Bitcoin

Alles was es gibt

---

21 Millionen

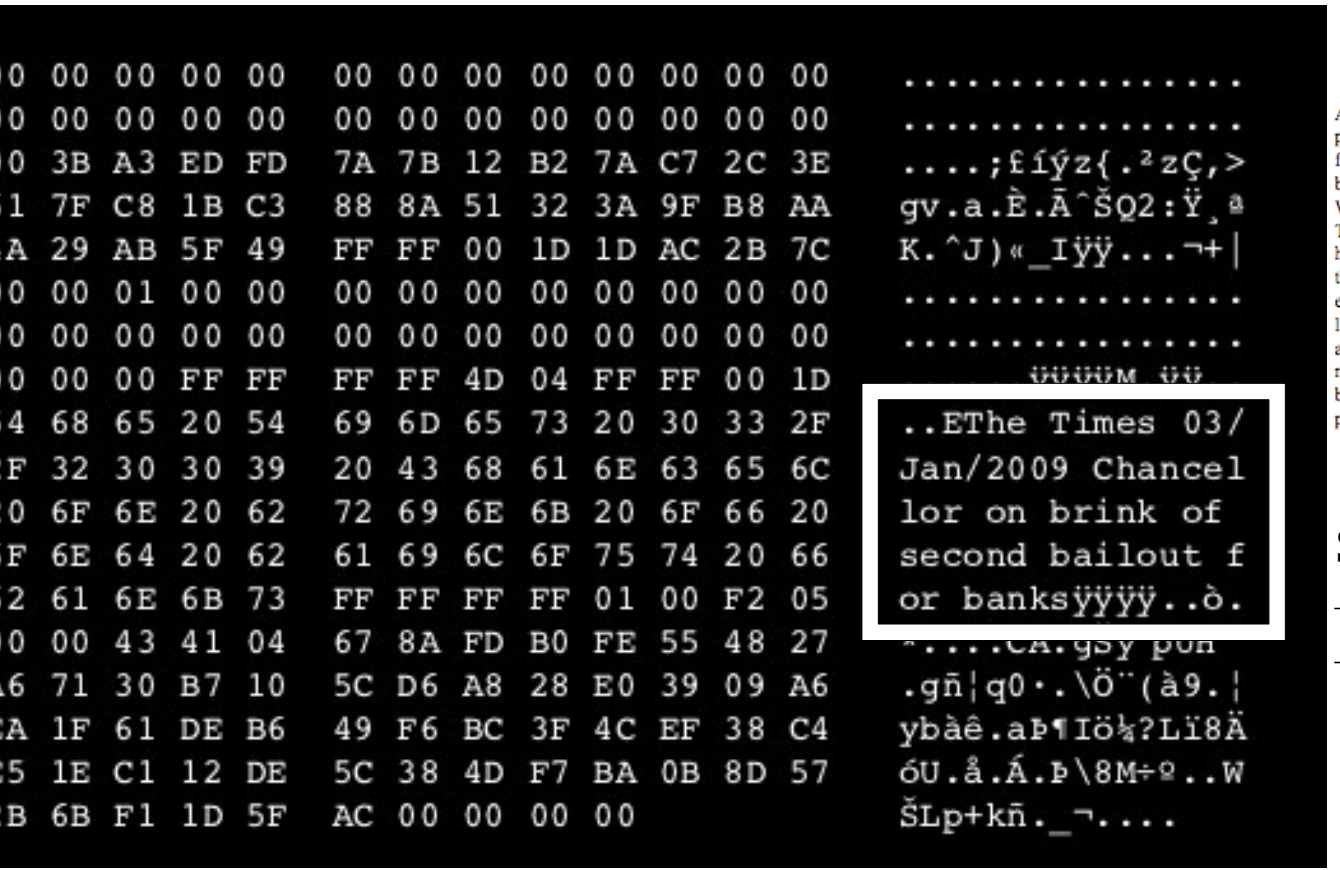
oder warum bitcoin so wertvoll ist

Überblick

- Was ist bitcoin
- Was ist Geld
- Wie läuft unser bisheriges Finanzsystem
- Warum ist bitcoin das beste Geld
- Wie funktioniert bitcoin
- Wieviel ist bitcoin wert
- Wie verändert bitcoin die Welt

Bitcoin ist eine der bedeutensten Erfindungen der Menschheitsgeschichte.

Was ist bitcoin



Bitcoin: A Peer-to-Peer Electronic Cash System

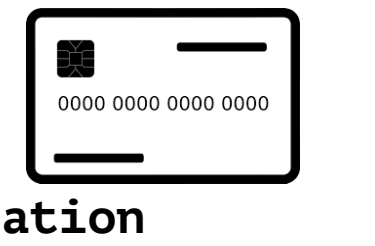
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Satoshi Nakamoto
→ 2008 white paper
→ 2009 Genesis block

Was ist Geld

- Eine der ältesten Technologien der Menschheit (mind 30 000 Jahre)
  - Buchführung über Schulden (Kerbholz)
  - Muscheln, Kühe, Glasperlen
  - Gold & Silber
  - Papiergeld
  - Digitales Geld



- **Grundlage für Zivilisation**
  - Handel ermöglicht Produktion und Austausch von fast allen Gütern
  - Handel bringt beiden Seiten einen Mehrwert mehr Handel → mehr Reichtum
  - Ohne Geld, welches Handel ermöglicht wäre unsere Gesellschaft nicht möglich
  - Geld → Kommunikation von Wert → Sprache

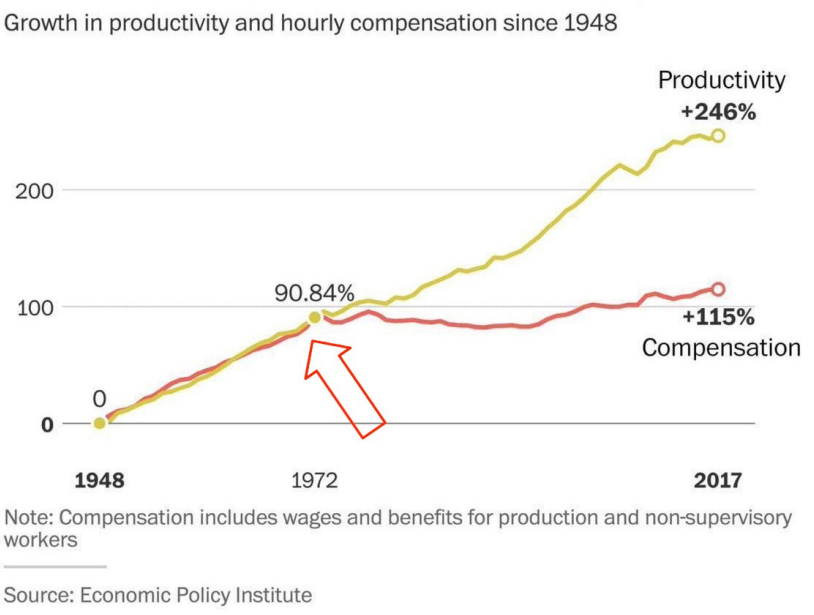
Wie läuft unser bisheriges Finanzsystem

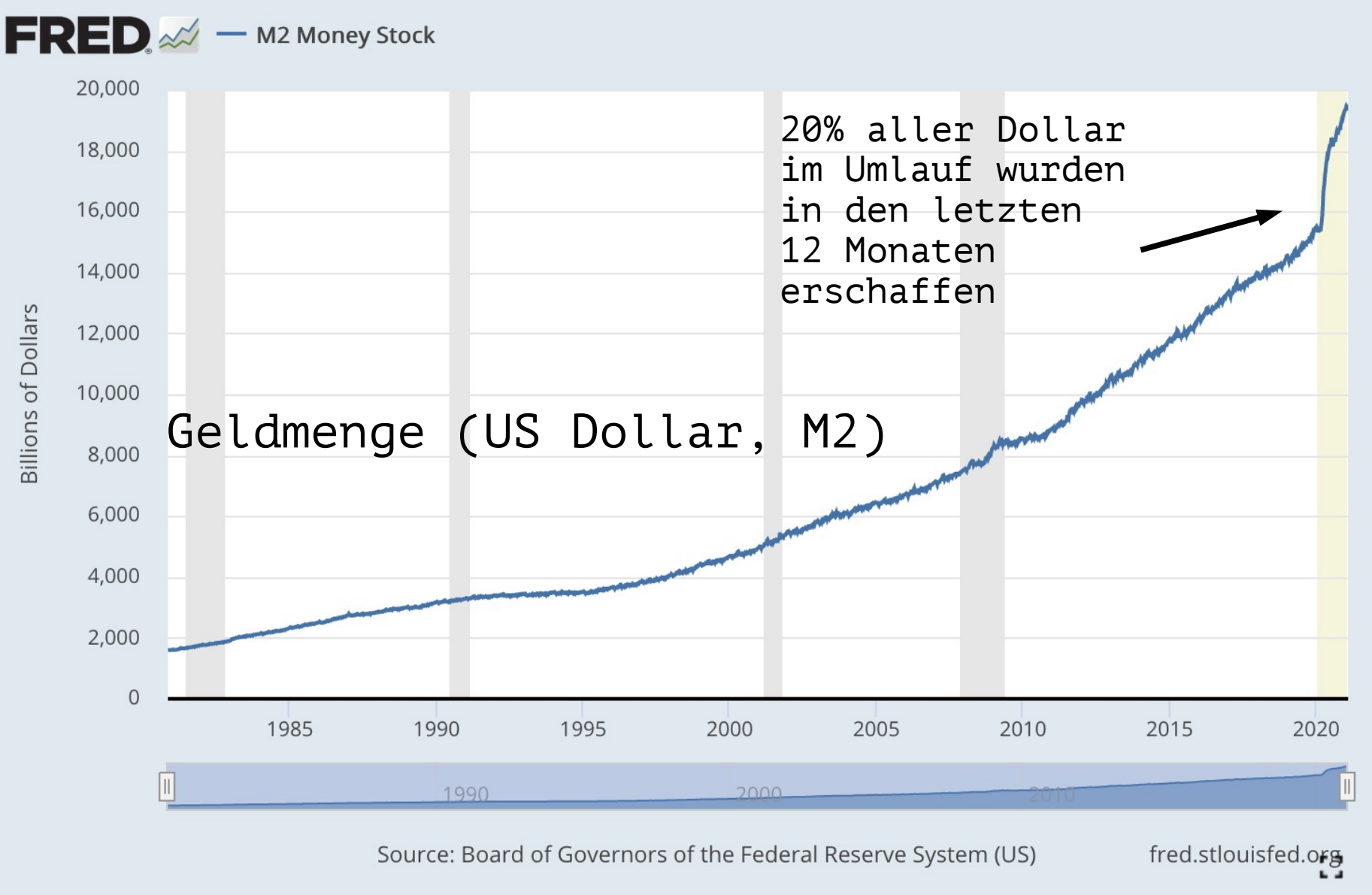
- Gold = Geld = Macht
- Fiatgeld aus dem lateinischen Wort fiat („Es sei getan! Es geschehe! Es werde!“)
  - 1913 Gründung des privaten Federal Reserve System
  - 1944 Bretton Woods → der Dollar wird Weltreservewährung
  - Goldverbot
  - 1971 Aufhebung der Golddeckung

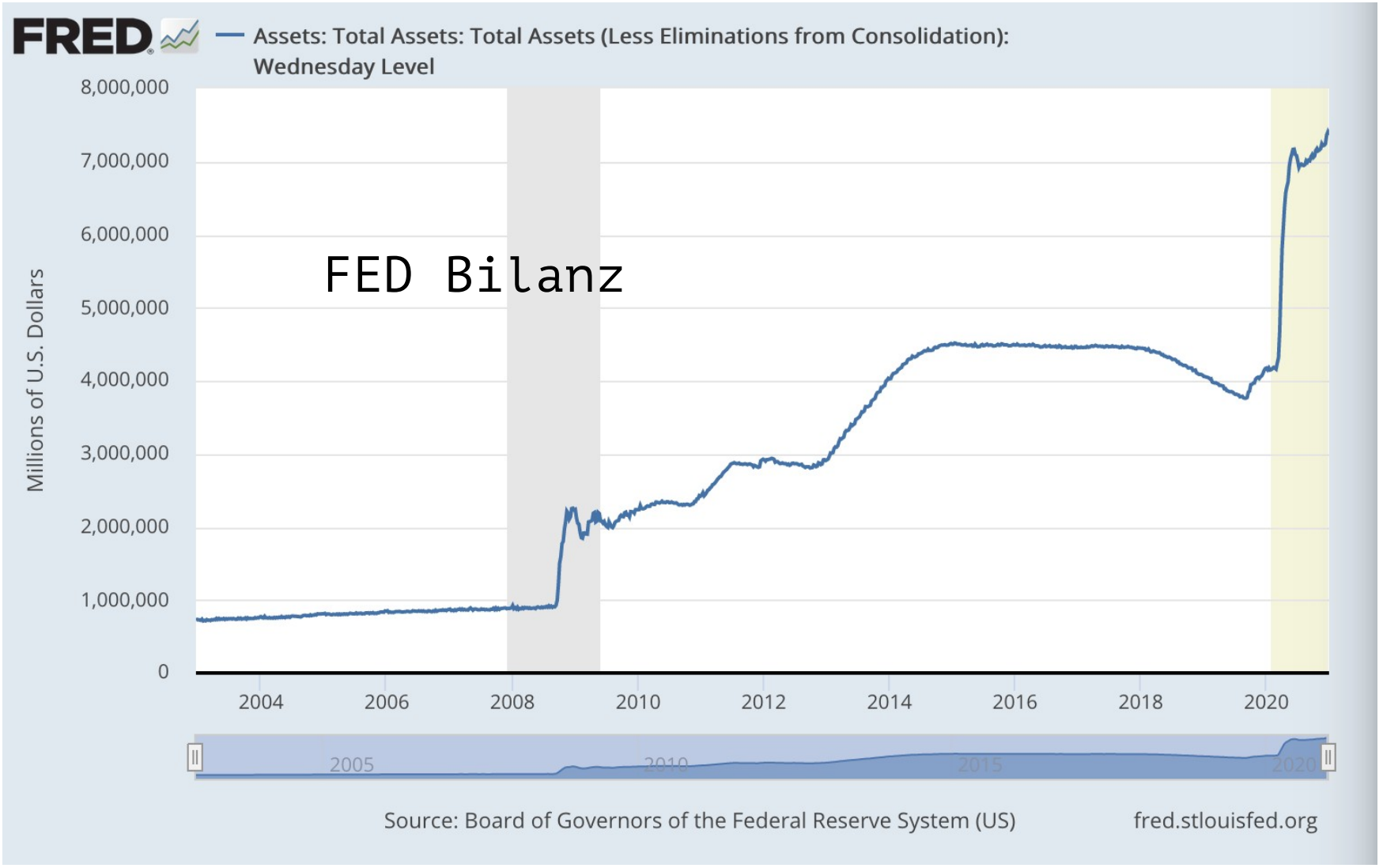
→ Zentralbanken können Geld aus dem nichts erschaffen.

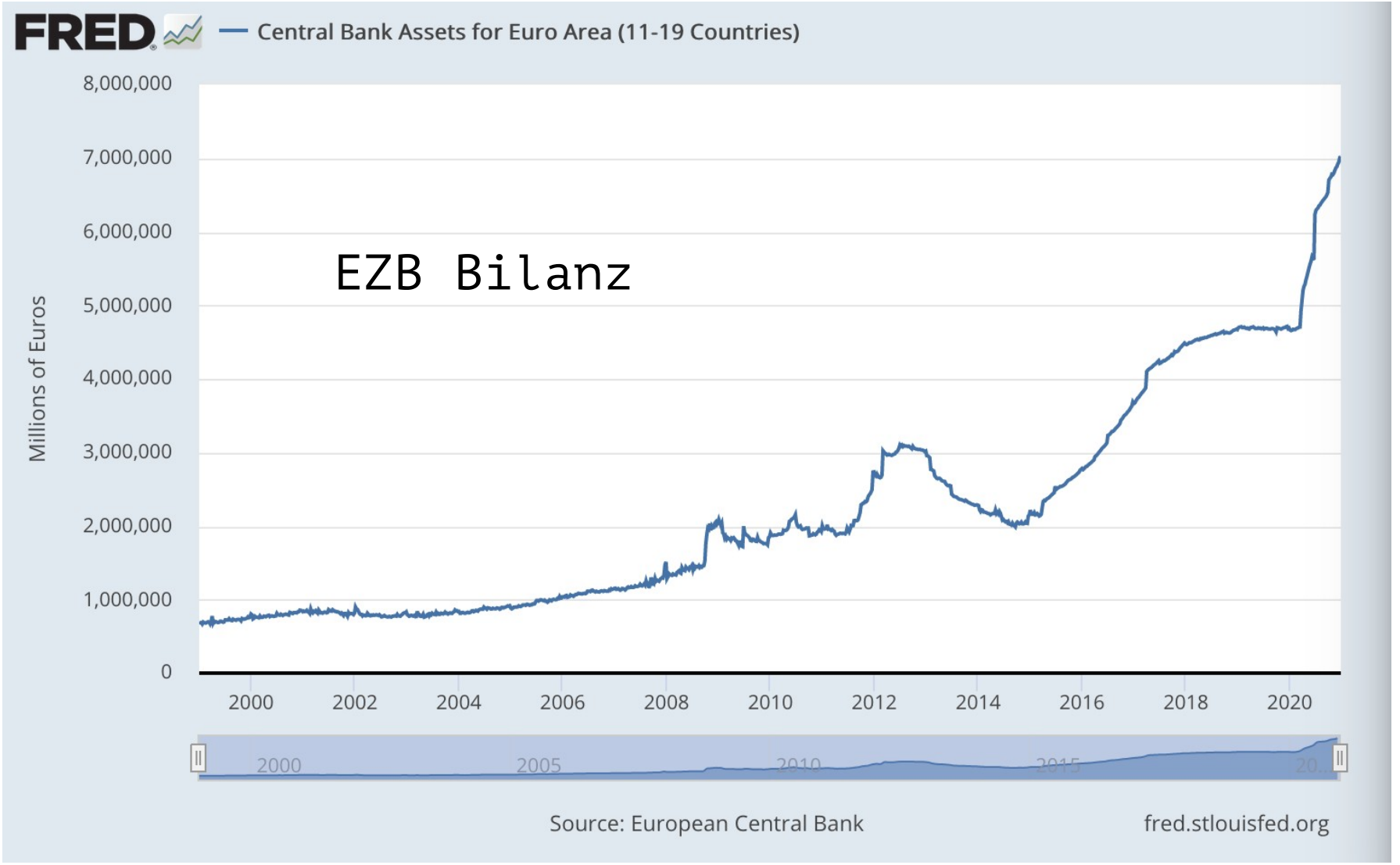
Das entwertet das Geld aller zugunsten derer,die es zuerst bekommen (→Cantillon Effekt)

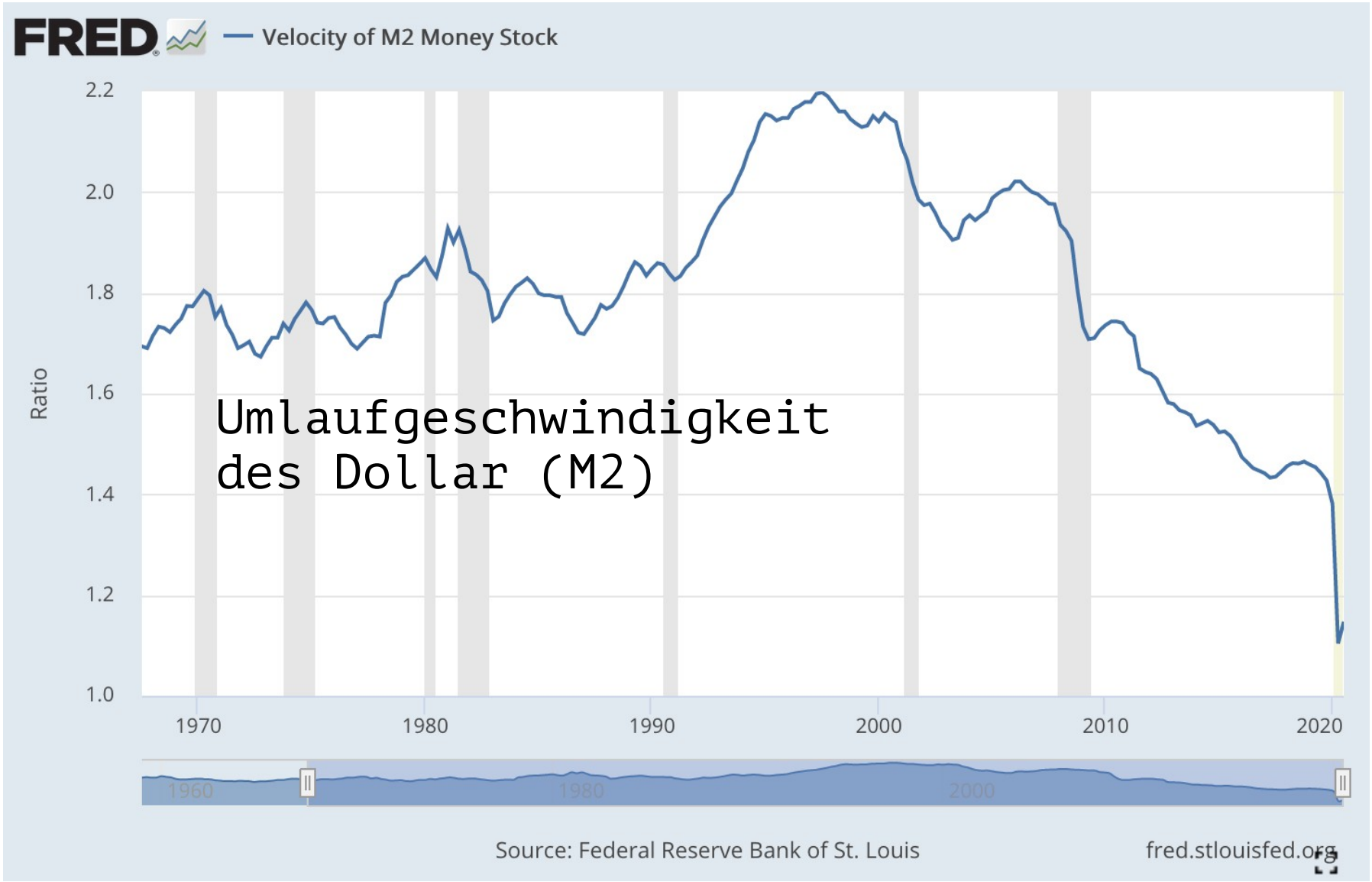
Umverteilung vom Volk an eine Elite
→ Schere geht auseinander




FRED
M2 Money Stock
20,000
18,000
16,000
14,000
12,000
10,000
8,000
6,000
4,000
2,000
0
Billions of Dollars
20% aller Dollar
im Umlauf wurden
in den letzten
12 Monaten
erschaffen
Geldmenge (US Dollar, M2)
1985
1990
1995
2000
2005
2010
2015
2020
Source: Board of Governors of the Federal Reserve System (US)
fred.stlouisfed.org


FRED
Assets: Total Assets: Total Assets (Less Eliminations from Consolidation): Wednesday Level
Millions of U.S. Dollars
8,000,000
7,000,000
6,000,000
5,000,000
4,000,000
3,000,000
2,000,000
1,000,000
0
FED Bilanz
2004
2006
2008
2010
2012
2014
2016
2018
2020
2005
2010
2015
2020
Source: Board of Governors of the Federal Reserve System (US)
fred.stlouisfed.org


FRED
Central Bank Assets for Euro Area (11-19 Countries)
EZB Bilanz
Millions of Euros
8,000,000
7,000,000
6,000,000
5,000,000
4,000,000
3,000,000
2,000,000
1,000,000
0
2000
2002
2004
2006
2008
2010
2012
2014
2016
2018
2020
2000
2005
Source: European Central Bank
fred.stlouisfed.org



Umlaufgeschwindigkeit des Dollar (M2)

Warum ist bitcoin das beste Geld

- Die Erfindung der absoluten Knappheit → 21 Millionen
- Dezentral
- Person-zu-Person

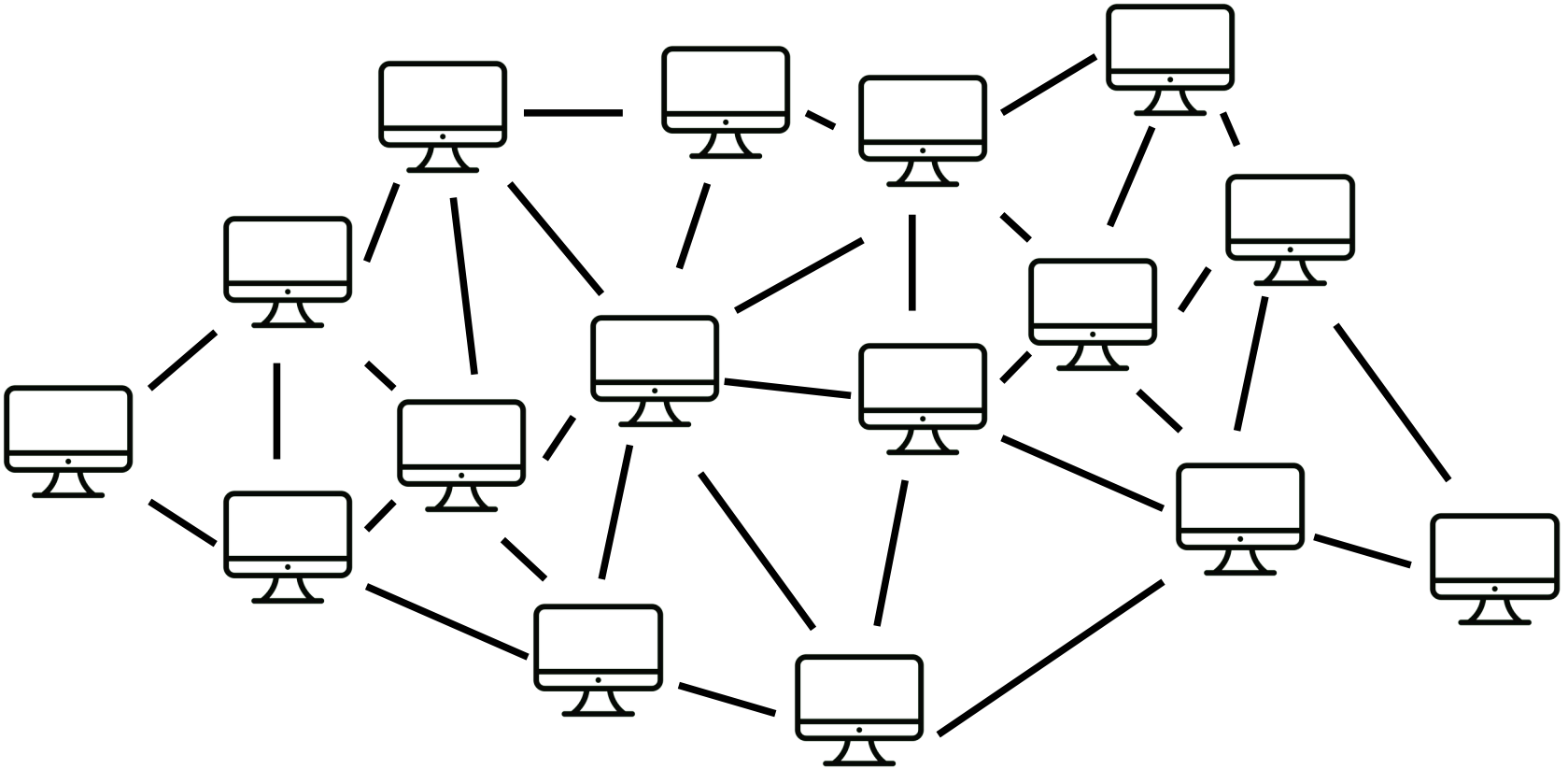
- Erfüllt alle wichtigen monetären Eigenschaften
  - Haltbar
  - Teilbar
  - Transportierbar / überweisbar
  - Nicht fälschbar
  - Nicht leicht nachproduzierbar
  - Verifizierbar

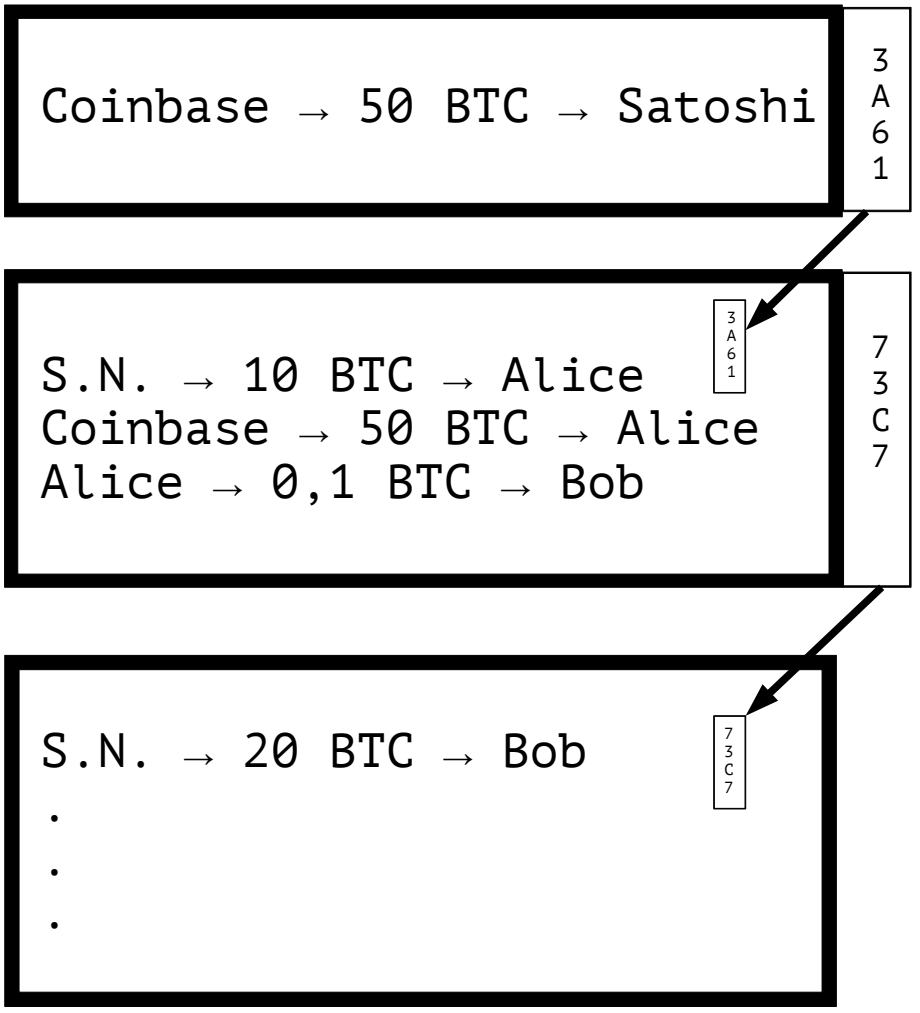
→ Besser als Gold

→ Besser als das derzeitige Finanzsystem

→ Besser als Altcoins

Wie funktioniert bitcoin

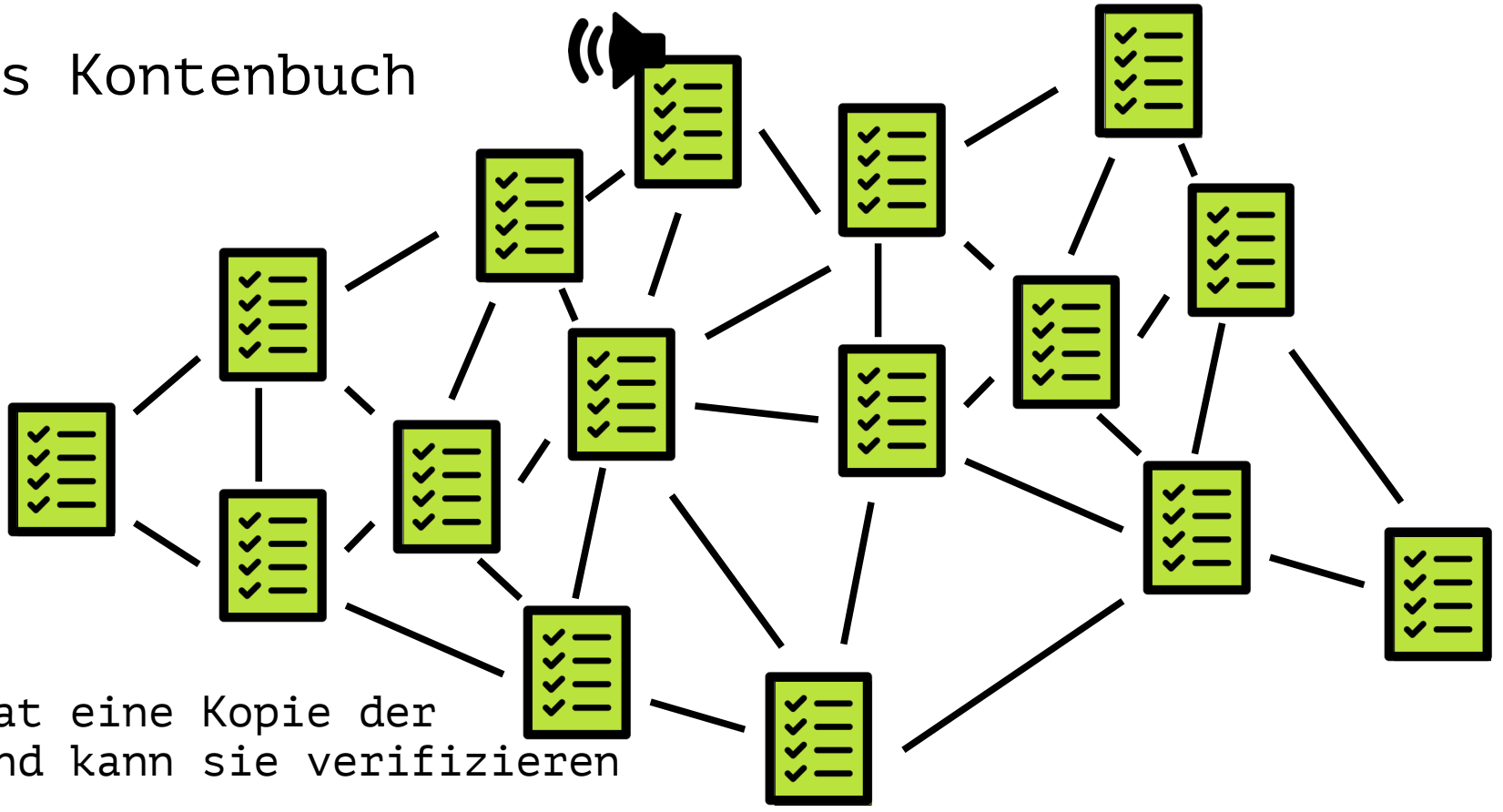




Blockchain

- Liste aller Transaktionen
- ~1 Block / 10 Minuten
- Jeder Block beinhaltet den Hash des vorherigen Blocks
  - Ähnlich wie Quersumme
  - Fingerabdruck

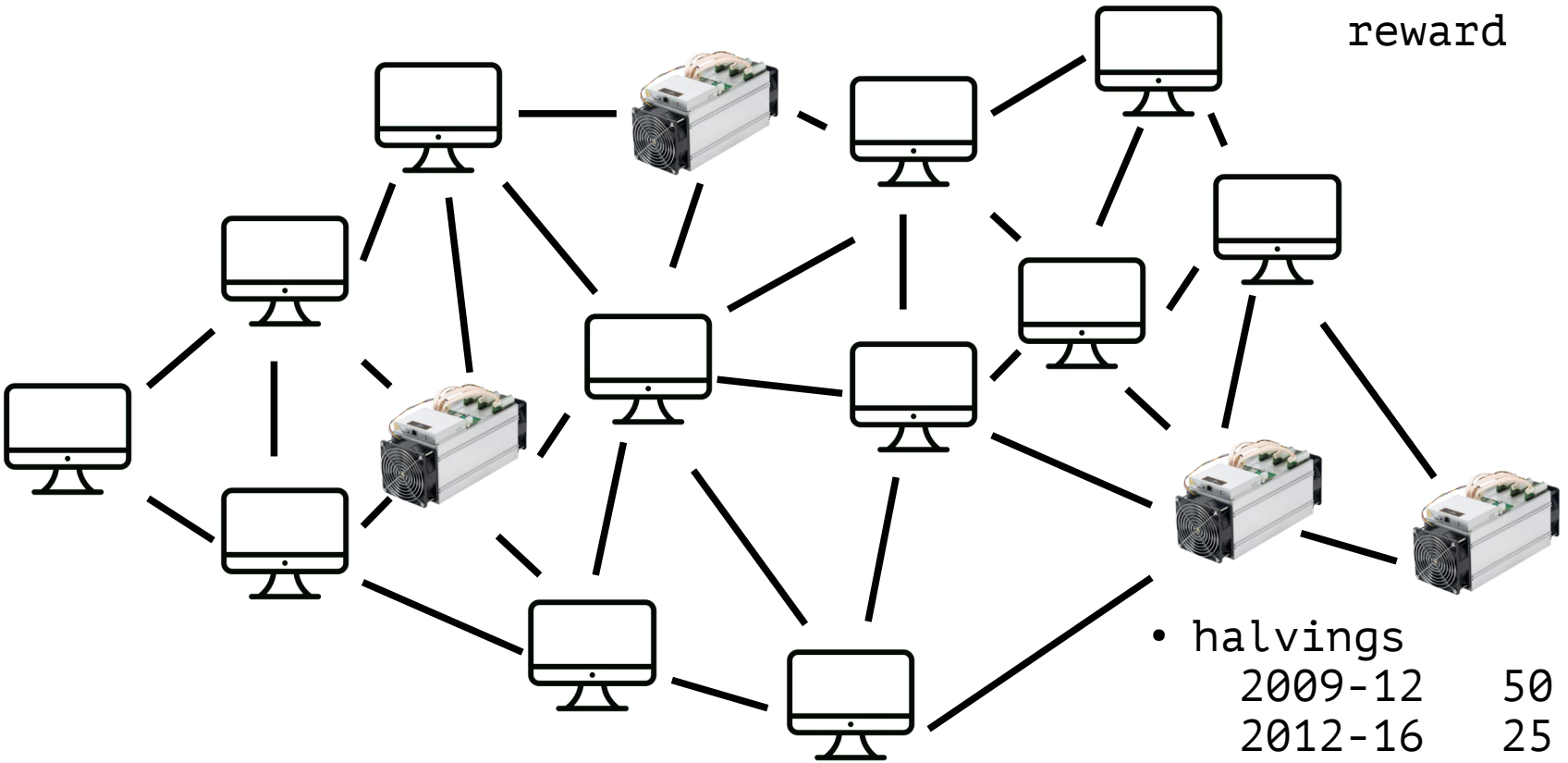
Verteiles Kontenbuch



- Jeder node hat eine Kopie der Blockchain und kann sie verifizieren
- Keiner kann die Historie ändern oder unberechtigt weiterschreiben
- Jeder hat alle Informationen
- Niemand muss um Erlaubnis fragen

mining

- Jeder darf minen
- Miner wetteifern um den mining reward



- halvings

2009-12	50	btc
2012-16	25	btc
2016-20	12,5	btc
2020-24	6,25	btc

mining

Aufgabe : einen passenden Hashwert finden → sha256

Kosten : Energie & hardware

Nutzen : Darf den nächsten Block aus den unbestätigten Transaktionen der letzten 10 Minuten schnüren. Dieser muss eine richtigen Hashwert enthalten → leicht überprüfbar

Belohnung: neuproduzierte bitcoin + Transaktionsgebühren

- Alle 2 Wochen wird die Schwierigkeit einen passenden Hashwert zu finden angepasst
- Anzahl der Transaktionen unabhängig vom Energieaufwand
- Sucht den günstigsten Strom → Überschuss

Energieverbrauch

- Transparenz - Bitcoin braucht viel Energie
- Energie vs CO2
- Überschussenergie
- Förderung von neuen günstigen Energiequellen
- Es ist diese Energie wert

Fiatsystem

Bitcoin

Was “habe” ich, wenn ich bitcoin habe

Private Key

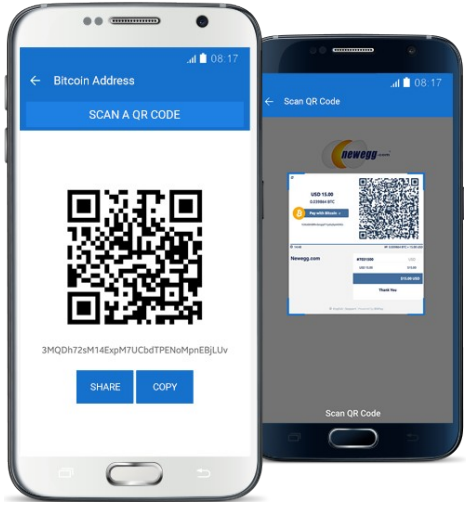
L3SgtZFTzasR9dkTt9PbW8a8hW
u8Ap3ErBn7zBkuLf386nXTCicp

- Der Zugang zu deinen bitcoin
- Wie ein “Passwort”
- Kann in Form von seed wörtern gespeichert werden (mnemonic)
- Absolut geheim

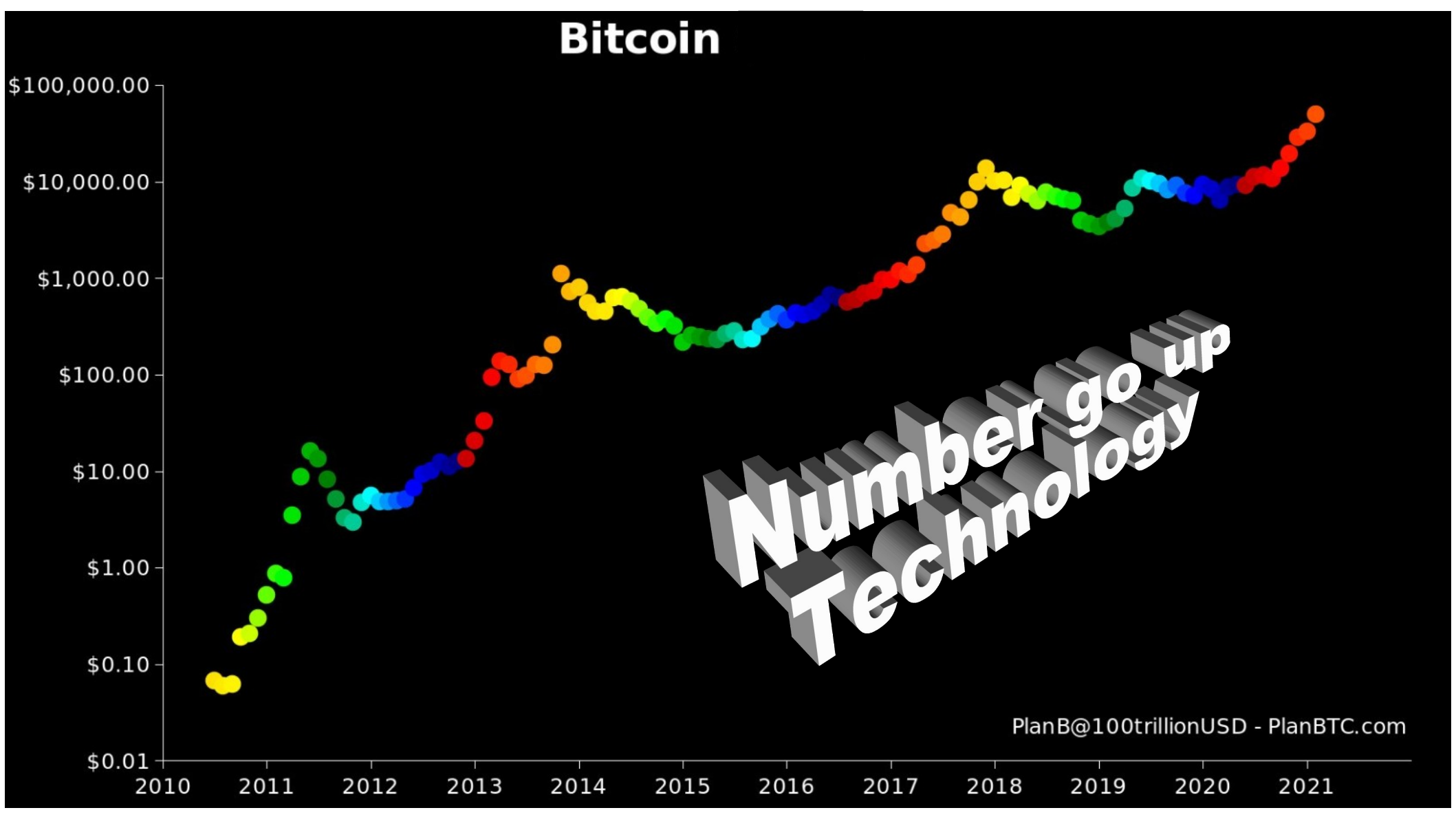
Public Key

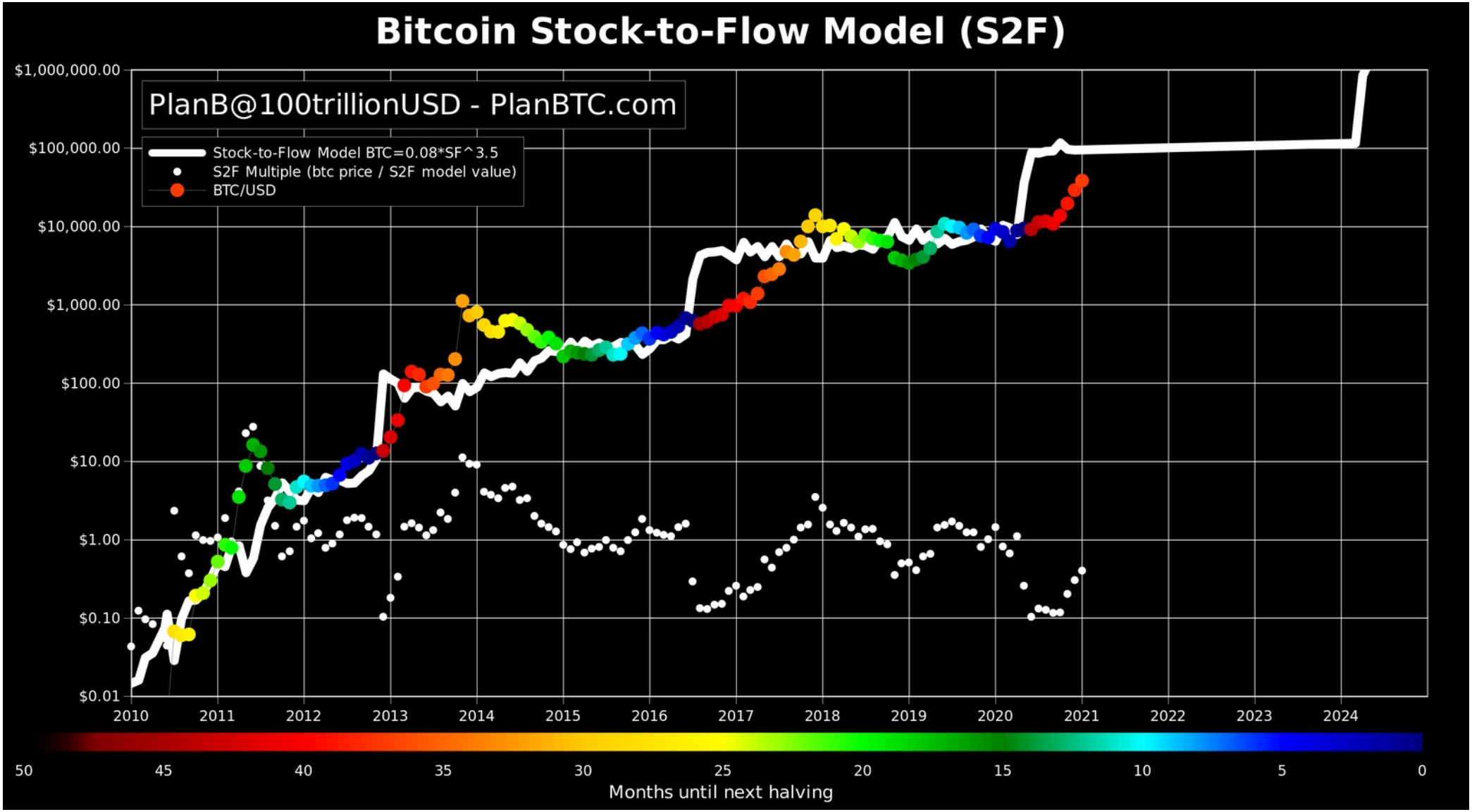
1CC3X2gu58d6wXUWMffpuz
N9JAfTUWu4Kj

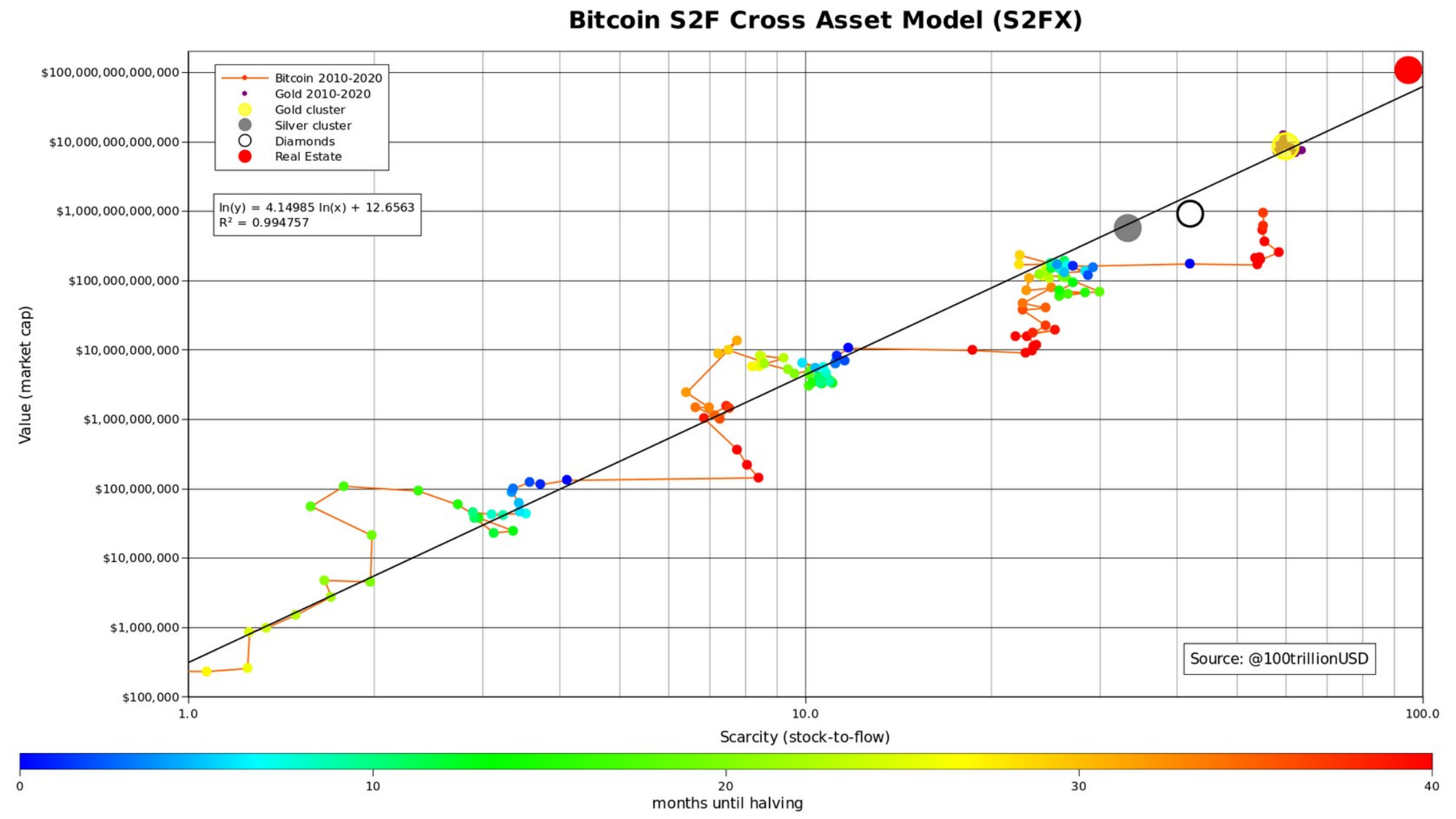
- Öffentliche Adresse
- Ähnlich wie eine IBAN / Kontonummer
- Empfangsadresse zum herzeigen und verschicken

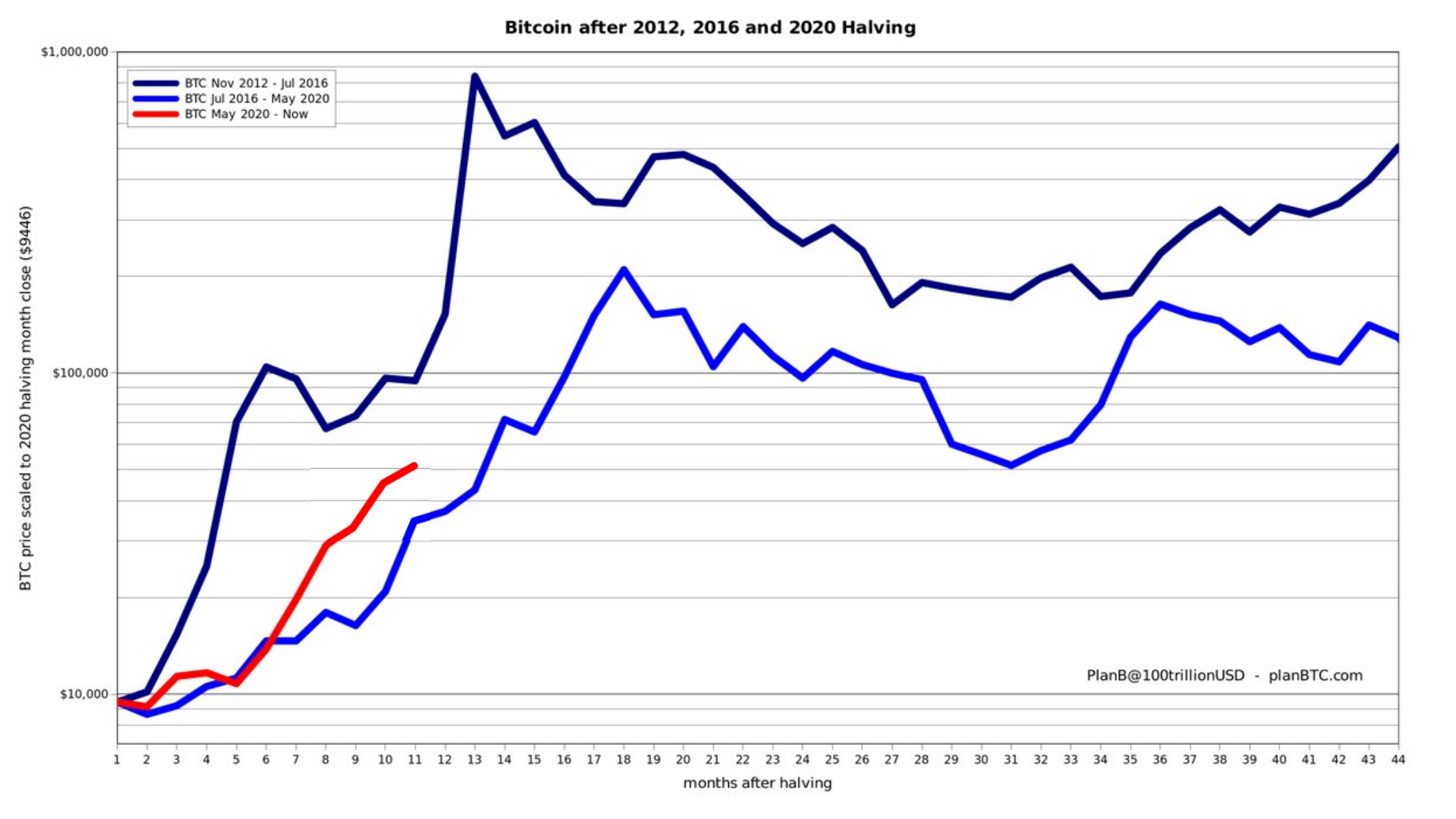


Wieviel ist bitcoin wert

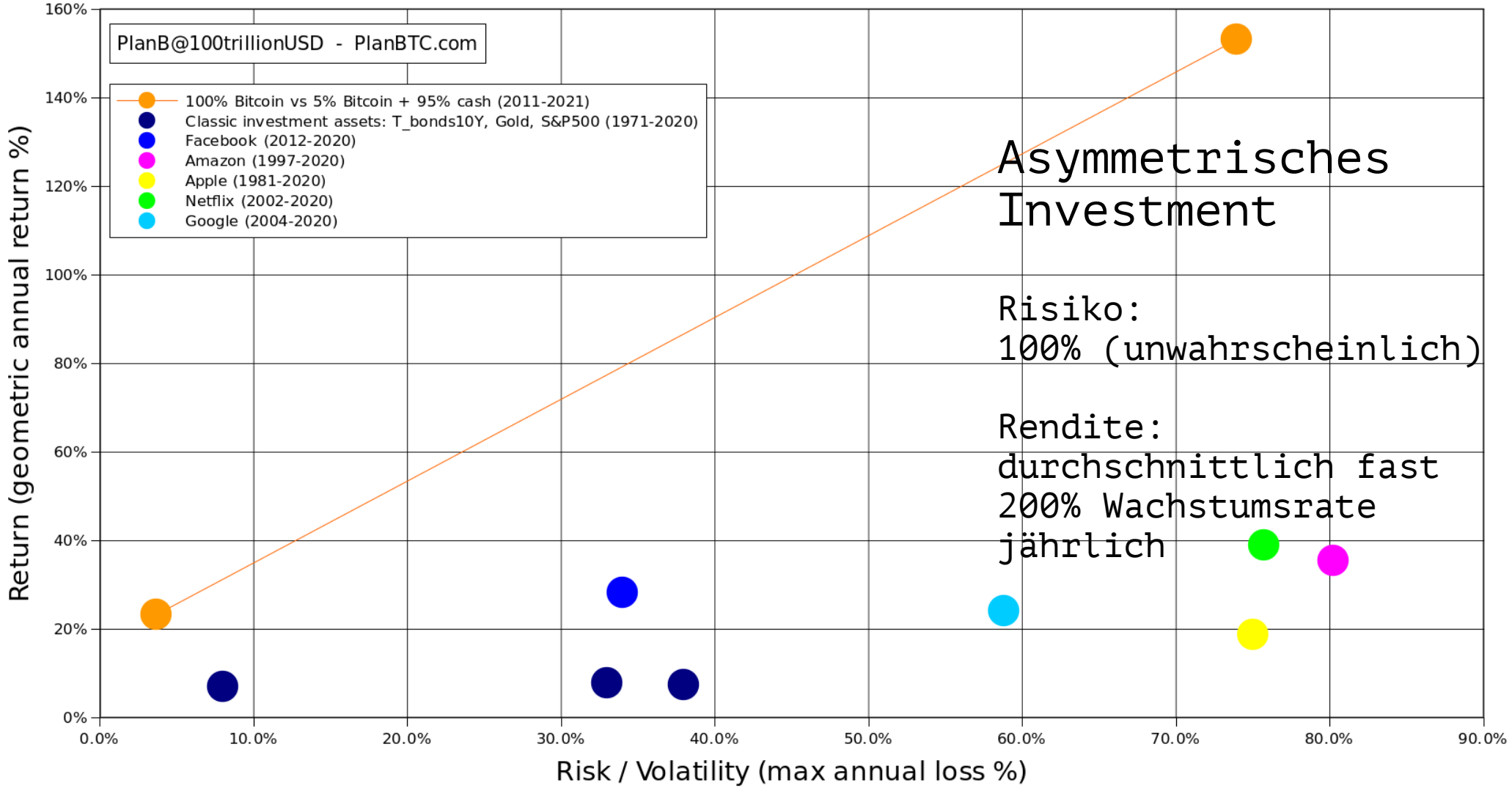

Bitcoin
$100,000.00
$10,000.00
$1,000.00
$100.00
$10.00
$1.00
$0.10
$0.01
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
Number go up
Technology
PlanB@100trillionUSD - PlanBTC.com


Bitcoin Stock-to-Flow Model (S2F)
PlanB@100trillionUSD - PlanBTC.com
Stock-to-Flow Model BTC=0.08*SF^3.5
S2F Multiple (btc price / S2F model value)
BTC/USD
$1,000,000.00
$100,000.00
$10,000.00
$1,000.00
$100.00
$10.00
$1.00
$0.10
$0.01
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
50
45
40
35
30
25
20
15
10
5
0
Months until next halving


Bitcoin S2F Cross Asset Model (S2FX)
Bitcoin 2010-2020
Gold 2010-2020
Gold cluster
Silver cluster
Diamonds
Real Estate
ln(y) = 4.14985 ln(x) + 12.6563
R² = 0.994757
Source: @100trillionUSD
Value (market cap)
$100,000,000,000,000
$10,000,000,000,000
$1,000,000,000,000
$100,000,000,000
$10,000,000,000
$1,000,000,000
$100,000,000
$10,000,000
$1,000,000
$100,000
1.0
10.0
100.0
Scarcity (stock-to-flow)
0
10
20
30
40
months until halving


Bitcoin after 2012, 2016 and 2020 Halving
$1,000,000
$100,000
$10,000
BTC Nov 2012 - Jul 2016
BTC Jul 2016 - May 2020
BTC May 2020 - Now
BTC price scaled to 2020 halving month close ($9446)
PlanB@100trillionUSD - planBTC.com
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44
months after halving

mehr Rendite UND/ODER weniger Risiko



Hodl

Wie verändert bitcoin die Welt

- Trennung von Staat & Geld
- Voraussehbare Nachproduktion
    - Ca im Jahr 2140 werden alle 21 Mio bitcoin erschaffen worden sein
- Eigenverantwortung
    - Jeder ist seine eigene Bank / ohne Mittelsmänner
- Inflation → Konsum
    - “lieber heute als morgen kaufen”
- Deflation → Sparen
    - Unternehmen können vorausplanen
    - Einzelpersonen kümmern sich um ihre Zukunft

Zeit & Energie

Das wertvollste was wir haben ist unsere Zeit und Energie.

Es macht Sinn sie gegen etwas einzutauschen was ähnlich wenig nachproduzierbar ist.

Wer Geld druckt klaut allen Zeit und Energie.

Bitcoin wird Welt-Reserve-Währung

- Netzwerkeffekt
  - Meiste Nutzer (Wikipedia kopieren bringt nichts)
  - durch die meiste Energie gesichert
  - Meiste Entwickler

- Geschichte nicht wiederholbar
  - Konnte sich in den ersten Jahre ungestört dezentralisieren
  - Man kann absolute Knappheit nur einmal erfinden (Erfindung der Null)

- Spieltheorie
  - Wer bitcoin hat gewinnt
  - Härteres Geld verdrängt inflationierbares Geld

- Bitcoin ist unaufhaltsam geworden

Alles was es gibt

---

21 Millionen