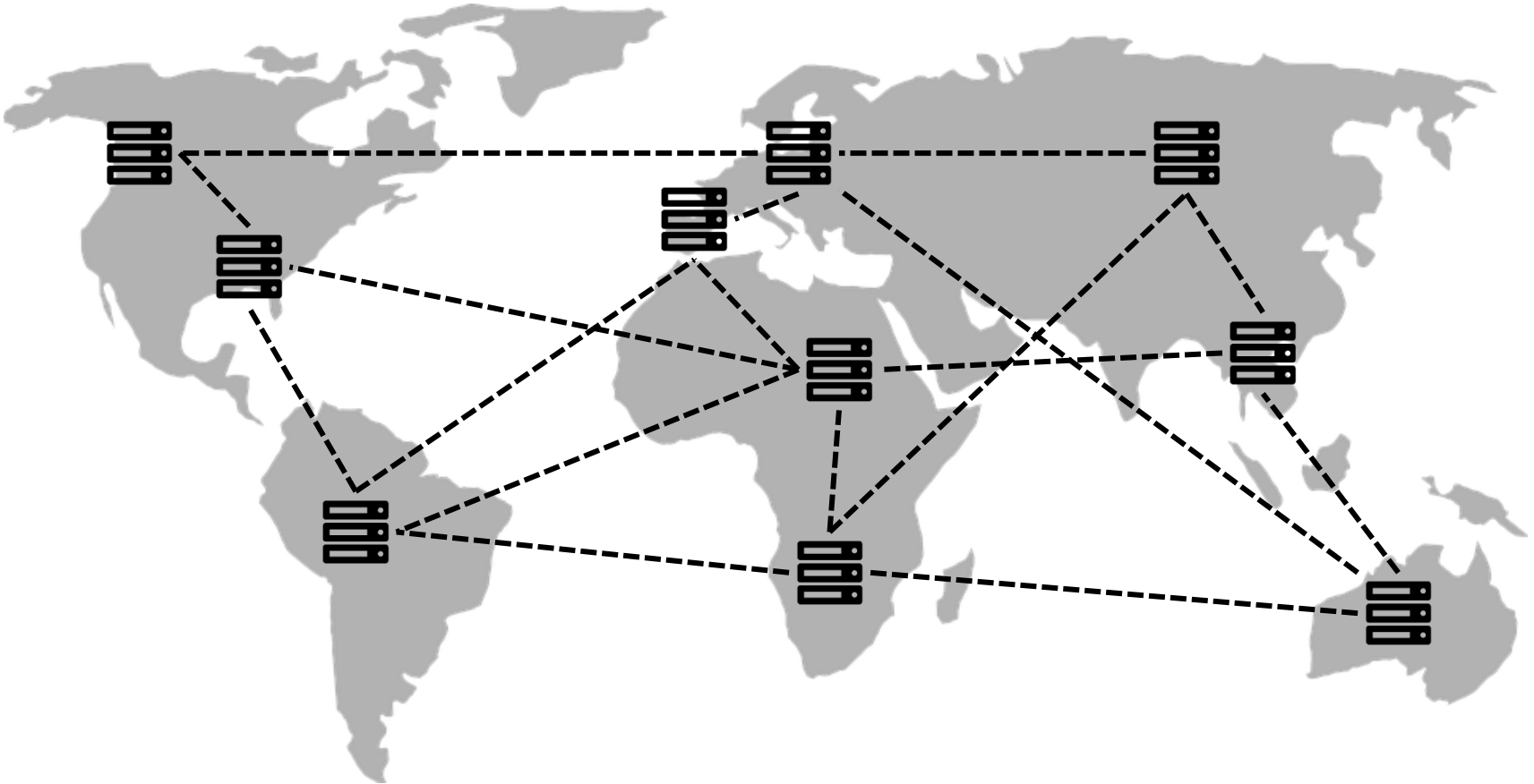
- Kaufkraftverlust USD seit 1971: 83,8%*



* https://fred.stlouisfed.org (30.10.2017)

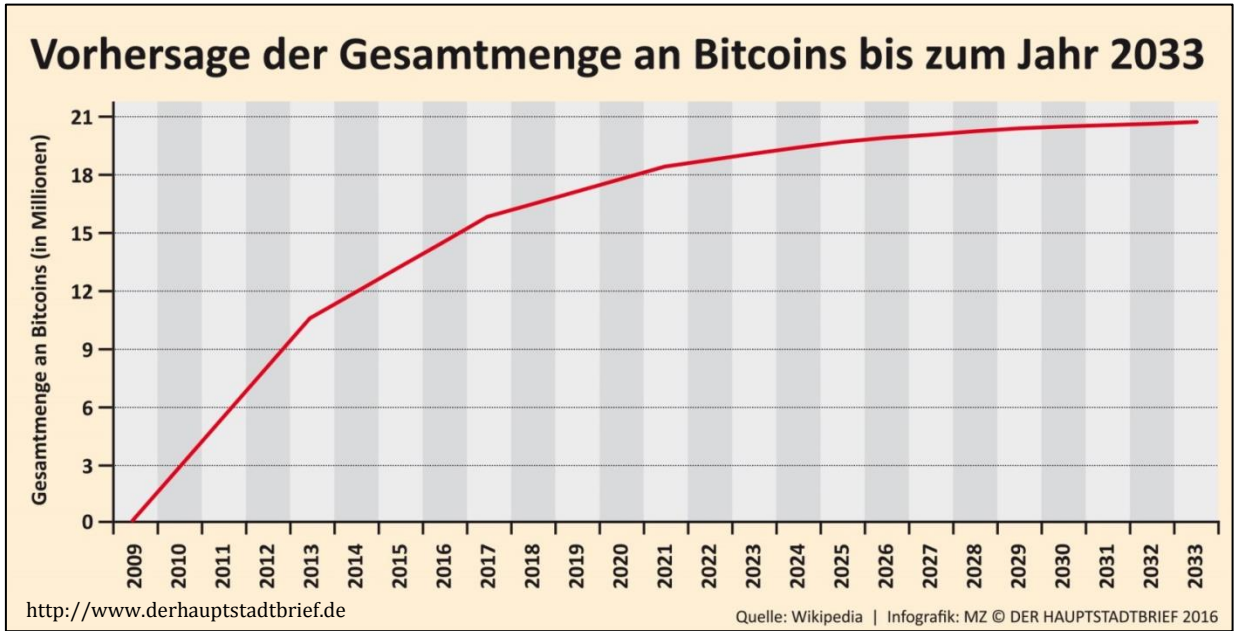
Blockchain

- Dezentrale Datenbank
- Enthält Transaktionshistorie



Bitcoin (1)

- Quelloffener Code („Open Source“)
- Begrenzte Inflation
- Interventionen durch zentrale Instanzen (fast) nicht möglich



Bitcoin (2)

- Beliebig viele Konten („Wallets“)
- Transaktionen ohne Freigabe durch Dritte
- Aktuelle Probleme:
  - Begrenzte Anzahl an Transaktionen
  - Hohe Transaktionsgebühren (ca. 50-100€)
  - Keine Fungibilität/Anonymität

Beispiel

- Erstellen von Bitcoin-Adressen („Paper-Wallet“)
- Nutzung am Bitcoin-Automaten

Wie funktioniert Bitcoin?

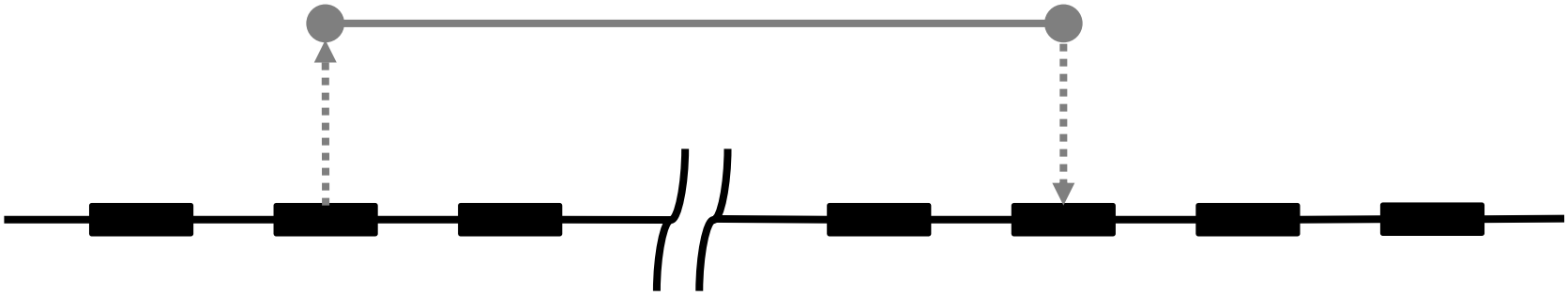
- Blöcke entstehen im Durchschnitt alle 10 Minuten
- Aktuell ca. 2000-3000 Transaktionen pro Block
  - 3-7 Transaktionen pro Sekunde
- Probleme
  - Begrenzte Anzahl an Transaktionen
  - Keine Fungibilität/Anonymität

Wie Skalieren?

- Größere Blöcke?
  - Skaliert nur linear
  - Führt zu Zentralisierung
    (höhere Bandbreite notwendig)
  - „Verwaiste“ Blöcke

- Alternative: „Lightning Network“
  - Transaktionen „außerhalb“ der Blockchain

Lightning Network (1)



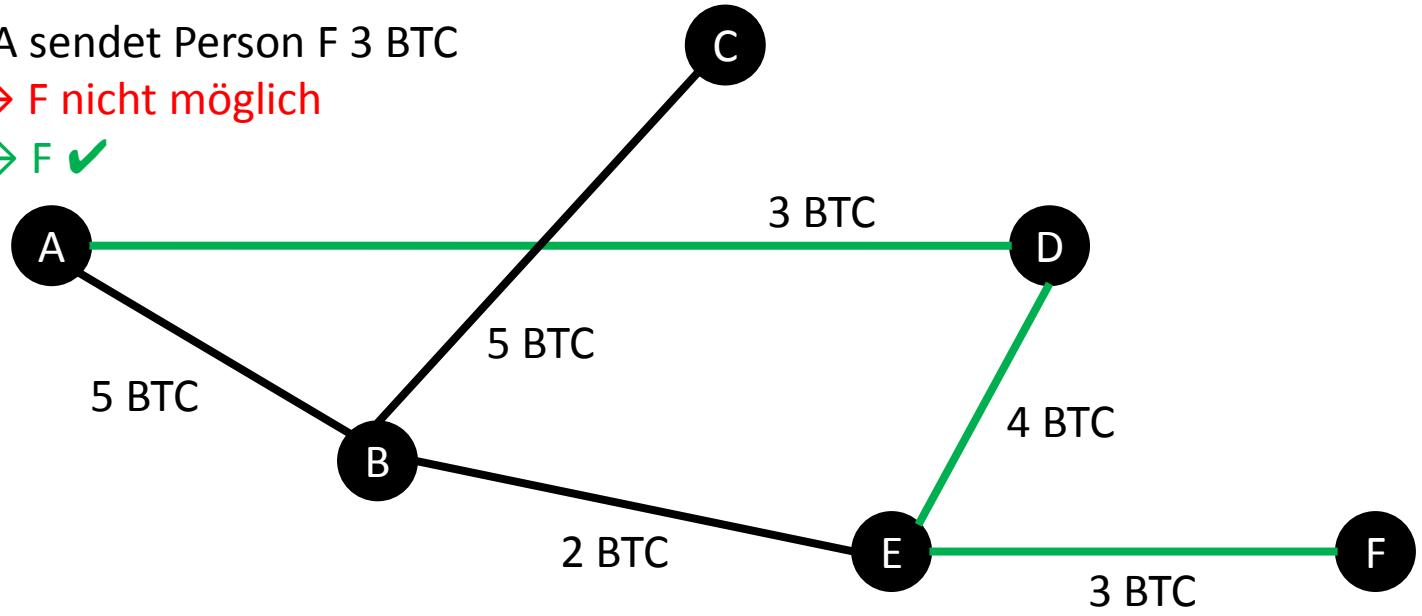
- „Payment channel“ zwischen *n* Personen
  - ∞ Transaktionen zwischen diesen *n* Personen
    - instantan
    - kostenlos
- 2 Transaktionen auf der Blockchain (Öffnen, Schließen)

Lightning Network (2)

Ziel: Person A sendet Person F 3 BTC

A → B → E → F nicht möglich

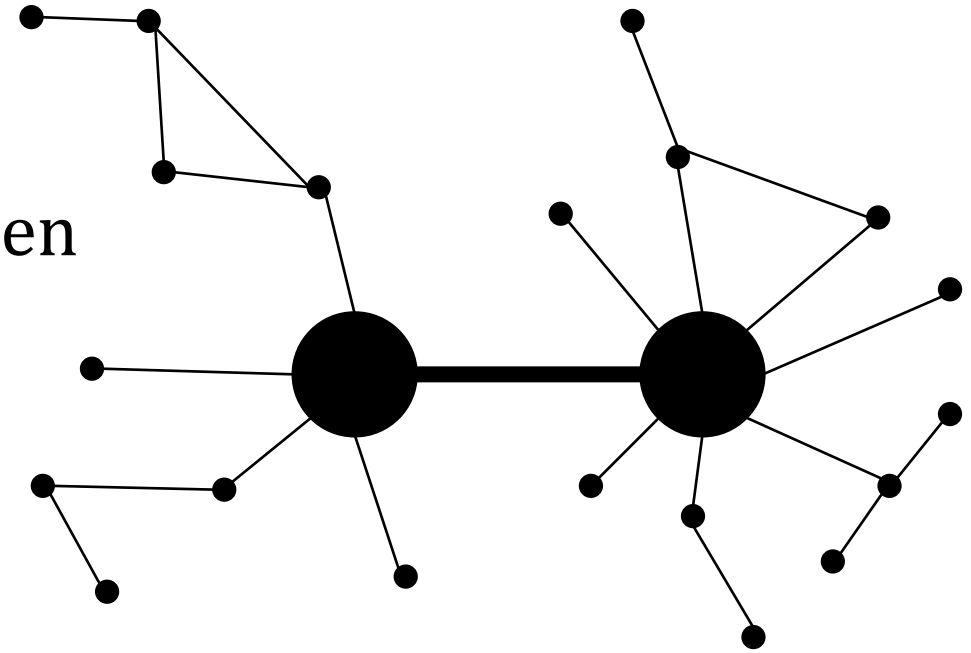
A → D → E → F ✔



- Automatisches „Routing“
- Fungibilität: Außenstehende sehen nicht dass Person A Person F 3 BTC gesendet hat

Lightning Network (3)

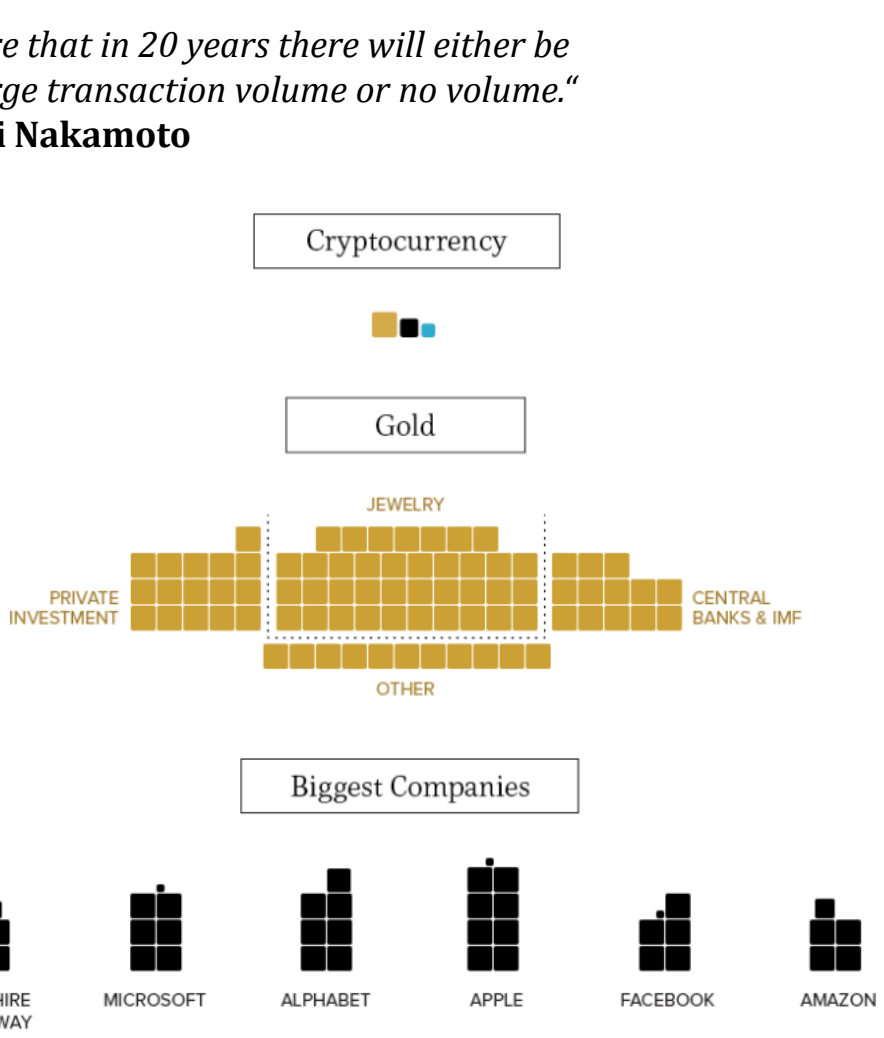
- Wichtig
  - Hohe Liquidität
  - Viele Verbindungen

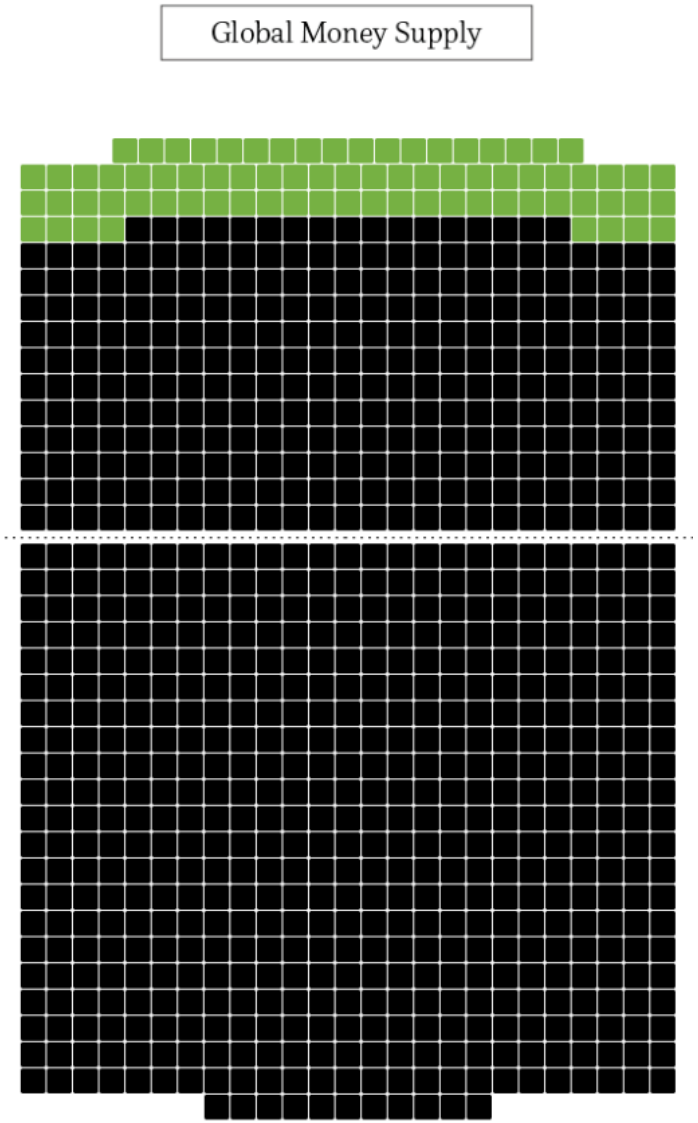


- Risiko
  - Zentralisierung
  - Durchschnittlicher Nutzer kommt mit Blockchain nicht in Kontakt
    - Vorteile der Blockchain gehen dadurch verloren

Marktüberblick

„I'm sure that in 20 years there will either be very large transaction volume or no volume."
Satoshi Nakamoto





http://visualcapitalist.com (26.10.2017)