Universität St.Gallen

Sind Kryptowährungen das Geld der Zukunft?

Vortrag ETH-Emeritenstamm, 25. November 2024

Johannes Binswanger, Universität St. Gallen

"From insight to impact"

Diskussionspunkte für heute

1. Was ist Geld?

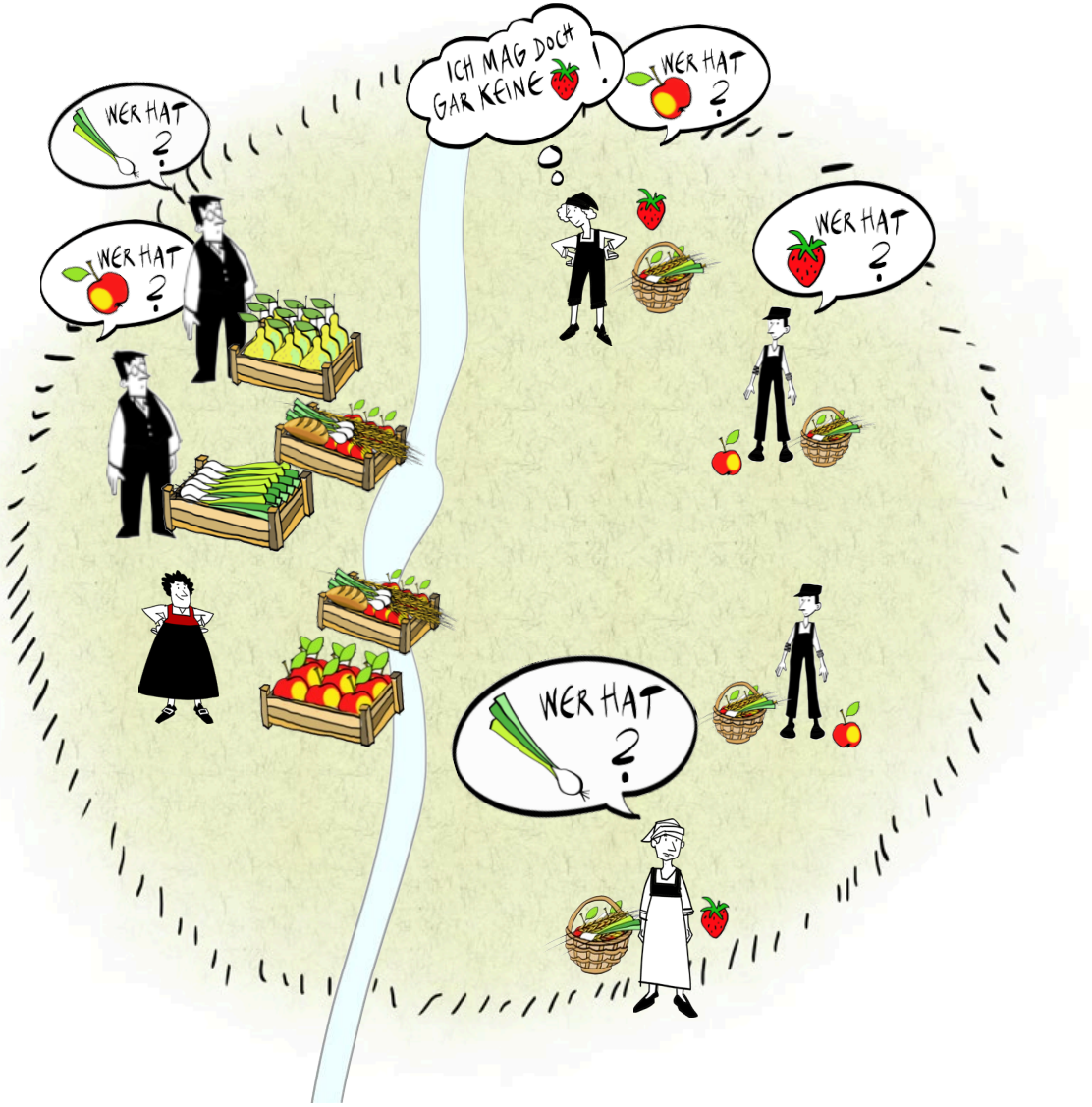
2. Was sind Kryptowährungen und wie funktionieren sie?

3. Sind Kryptowährungen das Geld der Zukunft?

Universität St.Gallen

Kontext: Funktionen von Geld und traditionelle Geldformen

Eine Welt ohne Geld



Geld

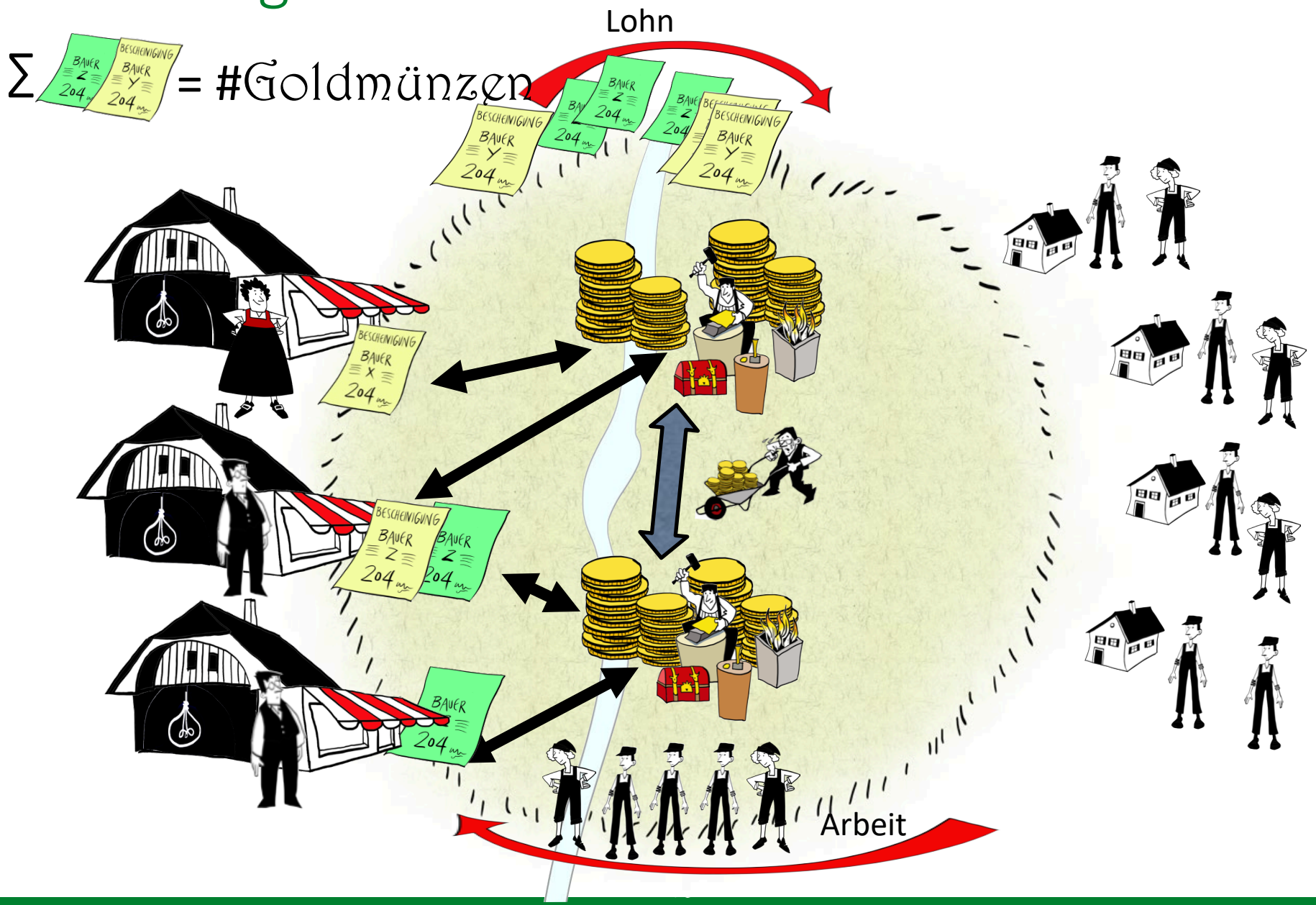
Funktionen von Geld

- Zahlungsmittel
- „Messlatte“
- Wertaufbewahrung

Anforderungen an Geld

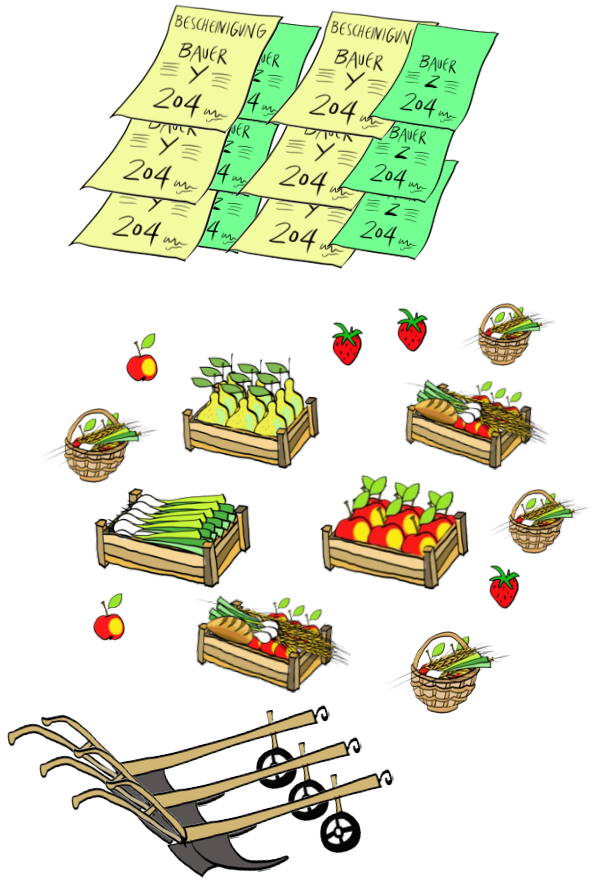
- Geldwertstabilität
- Effizienzsteigerung wirtschaftlicher Abläufe

Gold und Zettelgeld

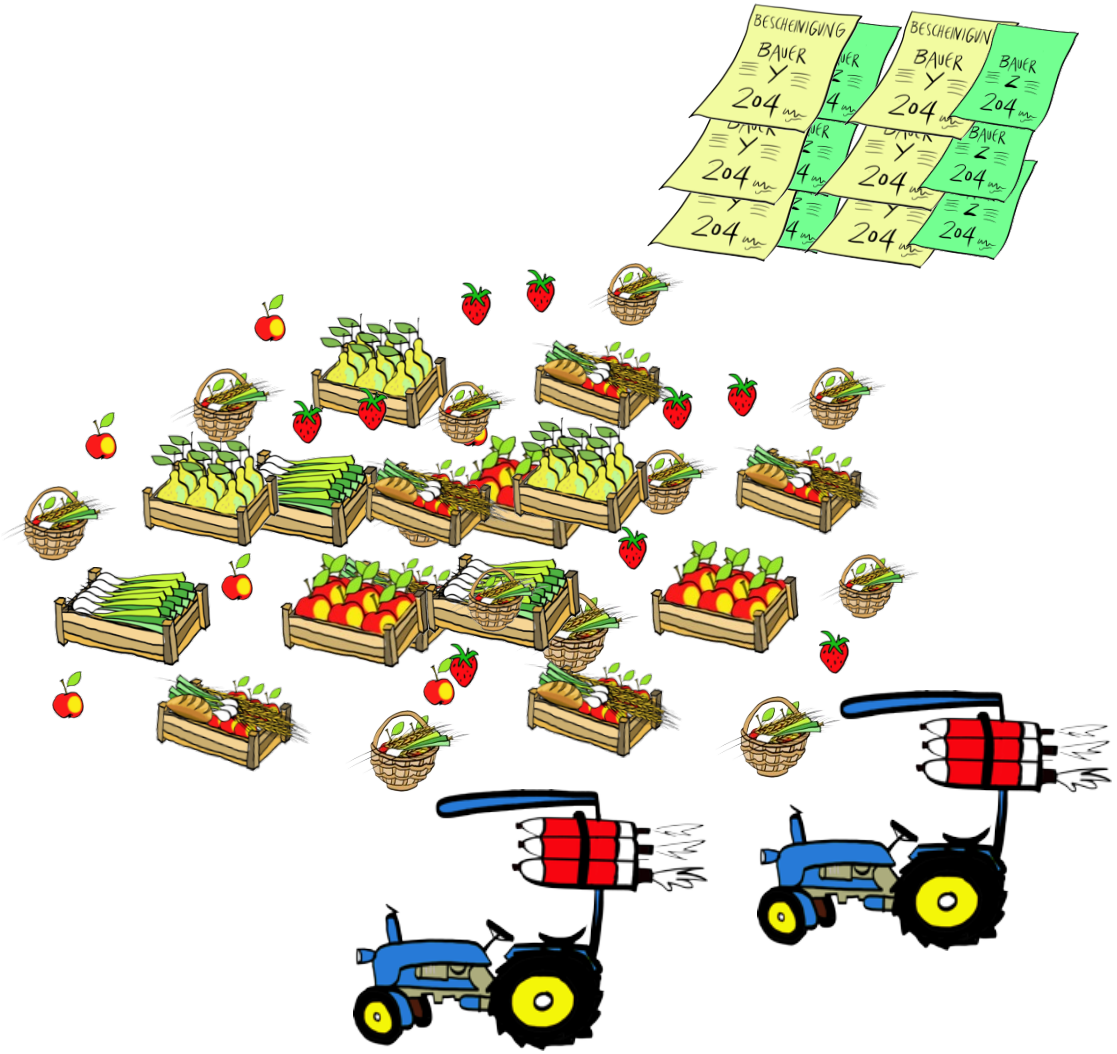


Probleme eines unflexiblen Geldangebotes (z.B. bei Golddeckung)

Vorher



Nachher



Elastisches Geldangebot

Früher

- Goldschmiede leihen bei Kreditgeschäften mehr Zettel aus als sie Gold haben

Heute

- Zentralbank kauft Anlagen mit neu geschaffenem Geld (v.a. Staatsanleihen)

Ziele von elastischem Geldangebot

- Preisstabilität
- Effizienzsteigerung der wirtschaftlichen Abläufe

Bilanz einer Zentralbank

Entwicklung der Bilanzsummen von Zentralbanken: Schweiz

Entwicklung der Bilanzsummen von Zentralbanken: USA

Universität St.Gallen

Kryptowährungen

Was macht eine Kryptowährung aus?

Definition

- Digitale Währung, welche **nicht durch eine zentrale Autorität, sondern durch ein dezentrales Netzwerk bereitgestellt** wird.

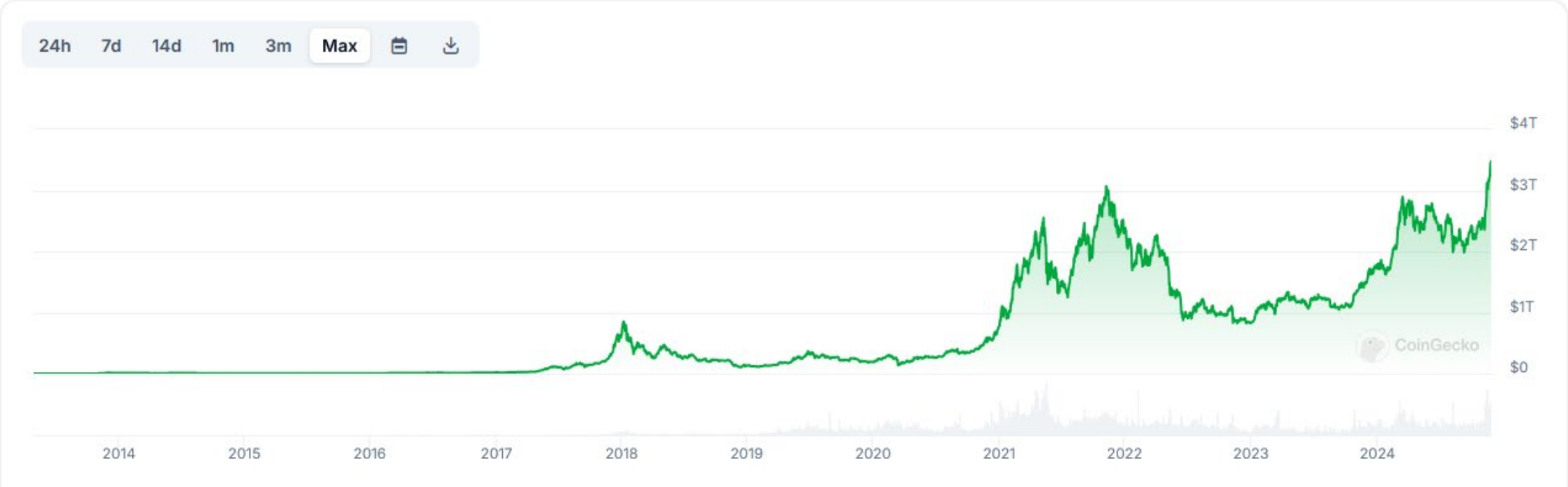
Motivation

- Libertärer Traum; Misstrauen in zentralisierte Organisationen
- Technologische Faszination

Zentrale Problemstellung

- Wie kann Sicherheit/Vertrauen ohne zentralisierte Autorität bereitgestellt werden?

Marktkapitalisierung von allen Kryptowährungen



Quelle: coingecko

Zum Vergleich: M3-Geldmenge in US$ beträgt aktuell rund $20T

Zusammensetzung von Kryptowährungen

Quelle: coingecko


CCC - CoinMarketCap • USD
Bitcoin USD (BTC-USD)
Follow
96,746.80 -1,040.59 (-1.06%)
As of 9:24 PM UTC. Market Open.
Data provided by CoinMarketCap
Comparisons
Indicators
Corporate Events
O 7,420.27 H 7,544.50 L 6,915.00 C 7,411.32 Vol 150b
vol undr 149,690,652,648.00
yahoo!finance
100,000.00
96,746.80
75,000.00
50,000.00
25,000.00
47.90B
2020
2021
2022
2023
2024

Hash

SHA-256 hash calculator

SHA-256 produces a 256-bit (32-byte) hash value.

Data

Econville

SHA-256 hash

332dc2ff69c8bcecfd779fe6d6a98a9ab0410ce580e4032fb2be75ebe9e22db1

Hash added to your clipboard. Simply press ⌘+V, CTRL+V to paste.

Calculate SHA256 hash

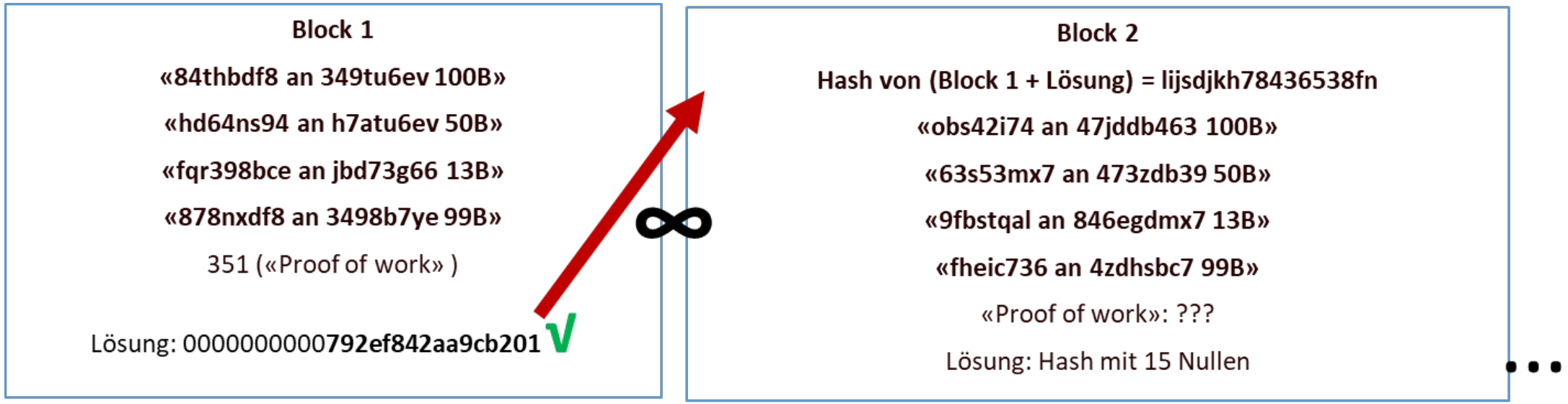
Link zu Xorbin

Block und Mining und Proof of Work (PoW)

Transaktionen	Hash des Blocks
<1> «Anna an Carla: 3»	00000000000000xxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxx
<2> «Bruno an Doris: 1»	
<3> «Carla an Emil: 8»	
<4> «Anna an Franni: 6»	
<5> «Anna an Bruno: 10»	
FINDE ZAHL…! (PoW)	

Zahl	Hash
1	07702255f33400aaa5409b363559ee57563d88ff640ba764754662c6f5769a11
2	525d22e43f99cbe369b4f6010640f6f7317acae0dcc7e7fde8b3442cfbddd49c
3	401b77326ca1165971e40e31ed0c66d8e68deb1ee27f7e8488d5adfad13a8108
4	e10caa9097c3a3b5d6e9d89a94b56e4a710072a57cc938bd85cde1f537489c23
5	48d5d10f7e342415f3bbe56c2e279f22ef4d1b6353ad3ef924dce0e4d68456e2

Verkettung von Blöcken → Blockchain



Konsensmechanismus: wenn es alternative Blockchainstränge gibt, ist die längste die richtige

Dezentrale Bereitstellung von Sicherheit

- Bitcoin beruht auf Proof-of-Work (PoW) Konsensmechanismus
- Herzstück des PoW: „Hash-Rätsel“
- Schwierigkeit des Hash-Rätsels (Anzahl Nullen) so, dass mit vorhandener Rechenleistung im Schnitt alle 10 Minuten eine Lösung gefunden wird
- Hauptproblem: Verminderung doppelter Ausgabe von Kryptogeld („double spending“)

Double Spending Attack

- Alice kauft Anlagewerte bei Bob und gibt Zahlung in Auftrag (Transaktion 1; T1)
- Danach sendet Alice die gleichen Bitcoins auf verschiedene andere Wallets, welche ihr gehören (T2) und einen neuen Block (bzw. neue Blöcke) bilden.
- Alice wartet Escrow-Perode („Treuhandperiode“) ab, so dass die Anlagewerte geliefert werden.
- Während dieser Zeit berechnet Alice die Hash-Rätsel („Mining“) für alternative Blöcke und sendet nach Erhalt der Anlagewerte die Lösung(en) für T2 ans Netzwerk.
- Mit genügend Rechenleistung schafft es Alice, die längste Blockchain zu erstellen.
- Per Protokoll ist die längste Blockchain die richtige.
- Die Wahrscheinlichkeit des Erfolgs einer solchen Attacke geht gegen 100% wenn Alices Anteil der Rechenleistung im System gegen 100% geht.

Wann lohnt sich eine Attacke nicht?

Wenn erwartete Kosten höher als erwarteter Ertrag sind…

- Erwarteter **Ertrag**: Summe aller verfügbaren Anlagewerte, welche über Kryptowährung gekauft werden können
- Erwartete Kosten: Hardware für Mining mit hinreichend mehr Rechenleistung als im gesamten existierenden Netzwerk, (nur) für Zeitraum bis Attacke validiert ist

$$N \times c \times T > V$$

- Einheitskosten c sind in einem Gleichgewicht proportional zum regulären ehrlichen Mining-Ertrag. Somit ist eine notwendige Bedingung, dass sich eine Attacke nicht lohnt:

$$\text{Ehrlicher Mining-Ertrag} > V / T \times \text{Konst.}$$

Warum ist Mining-Ertrag proportional zu Kosten?

- Skaliere Zeiteinheiten so, dass pro Einheit im Schnitt ein Block validiert wird (Poisson-Prozess)
- Mit M Miners im Netzwerk ist die Chance auf Lösen des Hash-Rätsels 1/M. Der erwartete Nettoertrag pro Mining-Einheit somit:

$$1/M \times \text{Mining-Ertrag} - c$$

- In einem Gleichgewicht muss dies 0 ergeben. Somit

$$c = 1/M \times \text{Mining-Ertrag}$$

Proof of Work führt zu sehr unvorteilhafter Skalierung

- Die Bedingung

$$\text{Ehrlicher Mining-Ertrag} > V / T \times \text{Konst.}$$

Hat dramatische Konsequenzen für die Sicherheitskosten einer Blockchain

- Der ehrliche Mining-Ertrag bestimmt die Operationskosten des Systems. Diese nehmen **linear** mit dem Wert der möglichen Transaktionen zu → Extrem schlechte Skalierungseigenschaft!
- Die Kosten jedes einzelnen Blocks müssen proportional zum Wert der möglichen Transaktionen steigen.
- Das ist wie wenn Transaktionsgebühren für eine Banküberweisung proportional zum Wert des globalen Kapitalmarktes sein müssten!
- In einem dezentralen System nehmen Operationskosten der Sicherheit hochgradig sublinear zu!

Beispielrechnungen

$$\text{Ehrlicher Mining-Ertrag } / V > 1 / T \times \text{Konst.}$$

- Eine plausible Kalibrierung der rechten Seite ergibt 7.6% pro Block; somit 1000% pro Tag, 400 000% pro Jahr!
- Für V = 1 Milliarden ergibt sich eine jährliche Summe für Mining-Erträge von 400 Billionen!

Fazit:

- Dezentrale Sicherheit rechnet sich nur, wenn V klein ist. Daher gab es bisher auch keine erfolgreichen Attacken.

Quelle: Budish, ``Trust at Scale: The Economic Limits of Cryptocurrencies and Blockchains'', Quarterly Journal of Economics, 2024

Energieverbrauch durch Proof of Work

- Bitcoin verbraucht zwischen 0.3% und 0.8% der globalen Elektrizität.
- Eine einzige Transaktion führt zu einem CO2-Fussabdruck, der einem Mittelstreckenflug entspricht.

Universität St.Gallen

Schlussfolgerungen

Skalierungsprobleme sind dramatisch

- Dezentrale Bereitstellung von Sicherheit basiert darauf, dass sich eine Attacke nicht lohnt
- Sobald der Wert der möglichen Transaktionen über eine Kryptowährung hinreichend hoch wird, kann dezentrale Sicherheit nur unter prohibitiven Kosten bereitgestellt werden.
- Schlussfolgerung: Kryptowährungen skalieren unzureichend

Fazit:

- Kryptowährungen mit Proof of Work werden nie das konventionelle Geldsystem ablösen!

Proof of Stake als alternativer Konsensmechanismus

- Ethereum (ETH) nutzt Proof of Stake
- Verifizierung der Transaktionen in einem Block erfolgt durch Teilnehmer im Netzwerk mittels „Stimmrecht“.
- Stimmrecht ist proportional zu einer „gestakten“ Summe an ETH, welche im Falle von Betrug an Wert verliert
- Eine mathematische Modellierung des Systems zeigt, dass auch dieser Mechanismus nicht gegen grosse Attacken sicher ist.

Fazit:

Proof of Stake skaliert besser als Proof of Work, ist jedoch bei hoher Skalierung (ebenfalls) nicht hinreichend sicher gegen Attacken.

Geldangebot sollte elastisch sein

- Hierbei ist der Faktor Mensch essenziell
- Menschen können mit besser mit unknown Unknows umgehen als menschengemachte Algorithmen

Algorithmische Finanzkonstruktionen in Black-Swan-Momenten

FORBES > MONEY

PANTERA

What Really Happened To LUNA Crypto?

Q.ai - Powering a Personal Wealth Movement Former Contributor
Making wealth creation easy, accessible and transparent.

Sep 20, 2022, 11:57am EDT

Updated Sep 21, 2022, 03:38pm EDT

This article is more than 2 years old.

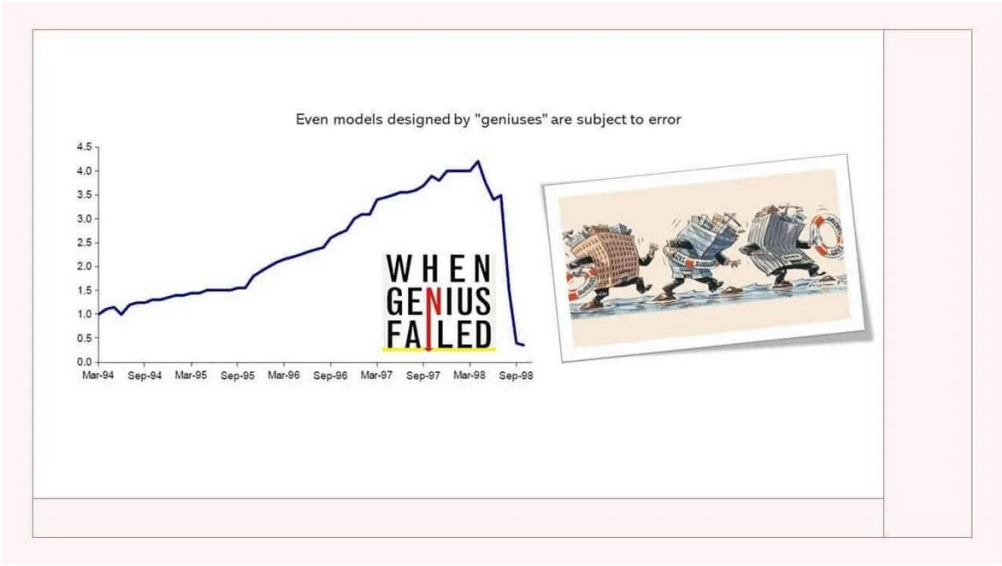
GETTY IMAGES

Key takeaways

- When the Luna crypto network collapsed, it's estimated that $60 billion got wiped out of the digital currency space.

What We Can Learn From The Long Term Capital Management Hedge Fund Collapse

BY THE INSTITUTE



In this article we are going to talk about financial market history and why it is important for both the fundamental investor and quantitative trader to know how these events unfolded and what impact they had on the market. We put our focus on the LTCM hedge fund collapse and the lessons you can learn from it.

Digitale Zentralbankwährungen

- Seit einigen Jahren sind Zentralbanken selbst an Block-Chain-Lösungen für digitales Zentralbankengeld interessiert
- In diesem Falle besteht jedoch eine zentrale Autorität. Daher handelt es sich hier nicht um Kryptowährungen im eigentlichen Sinne.

Zum Mitnehmen

- Dezentrale digitale Währungen skalieren zu schlecht und/oder sind hochskaliert nicht hinreichend gegen Attacken geschützt.
- Eine Geldsorte, die ihre Aufgaben erfüllen soll, muss elastisch im Angebot sein. Digitale Währungen können dies nicht hinreichend flexibel liefern.

In Summe: Kryptowährungen sind nicht das Geld der Zukunft!