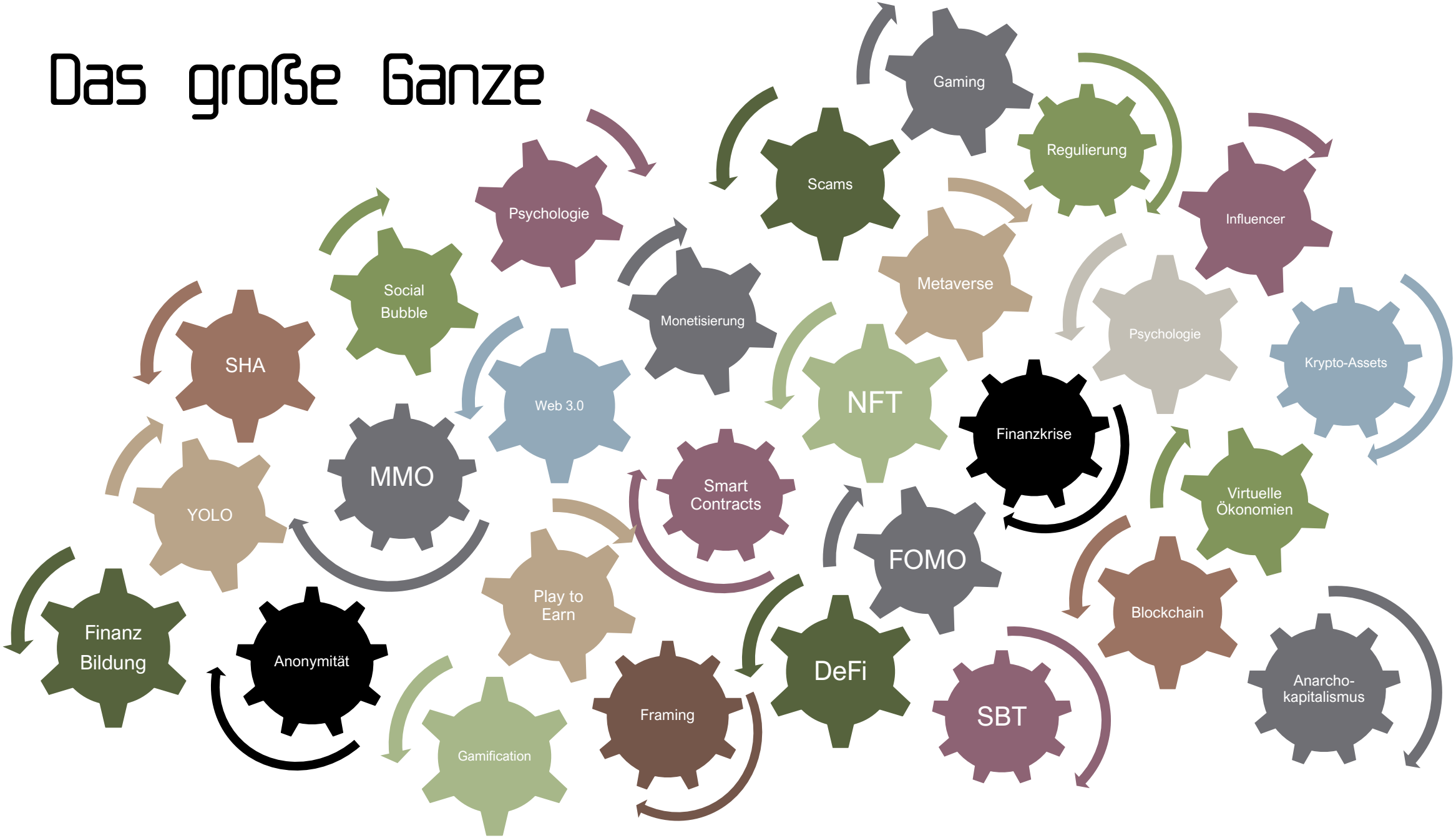
Pierre Rafih

AK Finanzen, 2. Juli 2022

Blockchain, Krypto, NFT, Metaverse und Co.

Hochschule für angewandtes Management

Das große Ganze



Kurzer Faktencheck

- Was war die erste erfolgreiche Digitale Währung? Wann war das ungefähr?

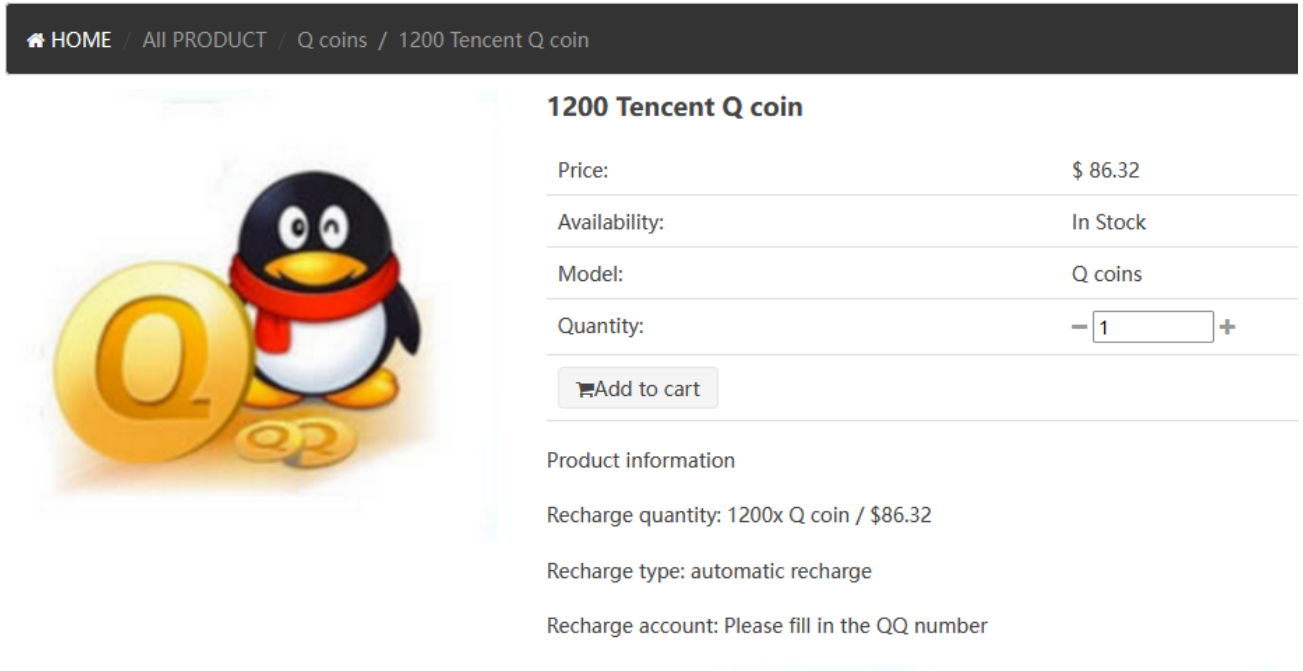
QQ Coin, die erste erfolgreiche digitale Währung

- Über OICQ (das spätere Tencent QQ) kann man, ab **2005 mit QQ Coins** seinen Avatar mit Kleider, Accessoires und Geschenken aufmotzen.

- Binnen ein Jahr entsteht, unerwartet, eine komplette Parallelwirtschaft. QQ Coin geht viral und wird fortan von zahlreichen Firmen als Zahlungsmittel angenommen. Die Unternehmen tauschen dann die QQ Coins bei spezialisierten privaten Wechselfirmen wieder in Staatswährung.

- In **2007** interveniert die Regierung, weil sie sich einer realen Bedrohung der Geldpolitik und Wirtschaft gegenüber stehen sieht. QQ Coins dürfen nur zum Kauf von virtuellen Gütern verwendet werden und nicht für einen höheren Wert in Yuan getauscht werden, als dafür gezahlt wurde. Das wird aber vielfältig durch Tricks umgangen, z. B. in dem ganze Accounts samt QQ Coins gehandelt werden.

- In **2010** verdiente Tencent, allein am Verkauf von QQ Avataren und Accessoires ca. 2 Mrd. US$, hatte über 600 Mio. aktive Nutzer und war das drittgrößte Internet-Unternehmen der Welt.



Quelle: Lehdonvirta & Castronova (2014), De Silva (2019)

Krypto-Financials (1. April 2021)

- Wie viele verschiedene gehandelte Kryptowährungen gab es?
  - 9.061 Kryptowährungen
- Wie hoch war der Gesamtmarktwert aller Kryptowährungen?
  - Ca. 1,6 Billionen €
- Welcher Wert wurde innerhalb von 24 Stunden weltweit mit Kryptowährungen gehandelt?
  - Ca. 146 Mrd. €
- Wie hoch war der Anteil von Bitcoin?
  - Ca. 942 Mrd. €
  - 58,2% Gewicht
  - BTC Preis, ca. 50.400 €

Die Marktkapitalisierung aller Unternehmen aus dem DAX belief sich zum 1. April 2021 auf rund 1,5 Billionen €.

Quelle: Deutsche Börse

10 wertvollsten Firmen vs. BTC	Markt Kap. in Mrd. €
1. Apple	1.948
2. Microsoft	1.726
3. Saudi Aramco	1.641
4. Amazon	1.481
5. Alphabet (Google)	1.331
6. Bitcoin	942
7. Meta (ehem. Facebook)	753
8. Tencent	669
9. Tesla	614
10. Alibaba Group	569
11. Berkshire Hathaway	540

Quelle: Statista, Stand 10.09.2021

Quelle: Coinmarketcap.com

Krypto-Financials (Stand: 16. Juni 2022, Δ zum 1. April 2021)

- Wie viele verschiedene gehandelte Kryptowährungen gab es?
  - 19.892 Kryptowährungen (+119,5%)
- Wie hoch war der Gesamtmarktwert aller Kryptowährungen?
  - Ca. 876 Milliarden € (-45,25%)
- Welcher Wert wurde innerhalb von 24 Stunden weltweit mit Kryptowährungen gehandelt?
  - Ca. 102,7 Mrd. € (-29,7%)
- Wie hoch war der Anteil von Bitcoin?
  - Ca. 389 Mrd. € (-58,7%)
  - 44,4% Gewicht
  - BTC Preis, ca. 20.216 € (-59,9%)

In den letzten 24 Stunden schwankte der Kurs um fast 12% von ca. 19.596 € bis 21.916 €

Im Gleichen Zeitraum:
DJIA 30 Industrial -7,5% *
EUROSTOXX 50 -10,5%*
* Vergleich der Schlusskurse vom 1. April 1, 2021 mit dem 15. Juni, 2022

Quelle: Finanzen.net

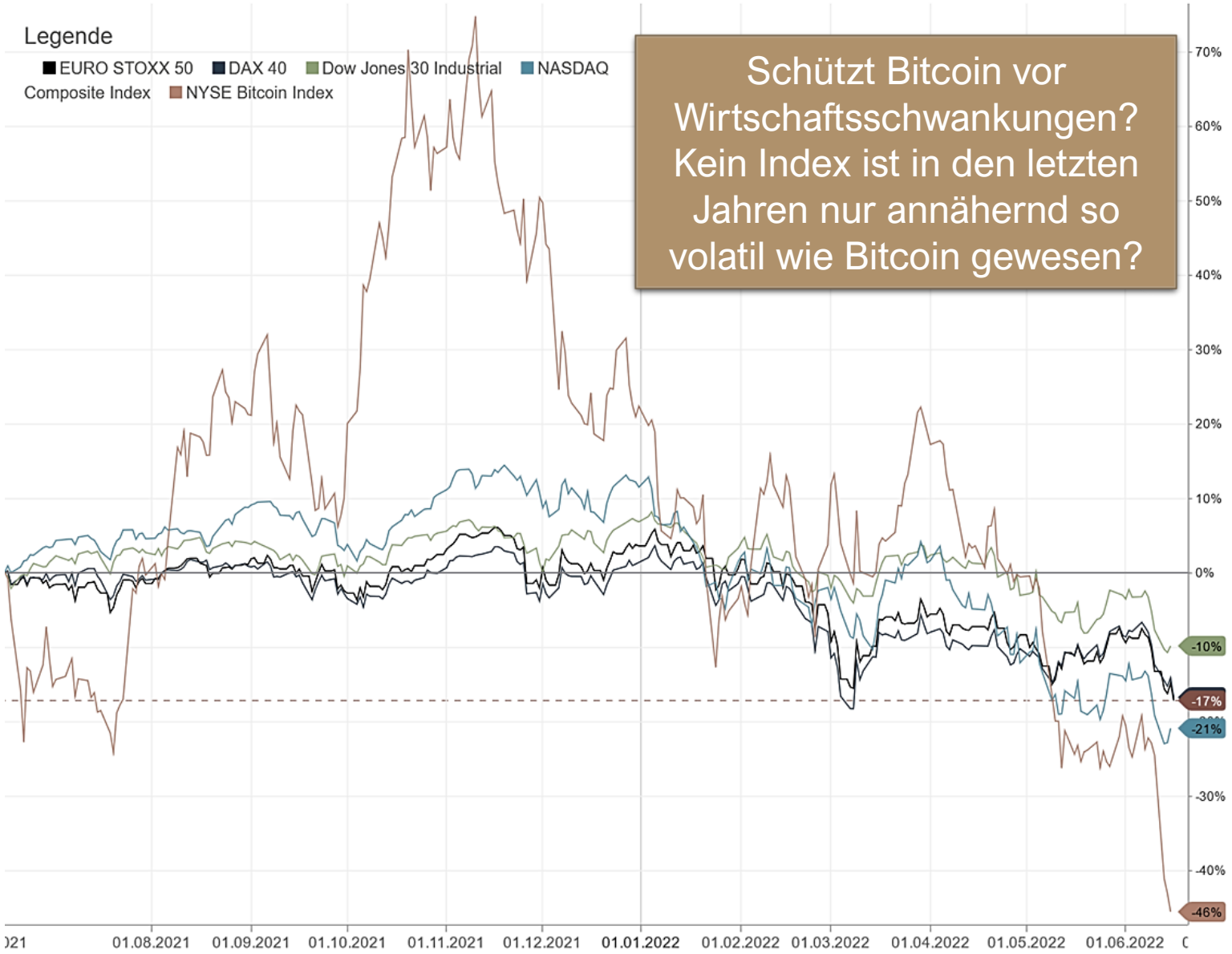
10 wertvollsten Firmen vs. BTC	Markt Kap. in Mrd. €
1. Saudi Aramco	2.185
2. Apple	2.107
3. Microsoft	1.810
4. Alphabet (Google)	1.394
5. Amazon	1.053
6. Tesla	696
7. Berkshire Hathaway	591
8. Tencent	451
9. Taiwan Semiconductor	445
10. Meta (ehem. Facebook)	441
:	:
14. Bitcoin	387

Krypto-Financials (Stand: 30. Juni 2022, Δ zum 1. April 2021)

- Wie viele verschiedene gehandelte Kryptowährungen gab es?
  - 20.070 Kryptowährungen (+121,5%)
- Wie hoch war der Gesamtmarktwert aller Kryptowährungen?
  - Ca. 817 Milliarden € (-48,9%)
- Welcher Wert wurde innerhalb von 24 Stunden weltweit mit Kryptowährungen gehandelt?
  - Ca. 61 Mrd. € (-58,2%)
- Wie hoch war der Anteil von Bitcoin?
  - Ca. 348 Mrd. € (-63%)
  - 44,4% Gewicht
  - BTC Preis, ca. 18.230 € (-63,8%)

Seit April 2021 werden täglich im Durchschnitt etwa 25 neue Kryptowährungen eingeführt. Wofür?

10 wertvollsten Firmen vs. BTC	Markt Kap. in Mrd. €
1. Saudi Aramco	2.180
2. Apple	2.160
3. Microsoft	1.865
4. Alphabet (Google)	1.412
5. Amazon	1.062
6. Tesla	681
7. Berkshire Hathaway	578
8. UnitedHealth	464
9. Johnson & Johnson	446
10. Tencent	437
:	:
16. Bitcoin	348



Vergleich der Wertentwicklung

Hochschule für angewandtes Management

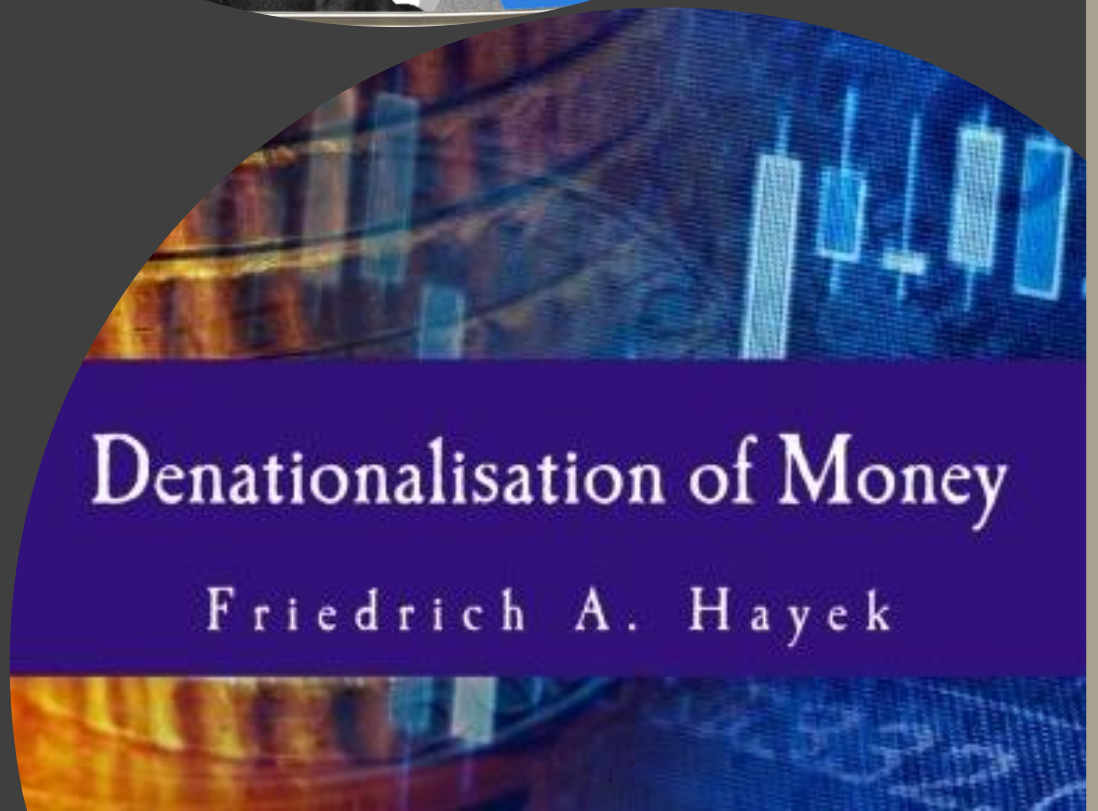
Übersicht

- Hintergründe
- Wann ist etwas eine Kryptowährung?
- Basics der Kryptographie in der Blockchain
- Blockchain an einem Beispiel
- Anwendungsmöglichkeiten der Blockchain
- Bitcoin, Strukturelle Betrachtung
- Soziokulturelles Phänomen
- Regulierung der Krypto-Asset Märkte
- Über die Natur von Bitcoin

HINTERGRÜNDE

Vor der 90ern

- Die Ursprung des Geldes liegt nicht bei Staaten oder Regierungen, obwohl wir es seit Jahrhunderten selbst nur als solches kennen und verstehen. Das erste Geld ist entstanden, weil Menschen mit Tauschhandel nicht mehr weiterkamen.
- Die moderne Idee eines privaten Geldes geht auf die Schriften des liberalen Ökonomen *Friedrich von Hayek* zurück.
- Seine Idee war, dass Geld ein Gut sei, das von Geschäftsbanken geschaffen und verwaltet werden sollte, die auf einem offenen Markt konkurrieren würden und nicht in der Hand von Zentralbanken oder Regierungen sein sollte.



Ende der 90er Jahre

- Als Pioniere des digitalen Geldes ist ihre Arbeit in der Öffentlichkeit weitgehend unbekannt, aber von Experten wirklich anerkannt.
- Erste ernsthafte Überlegungen und Versuche, Ende der 90er Jahre ein digitales Geld zu entwickeln, und Einführung von Elementen, die später zu Grundnahrungsmitteln von Kryptowährungen werden:
  - ✓ **Hashcash** von Adam Black (1997) entwickelt ein *Proof-of-Work-System* für E-Mail-Spam-Filter. Diese Art von Validierungssystem wird später für viele Kryptowährungen, einschließlich Bitcoin, implementiert.
  - ✓ **B-Money** von Wei Dai (1998). In seinem Artikel mit dem Titel "b-money, an anonymous, distributed electronic cash system" beschreibt er die grundlegenden Elemente, die heute Teil aller modernen Kryptowährungssysteme sind.
  - ✓ **Bit Gold** von Nick Szabo (1998). Ihm wird die Grundlagenforschung in sogenannten intelligenten (digitalen) Verträgen (*Smart Contracts*) zugeschrieben, die später die Grundlage für Kryptowährungen wie *Ethereum* bilden werden. Szabo entwickelte auch die Art von Architektur, bei der Netzwerkmitglieder ihre Rechenleistung zur Verfügung stellen, um kryptografische Probleme zu lösen. Genau die Art von System, das in vielen Kryptowährungen, einschließlich *Bitcoin*, implementiert ist.

Ende der 90er, Schlechtes Timing

- Ende der 90er Jahre steckt das Internet noch in den Kinderschuhen. Außerhalb des Silicon Valley wird die Vernetzung in der digitalen Welt nach wie vor stark von ISDN dominiert (Downloadraten von 14,4 kbit/s bis 128 kbit/s).
- Asymmetrische Kryptographie mit Hash-Algorithmen ist verfügbar, steckt aber noch in den Kinderschuhen. Zu diesem Zeitpunkt ist es noch schwer, sich die Rechenleistung die 10 Jahre später erreicht wird. Auch das Konzept des Quantencomputings ist immer noch Science-Fiction.
- Während Apple zu kämpfen hat und Steve Jobs gerade zurückgekommen ist, wird das erste iPhone erst in 10 Jahren auf den Markt kommen. So etwas wie eine mobile Internetnutzung gibt es nicht.
- Menschen surfen auf ihren PCs. Man kann zusehen, wie sich jede Grafik auf Webseiten ladet. Online-Shopping ist inexistent, es gibt keine wirklichen Anwendungsfälle für ein rein digitales Geld. Bei einer Top-Leitung in 1999 dauert es 5 Minuten um einen Song aus dem Internet herunterzuladen.
- Es wird Jahre dauern, bis Amazon, eBay, Facebook zu Standards werden. Die E-Economy ist noch eine Sache der Zukunft, von der Experten sprechen.
- Etwa zu dieser Zeit gründeten Peter Thiel und Elon Musk PayPal, das 2002 nach dem Verkauf an eBay abhob.

Satoshi Nakamoto

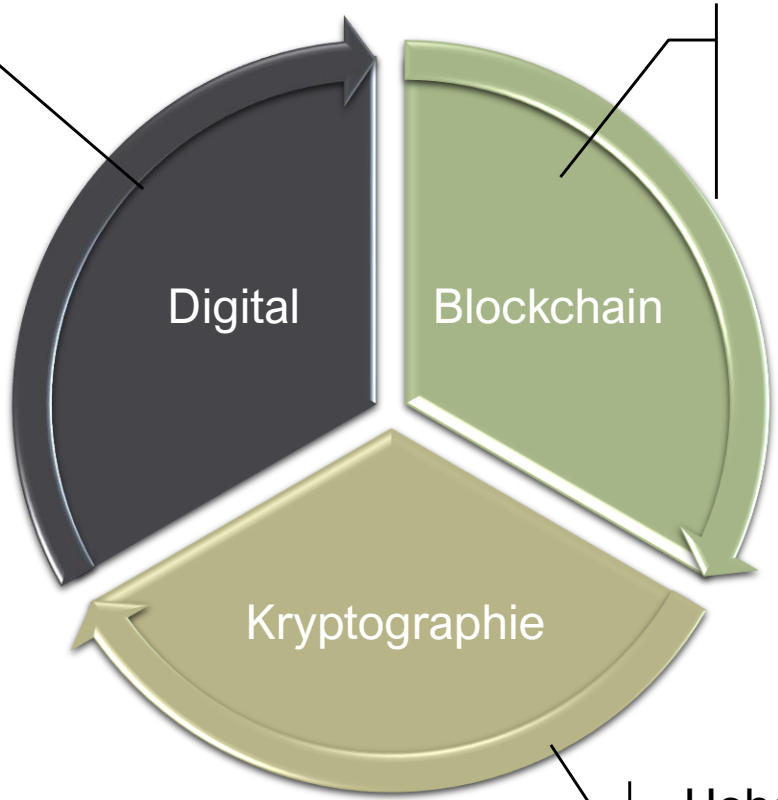
- Im Jahr 2008 veröffentlichte eine bis heute unbekannte Person oder Gruppe ein Whitepaper mit dem Titel *Bitcoin: A Peer-to-Peer Electronic Cash System*, das genau beschrieb, was Bitcoin werden sollte.
- Anfang 2009 wurde der Entstehungsblock (Block 0) der Bitcoin-Blockchain von derselben Person oder Gruppe initiiert.
- Nakamoto entwickelte Bitcoin nach seiner Einführung weiter und fügte beispielsweise die Blockgrößenbeschränkung von einem MB hinzu. Er verschwand spurlos Mitte 2010 nachdem er die Kontrolle an eine Gruppe vertrauenswürdiger Mitarbeiter und Bitcoin-Community-Mitglieder übergeben hatte.
- Die Identität der Person oder Gruppe ist bis heute unbekannt. Er wurde mit vielen Informatikern in Verbindung gebracht, darunter Szabo, Dai, Black und viele andere.
- Craig Wright, ein australischer Akademiker, der wegen Steuerhinterziehung unter die Lupe genommen wird, gibt vor Nakamoto zu sein, aber seine Behauptung wird von den meisten Experten als Betrug angesehen.
- Nakamoto besitzt angeblich zwischen 750.000 und 1,1 Mio. Bitcoins, was ihn theoretisch zu einem der 15 reichsten Menschen der Welt machen würde[1].

[1] Cuthbertson, A., (2021). Bitcoin creator Satoshi Nakamoto now 15th richest person in the world. The Independent, November 15, 2021. https://www.independent.co.uk/life-style/gadgets-and-tech/bitcoin-satoshi-nakamoto-wealth-net-worth-b1957878.html. [retrieved March 16th, 2022]

Wann ist etwas eine Kryptowährung?

Wann ist etwas eine Kryptowährung?

Schnell und einfach skalierbar

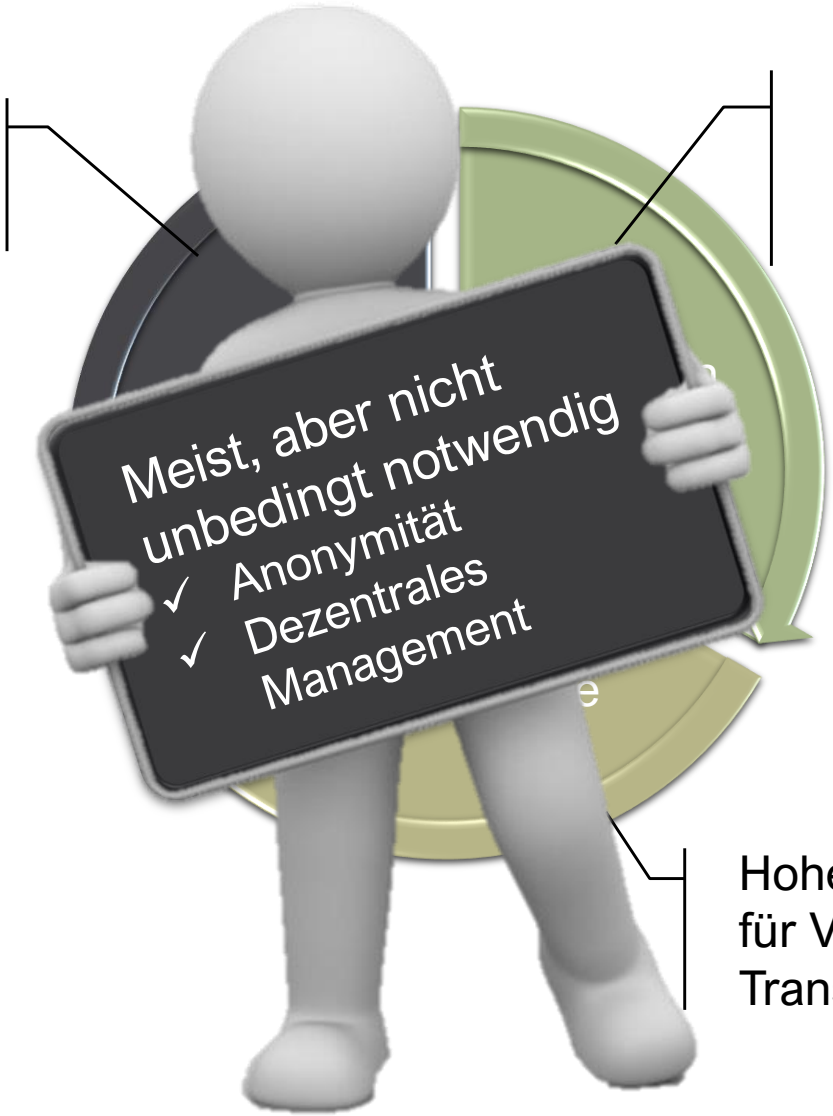


Datenaufzeichnung und Managementsystem

Hohe Sicherheit für Verwahrung & Transaktionen

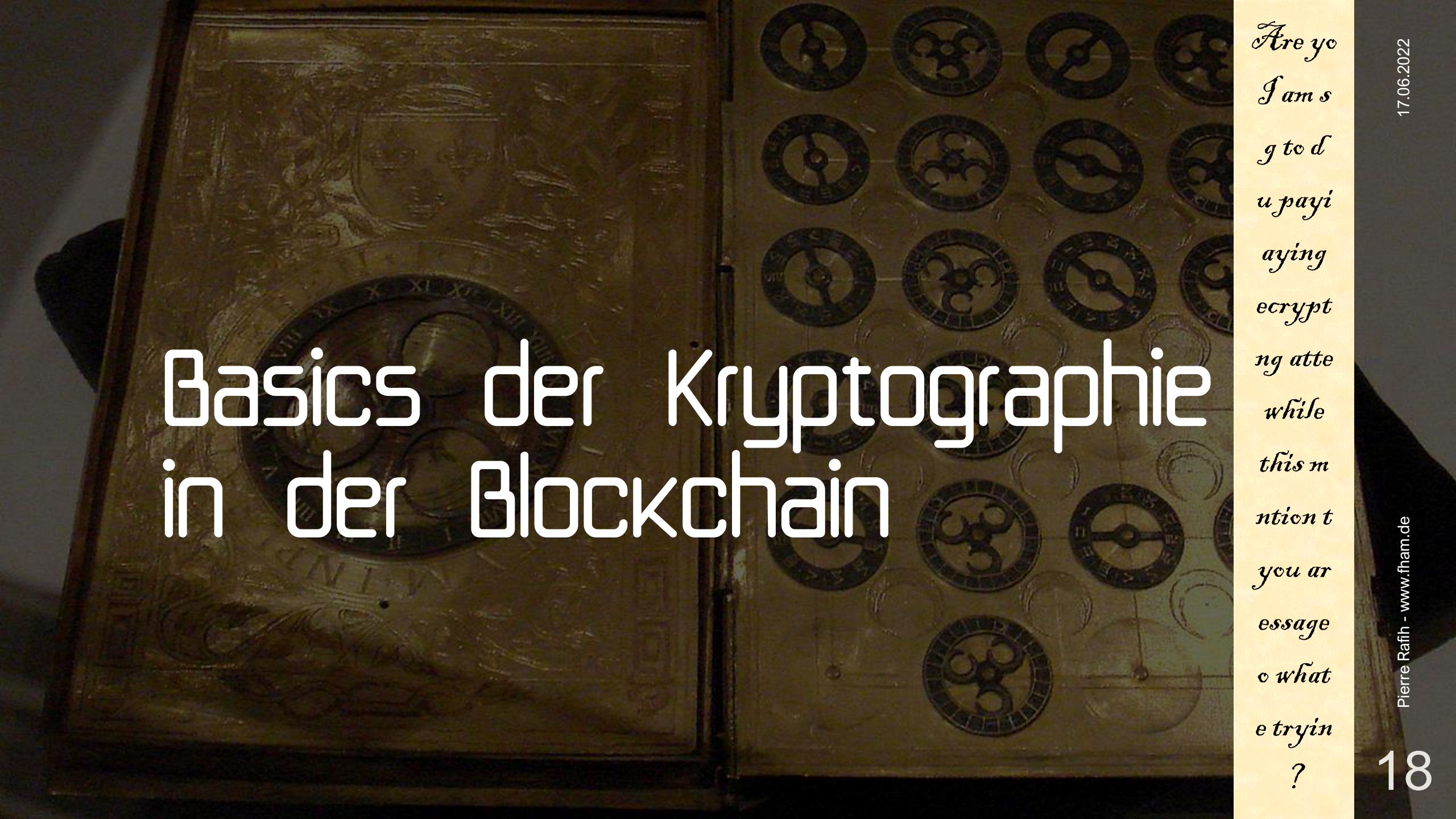
Wann ist etwas eine Kryptowährung?

Schnell und einfach skalierbar



Datenaufzeichnung und Managementsystem

Hohe Sicherheit für Verwahrung & Transaktionen



Basics der Kryptographie in der Blockchain

Are yo
I am s
g to d
u payi
aying
ecrypt
ng atte
while
this m
ntion t
you ar
essage
o what
e tryin
?

Are yo I am s g to d u payi aying ecrypt ng atte while this m ntion t you ar essag e o what e tryin ?

Altgriechische Skytale

Deutsche Enigma-Maschine

Kurzer historischer Hintergrund

- Die Kryptographie reicht bis in die Antike zurück. Seine Entwicklung wird stark vom Militär und der Diplomatie vorangetrieben, um Spionage- und Spionageaktivitäten abzuwehren.
- In der Vergangenheit waren kryptografische Systeme symmetrisch, was bedeutet, dass derselbe Schlüssel / Code zum Verschlüsseln und Entschlüsseln von Informationen verwendet wird.
- Die moderne Kryptographie profitierte von den Fortschritten in Mathematik, Technologie und Digitalisierung. Verwurzelt in einem Artikel von *Withfield Diffie* und *Martin Hellman* aus dem Jahr 1976, verwendet die moderne Kryptographie asymmetrische Verschlüsselung, die öffentliche und private Schlüssel kombiniert.
- Asymmetrische Kryptographie ist das, worauf wir uns im Zusammenhang mit Blockchains und Kryptowährungen beziehen.

Moderne asymmetrische Kryptographie

- In einer Arbeit von 1976 *führten Whitfield Diffie* und *Martin Hellman* erstmals den Begriff der asymmetrischen Schlüssel ein.

- Das System arbeitet mit öffentlichen und privaten Schlüsseln.
  - ✓ Öffentlichen Schlüssel ermöglichen es, die Teilnehmer der Transaktion zu identifizieren, sie werden oft als "Adressen" bezeichnet.
  - ✓ Nur wer den privaten Schlüssel der Adresse hat, kann auf dessen Inhalt zugreifen.

- Ein Beispiel für eine einfache Verschlüsselungstechnik basiert auf Primzahlen.
  - ✓ Privater Schlüssel: 2 Primzahlen
  - ✓ Öffentlicher Schlüssel/Adresse: Produkt der beiden Primzahlen

Grundlagen der asymmetrischen Kryptographie

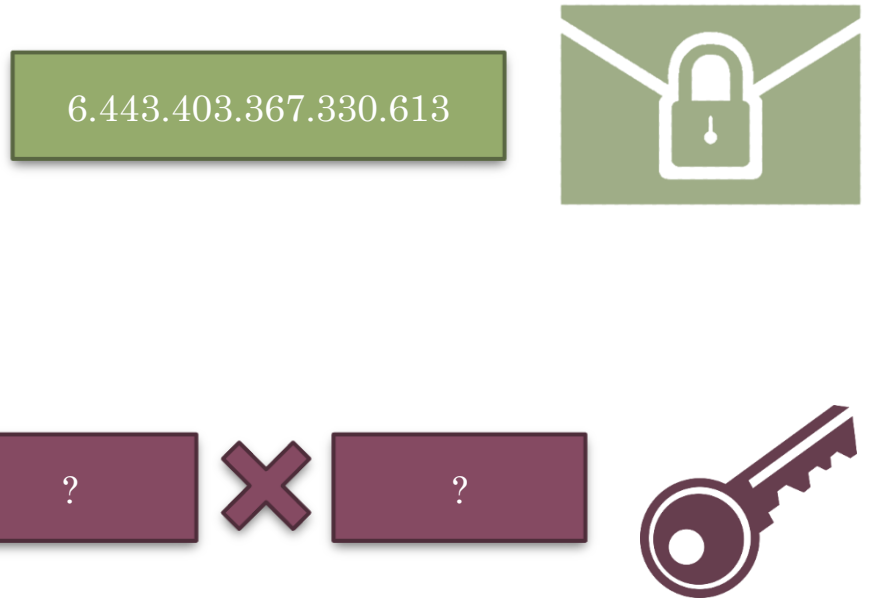
- Betrachten wir den folgenden **privaten Schlüssel**, der aus zwei Primzahlen besteht. Wenn man die kennt, lässt sich der **öffentlichen Schlüssel**, der aus dem Produkt der beiden besteht, leicht ermitteln.

3,502,273 × 7,894,573

26,648,949,864,429

Grundlagen der asymmetrischen Kryptographie

- Können Sie anhand des **öffentlichen Schlüssels** den **privaten Schlüssel** ermitteln, der aus zwei Primzahlen besteht?

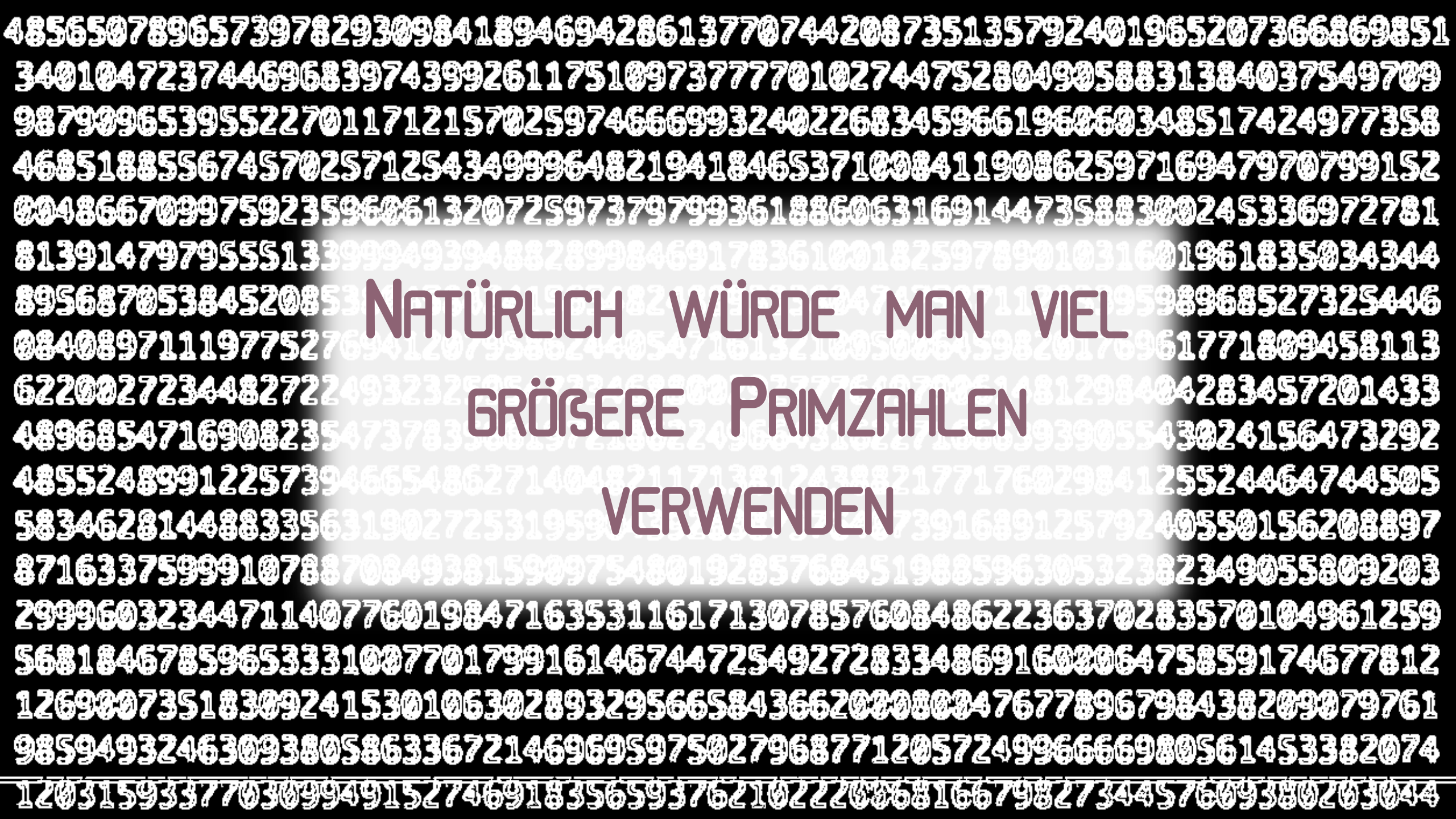


Grundlagen der asymmetrischen Kryptographie

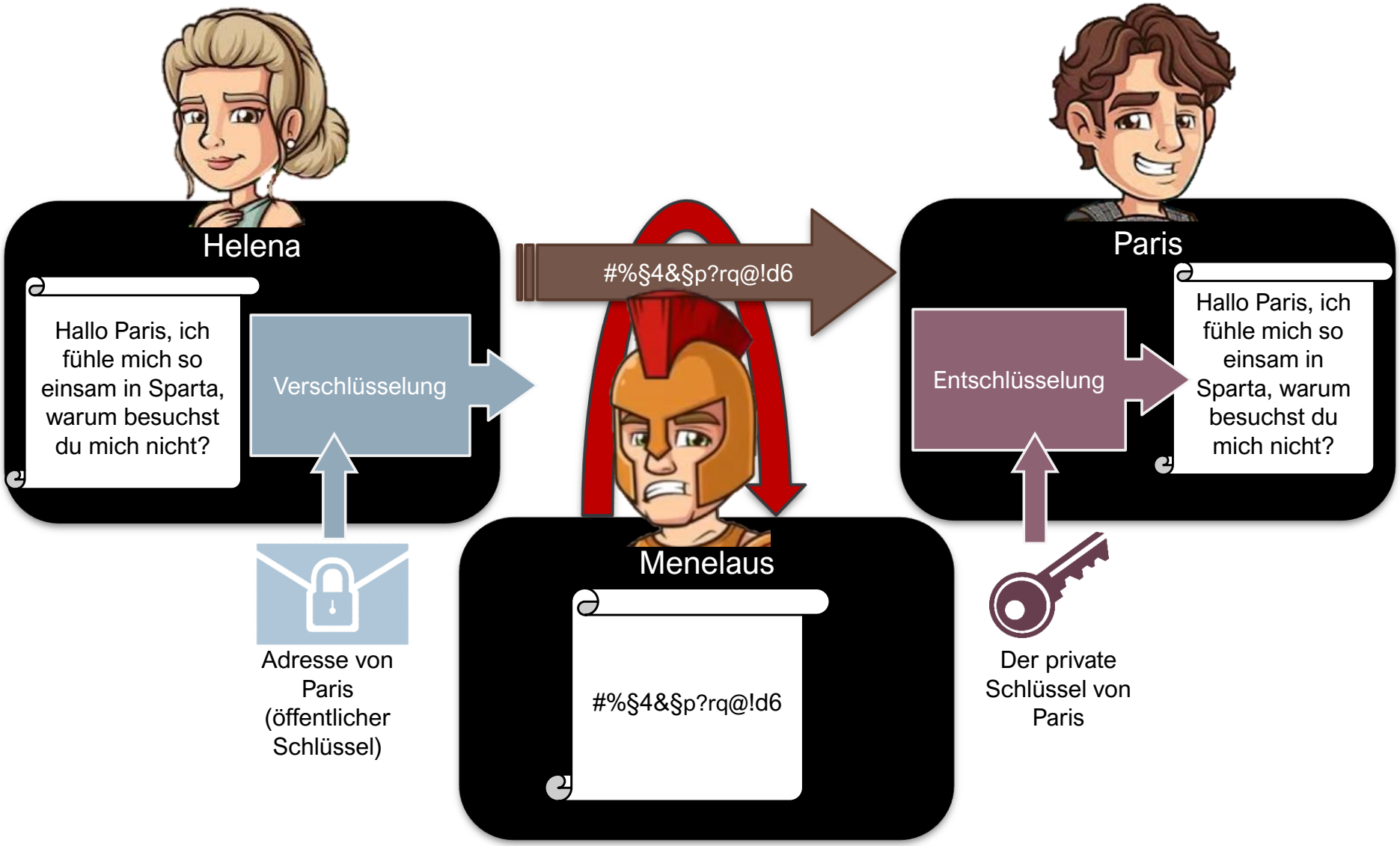
- Können Sie anhand des **öffentlichen Schlüssels** den **privaten Schlüssel** ermitteln, der aus zwei Primzahlen besteht?

6.443.403.367.330.613

6.523.939 × 987.655.367


Natürlich würde man viel
größere Primzahlen
verwenden

Asymmetrische Nachrichtenverschlüsselung



Verschlüsselungssystem für Kryptowährungen

- Kryptowährungen verwenden Hash-Funktionen, die eine unendliche Anzahl von asymmetrischen Schlüsseln generieren können.
- Die sog. Secured Hash Algorithmen (SHA) wurden vom National Institute of Standards and Technology (NIST) entwickelt und von der NSA entworfen. Die Patente wurden dann als gebührenfreie Lizenzen zur Verfügung gestellt.
- Es gibt mehrere Iterationen oder Unterkategorien von SHA. Viele Kryptowährungen, einschließlich Bitcoin, verwenden die SHA-256 (SHA-2-Familie), die erstmals 2001 entwickelt wurde. Es ist derzeit auch der Standard, der von der US-Regierung für ihre eigenen Behörden unterstützt wird.
- Die neueste Entwicklung ist die SHA-3-Generation, die 2012 entwickelt wurde. SHA-3 „sollte“ in der Lage sein Quantencomputern zu widerstehen, aber da es noch keine zum testen gibt…

Blockchain an einem Beispiel

DLT – Distributed Ledger Technology

- Ein digitales Netzwerk, in dem jedes Mitglied eine identische Kopie des gesamten Registers aller Positionen und Transaktionen hat.
- Änderungen innerhalb des Netzwerks werden erfasst, nachdem sie mit einem Validierungssystem geprüft und genehmigt wurden.
- Dieses Validierungssystem basiert entweder auf einem Konsens (Mehrheitsbeschluss) oder auf die Prüfung durch eine Kontrollgruppe, z. B. der Mitglieder des Netzwerks mit den höchsten Einsätzen.
- Jedes Mal, wenn eine Änderung im Netzwerk auftritt (eine Transaktion, ein neues Mitglied), wird das Register jedes Netzwerkmitglieds gleichzeitig aktualisiert.
- Das Netzwerk vertraut niemandem, alles steht allen offen. Mitglied A weiß sowohl wann sich die Mitglieder B und C an einer Transaktion beteiligen, als auch das Volumen der Transaktion.
- Ziel dieser Mechanik ist es, sogenanntes **Double Spending** zu verhindern. Dies funktioniert verlässlich in Netzwerken die keine hohen Transaktionsdichte aufweisen.

Blockchain

Blockchain

- Änderungen im Netzwerk werden nicht sofort aktualisiert. Transaktionsanforderungen werden in "Blöcken" gesammelt. Alle Transaktionen in einem Block werden gleichzeitig geprüft und validiert.
- Transaktionen werden Block für Block zur Registrierung hinzugefügt, daher der Name Blockchain.
- Um Manipulationen zu vermeiden, ist jeder Block auch mit einem kryptografischen Schlüssel signiert, der verhindert, dass gefälschte Blöcke zur Kette hinzugefügt werden.
- Dies funktioniert auch in Netzwerken mit einer sehr hohen Transaktionsdichte besser als eine einfache DLT, um Doppelausgaben zu verhindern.

Die Bitcoin-Blockchain

Bitcoin

- Bitcoin hat eine sogenannte offene Blockchain, was bedeutet, dass jeder dem Netzwerk jederzeit ohne Bedingung beitreten kann.
- Um Änderungen in der Blockchain zu validieren, verwendet Bitcoin eine sogenannte "Proof-of-Work" Mechanik, eine Art Mehrheitsabstimmung.
- Der Bitcoin-Algorithmus ist so programmiert, dass ein Block eine Größe von nicht mehr als 1 MB (Blockgröße) hat und etwa alle 10 Minuten ein neuer Block zur Kette hinzugefügt werden soll (Blockgenerierungszeit).

Double Spending

Anna

Register
Anna: 1 BTC Betty: 0 BTC Carlo: 0 BTC

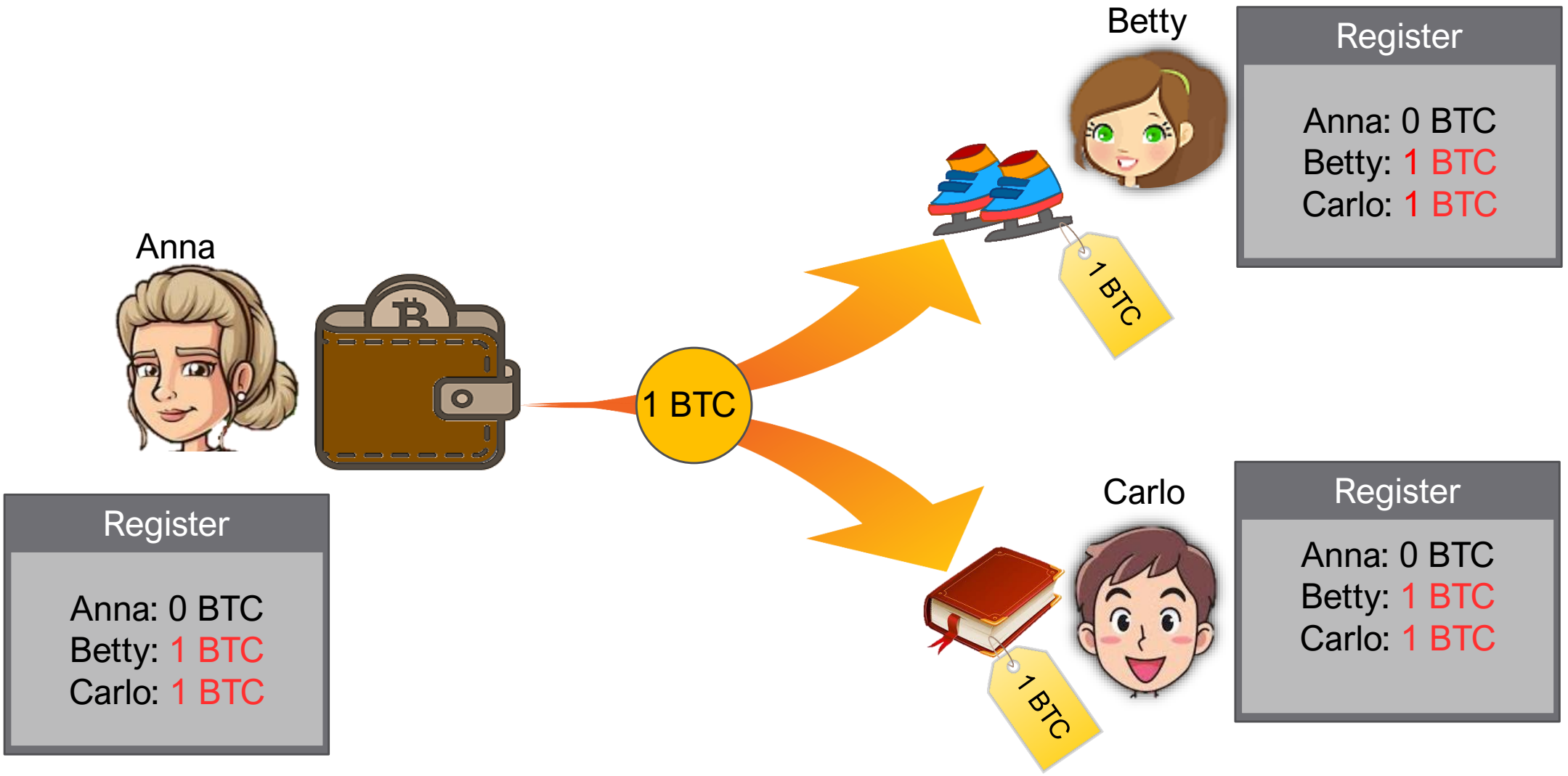
Betty

Register
Anna: 1 BTC Betty: 0 BTC Carlo: 0 BTC

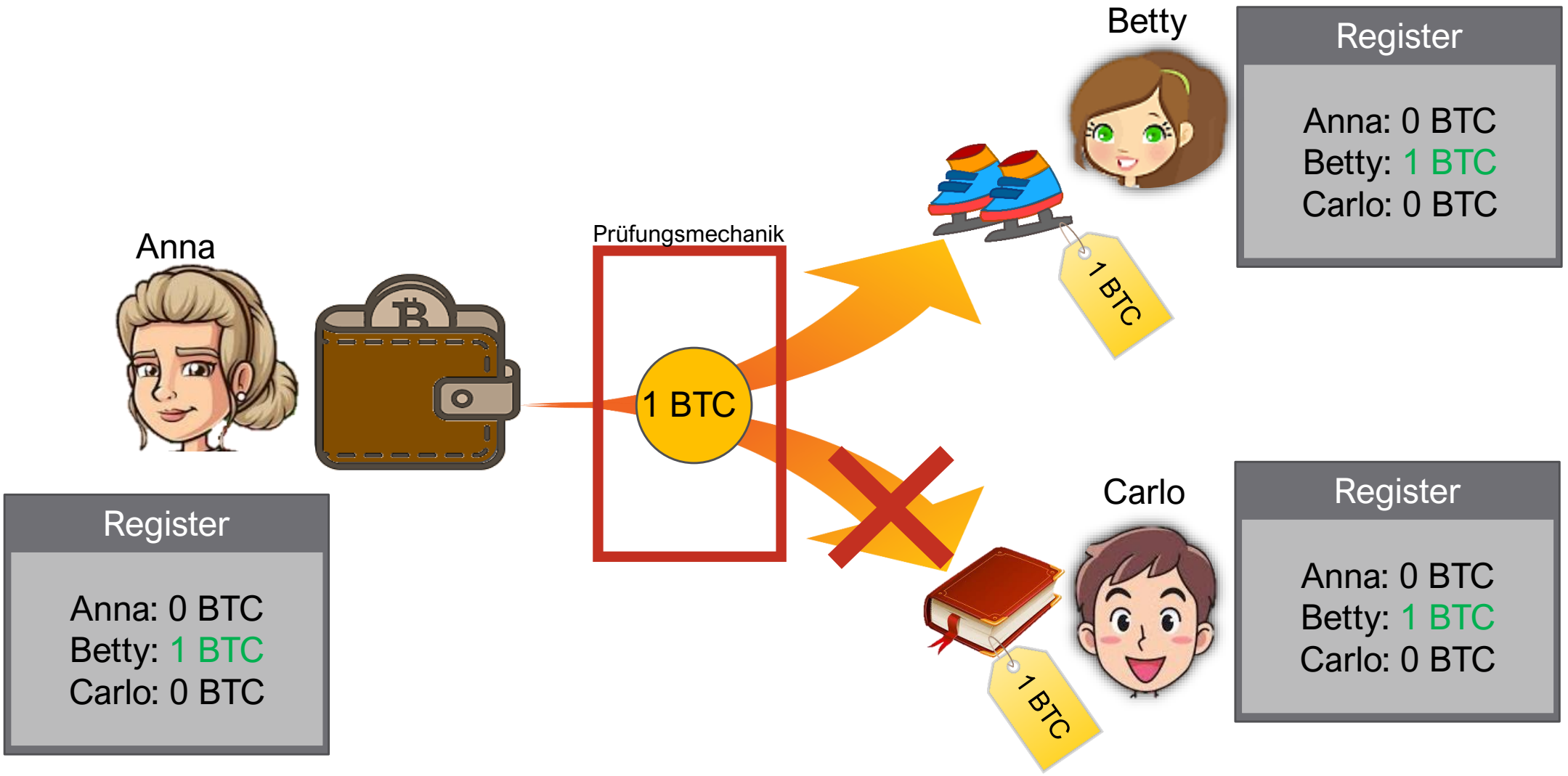
Carlo

Register
Anna: 1 BTC Betty: 0 BTC Carlo: 0 BTC

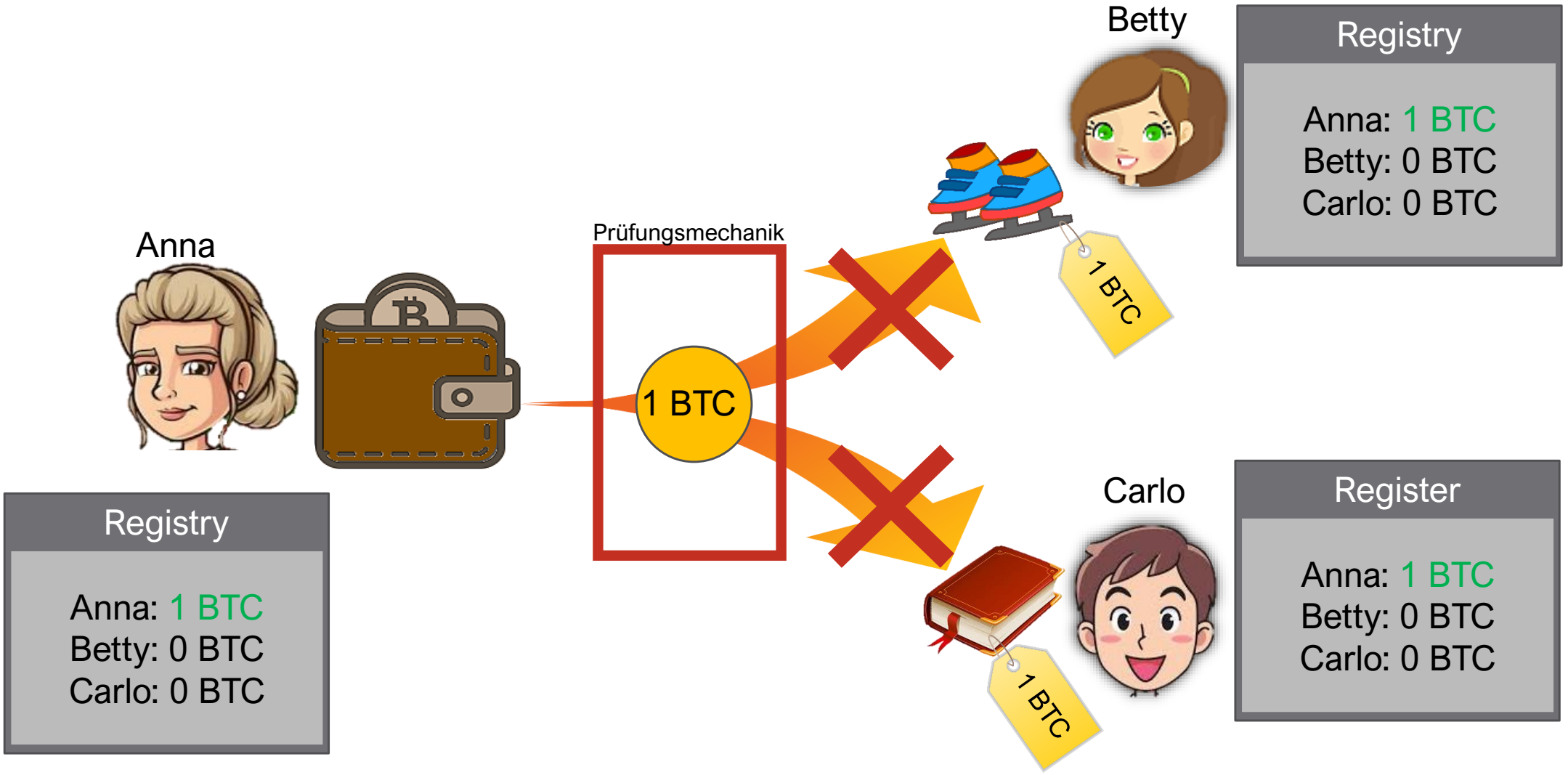
Double Spending



Double Spending



Double Spending



Die Bitcoin Blockchain – Begriffe

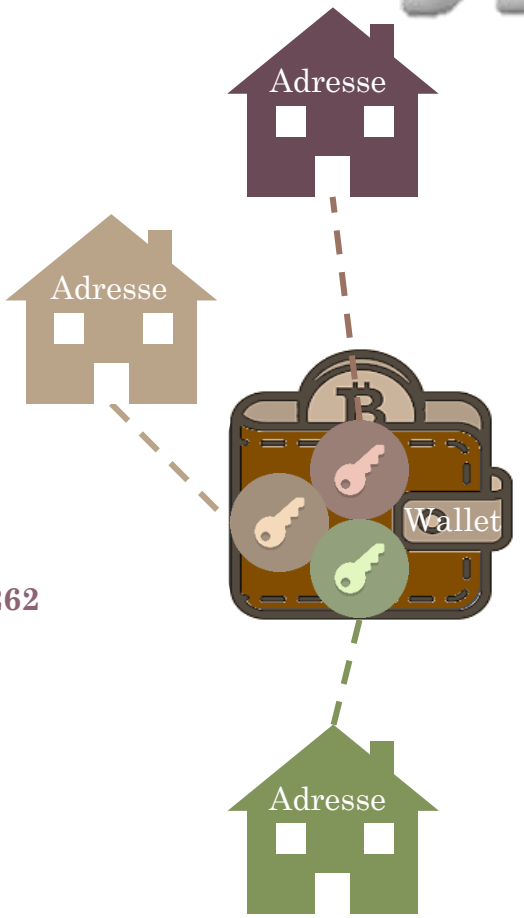
- Adressen
  - Der virtuelle Ort, an dem Bitcoins gespeichert werden. Die Adresse ist öffentlich bekannt und sichtbar, bestehend aus 26 bis 35 alphanumerischen Zeichen

    1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2

- Privatschlüssel
  - Nur damit kann man auf die Bitcoins einer Adresse zugreifen. In Bitcoin, eine 256-Bit-Zahl, alphanumerisch von 64 Zeichen.

    E9873D79C6D87DC0FB6A5778633389F4453213303DA61F20BD67FC233AA33262

- Wallets (Brieftaschen)
  - Sammlung der Privatschlüssel aller Adressen des Eigentümers.



Die Bitcoin Blockchain – Begriffe

Miner (Schürfer)

Stellen dem gesamten System eigene Rechenleistung zur Verfügung, um Blöcke zu entschlüsseln.

Hashrate

Maß für die Rechenleistung des globalen Bitcoin-Netzwerks. Ein Wert von 221 EH/s (30.06.2022) bedeutet, dass 222 $x10^{18}$ (222 Milliarden Milliarden) Berechnungen pro Sekunde durchgeführt werden.

Difficulty (Komplexität/Schwierigkeit)

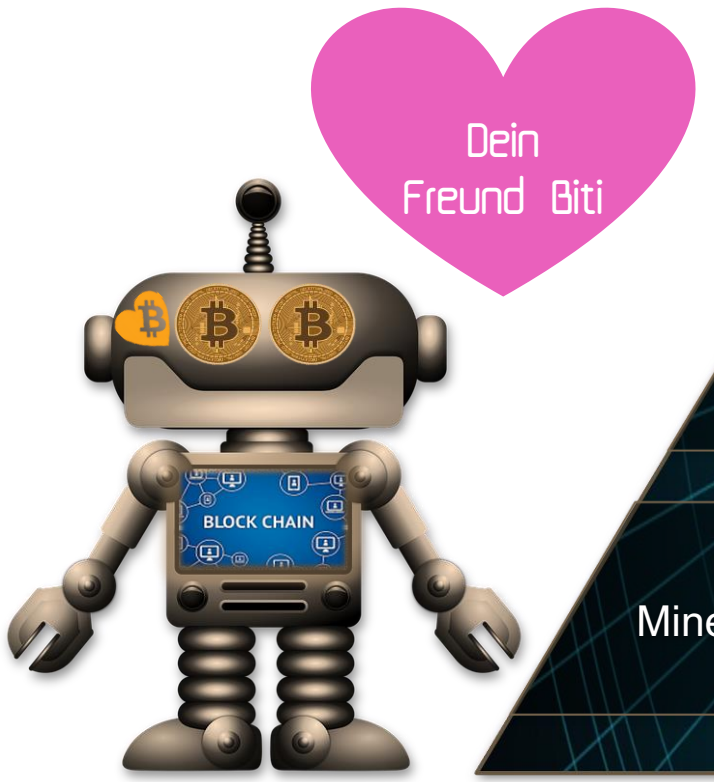
Stellt die Komplexität der Verschlüsselung dar, die von Miner gelöst wird. Passt sich der Hashrate alle 2016-Blockiterationen an (ca. 2 Wochen). Ziel ist es, die Blockgenerierungszeit bei 10 Minuten zu halten.

Die Bitcoin Blockchain – Begriffe

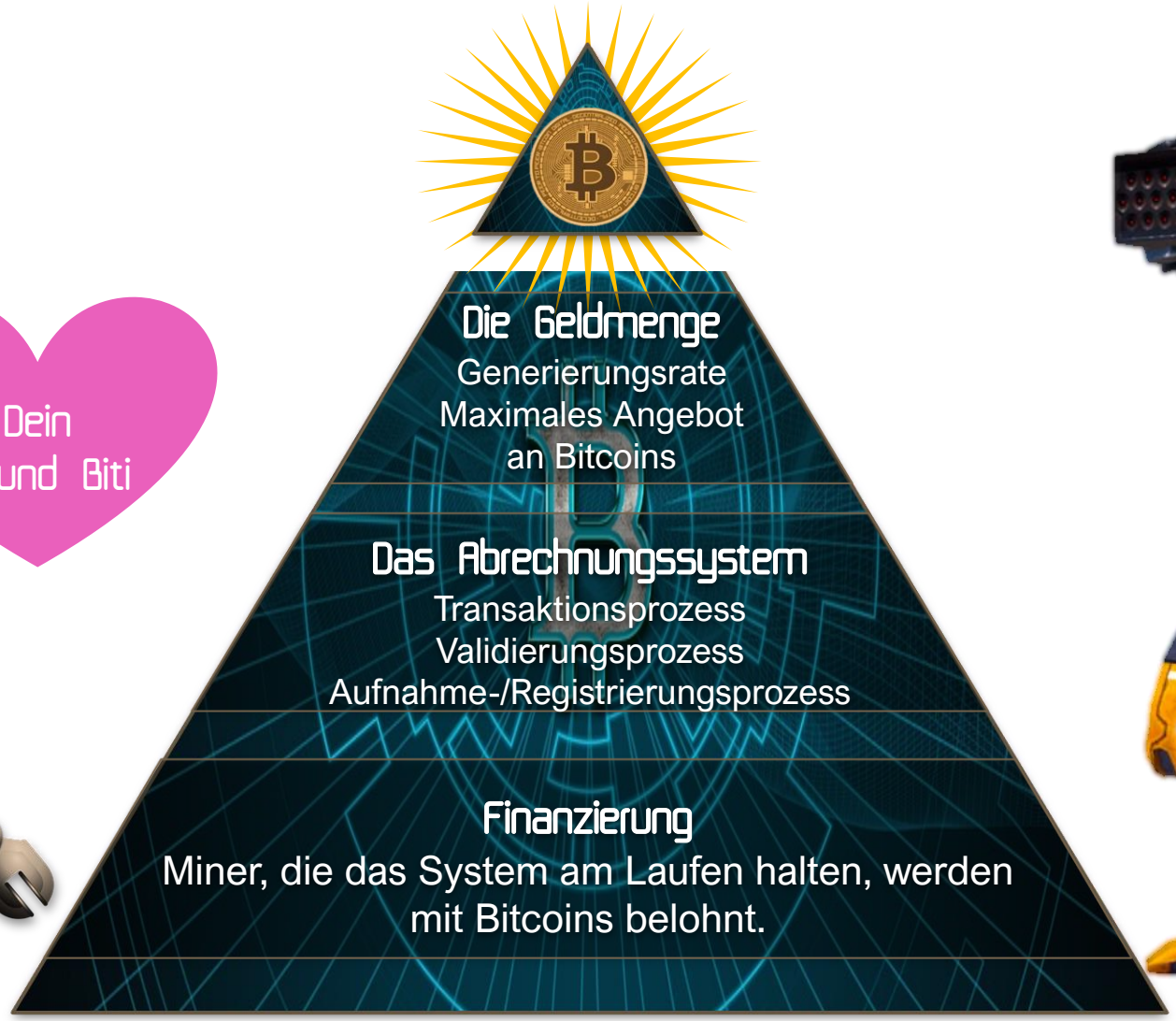
Wie kann man sich die Difficulty vorstellen, mit der die Miner konfrontiert sind?

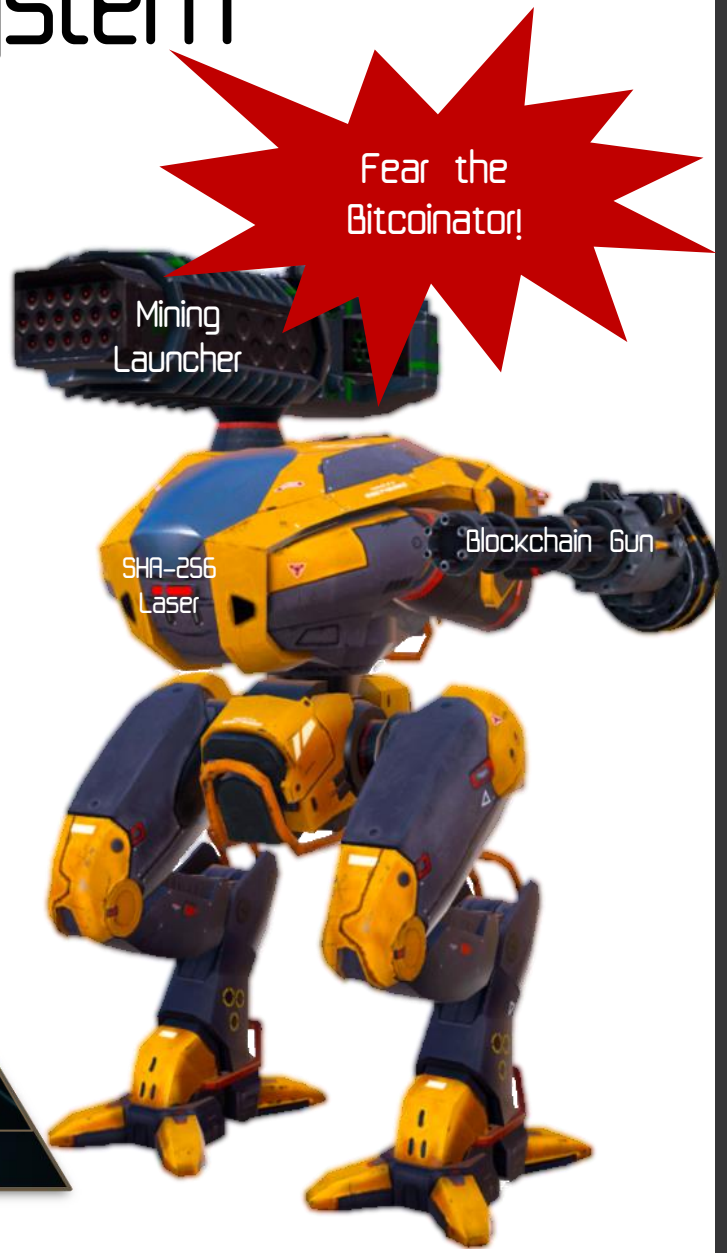
Man könnte sich einen Block wie einen Koffer vorstellen, der durch ein Zahlenschloss verriegelt wird. Die Difficulty wäre die Komplexität dieses Zahlenschlosses, gemessen an der Zahl der Zahnräder. Je mehr Zahnräder das Schloss hat, umso schwerer ist es, den Koffer zu öffnen, wenn man die Kombination nicht kennt. Diese müssen die Miner herausfinden, indem sie zufällige Kombinationen ausprobieren. Je mehr Rechenleistung sie haben, umso schneller sie dabei sind (Hashrate), desto höher ist die Chance, dass sie Die Ersten sind, die das Schloss knacken.

Autonomes, selbstregulierendes System

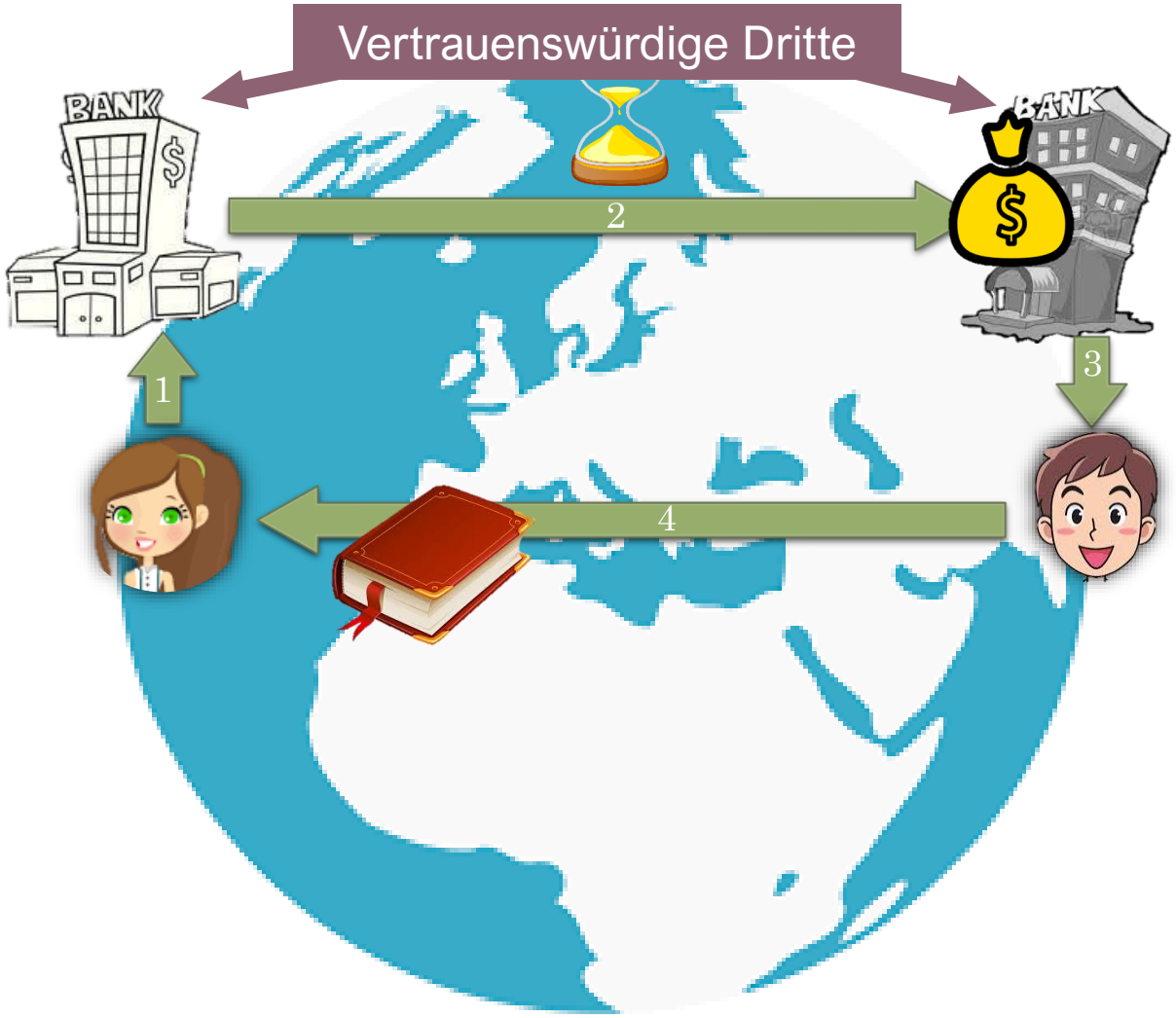


Dein
Freund Biti

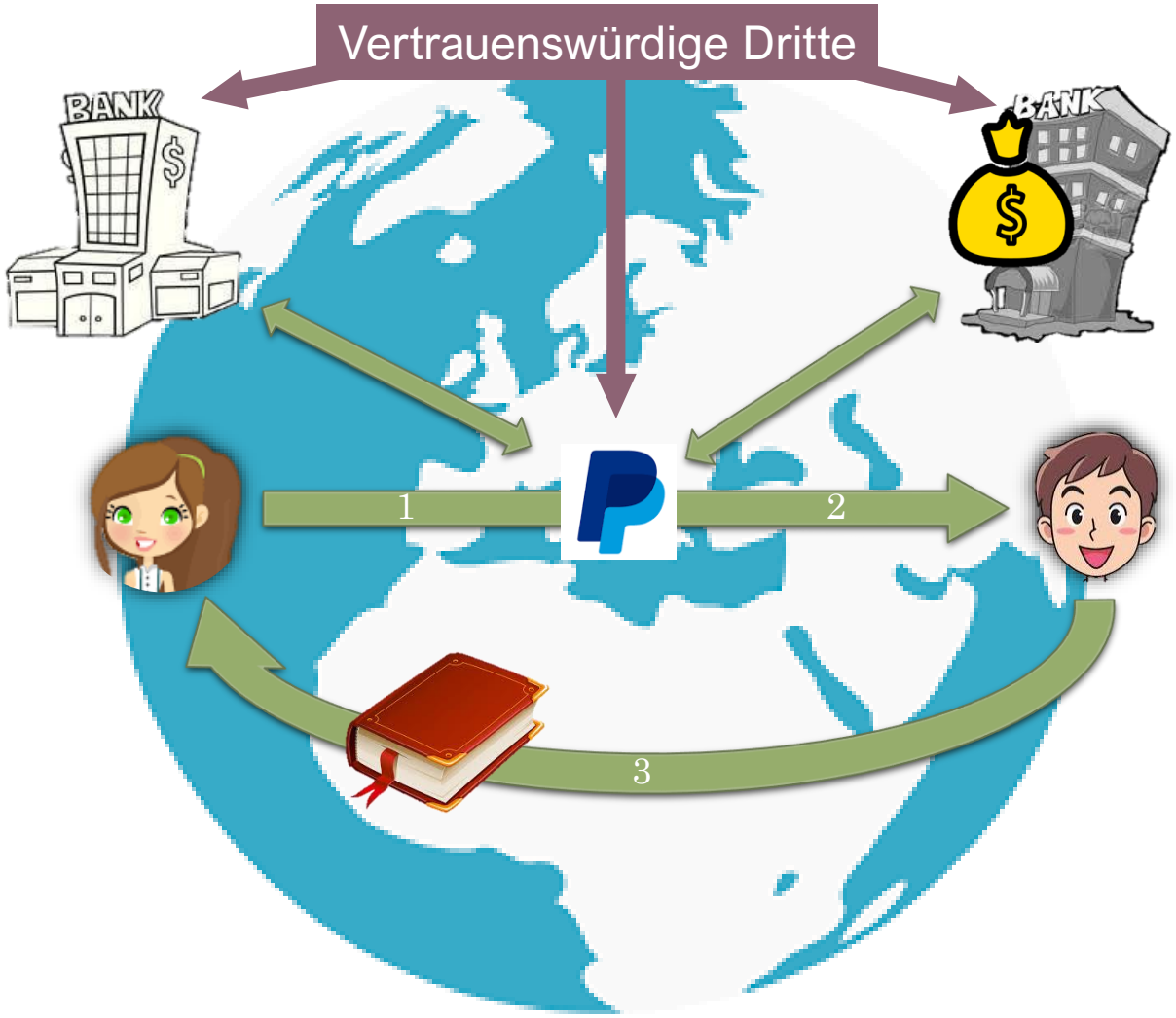




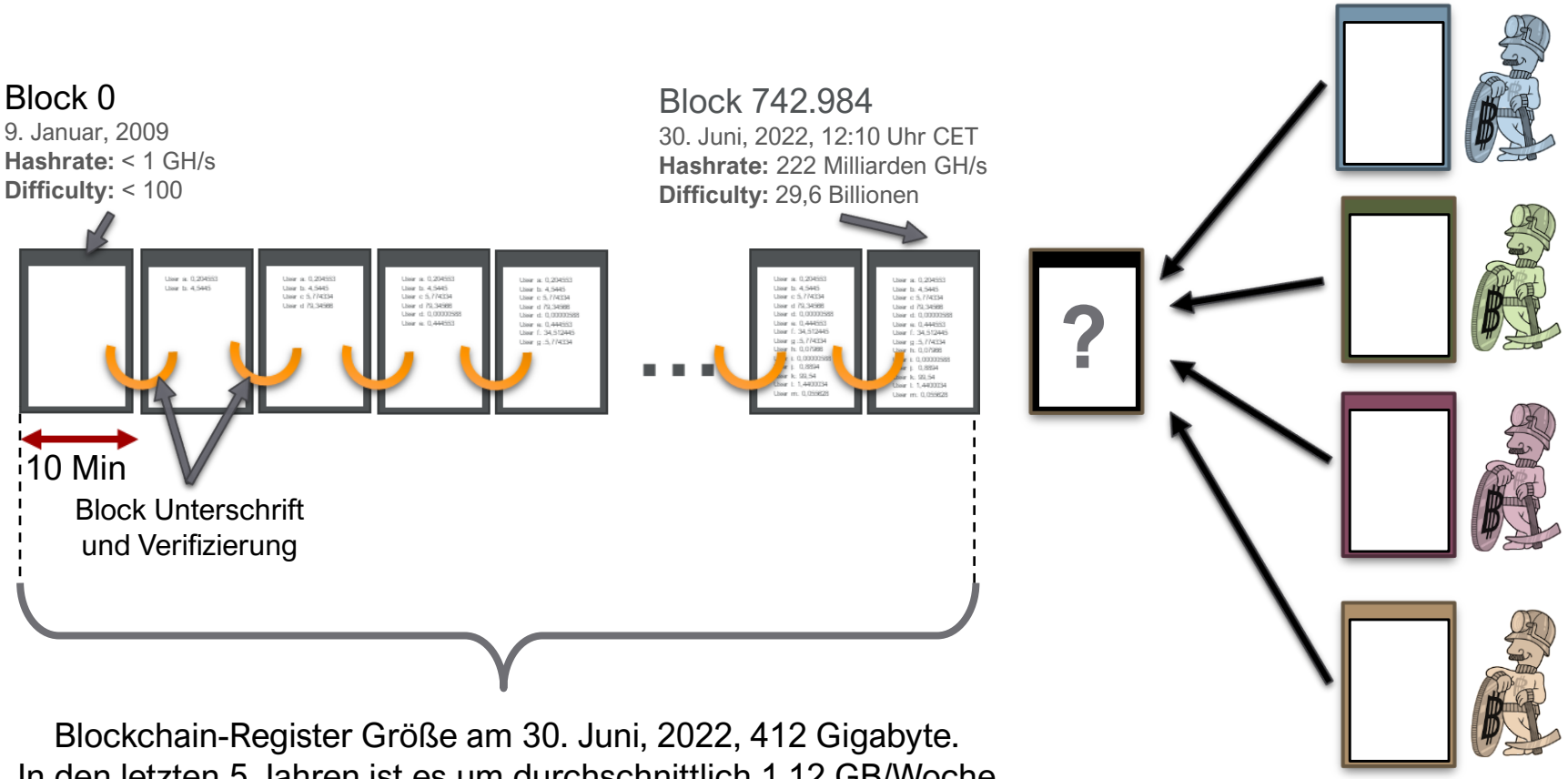
Traditionelles bankbasiertes Bezahlen



Traditionelles bankbasiertes Bezahlen



Die Bitcoin-Blockchain



Blockchain-Register Größe am 30. Juni, 2022, 412 Gigabyte.
In den letzten 5 Jahren ist es um durchschnittlich 1,12 GB/Woche gewachsen. Zu diesem Rhythmus braucht man in weniger als 10 Jahren allein für das Register schon über 1 TB Speicher.

Die Bitcoin-Blockchain

Das bedeutet, dass alle Miner im Bitcoin-Netzwerk jede Sekunde 222 Milliarden Milliarden verschiedene Kombinationen ausprobieren um das Schloss des Blocks zu knacken

Wieso dauert es dann 10 Minuten bei soviel Rechenleistung?

Hashrate: 222 Milliarden GH/s
Difficulty: 29,6 Billionen

Das Schloss dieses Blocks besteht aus einer Kombination, die 29.570.168.636.357 Zahnräder hat, wobei jedes Zahnrad 16 verschiedene Positionen hat: 0 1 2 3 4 5 6 7 8 9 A B C D E oder F.
Es gibt also insgesamt $16^{29.570.168.636.357}$ Kombinationen!
Im Vergleich, wenn man das gesamte bekannte Universum mit Sandkörner füllen würde, bräuchte man „nur“ 10^{90} davon.

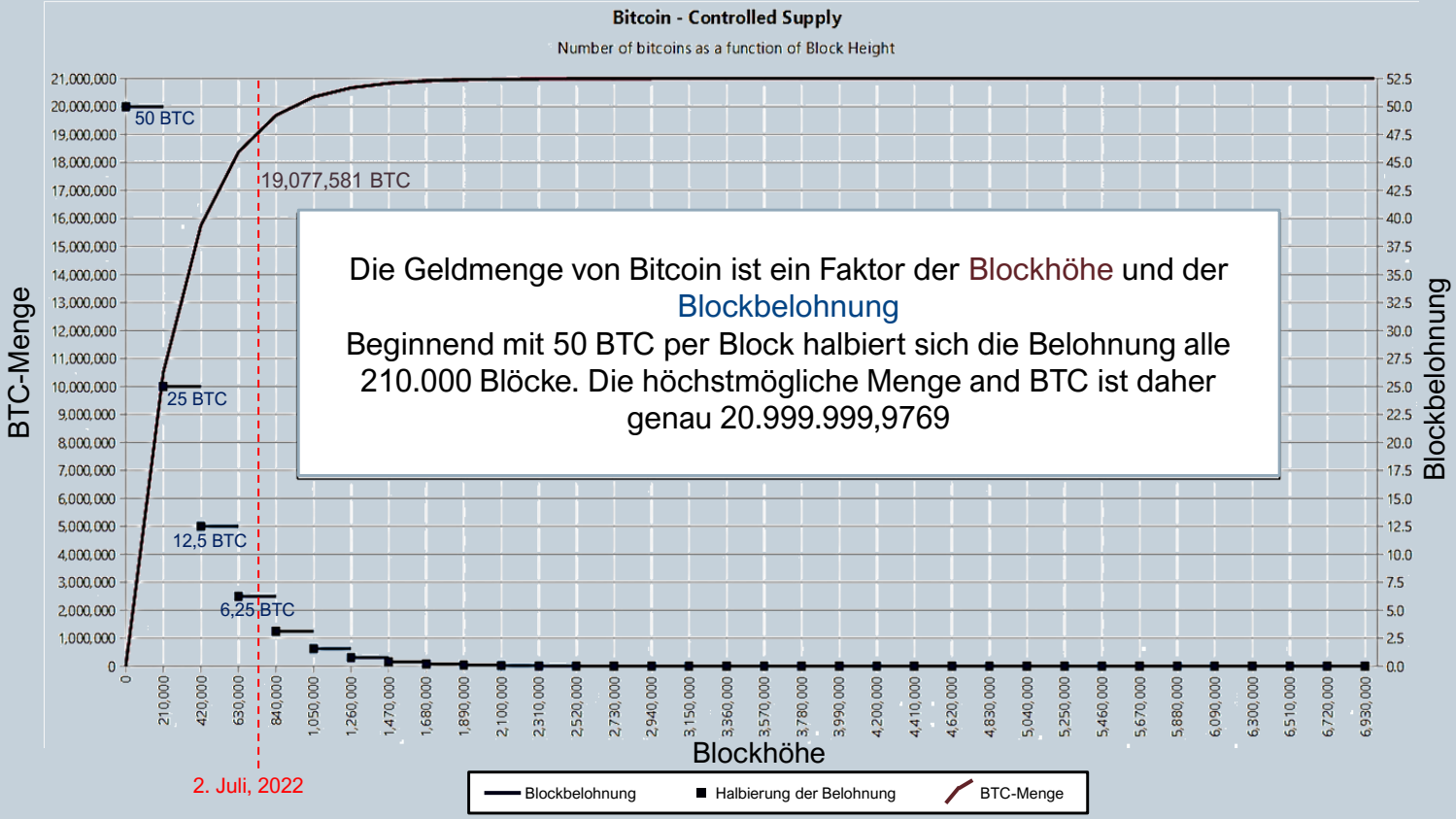
Die Bitcoin-Blockchain

Das bedeutet, dass alle Miner im Bitcoin-
Milliarden Milliarden verschiedene Kom
Schloss des Block

Wieso dauert es dann 10 Minuten bei soviel Rechenleistung?

Aber warum ist die Difficulty überhaupt so hoch?

Das Schloss dieses Blocks besteht aus einer Kombination, die 29.570.168.636.357 Zahnräder hat, wobei jedes Zahnrad 16 verschiedene Positionen hat: 0 1 2 3 4 5 6 7 8 9 A B C D E oder F.
Es gibt also insgesamt $16^{29.570.168.636.357}$ Kombinationen!
Im Vergleich, wenn man das gesamte bekannte Universum mit Sandkörner füllen würde, bräuchte man „nur“ 10^{90} davon.



Die Geldmenge von Bitcoin ist ein Faktor der Blockhöhe und der Blockbelohnung

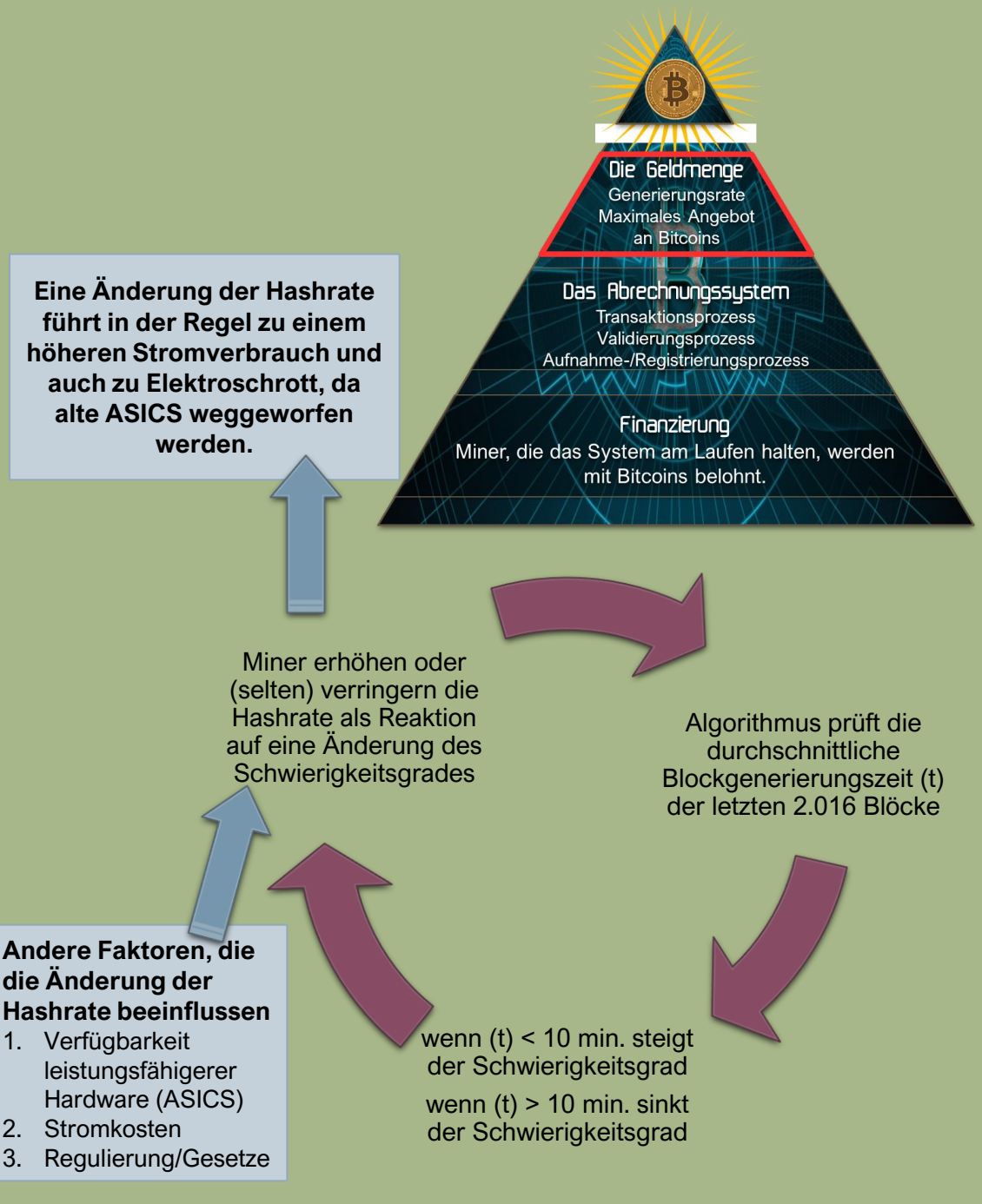
Beginnend mit 50 BTC per Block halbiert sich die Belohnung alle 210.000 Blöcke. Die höchstmögliche Menge and BTC ist daher genau 20.999.999,9769

Zusammenhang zwischen Difficulty und Hashrate

- Der Bitcoin-Algorithmus hat eine integrierte Funktion als Teil seiner Mechanik, um das Angebot an neuen Münzen zu steuern.
- Jedes Mal, wenn ein neuer Block validiert wird, werden neue Bitcoins erstellt. Das ist die Geldpolitik im Bitcoin-Netzwerk. Die Anzahl der erzeugten Bitcoins wird durch die Blockhöhe (Blocknummer) bestimmt. Alle 210.000 Blöcke halbiert sich diese Zuführung.
- Davon ausgehend, dass der Algorithmus alle 10 Minuten einen neuen Block generieren möchte, entsprechen 210.000 Blöcke fast perfekt 4 Jahren. Wir können also ziemlich genau abschätzen, wann das nächste Mal die Zuführung halbiert wird.
- Bei den ersten 210.000 Blöcke wurden 50 neue Bitcoins dem System zugeführt. Für die nächsten 210.000 Blöcke waren es 25 neue Bitcoins pro Block. Aktuell sind es 6,25 neue Bitcoins pro Block. Wenn das System Block 840.000 erreicht, wird die Rate auf 3.125 neue Bitcoins pro Block halbiert.
- Aber während der Algorithmus die Anzahl der pro Block erstellten Bitcoins perfekt kontrollieren kann, kann er die Zeit, die benötigt wird, um einen neuen Block zu generieren, nicht perfekt kontrollieren.

Zusammenhang zwischen Difficulty und Hashrate

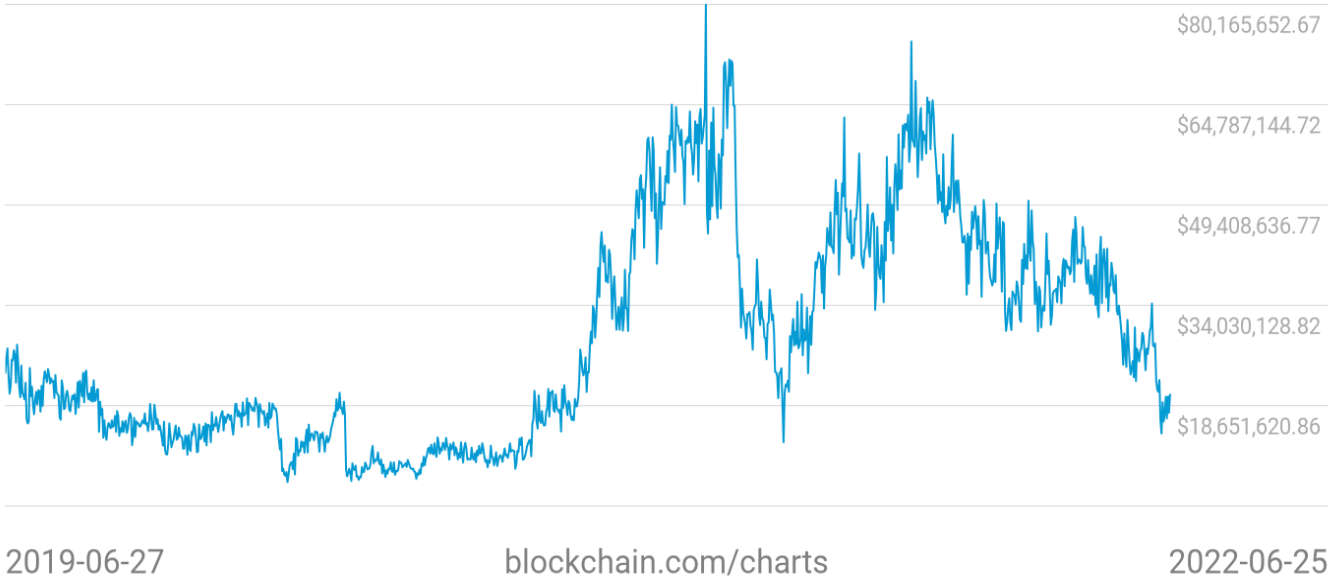
- Was der Algorithmus auch zu kontrollieren versucht, aber nicht perfekt kann, ist die Blockgenerierungszeit. Der Algorithmus versucht, die Generierungszeit so nahe wie möglich bei 10 Minuten zu halten.
- Diese Zeit hängt jedoch von der im System verfügbaren Rechenleistung ab. Je mehr Rechenleistung im System ist, desto schneller lösen die Miner die Schwierigkeit des Blocks.
- Der Algorithmus steuert die Blockgenerierungszeit durch Überprüfung der durchschnittlichen Zeit, die benötigt wurde, um die letzten 2.016 Blöcke (ca. 2 Wochen) zu generieren.
- Wenn die durchschnittliche Generationszeit kürzer als 10 Minuten ist, erhöht sich der Schwierigkeitsgrad, wenn sie länger als 10 Minuten ist, verringert sich der Schwierigkeitsgrad.
- Wenn der Schwierigkeitsgrad steigt, erhöhen die professionellen Miner (die viel in Mining-Leistung investiert haben) natürlich ihre Rechenleistung, um an der Spitze zu bleiben.
- Der Anstieg der Rechenleistung wird auch durch die Verfügbarkeit besserer Hardware, durch die Stromkosten und einige regulatorische Faktoren wie Gesetze, die die Verwendung von Strom für KryptoMining verbieten, beeinflusst.



Zusammenhang zwischen Difficulty und Hashrate

- Das Problem liegt in der Tatsache, dass die neu geschaffenen Bitcoins, so wie das System funktioniert, an den Miner vergeben werden, der diesen Block gelöst hat.
- Dieses System wurde als eine Möglichkeit konzipiert, Netzwerkmitglieder zu belohnen, die ihre Rechenleistung zur Verfügung stellen und das Netzwerk so unterstützen.
- Als Bitcoin an Wert gewann und die Belohnung für einen Block in die Höhe schoss (aktuell 6,25 BTC = 125.000 $), wurde Mining für einige Mitglieder zu einem Geschäftsmodell, was in diesem Ausmaß nie das ursprüngliche Ziel war.
- Dies ist eine Art Hamsterrad, das erklärt, warum das System so lächerlich hohe Grade an Schwierigkeit und Hashrate (Rechenleistung) erreicht hat.
  Solange die Miner weiterhin Rechenleistung hinzufügen, wird der Algorithmus den Schwierigkeitsgrad weiter erhöhen.
- Das Problem ist nicht nur der Algorithmus, sondern auch, dass Mining zu einem Geschäftsmodell geworden ist, unter anderem Dank günstiger Strompreise und technologischen Fortschritts. Professionelle Mining Pools agieren wie Konzerne, die um mehr Rechenleistung konkurrieren, denn mehr Rechenleistung bedeutet eine höhere Wahrscheinlichkeit, als erster den nächsten Block zu minen und somit mit neu geschaffenen Bitcoins belohnt zu werden. Es kann nur einen Gewinner pro Block geben.
- Bei einem Kurs von etwa 20.000 €, fließen pro Tag etwa 18 Mio. € Umsatz in Bitcoins an die Miner, zuzüglich etwaige freiwilliger Gebühren, die je nach Phase mehrere Prozent hoch sein können.

Daily Mining Revenues from the Bitcoin Blockchain



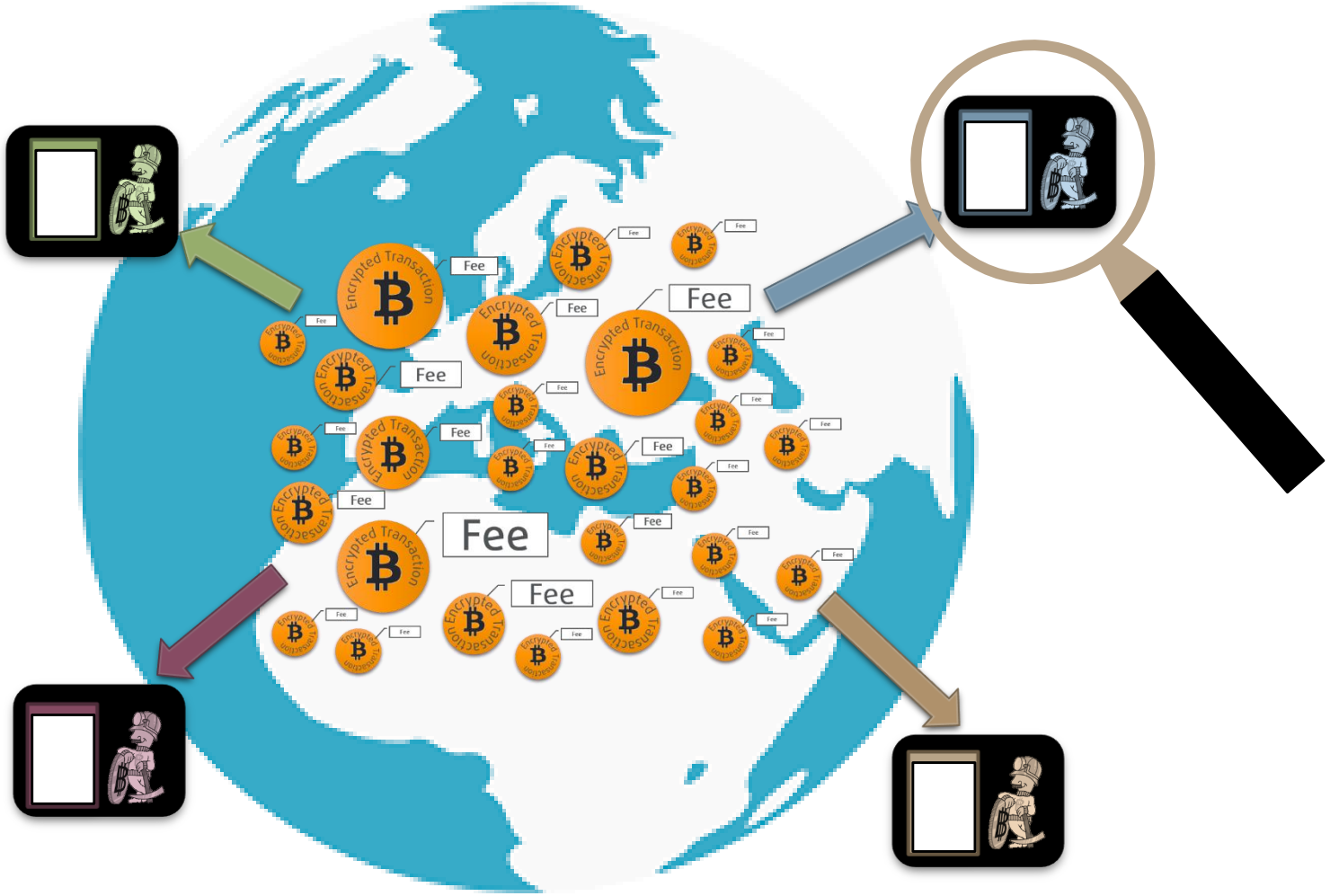
Dezentrales/Misstrauensbasiertes System

Dezentrales/Misstrauensbasiertes System

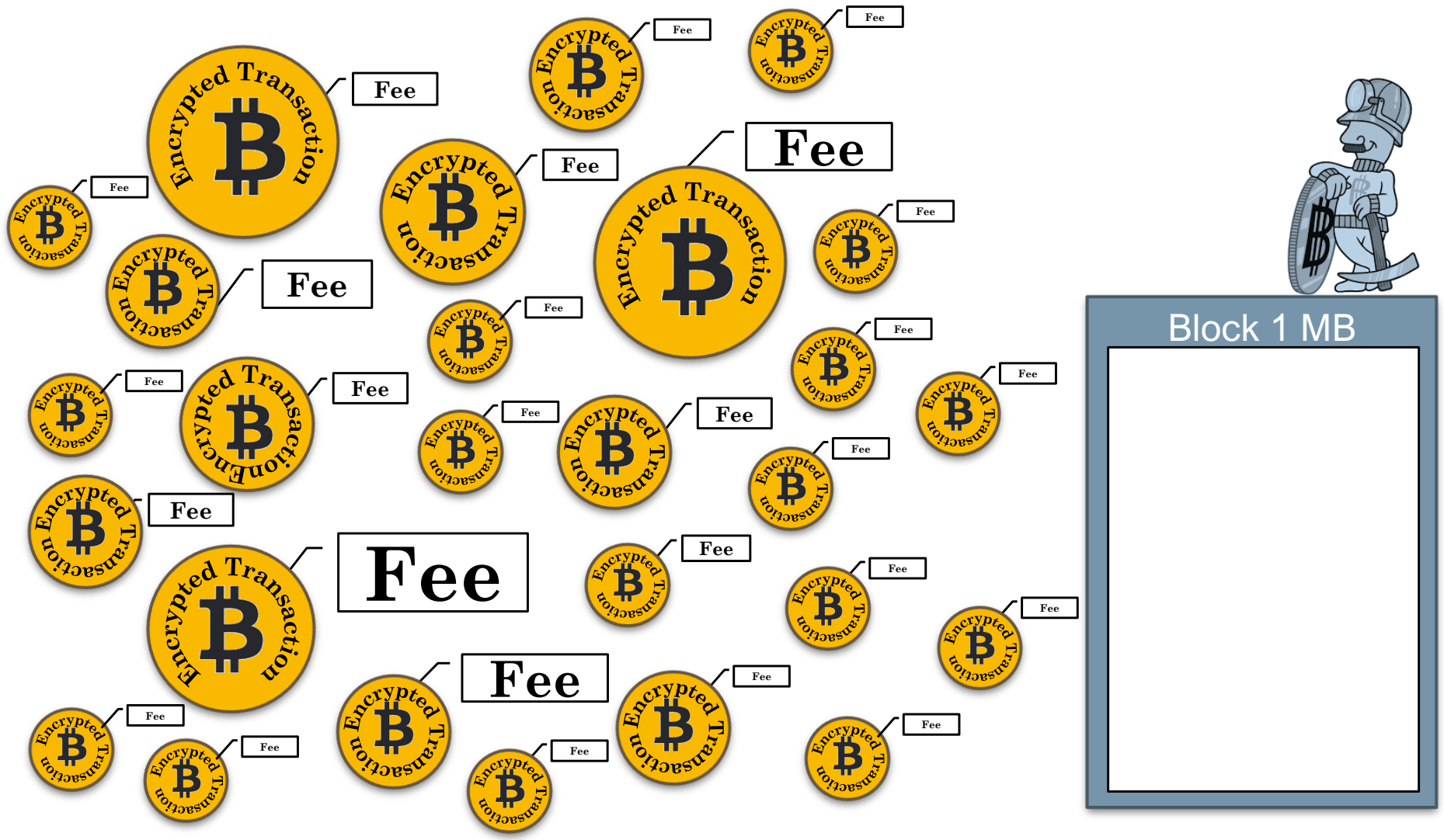
Dezentrales/Misstrauensbasiertes System

Dezentrales/Misstrauensbasiertes System

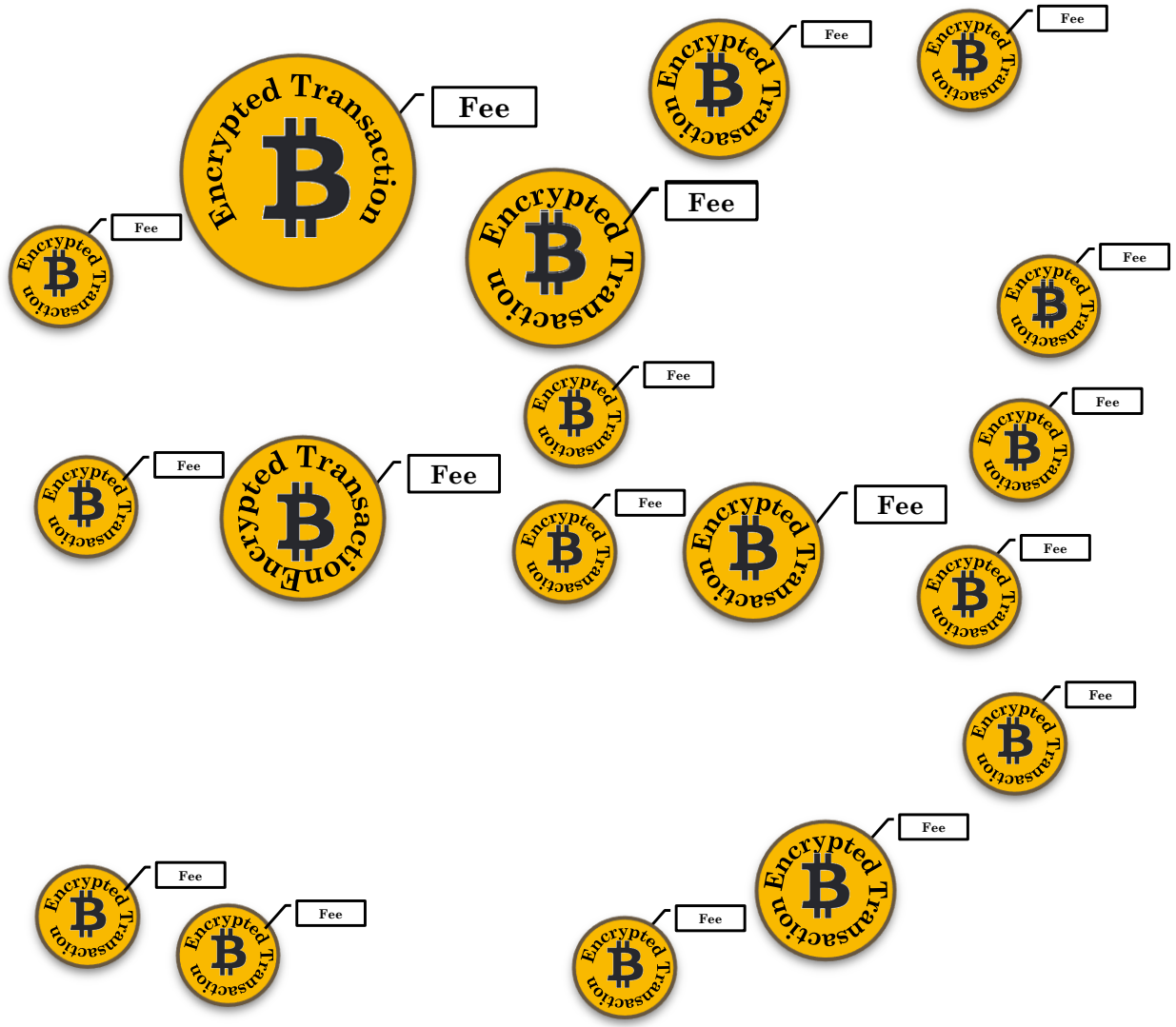
Dezentrales/Misstrauensbasiertes System

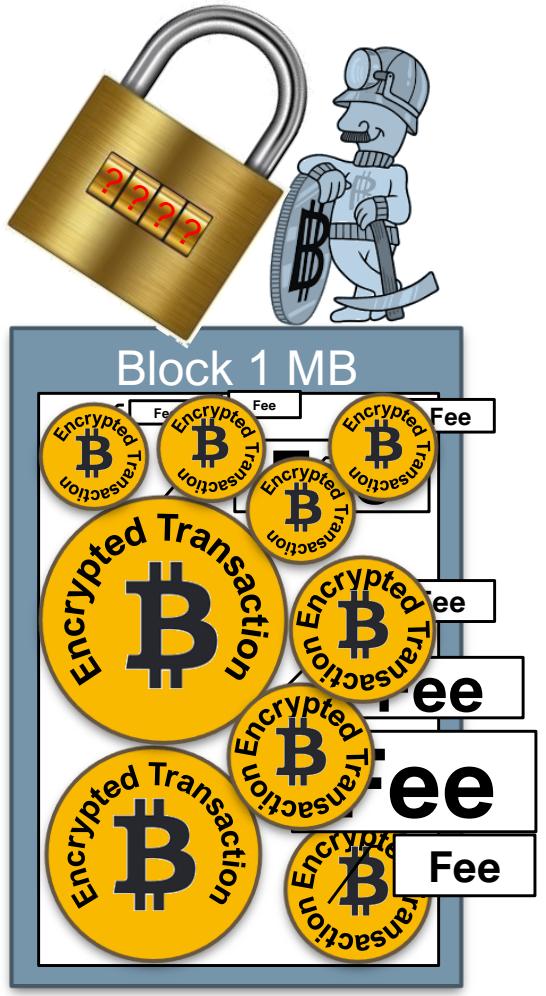


Mining in der Bitcoin Blockchain



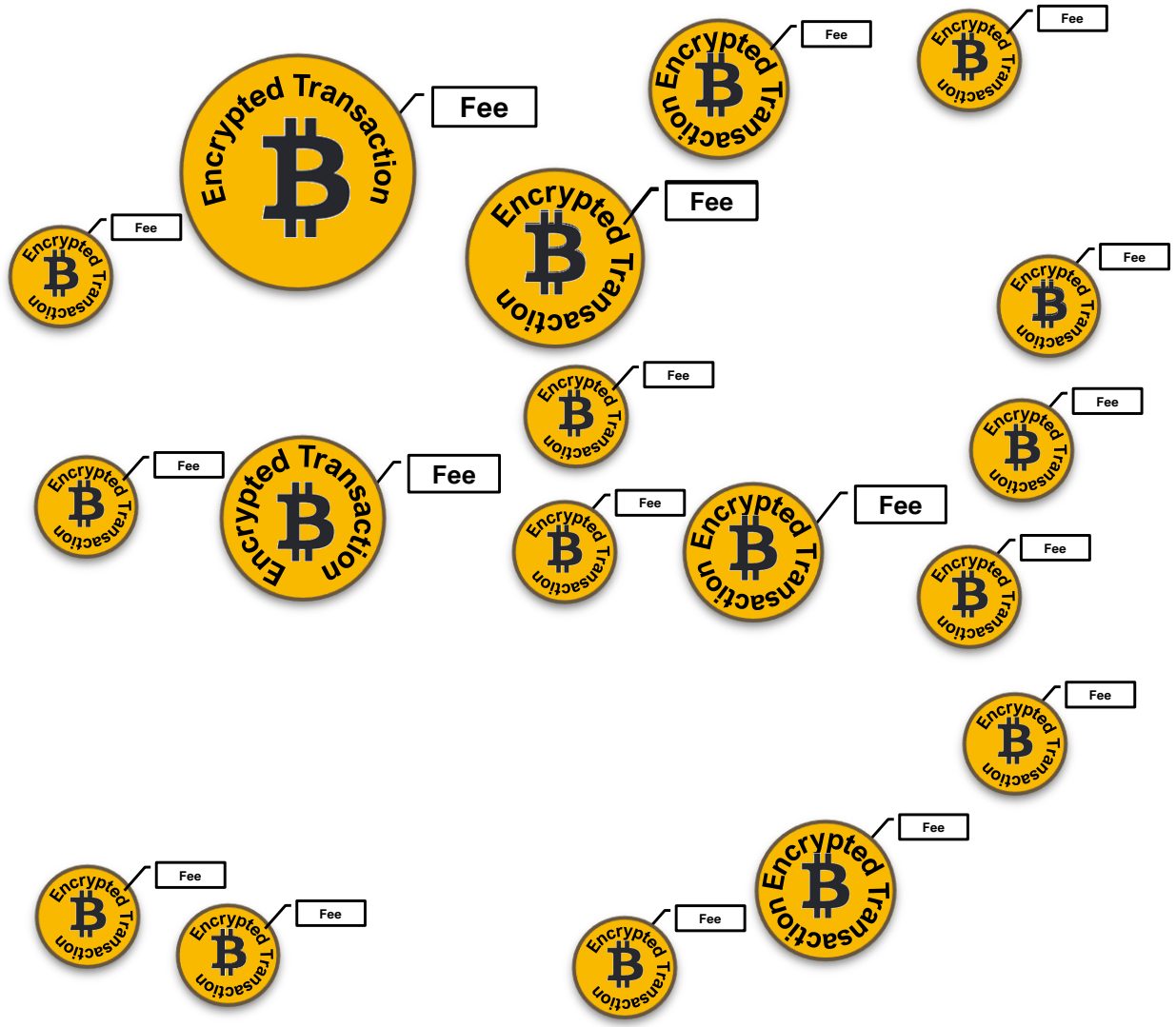
Mining in der Bitcoin Blockchain

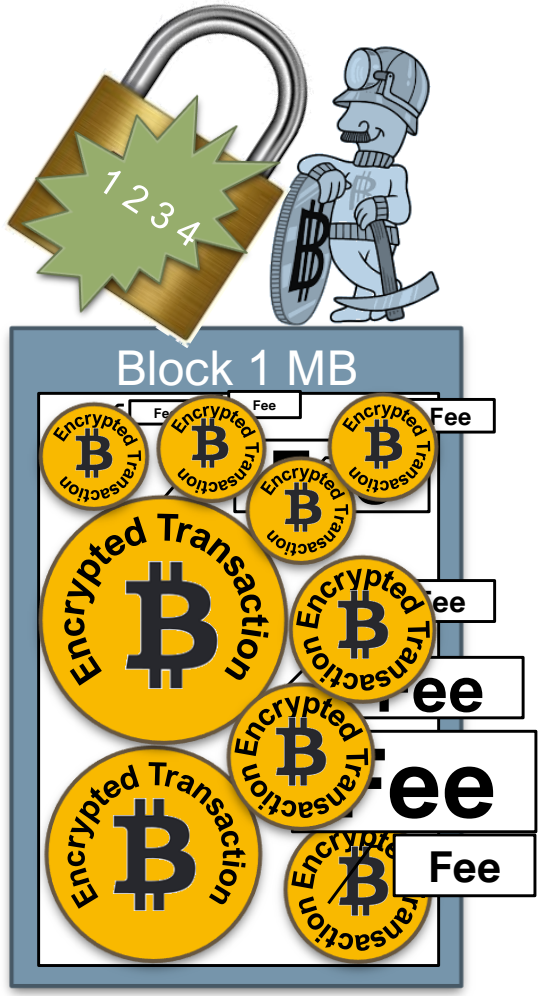




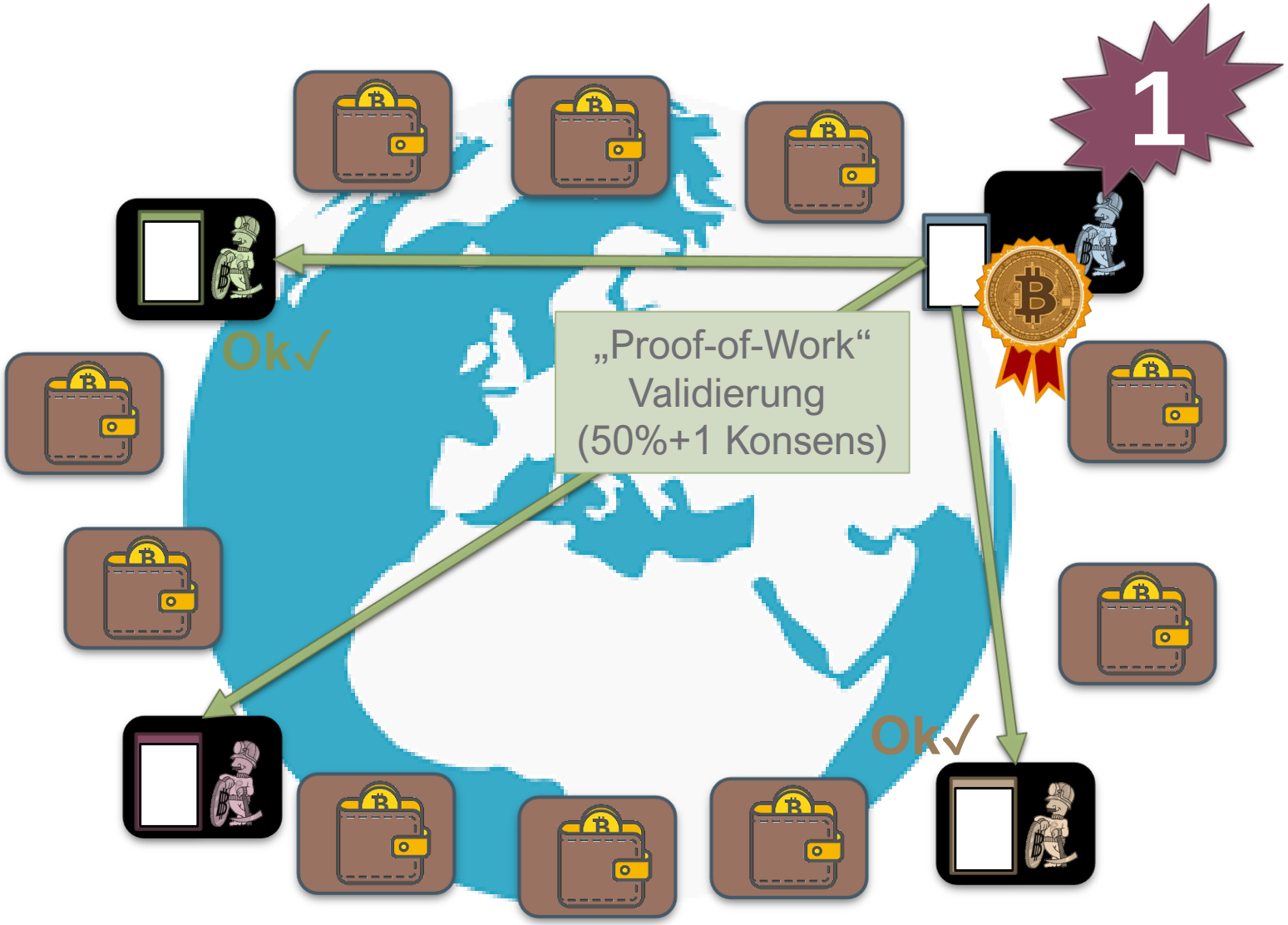
Und Millionen von ASICS legen los...

Mining in der Bitcoin Blockchain

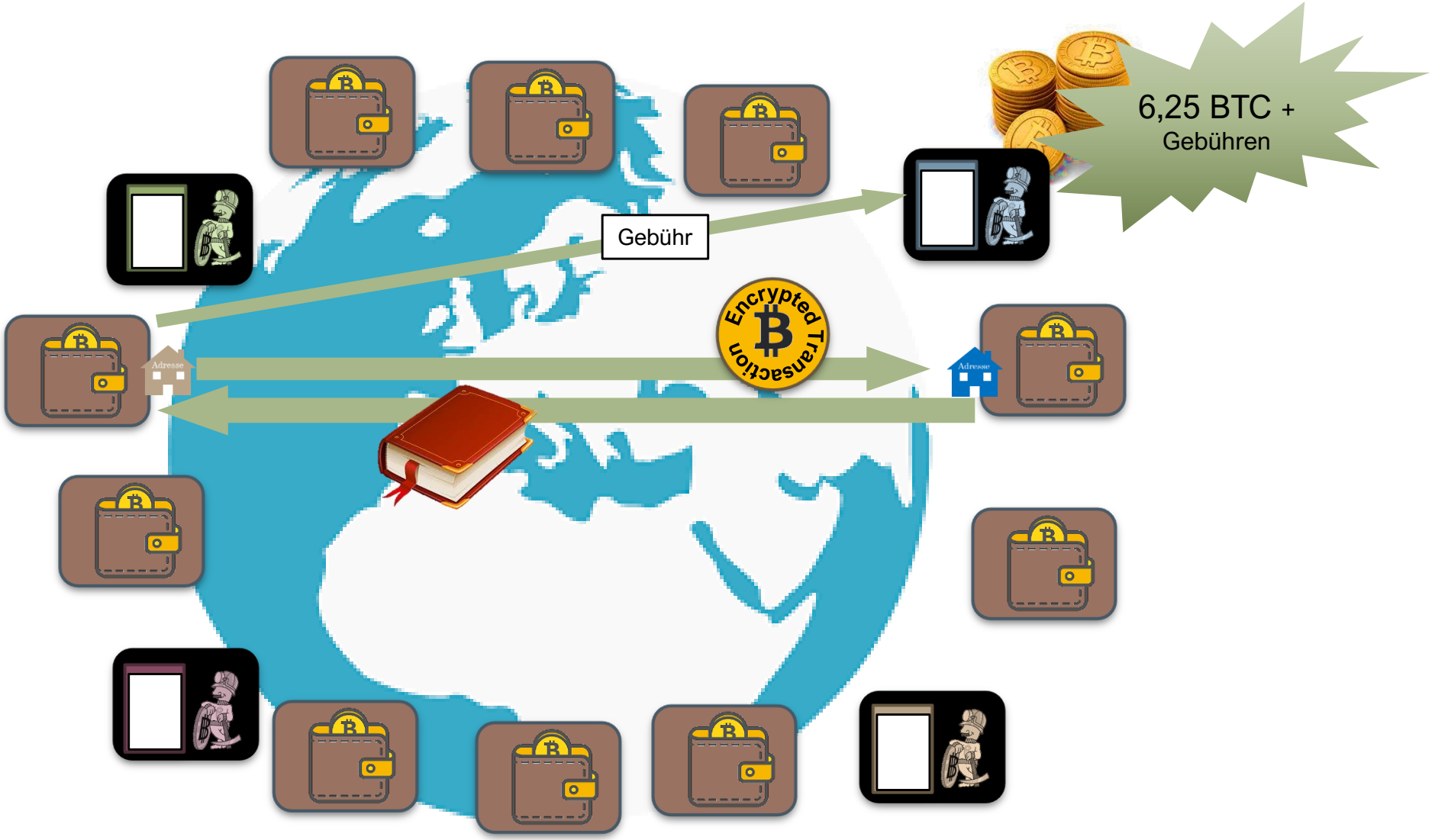




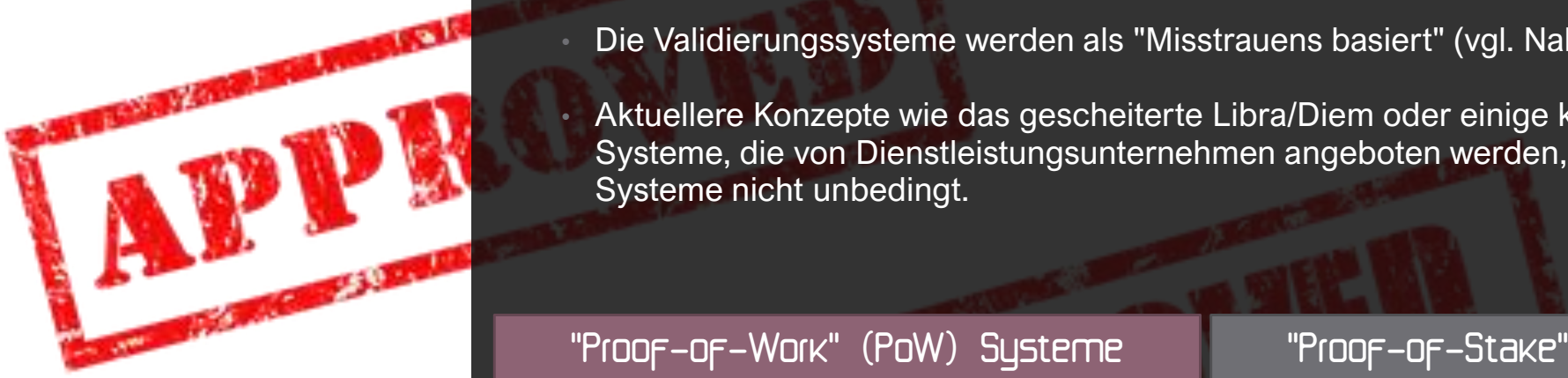
Validierung durch "Proof-of-Work"



Sofortige unwiderrufliche Zahlung



„Misstrauensbasierte" Validierungssysteme



- Die Validierungssysteme werden als "Misstrauens basiert" (vgl. Nakamoto) bezeichnet.
- Aktuellere Konzepte wie das gescheiterte Libra/Diem oder einige kommerzielle Systeme, die von Dienstleistungsunternehmen angeboten werden, verwenden solche Systeme nicht unbedingt.

"Proof-of-Work" (PoW) Systeme

Wird am häufigsten (Bticoin) verwendet. Ein Mitglied (Prover) beweist den anderen, dass es eine gewisse Rechenleistung zur Lösung eines Problems eingesetzt hat.
Diese Form des Konsensmechanismus wird auch als CPU-Kosten-Preis-Funktion oder Client-Puzzle bezeichnet.
Bei Krypto-Assets ist es oft mit einem Anreiz verbunden, der die Teilnehmer dafür entlohnt, dass sie Rechenleistung (und damit Strom) zur Verfügung stellen.

"Proof-of-Stake" (PoS) Systeme

Mitglieder, die ein Merkmal erfüllen, arbeiten als Controller / “Validatoren“ (Ethereum).
Am häufigsten bezieht sich dieses Merkmal auf die Höhe der Bestände in dem Asset.
Alternativ könnte auch Seniorität der bestimmende Faktor sein, oder beide.
Denkbar wären in nicht-anonymen Netzwerken die regionale Nähe oder spezifische Aufgaben.
Die erste Kryptowährung mit PoS (Peercoin) wurde 2012 eingeführt.

Anwedungsmöglichkeiten der Blockchain

Einsatzgebiete für Blockchain

Industrie	IoT, DAO
Logistik	Flottenmanagement, Fehlerverfolgung, Supply Chain Tracking (QM, ESG-Standards)
Finanz	Fonds-/Vermögensverwaltung, Versicherungspolice und Schadenmanagement, Zahlungsverkehr
Dienstleistungen	Buchungsmanagement (On-Demand-Services), Schadensmanagement, DAO (Taxi- oder Logistikdienstleistungen)
Handel	C-to-C, B-to-C, B-to-B
Recht	Rechtsberatung, Notarielle Dienstleistungen, Lizenz- und Rechtemanagement
Öffentliche Hand	Wahlsysteme, Smart Cities, Gesundheitssysteme
Gesundheit, Pflege	Krankenakten, Beratung, Betreuung, Notfall- & Priorisierung

Wann ist der Einsatz einer Blockchain sinnvoll?

- Skalierbarkeit ist wichtig
- Ausführungsgeschwindigkeit ist wichtig
- Entscheidungsprozesse sind standardmäßig einfach
- Offenheit ist gefragt
- Stabilität und Sicherheit sind wichtig
- Genaue/zeitnahe Transaktionsaufzeichnung wichtig
- Die Kosten für Vermittler/Treuhänder sind hoch

- Notwendigkeit der prozessinternen Interaktion
- Vor- oder Nachbereitungstätigkeiten unvermeidbar
- Intermediäre bieten zusätzliche Vorteile
- Rechtliche Aspekte (Verordnungen, Gesetze, ...)
- Fähigkeit/Anforderungen der Mitglieder heterogen

Wie meine Freunde mich Sehen

Wie meine Mutter mich sieht

Wie die Gesellschaft mich sieht

Bitcoin, Strukturelle Betrachtung

Wie manche Politiker mich sehen

Wie ich mich selbst sehe

Was ich wirklich tue

Bitcoin Statistiken

Statistik, Stand 30. Juni, 12:20 Uhr, MEZ	Stand 19. Mai, 15:30 MEZ	Stand 30. Juni, 12:20 MEZ	Kommentar
Gesamtzahl der BTC	19.043.950	19.068.963	90,7% von 21 Millionen (sollte im Jahr 2140 erreicht werden))
Block Generierungszeit	10:35 min	09:02 min	Das System zielt auf eine Erzeugungszeit von 10 Minuten ab
Difficulty	31.251.101.365.711	29.570.168.636.357	Initial Difficulty (Jan. 2009) war 1.
Blöcke bis nächste Difficulty	823	919	Alle 2.016 Blöcke neu angepasst.
Zeit bis zur nächsten difficulty	5 Tage 17 Stunden	6 Tage 10 Stunden	Theoretisch alle 14 Tage, wenn die Blockgenerierung genau 10 Minuten beträgt.
Hash Rate	205.062.089.115 GH/S	221.961.099.442 GH/S	1 GH = 1 Milliarde Hashes pro Sekunde
Marktkapitalisierung	523 Mrd. €	348 Mrd. €	Wechselkurs ca. 1,1 $/€ bzw. ca. 1,04 $/€
BTC Preis	€ 27.398	€ 18.230	Coinbase Exchange
Block Höhe	737.032	742.894	Generationsblock (0) Jan. 2009
Blocks vor der Halbierung	102.968	97.016	Alle 210.000 Blocks (≈4 Jahre)
ETA nächste Halbierung	742 Tage 9 Stunden	607 Tage 16 Stunden	Geschätzt Anfang März, 2024
Kleinste Werteinheit	1 Satoshi	1 Satoshi	1 BTC = 100 Millionen Satoshi

Source: Coinmarketcap.com

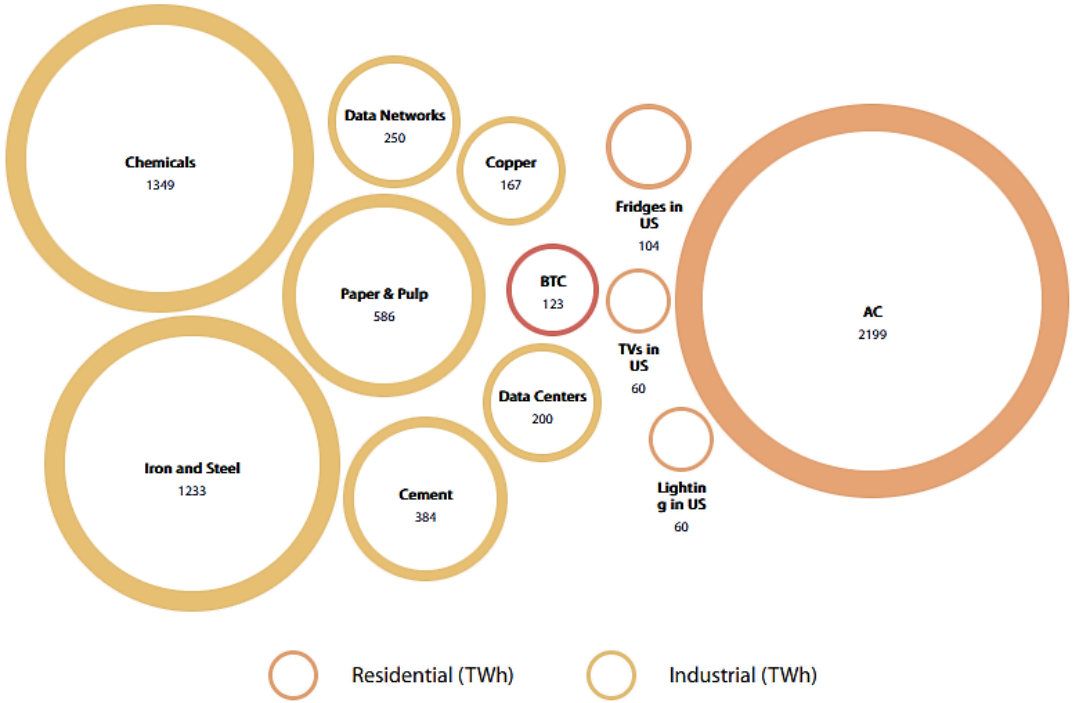
Statistik, Stand 16. März, 15:46 Uhr, MEZ		
Block Größe	1 Megabyte	Eingeführt in 2010
Transaktionen per Block	Ca. 2.000	Kann variieren
Durchschnittl. Anzahl Transktion pro Std. & Sek.*	11.495/h or 3,2/s	Im Vergleich Visa 50.000/s
Zeit bis zur Transaktionsvalidierung	9 bis 127 min	Ohne Lightning Netzwerk
BTC Transaktionen pro Tag*	273.832	
Durchschnittlicher Transaktionswert*	1,98 BTC	72.945 €
Medianer Transaktionswert*	0,014 BTC	501 €
Mining Rentabilität pro THash/s	0,1767 €/Day	
Block Belohnung in BTC (Inkl. Gebühren)*	6,31937 BTC	234.275 €, (34,2 Mio. €/Tag)
% Gebühren	1,1 %	Sehr variabel

Source: Coinmarketcap.com

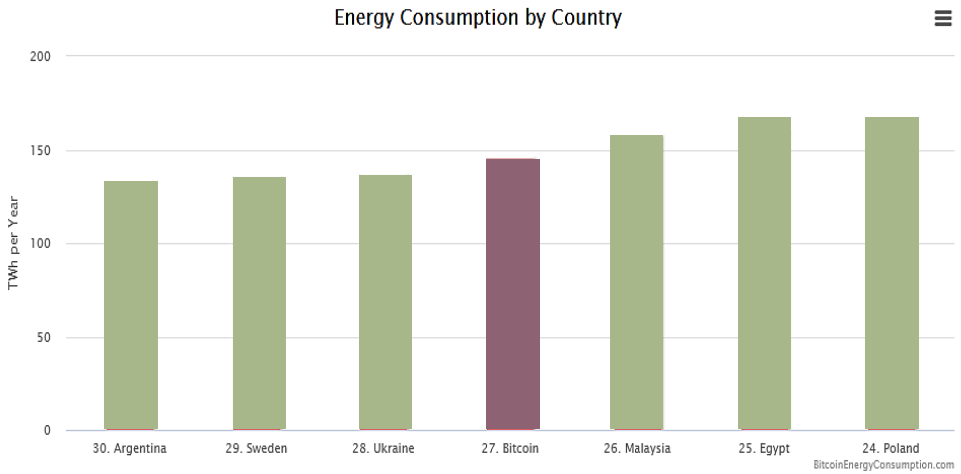
* Source: Bitinfocharts.com

Bitcoin Statistiken

Bitcoin Energieverbrauch (annualisiert TWh)



Ca. so viele TWh wie weltweit für den Goldbergbau eingesetzt werden



Ca. 36% des deutschen Energieverbrauchs

https://ccaf.io/cbeci/index [retrieved June 16, 2022]

https://digiconomist.net/bitcoin-energy-consumption [retrieved June 16, 2022]

Bitcoin-Fußabdrücke

CO2 Fußabdruck	Stromverbrauch	Elektroschrott
80,14 Mt CO2	**143,69 TWh**	**37,06kt**
Vergleichbar mit der Tschechischen Republik	Vergleichbar mit der Ukraine	Vergleichbar mit den Niederlanden

Global über ein Jahr

CO2 Fußabdruck	Stromverbrauch	Elektroschrott
866,68 kg CO2	**1553,86 kWh**	**400,70 g**
Vergleichbar etwa 1,9 Millionen Transaktionen mit einer VISA-Karte oder 144 Tausend Stunden YouTube Videos sehen	Vergleichbar mit dem Stromverbrauch eines durchschnittlichen US-Haushaltes über mehr als 53 Tage.	Vergleichbar mit Gewicht von 2,44 iPhones 12 oder 0,82 iPads

Für eine einzige Transaktion

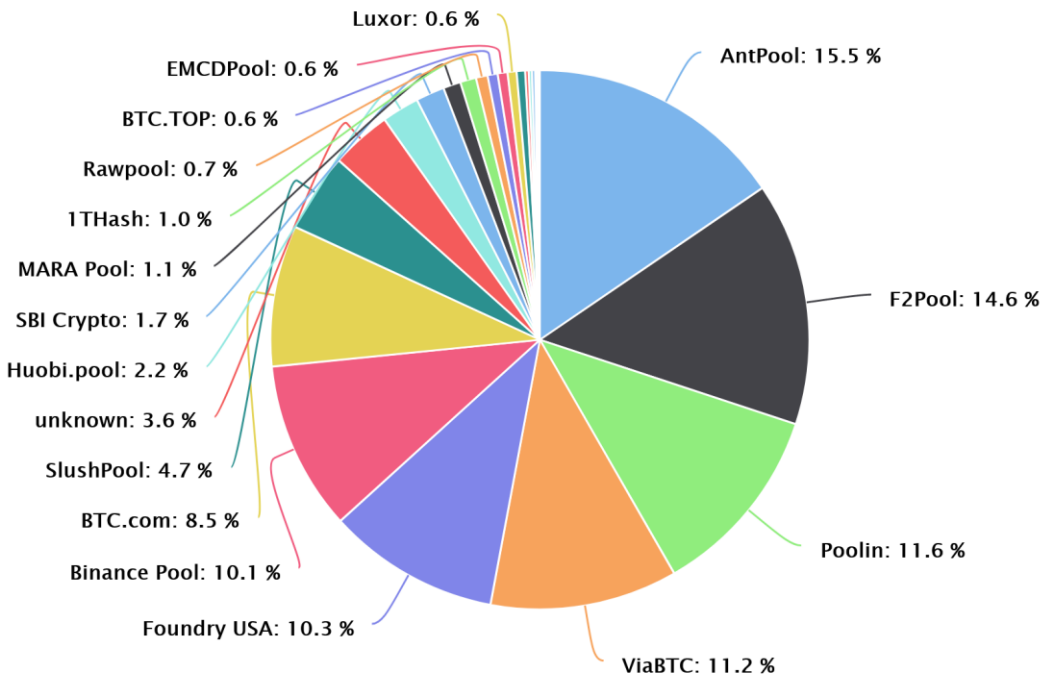
Source: https://digiconomist.net/bitcoin-energy-consumption [retrieved June 17, 2022]

Oligopolistische Mining Industrie

Wenig Veränderung in den letzten 5 Jahren, immer die gleichen Spieler an der Spitze

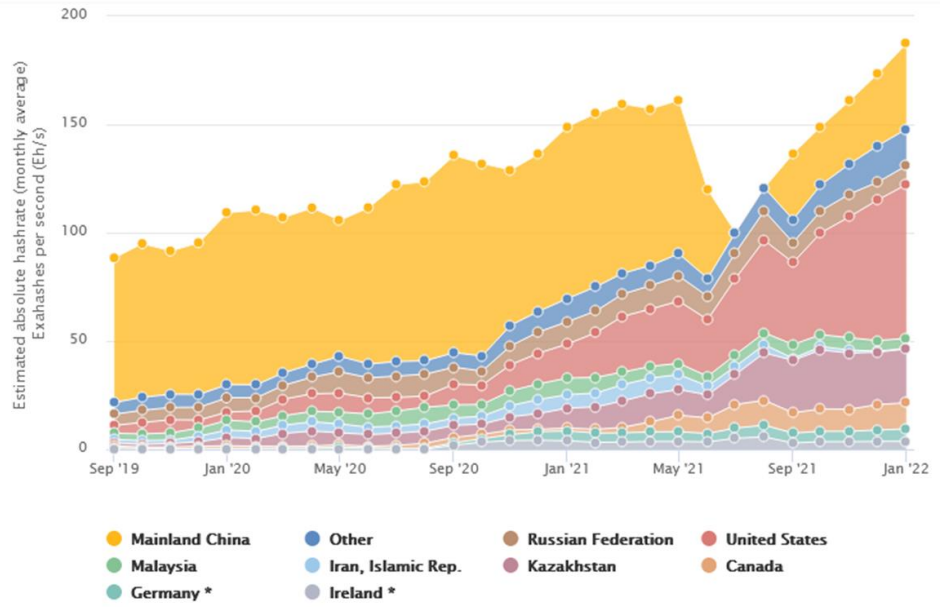
- Der einzige neue Top-Player ist Foundry USA. Weitere Top-10-Spieler unverändert
- Die Bitcoin-Mining-Industrie zeichnet sich durch eine eindeutig oligopolistische Struktur aus, die an die Strukturindustrien wie den Diamantenabbau erinnert.
- Eine einzelne Organisation könnte ihre Kapazität auf mehrere Pools verteilen.
  - Top 5 = ca. 63,2%
  - Top 10 = ca. 92,5%

Verteilung der erfolgreich abgebauten Blöcke im letzten Jahr



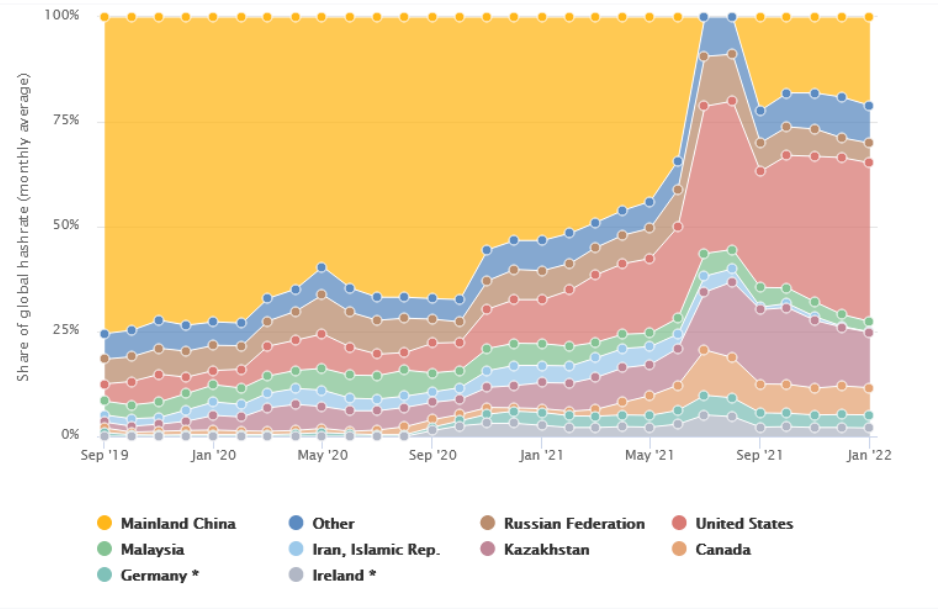
Evolution der Hashraten im BTC-Netzwerk

Entwicklung der Hashrate des BTC-Netzwerkes in Eh/s



* To our knowledge, there is little evidence of large mining operations in Germany or Ireland that would justify these figures. Their share is likely significantly inflated due to redirected IP addresses via the use of VPN or proxy services.

Entwicklung der Hashrate des BTC-Netzwerkes nach Ländern in %



Source: https://ccaf.io/cbeci/mining_map [Retrieved June 16, 2022]

Vermögensaufteilung im BTC-Netzwerk

Die folgenden Daten sind eine Übersicht über bestehende Adressen, nicht über Wallets. Eine Brieftasche kann eine beliebige Anzahl verschiedener Adressen besitzen. Auf der anderen Seite sind viele der größeren Adressen im Besitz von Exchange, die BTC auf diesen Adressen als Proxys für ihre Investoren verwalten. Während es nicht möglich ist, das Eigentum an den Adressen zu ermitteln, gibt es dennoch einen groben Überblick über die Vermögensverteilung im BTC-Netzwerk.

Bitcoin Rich List, 14. Oktober 2018 (BTC-Preis ≈ 6.340 $)

BTC Saldo	Anzahl Adressen	% der Adressen (aggregiert)	Bitcoins insgesamt	USD-Wert	% Bitcoins (aggregiert)
(0 – 0,001)	11.221.026	49,43% (100%)	2.297	14.561.953	0,01% (100%)
[0,001 – 0,01)	5.084.977	22,4% (50,57%)	20.882	132.370.667	0,12% (99,99%)
[0,01 – 0,1)	3.911.077	17,23% (28,17%)	152.212	793.700.000	0,72% (99,87%)
[0,1 – 1)	1.760.635	7,76% (10,94%)	570.808	3.618.260.897	3,3% (99,14%)
[1 – 10)	575.302	2,53% (3,19%)	1.500.002	9.508.281.451	8,66% (95,85%)
[10 – 100)	132.113	0,58% (0,65%)	4.366.599	27.679.195.997	25,21% (87,19%)
[100 – 1.000)	14.832	0,07% (0,07%)	3.720.873	23.586.036.133	21,48% (61,97%)
[1.000 – 10.000)	1.580	0,01% (0,01%)	3.438.472	21.795.940.886	19,85% (40,49%)
[10.000 – 100.000)	123	0% (0%)	3.157.782	20.016.689.552	18,23% (20,63%)
[100.000 – 1.000.000)	3	0% (0%)	415.692	2.635.004.623	2,4% (2,4%)

Source: bitinfocharts.com [Retrieved October 14, 2018]

Vermögensaufteilung im BTC-Netzwerk

Bitcoin Rich List, 31. Oktober 2021 (BTC-Preis ≈ 61.300 $)

BTC Saldo	Anzahl Adressen	% der Adressen (aggregiert)	Bitcoins insgesamt	USD-Wert	% Bitcoins (aggregiert)
(0 – 0,001)	19.891.981	51,35% (100%)	4.067	253.569.906	0,02% (100%)
[0,001 – 0,01)	9.683.482	25% (48,65%)	36.879	2.299.086.179	0,2% (99,98%)
[0,01 – 0,1)	5.916.525	15,27% (23,65%)	191.753	11.954.080.897	1,02% (99,78%)
[0,1 – 1)	2.438.835	6,3% (8,38%)	759.275	47.334.023.730	4,03% (98,77%)
[1 – 10)	660.135	1,7% (2,08%)	1.683.719	104.964.815.226	8,93% (94,74%)
[10 – 100)	131.148	0,34% (0,38%)	4.270.425	266.222.822.802	22,65% (85,81%)
[100 – 1.000)	14.012	0,04% (0,04%)	3.993.166	248.938.206.439	21,18% (63,16%)
[1.000 – 10.000)	2.069	0,01% (0,01%)	5.293.970	330.031.725.770	28,07% (41,99%)
[10.000 – 100.000)	83	0% (0%)	2.049.316	127.756.511.327	10,87% (13,91%)
[100.000 – 1.000.000)	3	0% (0%)	574.031	35.785.687.304	3,04% (3,04%)

Source: bitinfocharts.com [Retrieved October 31, 2021]

Vermögensaufteilung im BTC-Netzwerk

Bitcoin Rich List, 17. März 2022 (BTC-Preis ≈ 40.920 $ um 16:20 Uhr MEZ)

BTC Saldo	Anzahl Adressen	% der Adressen (aggregiert)	Bitcoins insgesamt	USD-Wert	% Bitcoins (aggregiert)
(0 – 0,001)	21.235.551	51,81% (100%)	3.744	175.113.521	0,02% (100%)
[0,001 – 0,01)	10.083.151	24,6% (48,18%)	38.368	1.568.655.595	0,2% (99,98%)
[0,01 – 0,1)	6.274.161	15,31% (23,58%)	203.197	8.307.640.177	1,07% (99,78%)
[0,1 – 1)	2.564.736	6,26% (8,27%)	794.031	32.463.716.137	4,18% (98,7%)
[1 – 10)	678.221	1,65% (2,01%)	1.722.319	70.416.486.495	9,07% (94,52%)
[10 – 100)	130.446	0,32% (0,36%)	4.257.574	174.069.596.209	22,43% (85,45%)
[100 – 1.000)	13.662	0,03% (0,04%)	3.922.223	160.358.840.792	20,66% (63,02%)
[1.000 – 10.000)	2.201	0,01% (0,01%)	5.251.951	214.724.384.187	27,67% (42,36%)
[10.000 – 100.000)	80	0% (0%)	2.125.566	86.903.108.074	11,2% (14,69%)
[100.000 – 1.000.000)	4	0% (0%)	663.637	27.132.587.742	3,5% (3,5%)

Source: bitinfocharts.com [Retrieved March 17, 2022]

Vermögensaufteilung im BTC-Netzwerk

Bitcoin Rich List, 17. Juni 2022 (BTC-Preis ≈ 20.845 $ ca. 9:30 MEZ)

BTC Saldo	Anzahl Adressen	% der Adressen (aggregiert)	Bitcoins insgesamt	USD-Wert	% Bitcoins (aggregiert)
(0 – 0,001)	21.673.729	51,23% (100%)	4.423	92.201.510	0,02% (100%)
[0,001 – 0,01)	10.453.920	24,71 (48,77%)	39.657	826.652.142	0,21% (99,98%)
[0,01 – 0,1)	6.600.207	15,60% (24,05%)	214.799	4.477.457.346	1,13% (99,77%)
[0,1 – 1)	2.715.795	6,42% (8,45%)	839.079	17.490.491.814	4,4% (98,64%)
[1 – 10)	711.999	1,68% (2,03%)	1.800.508	37.531.368.784	9,44% (94,24%)
[10 – 100)	131.719	0,31% (0,35%)	4.257.484	88.746.711.331	22,33% (84,80%)
[100 – 1.000)	13.638	0,03% (0,04%)	3.848.343	80.218.223.923	20,18% (62,47%)
[1.000 – 10.000)	2.118	0,01% (0,01%)	5.119.141	106.707.855.500	26,85% (42,29%)
[10.000 – 100.000)	88	0% (0%)	2.132.755	44.457.017.747	11,19% (15,44%)
[100.000 – 1.000.000)	5	0% (0%)	810.648	16.897.847.716	4,25% (4,25%)

Source: bitinfocharts.com [Retrieved June 17, 2022]

Vermögensaufteilung im BTC-Netzwerk

Bitcoin Rich List, 17. Juni 2022 (BTC-Preis ≈ 20.845 $ ca. 9:30 MEZ)

Adressen mit einem BTC-Wert von höchstens						
$1	$100	$1.000	$10.000	$100.000	$1.000.000	$10.000.000
7.727.658	28.818.308	37.165.045	40.857.643	42.053.687	42.238.593	42.298.345
18,27%	68,12%	87,85%	95,58%	99,41%	99,85%	99,99%

Source: bitinfocharts.com [Retrieved June 16, 2022]

Vermögensaufteilung im BTC-Netzwerk

Bitcoin Rich List, 16. vs. 17. Juni 2022

BTC Saldo in $ (Kurs vom 17. Juni)	Anzahl Adressen	Bitcoins insgesamt	USD-Wert
(0 – 20,85$)	21.673.729 (+4.990)	4.423 (+2)	92.201.510 (-1.358.132)
[20,85$ – 208,45$)	10.453.920 (+17.557)	39.657 (+70)	826.652.142 (-11.108.691)
[208,45$ – 2.084,50$)	6.600.207 (+16.405)	214.799 (+608)	4.477.457.346 (-55.333.548)
[2.084,50$ – 20.845$)	2.715.795 (+3.978)	839.079 (+768)	17.490.491.814 (-250.185.953)
[20.845$ – 208.450$)	711.999 (+1.176)	1.800.508 (+3.183)	37.531.368.784 (-502.455.740)
[208.450$ – 2.084.500$)	131.719 (+122)	4.257.484 (+4.402)	88.746.711.331 (-1.258.765.328)
[2.084.500$ – 20.845.000$)	13.638 (+14)	3.848.343 (-1.579)	80.218.223.923 (-1.255.417.117)
[20.845.000$ – 208.450.000$)	2.118 (+3)	5.119.141 (+15.285)	106.707.855.500 (-1.302.049.337)
[208.450.000$ – 2.084.500.000$)	88 (-2)	2.132.755 (-38.054)	44.457.017.747 (-1.482.541.939)
[2.084.500.000$ – 20.845.000.000$)	5 (+0)	810.648 (+15.832)	16.897.847.716 (+77.629.007)
Gesamtwerte	**42.303.218 (+44.243)**	**19.066.837 (+607)**	**397.445.827.813 (-6.041.586.778)**

Vermögensaufteilung im BTC-Netzwerk

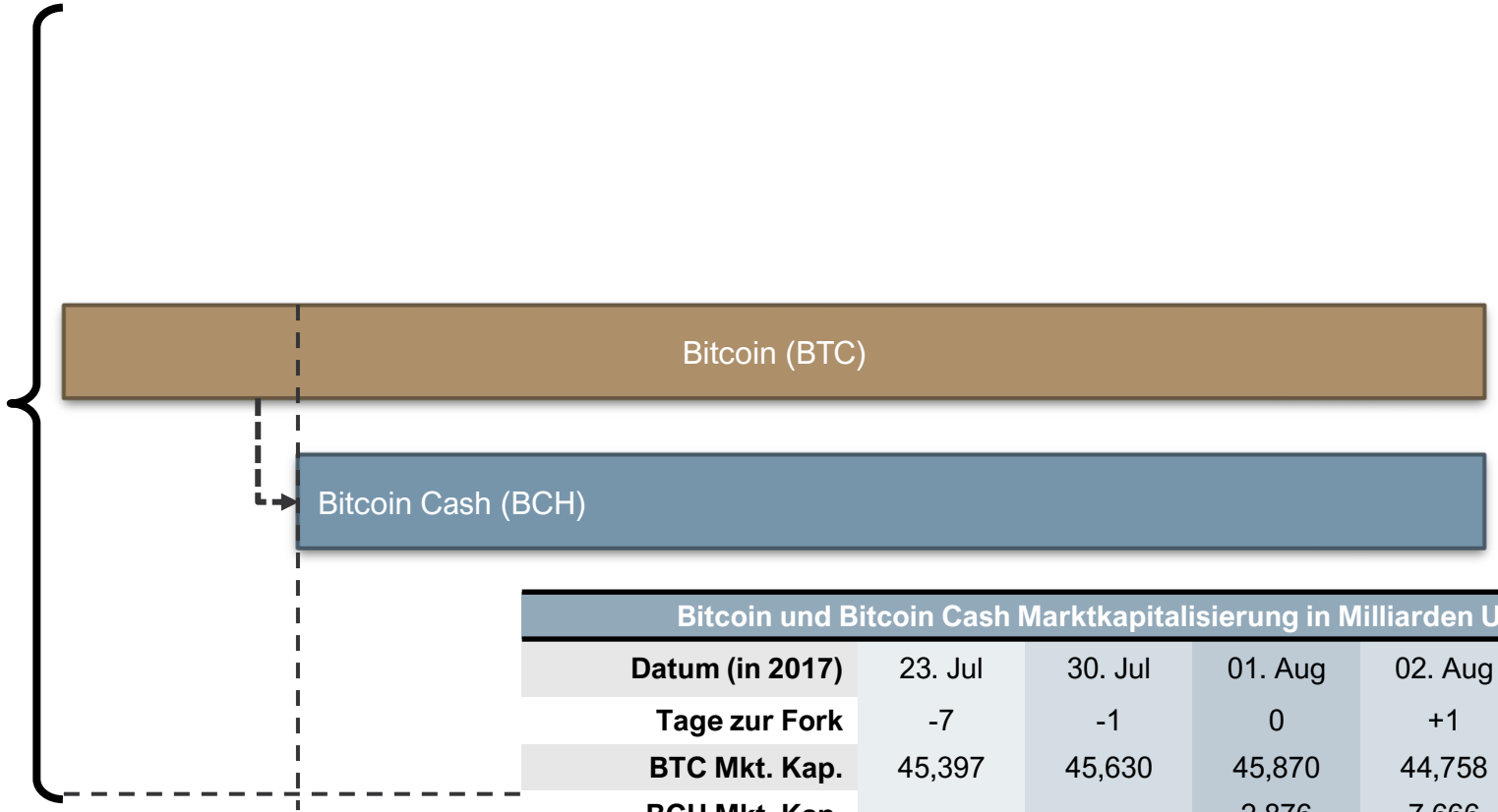
Bitcoin Rich List, Vergleich 14. Oktober 2018 mit 17. Juni 2022

BTC Saldo	Adressen 14. Okt. 2022	Bitcoins 14. Okt. 2018	Bitcoins 17. Jun. 2022	Adressen 17. Juni 2022
(0 – 0,001)	11.221.026	2.297	4.423 (+92,57%)	21.673.729 (+93,15%)
[0,001 – 0,01)	5.084.977	20.882	39.657 (+89,91%)	10.453.920 (+105,58%)
[0,01 – 0,1)	3.911.077	125.212	214.799 (+71,55%)	6.600.207 (+68,76%)
[0,1 – 1)	1.760.635	570.808	839.079 (+47,00%)	2.715.795 (+54,25%)
[1 – 10)	575.302	1.500.002	1.800.508 (+20,03%)	711.999 (+23,76%)
[10 – 100)	132.113	4.366.599	4.257.484 (-2,50%)	131.719 (-0,30%)
[100 – 1.000)	14.832	3.720.873	3.848.343 (+3,43%)	13.638 (-8,05%)
[1.000 – 10.000)	1.580	3.438.472	5.119.141 (+48,88%)	2.118 (+34,05%)
[10.000 – 100.000)	123	3.157.782	2.132.755 (-32,46%)	88 (-28,46%)
[100.000 – 1.000.000)	3	415.692	810.648 (+95,01%)	5 (+66,67%)
Gesamtwerte	**22.701.668**	**17.318.619**	**19.066.837 (+10,09%)**	**42.303.218 (+86,34%)**

Was sind Hard Forks

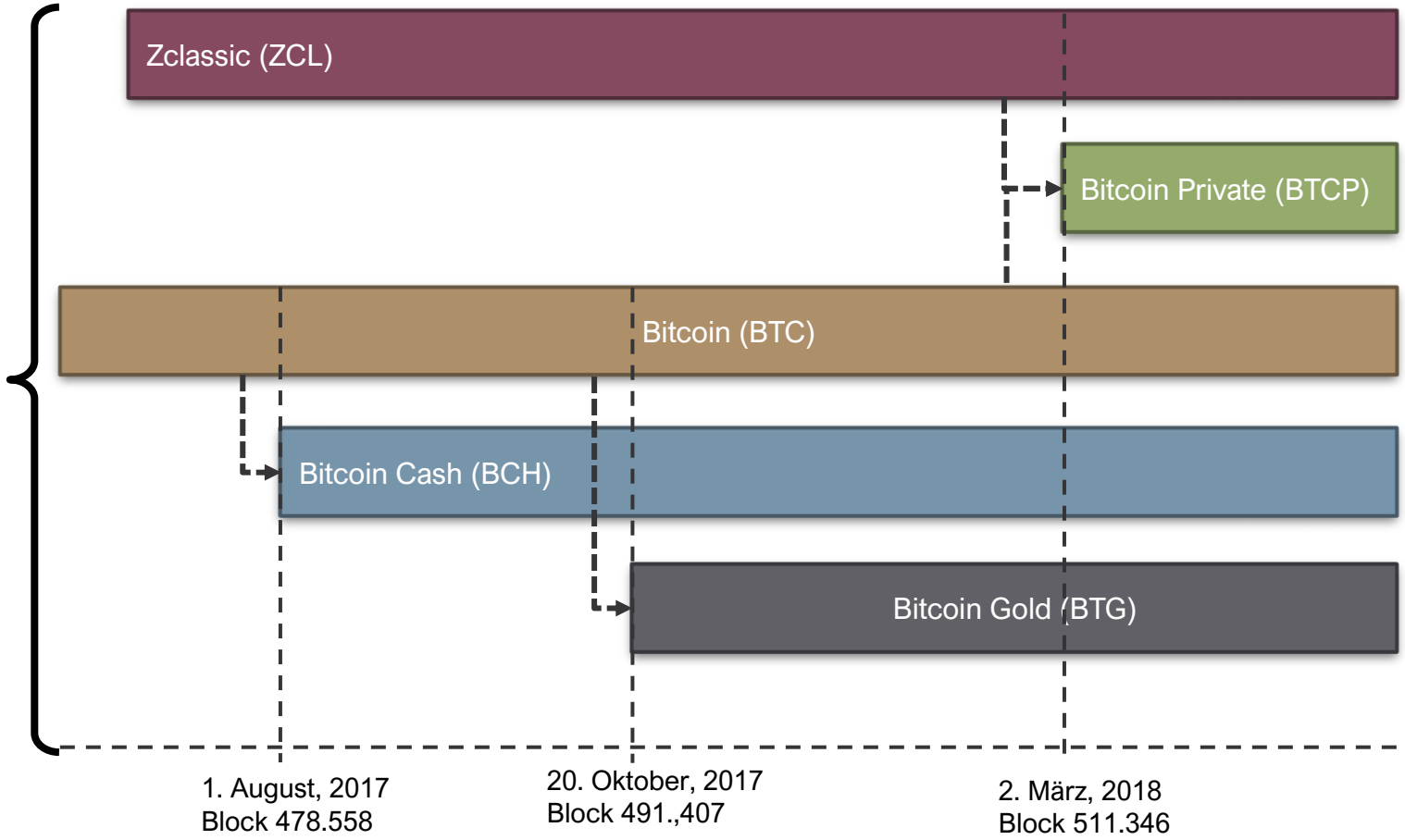
- Eine Hard Fork entsteht wenn ein Teil der Community eine Änderung des Codes einer Kryptowährung vorschlägt und entweder dabei keinen Konsens erreicht oder das Register der ursprünglichen Blockchain nicht rückwirkend korrigiert werden kann.
- Bei einer Hard Fork wird das Register der ursprünglichen Kryptowährung geklont und für den Klon der Code entsprechend der Vorstellungen geändert. Inhaber der ursprünglichen Kryptowährung (die weiter besteht) erhalten eine gleiche Menge der neu entstandenen Währung, die dem geänderten Algorithmus folgt.
- Eines von vielen Beispielen ist die Kryptowährung Bitcoin Cash (BCH), die am 1. August 2017 aus einem Klon der Bitcoin (BTC) Blockchain entstand. Hierbei wollten die Entwickler und Befürworter von Bitcoin Cash, die Blockgröße von 1 MB, die in der BTC-Blockchain festgelegt ist, erhöhen.
- Durch eine Hard Fork entsteht nicht nur eine neue Kryptowährung. Da diese neue Kryptowährung ja auch gehandelt wird, entsteht aus dem Nichts ein Wert.
- Am Beispiel der Bitcoin Cash Fork erkennt man, wie auf einen Schlag neuer Wert geschaffen wird. Die Marktkapitalisierung von BCH liegt zum 1. Juli, 2022 bei etwa 1,9 Mrd. USD. Da die BCH Blockchain ein Klon der BTC Blockchain ist, entwickelt sie sich identisch in Bezug auf die Token-Generierung, Mining-Mechanik und maximale Stückzahl.

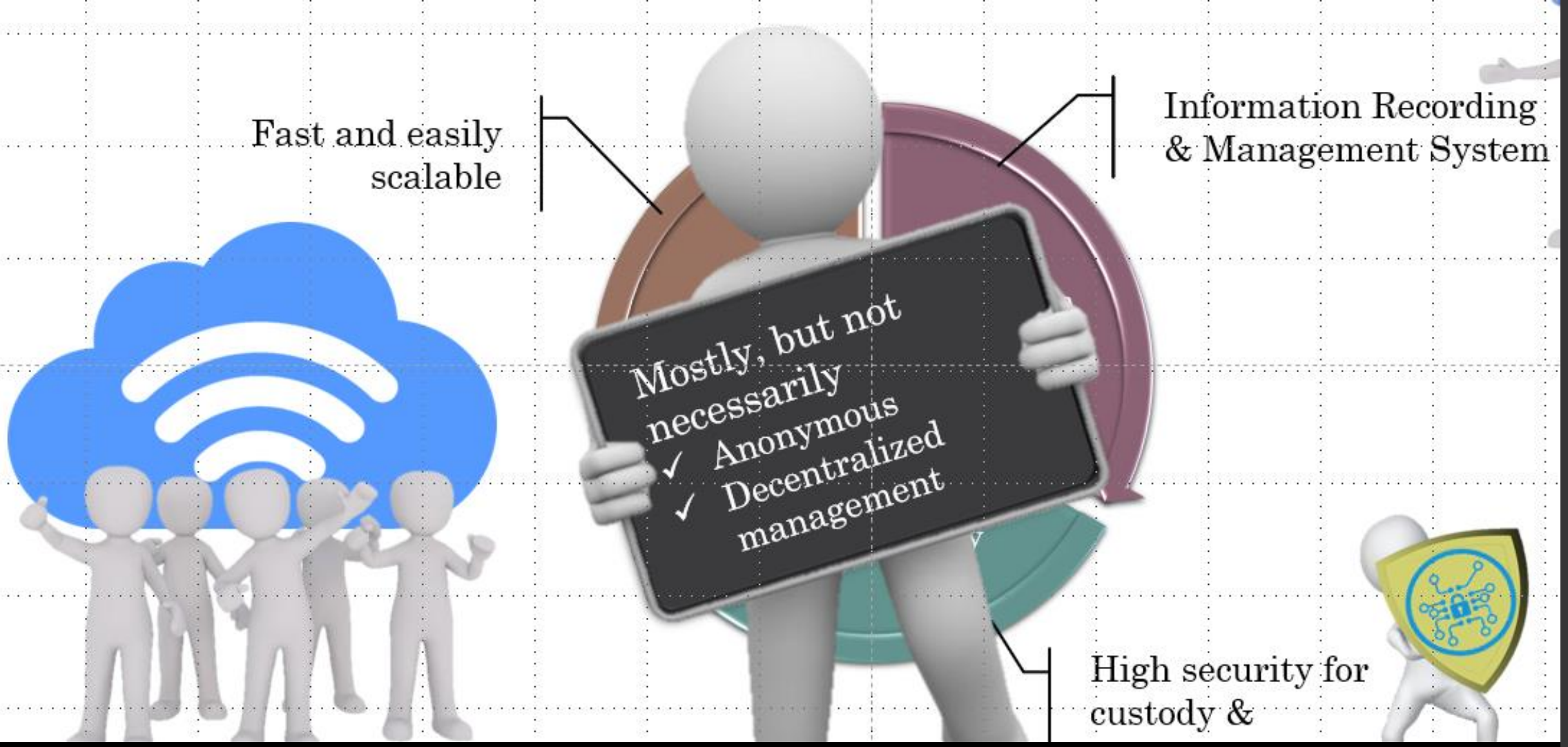
Die BCH Hard Fork



Bitcoin und Bitcoin Cash Marktkapitalisierung in Milliarden USD					
Datum (in 2017)	23. Jul	30. Jul	01. Aug	02. Aug	08 Aug.
Tage zur Fork	-7	-1	0	+1	+7
BTC Mkt. Kap.	45,397	45,630	45,870	44,758	56,407
BCH Mkt. Kap.	--	--	2,876	7,666	5,557
Aggregierte Mkt. Kap.	**45,397**	**45,630**	**48,746**	**52,423**	**61,964**

Weitere Hard Forks der BTC-Blockchain





Soziokulturelles Phänomen

Social Bubbles, Anonymität, Dezentralisierung

Zitate von Experten

"... Ich würde Bitcoin nicht als Währung bezeichnen [...] Währungen werden von Zentralbanken oder Regierungen unterstützt. Niemand unterstützt Bitcoin. Und übrigens, ich habe schon [...] viele Fragen gesehen, ob die EZB Bitcoin verbieten oder regulieren wird. Es liegt nicht in der Verantwortung der EZB, dies zu tun.„

Mario Draghi (Chef der EZB, 2018)

"Ich glaube, dass das Internet eine der stärksten Kräfte sein wird, um die Rolle der Regierungen zu reduzieren. Das einzige, was fehlt, aber bald entwickelt wird, ist ein zuverlässiges E-Geld.„

Milton Friedman (Ökonom, 1999)

"Also, brauchen wir eine neue Art von Geld [Bitcoin]? Ich denke, man könnte dafür argumentieren, wenn sich unser derzeitiges Geld schlecht entwickeln würde. Tut es aber nicht. Wir haben große wirtschaftliche Probleme, aber Banknoten gehören nicht dazu – und wir sollten sie in Ruhe lassen.„

Paul Krugman (Ökonom)

"Ich glaube wirklich, dass Bitcoin die erste [Kryptowährung] ist, die das Potenzial hat, so etwas wie die Welt zu verändern.„

Peter Thiel (Mitgründer von PayPal)

"Vor nicht allzu langer Zeit argumentierten einige Experten, dass der PC niemals angenommen werden würde und dass Tablets nur als teure Küchenbretter enden würden, also denke ich, dass es nicht klug wäre, virtuelle Währungen zu verwerfen.„

Christine Lagarde (Chefin des IMF, 2017)

Zitate von Laien

Niemand weiß, wie es funktioniert. Niemand!
Jeder spricht über Bitcoin, und niemand versteht es.
Es ist wie eine dramatische Wendung in einem verwirrenden Film.„
Ellen Degeneres (Schauspielerin, TV host)

"Bitcoin ist die Währung des Widerstands. Wenn Satoshi Bitcoin 10 Jahre früher veröffentlicht hätte, wäre der 11. September nie passiert!„
Max Keiser (Journalist, Publizist)

"Bitcoin ist eine Währung für Internet-Snobs ..."
William Shatner (Actor)

"Der relative Erfolg von Bitcoin beweist, dass Geld in erster Linie vom Vertrauen abhängt. Weder Gold noch Anleihen werden benötigt, um eine Währung zu stützen.„
Arnon Grunberg (Schriftsteller)

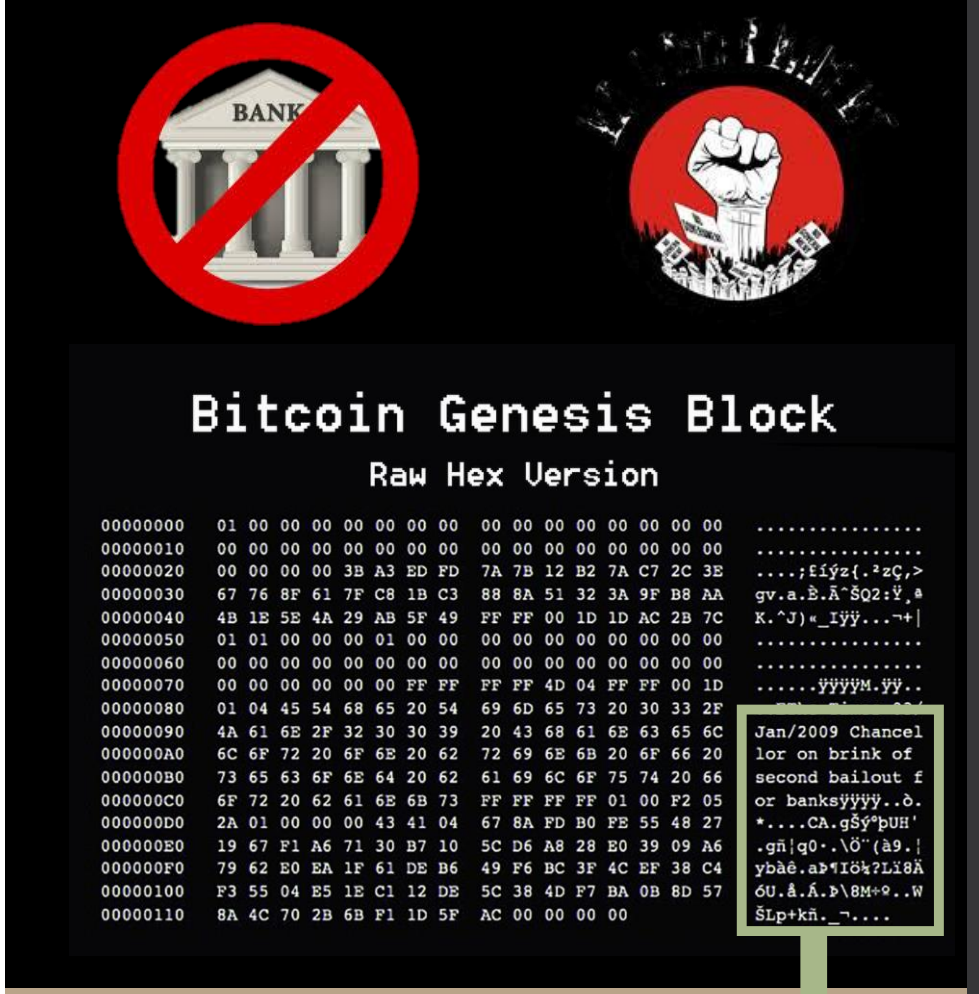
„Es ist das Gold der Nerds.“
Stephen Colbert (Autor, TV-Moderator)

Kontext und Zweck der Entwicklung von Bitcoin

- Die Schaffung eines dezentralen "reinen elektronischen Peer-to-Peer-Zahlungssystems" (Nakamoto, 2008)
  - ✓ Bitcoin wurde entwickelt, um ein Mittel zu sein, kein Selbstzweck!

- Ideologisch verankert in der digitalen liberalen Kultur bis hin zum sog. Anarchokapitalismus.
  - ✓ Beworben und gelobt als Alternative zum klassischen Geldsystem
  - ✓ Unmissverständliche Kritik an der Politik von Regierungen und Banken nach der Bankenrettung nach der Finanzkrise

- Der allererste Bitcoin-Block, der von Satoshi Nakamoto erstellt wurde, wurde von einem Textteil begleitet, der auf die URL eines Artikels in der Zeitung UK Times verwies, der sich auf den britischen Finanzminister bezog.



Warum sind die meisten Krypto-Assets besonders?

- Anonymität der Entwickler und Herausgeber.
- Keine Dysfunktion bestehender Zahlungssysteme (Kreditkarten, PayPal)
- Coolness-Faktor, „Robin-Hood“ Aura.

- Unklarer Rechtsstatus. In sehr wenigen Ländern als Währung anerkannt, in einigen verboten.
- Kein Anlegerschutz (kein Schutz vor Betrügern und Hackern).
- Private Schlüssel verloren = Bitcoins für immer weg.
- Betrugsmaschen sind gang und gäbe.

- Der Wert basiert auf dem Glauben an das System, nicht durch Investitionen, Sicherheiten, Garantien oder irgendeine wertschöpfende Kraft oder Tätigkeit.

- Kein Käuferschutz.
- Sehr illiquide, nicht ausreichend für die Supermarktkasse
- Bei hohen Transaktionsvolumina steigen die Gebühren.
- Extrem hohe Volatilität, Spielball von Spekulanten

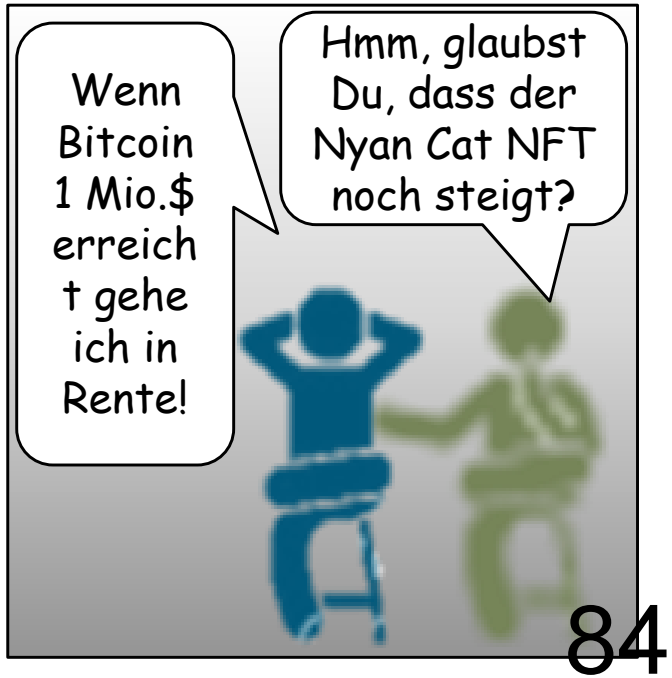

Hast Du die News gesehen? Bitcoin ist wieder Lambo!.
Vermutlich wieder ein Tweet Elon Musk, ein Scam oder Wash Trader am Werk.
Nee, Ich habe die Bitcoin Days Destroyed geprüft. Das ist 'ne echte Moonphase!


Ja! Das hodlen zahlt sich jetzt aus!
Wart's nur ab, der nächste Mtgox, Silk Road, ICO-Scam oder Crypto-Jack kommt bald. Ich bleibe No-Coiner

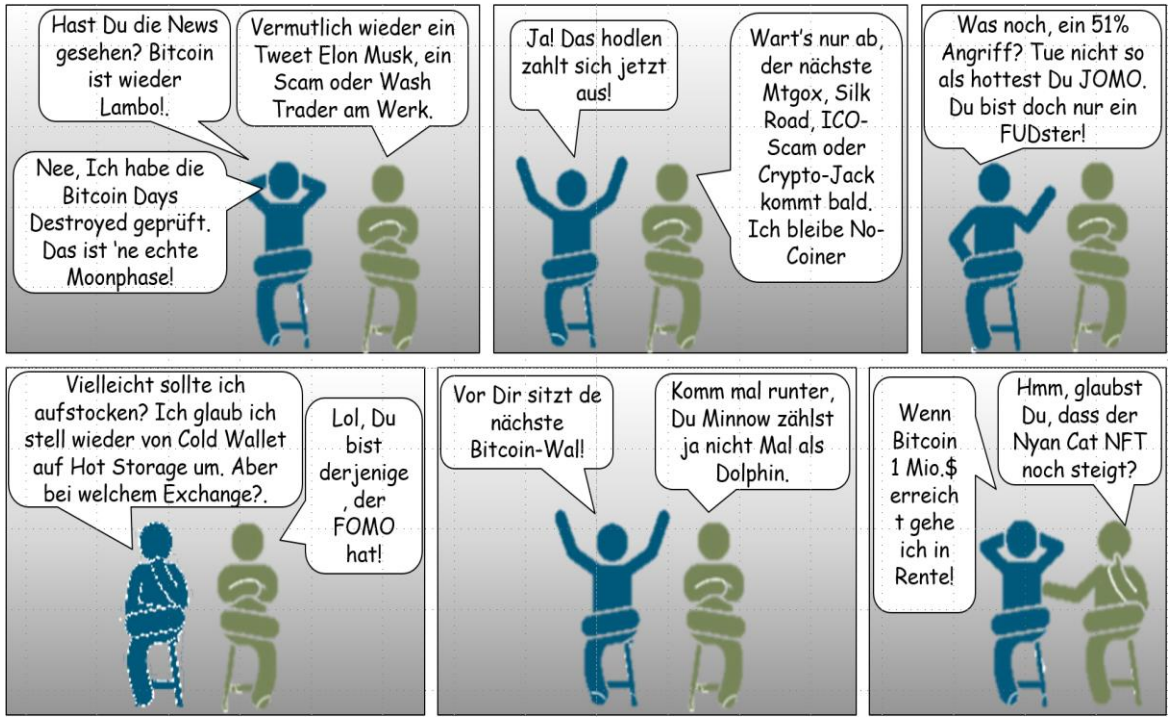

Was noch, ein 51% Angriff? Tue nicht so als hottest Du JOMO. Du bist doch nur ein FUDster!


Vielleicht sollte ich aufstocken? Ich glaub ich stell wieder von Cold Wallet auf Hot Storage um. Aber bei welchem Exchange?.
Lol, Du bist derjenige, der FOMO hat!


Vor Dir sitzt de nächste Bitcoin-Wal!
Komm mal runter, Du Minnow zählst ja nicht Mal als Dolphin.


Wenn Bitcoin 1 Mio.$ erreicht gehe ich in Rente!
Hmm, glaubst Du, dass der Nyan Cat NFT noch steigt?

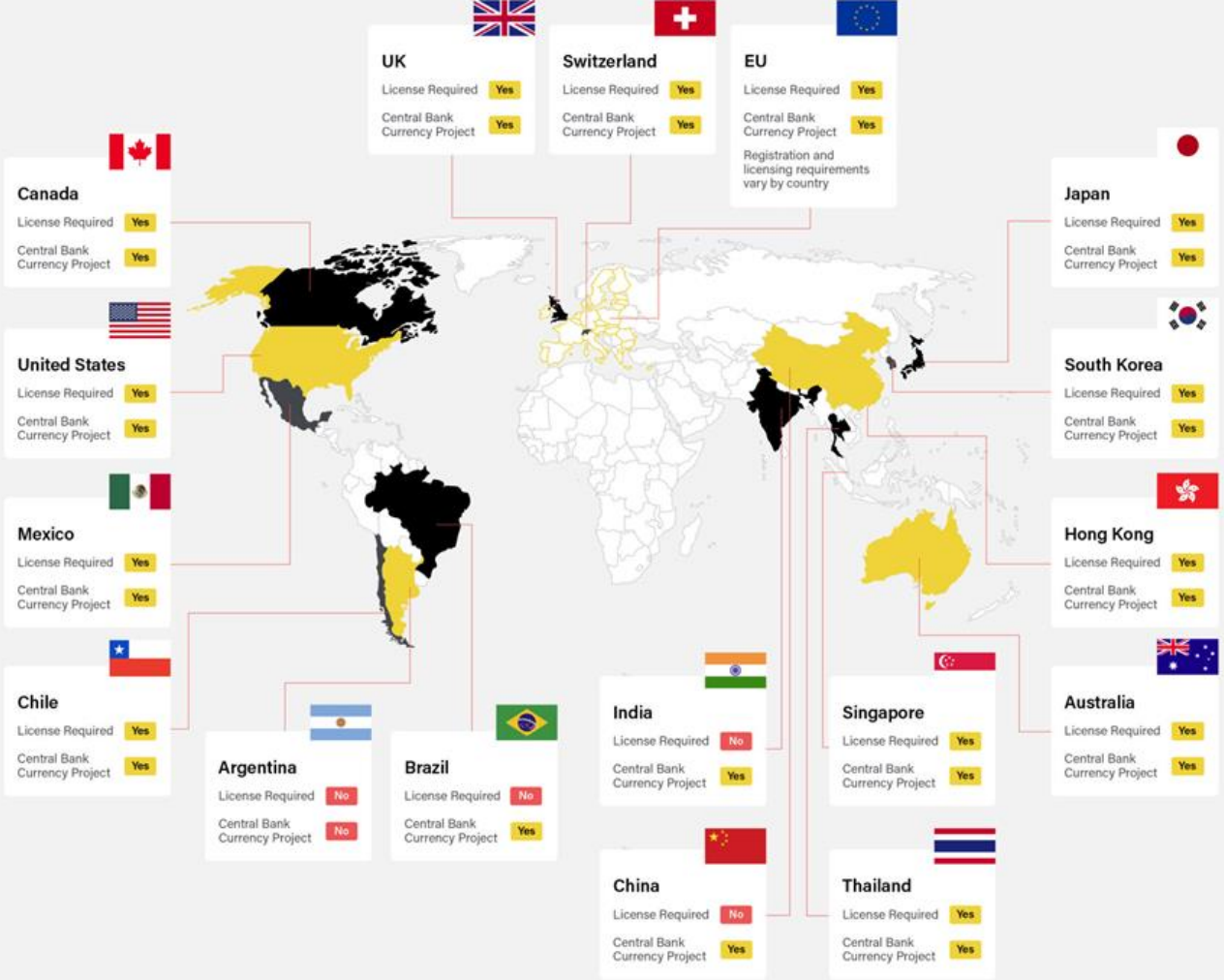
Narrativ und Social Bubbles



- Ein Teil der Interessenten die sich mit Kryptowährungen auseinandersetzen sind der sog. Crypto Bro Community zuzuordnen, die als soziales Konstrukt, wenn nicht sogar als Subkultur zu bezeichnen ist. Sie hat identitären Charakter.
- Artefakte sind das Narrativ, das mit dem „Wir gegen das System“ bei Bitcoin begann. Eindeutig ist die Entwicklung eines eigenen Slangs, der sich sowohl aus Begriffen der Finanzwelt, wie auch aus denen der Computer-/Onlinespielwelt bedient. Durch Erfolgsgeschichten von Krypto-Investoren wird auch eine Art Heldenepos entwickelt, wobei die Idee, dass WAGMI „We're All Gonna Make It“ eine wichtige Rolle spielt.
- Strukturell wird dies, wie auch anderswo, über Social Media Bubbles, gefestigt. Crypto Bros finden sich und tauschen sich in dedizierten Online Plattformen aus, die auch von den Betreibern hinsichtlich der Inhalte kontrolliert werden, indem Sinne, dass kritische Stimmen sofort aus den Telegram, Discord oder Instagram Kanälen gesperrt werden, sobald sie irgendwas hinterfragen
- Problematisch ist, dass kritisches Hinterfragen – z. B. in Bezug auf die Problematik der immensen Stromverschwendung im Zusammenhang mit PoW-Systemen, oder bezogen auf die nicht enden wollenden Betrugsmaschen – nicht erwünscht ist, bzw. durch fadenscheinige Gegenargumente oder sofortige Aussperrung im Keim erstickt wird.
- Es findet kein wirklicher Diskurs statt. Akademisches Interesse wird ebenso dem etablierten „System“ zugeordnet wie seriöse Medien als Handlanger des gleichen.
- Weitere Entwicklungen, wie NFT tragen weiter zur sozialen Identifizierung bei, indem sie von den Mitgliedern als Avatare ihrer Online-Identitäten verwendet werden. Wer augenscheinlich ein teures NFT als Avatar aufweist, zeigt, dass er dazugehört.
- Entwickler von Kryptowährungen und Influencer fungieren hierbei als „Priester und Propheten“ der Crypto Bro Gemeinschaften, die sie wie Herden halten und melken.

Regulierung der Krypto-Asset Märkte

Allgemeines, USA, EU



Source: https://complyadvantage.com/insights/cryptocurrency-regulations-around-world/ [Retrieved March 17, 2022]

Generell:

- ✓ Die Regulierung entwickelt sich, von Auflagen bis zum völligen Verbot reicht.
- ✓ Kryptowährungen werden meist als finanzielle Vermögenswerte betrachtet und nicht von Zentralbanken, sondern von Finanzmarktaufsichtsbehörden reguliert.
- ✓ Viele Länder arbeiten daran, neue regulatorische Rahmenbedingungen zu schaffen, um bestehende Kryptowährungen, zukünftige Initiativen wie Diem und andere Entwicklungen wie NFTs und CBDCs zu berücksichtigen.

Die Perspektive der Regulierungsbehörden Allgemeines

- Das regulatorische Problem betrifft nicht nur Offshore-Börsen und anonyme Kryptowährungsprojekte. Es ist auch ein Problem, wenn die Börsen, Investoren und Projekteigentümer bekannt sind und sich in Ländern befinden, in denen die Regulierungsbehörden sie erreichen können. Die Reaktion von Staaten und Regulierungsbehörden ist unterschiedlich. Einige Staaten greifen auf ein vollständiges Verbot von Aktivitäten im Zusammenhang mit Kryptowährungen zurück, einschließlich Mining, Handel und Eigentum.
- Dies in China der Fall, das bis zum letzten Jahr ein globales Zentrum des Kryptowährungs-Minings war. Andere Länder verlangen von Kryptowährungsbesitzern und -börsen, dass sie Identitäten und Bestände preisgeben, während einige Länder noch keine Form der Regulierung durchgesetzt haben.
- Kryptowährungen werden kaum als gesetzliches Zahlungsmittel anerkannt. In einigen Ländern (Mexiko, Argentinien, Brasilien, Venezuela und Chile) werden Kryptowährungen vom einigen Einzelhändlern allgemein als Zahlungsmittel akzeptiert.
- In den meisten Ländern, in denen der Handel erlaubt ist, müssen sich die Börsen bei den lokalen Behörden registrieren. Da Kryptowährungen nicht als Geld anerkannt werden, werden sie in der Regel nicht von den Zentralbanken, sondern von den Finanzmarktbehörden, wie der SEC in den USA oder der BaFin in Deutschland, reguliert. In einigen Ländern verlangt die Regulierung, dass Eigentümer offengelegt werden.
- Einige Länder, darunter Indien, arbeiten noch an einem ersten Regulierungsrahmen.
- Viele Länder, darunter China, die USA, die EU, Japan, aber auch supranationale Institutionen wie IWF, EZB etc. arbeiten an eigenen digitalen Währungen, sogenannten Central Bank Digital Currencies (CBDCs).

Die Perspektive der Regulierungsbehörden

USA

- Die Vereinigten Staaten, die seit jeher eine führende Rolle bei der Definition von Standards für die Finanzmarktregulierung und die Durchsetzung von Regeln spielen, haben das Thema entschieden auf die öffentliche Tagesordnung gesetzt. Sowohl der SEC-Vorsitzende Gary Gensler als auch der CFTC-Vorsitzende Rustin Behnam haben offen für mehr Regulierung und Kontrolle der Krypto-Asset-bezogenen Märkte gedrängt.

- In einer Anhörung mit dem US-Senat am 9. Februar 2022 sprach der CFTC-Vorsitzende Behnam das Thema mit folgenden Worten an: "Wir haben eine Reihe von börsengehandelten Derivaten auf Krypto-Assets an mehreren registrierten CFTC-Börsen, aber die Sichtbarkeit des zugrunde liegenden Marktes ist höchstens begrenzt. […] Im Wesentlichen handelt es sich um einen unregulierten Markt [...] es gibt so vieles, was wir aufgrund dieser begrenzten Autorität nicht sehen können." Nichtsdestotrotz hat die CFTC seit 2021 in mehreren Fällen Maßnahmen gegen Kryptowährungsbörsen und -unternehmen ergriffen, darunter die Krypto-Derivatebörse BitMEX, die sich bereit erklärte, eine Strafe in Höhe von 100 Mio. USD zu zahlen, sowie Tether und BitFinex, die die Kommission im Oktober mit einer Geldstrafe von 42,5 Mio. USD belegte.

- In einer öffentlichen Erklärung, die auf der CFTC-Website zu lesen ist, macht Behnam eine analytische Aussage über den Markt für digitale Vermögenswerte, die Kryptowährungen und ihre Derivate, aber auch andere Formen von Vermögenswerten wie NFTs umfasst. Dies ist eine repräsentative Ansicht, die der Art und Weise entspricht, wie Regulierungsbehörden in anderen Ländern die Krypto-Asset-Märkte betrachten.* (Volltext auf der Kursplattform verfügbar)

- Es besteht kein Zweifel, dass viele Nationen bald neue regulatorische Rahmenbedingungen für die Krypto-Asset-Märkte implementieren werden. Tatsächlich publizierte die CFTC am 9. März 2022 nach der Veröffentlichung einer Executive Order on Ensuring Responsible Development of Digital Assets (Volltext auf der Kursplattform verfügbar) des Weißen Hauses.**

- In einer Rede, die am 4. April 2022 an der University of Pennsylvania Law School gehalten wurde, erklärte der SEC-Vorsitzende Gary Gensler, dass er die SEC-Mitarbeiter auffordert, Regulierungs- und Kontrollmechanismen für das gesamte Spektrum der marktbezogenen Krypto-Asset-Aktivitäten zu entwickeln und vorzuschlagen, einschließlich zentralisierter und dezentraler Plattformen, stabiler Münzen und anderer Formen von Token.

* **"…The Digital Asset Market**

There are now hundreds of thousands of unique digital assets in circulation with a combined market capitalization of approximately $2 trillion. At the center of this burgeoning industry are the trading platforms where most investors access this market. Several of these platforms operate on a global scale and host marketplaces for trading both in the underlying digital assets, as well as derivative contracts referencing those assets. According to public data, every month in 2021 except one saw over $1 trillion in monthly trading volume in the digital asset cash market, with a high of $2.23 trillion in trading volume in May 2021. And the derivatives market is even larger, with notional exchange volumes in just bitcoin futures surpassing those numbers.

Although the CFTC's core responsibility is regulating the commodity derivatives market, there are several unique elements of the digital asset commodity cash market that distinguish it from other cash commodity markets, suggesting it would benefit greatly from CFTC oversight. For example:

- Unlike most cash commodity markets, which are dominated by wholesalers and large financial institutions facilitating the transfer of commodities for commercial use and consumption, the cash market for digital assets is currently characterized by a high number of retail investors mostly engaged in price speculation.
- The speculative fervor around digital assets, frequently feeling like a modern gold rush, has led many investors to regularly take on high levels of leverage when trading, leading to heightened price volatility, often exacerbated by cascading liquidations during price downturns.
- Most investors in the cash market entrust their digital assets to the platforms upon which they trade, failing to differentiate this type of custody arrangement from that offered by the traditional regulated banking industry. The technical complexities around securing and transacting in digital assets, particularly issues around custody, have resulted in numerous platforms losing funds to hacks, exploits, and poor cyber security.

I believe these unique characteristics, combined with the growing size and customer, operational, and potential future financial stability risks associated with the cash market necessitate a proactive federal regulatory approach to ensure that the standards that American investors have come to expect from our financial markets are equally present in digital markets.

I also believe that in order to reach the lofty goals that many of the technology's most ardent proponents advocate, it is important that we find ways to sensibly bring this emerging market within the regulatory fold. If in fact the future global economy holds a place for digital assets, tokenization, blockchain technology, decentralized finance, and other elements of the FinTech driven ecosystem, then the need to uphold American leadership and stewardship of this technology is clear. Critical issues, such as national security, trade, and effectively addressing climate change risks, to name a few, will also be at stake. …"

Testimony of Chairman Rostin Behnam Regarding "Examining Digital Assets: Risks, Regulation, and Innovation

** **Washington, D.C. —** Commodity Futures Trading Commission Chairman Rostin Behnam today released the following statement on the Executive Order on Digital Assets signed by President Biden today:

"The Executive Order signed by President Biden today marks a significant step. The EO will ensure greater cooperation and coordination between various cabinet-level agencies, the independent market regulators and prudential regulatory bodies. With increased adoption and growth in the digital asset market comes the need for increased education and outreach to protect against new and emerging risks. President Biden is right to emphasize the need for increased customer education and consumer protection, while combating illicit activity and safeguarding financial stability."

-CFTC-

Die Perspektive der Regulierungsbehörden EU

- In einer 2019 gestarteten Initiative entwickelt die EU einen Vorschlag für den Regulierungsrahmen von Krypto-Assets für ihre Mitglieder. Dies führte zu einem vorgeschlagenen Regulierungsrahmen, der 2020 fertiggestellt und dem EU-Parlament vorgelegt wurde (Volltexte auf der Kursplattform verfügbar). Die Gründe und Ziele des Vorschlags sind im Memorandum des Dokuments festgelegt, von dem ein Auszug hierin zu finden ist*
- Der 168 Seiten lange EU-Vorschlag deckt eine Vielzahl von Aspekten ab, insbesondere den Vorschlag von Regulierungsoptionen, bei denen zwischen verschiedenen Arten von Krypto-Assets unterschieden wird. Während er eindeutig die Anfälligkeit von Verbrauchern und Investoren im Kontext der Krypto-Asset-Märkte aufzeigt, berücksichtigen der Vorschlag und die Folgenabschätzung auch die Perspektive und die legitimen Interessen der Krypto-Asset-Industrie, den Wert der Nichtbankenfinanzierung zur Förderung der Geschäftsentwicklung sowie die Kosten der Regulierung.
- Der EU-Vorschlag konzentriert sich nicht nur auf die Perspektive einer Regulierungsbehörde, sondern wägt Risiken, Kosten und Nutzen für Bürger, Staaten und Privatunternehmen ab.
- Es gibt einen bemerkenswerten Fokus auf die Differenzierung des regulatorischen Ansatzes basierend auf der Art der Kryptowährung (stabil vs. instabil, offene vs. geschlossene Blockchain) in Bezug auf DLT-basierte Plattformen und Modelle.
- Während die Vorschläge von den Mitgliedstaaten überprüft werden, ist es sicher, dass es einen allgemeinen Konsens unter den Staaten für eine Regulierung gibt, und es ist zu erwarten, dass eine solche Regulierung in den kommenden Jahren in der EU Rechtsform annehmen wird.

- **Reasons for and objectives of the proposal**

This proposal is part of the Digital Finance package, a package of measures to further enable and support the potential of digital finance in terms of innovation and competition while mitigating the risks. It is in line with the Commission priorities to make Europe fit for the digital age and to build a future-ready economy that works for the people. The digital finance package includes a new Strategy on digital finance for the EU financial sector with the aim to ensure that the EU embraces the digital revolution and drives it with innovative European firms in the lead, making the benefits of digital finance available to European consumers and businesses. In addition to this proposal, the package also includes a proposal for a pilot regime on distributed ledger technology (DLT) market infrastructures, a proposal for digital operational resilience, and a proposal to clarify or amend certain related EU financial services rules.

One of the strategy's identified priority areas is ensuring that the EU financial services regulatory framework is innovation-friendly and does not pose obstacles to the application of new technologies. This proposal, together with the proposal on a DLT pilot regime, represents the first concrete action within this area.

Crypto-assets are one of the major applications of blockchain technology in finance. Since the publication of the Commission's Fintech Action plan, in March 2018, the Commission has been examining the opportunities and challenges raised by crypto-assets. Following a big surge in the market capitalisation of crypto-assets during 2017, in December 2017, Executive Vice-President Dombrovskis, in a letter addressed to the European Banking Authority (EBA) and the European Securities and Markets Authority (ESMA), urged them to reiterate their warnings to investors. In the 2018 FinTech Action plan, the Commission mandated the EBA and ESMA to assess the applicability and suitability of the existing EU financial services regulatory framework to crypto-assets. The advice, issued in January 2019, argued that while some crypto-assets could fall within the scope of EU legislation, effectively applying it to these assets is not always straightforward. Moreover, the advice noted that provisions in existing EU legislation may inhibit the use of DLT. At the same time, the EBA and ESMA underlined that – beyond EU legislation aimed at combating money laundering and terrorism financing – most crypto-assets fall outside the scope of EU financial services legislation and therefore are not subject to provisions on consumer and investor protection and market integrity, among others, although they give rise to these risks. In addition, a number of Member States have recently legislated on issues related to crypto-assets leading to market fragmentation.

A relatively new subset of crypto-assets – the so-called 'stablecoins' – has recently emerged and attracted the attention of both the public and regulators around the world. While the crypto-asset market remains modest in size and does not currently pose a threat to financial stability, this may change with the advent of 'global stablecoins', which seek wider adoption by incorporating features aimed at stabilising their value and by exploiting the network effects stemming from the firms promoting these assets.

Given these developments and as part of the Commission's broader digital agenda, President Ursula von der Leyen has stressed the need for "a common approach with Member States on cryptocurrencies to ensure we understand how to make the most of the opportunities they create and address the new risks they may pose". While acknowledging the risks they may present, the Commission and the Council also jointly declared in December 2019 that they "are committed to put in place a framework that will harness the potential opportunities that some crypto-assets may offer". More recently, the European Parliament is working on a report on digital finance, which has a particular focus on crypto assets.

To respond to all of these issues and create an EU framework that both enables markets in crypto-assets as well as the tokenisation of traditional financial assets and wider use of DLT in financial services, this Regulation will be accompanied by other legislative proposals: the Commission is also proposing a clarification that the existing definition of 'financial instruments' - which defines the scope of the Markets in Financial Instruments Directive (MiFID II) - includes financial instruments based on DLT, as well as a pilot regime on DLT market infrastructures for these instruments. The pilot regime will allow for experimentation within a safe environment and provide evidence for possible further amendments.

This proposal, which covers crypto-assets falling outside existing EU financial services legislation, as well as e-money tokens, has four general and related objectives. The first objective is one of legal certainty. For crypto-asset markets to develop within the EU, there is a need for a sound legal framework, clearly defining the regulatory treatment of all crypto-assets that are not covered by existing financial services legislation. The second objective is to support innovation. To promote the development of crypto-assets and the wider use of DLT, it is necessary to put in place a safe and proportionate framework to support innovation and fair competition. The third objective is to instil appropriate levels of consumer and investor protection and market integrity given that crypto-assets not covered by existing financial services legislation present many of the same risks as more familiar financial instruments. The fourth objective is to ensure financial stability. Crypto-assets are continuously evolving. While some have a quite limited scope and use, others, such as the emerging category of 'stablecoins', have the potential to become widely accepted and potentially systemic. This proposal includes safeguards to address potential risks to financial stability and orderly monetary policy that could arise from 'stablecoins'.

Über die Natur von Bitcoin

Ist Bitcoin Geld?

- Jevons führte die Funktionen des Geldes ein. Es gibt einen Konsens unter allen Experten aus allen Bereichen über die ersten beiden Funktionen, viele bestehen auch auf der Bedeutung der letzten beiden, aber wir werden sie für unseren Zweck als sekundär betrachten..
- Zwei Hauptfunktionen:
  - ✓ Bitcoin ist kein Tauschmittel, es ist ein Vermögenswert, der ausgetauscht wird.
  - ✓ Bitcoin ist kein übliches Wertmaß. Menschen messen nicht den Wert von Waren in Bitcoin.
- Zwei sekundäre Funktionen:
  - ✓ Bitcoin ist kein Wertmaßstab. Bitcoin wird nicht verwendet, um aufgeschobene Zahlungen (Kredit) zu leisten.
  - ✓ Ist Bitcoin ein Wertspeicher??
- Allein aus diesen Tatsachen können wir schließen, dass Bitcoin derzeit kein Geld ist. Aber könnte es Geld werden??

Was ist mit den Nebenfunktionen?

- Betrachtet man abgeleitete Funktionen und Nebenmerkmale, so können wir in Bezug auf Bitcoin davon ausgehen, dass:
  - **Übertragbarkeit**. Als rein digitales Gut ist es einfach, Bitcoin schnell und einfach zu bewegen. Aber die Blockgenerierungs-mechanik (1 MB pro 10 Minuten) behindert diese grundlegende Kapazität. Das Lightning-Netzwerk behebt das Problem nur teilweise.
  - **Teilbarkeit/Fungibilität**. Bitcoin ist leicht fungibel und bis in kleinste Mengen teilbar (1 Satoshi = 10^{-8} BTC).
  - **Verfügbarkeit**. Schwer einzuschätzen. Auf der einen Seite werden wahrscheinlich nie mehr als 20 Millionen Bitcoins im Umlauf sein (Verluste zählen), aber wir sollten eher über 2 Billiarden Satoshi sprechen, das wäre die Währungsbasis. Nicht genug für eine globale Wirtschaft. Würde es für b-to-c und c-to-c ausreichen? Für eine Zeit Vielleicht.
  - **Stabilität**. Derzeit ist Bitcoin alles andere als stabil, es ist volatiler als durchschnittliche Aktien, und die Intraday-Volatilität bringt es in den Bereich der kurzfristigen Derivate und spekulativen Vermögenswerte.
  - **Sicherheit**. Theoretisch ist das kryptografische System sehr sicher, leidet aber unter der Komplexität für die meisten Benutzer und unter der Tatsache, dass es seit 2009 nicht mehr aktualisiert wird. Derzeit nicht gegeben, wegen der Praxis, Bitcoins über Vermittler (Börsen) zu kaufen, anstatt Cold Wallets zu verwenden. Es laufend Fälle von Diebstählen. Ein weiterer Aspekt ist die relative Komplexität des Systems. Wenn Sie Ihren privaten Schlüssel verlieren, verlieren Sie die Bitcoins unwiderruflich.

Bitcoin ist keine Währung

- Man kann ohne Zweifel sagen, dass Bitcoin weit davon entfernt ist, den Ansprüchen einer Währung gerecht zu werden.
- Eine Beobachtung der Kursentwicklungen, der Strukturen der Mining-Industrie sowie des Verhaltens der Investoren und Märkte, lässt nicht Mal ansatzweise erkennen, dass sich das Token in Richtung Währung entwickeln würde.
- Bitcoin ist, außer zur Finanzierung krimineller Aktivitäten, kaum als Zahlungsmittel verwendet.
- Sollte sich Bitcoin dennoch so entwickeln, dass es eine Funktion als Währung einnehmen würde, dann ist damit zu rechnen, dass nationale und supranationale Regulierungsbehörden nicht tatenlos zusehen. Das kann sehr eindeutig am gescheiterten Libra/Diem Projekt von Meta erkannt werden. Obwohl das Projekt durch ein mächtiges Konsortium gestützt war, musste Meta es aufgeben, nachdem international Politik und Zentralbanken auf die Barrikaden gingen.
- Ein nicht vollständige Liste der Probleme, für die Bitcoin eine Antwort finden muss, um langfristig erfolgreich als Währung fungieren zu können, würde eine Auseinandersetzung mit folgenden Fragestellungen voraussetzen:

Hochvolatil (Spielball der Spekulanten)
Hochgradig deflationär (max. 21 Mio., davon bereits > 3 Mio. verloren)
Mangel an Liquidität (Blockgenerierungszeit)
Kein Käuferschutz
Praktisch kaum für reale Einkäufe verwendet (< 1%)
Kein Anlegerschutz (privater Schlüssel verloren = Bitcoins weg)
Kaum Anerkennung durch öffentliche/staatliche Behörden
Struktur und Interessen des Mining-Industrie
Bevorstehende Regulierung/Verbot im Erfolgsfall (vgl. Aufschrei bei Libra)
Verwendung zur Finanzierung von (nicht nur) Internet-Kriminalität
Regelmäßige Fälle von Betrug und Diebstahl von Konten auf Börsen
Eigentumsverteilung (<0,4% der Adressen besitzen mehr als 85%, >51% Adressen besitzen nur 0,02%)

Bitcoin ist Zweck, nicht Zahlungsmittel

"... eine dominante Gruppe [...] nutzt Bitcoin als Investition, etwa ein Drittel aller Bitcoins werden von Investoren gehalten [...] die nur Bitcoins erhalten und diese niemals an andere senden“

(Baur et al., 2018, pp 8-10)

"[Die Tatsache, dass viele Benutzer Bitcoins offline speichern] ist vielleicht der beste Indikator dafür, wie Bitcoin und andere digitale Währungen als Goldspeicher behandelt werden.”

- *(Brennan, et al., 2018, p. 21)*

Bitcoin, Digitales Gold?

- Seltenheit (21 Millionen Maximalmenge)
- Langlebig, nicht verderblich (digitale Daten verderben nicht)
- Generierungsmechanik, Mining (prinzipiell unabhängig von politischem Einfluss oder Geldpolitik, losgelöst von Konjunkturzyklen)
- Verhalten einer beträchtlichen Anzahl von Anlegern die Bitcoins kaufen und halten
- Hervorgehobene Rolle und Aura innerhalb der Krypto-Assets und Krypto-Asset Community als erstes und größtes Krypto-Asset
- Design (goldene Münze) & Narrativ "Das stetige Hinzufügen einer konstanten Menge an neuen Münzen ist analog zu Goldminenarbeitern, die Ressourcen aufwenden, um Gold in den Umlauf zu bringen." (Nakamoto, 2008, S. 4)

Besonderheiten von Bitcoin in Bezug auf den Wertspeicher

- Mehrere bereits erwähnte Eigenschaften zeichnen Bitcoin aus, die einen Einfluss darauf haben könnten, inwiefern sich Bitcoin (BTC) langfristig zu einem Wertspeicher entwickeln könnte.
  - Bitcoin hat keine physische Repräsentation. Das kann ein starker Nachteil sein, wenn wir einen Wertspeicher als Warengeld mit einem inneren Wert definieren. Aber wenn man sieht, wie virtuelle Ökonomien in einer bestimmten geschlossenen Umgebung funktionieren und unter Berücksichtigung der Idee von NFTs, ist dieser fehlende intrinsische Wert möglicherweise kein solches Hindernis..
  - Digital zu sein bietet Vorteile gegenüber Gold. BTC ist sehr leicht teilbar und fungibel, Sie müssen nicht schmelzen, es hat einen größeren Brocken bekommen oder es in kleinere Stücke geteilt. Sie brauchen auch keinen Experten, um die Reinheit zu garantieren oder ihren Wert zu bestimmen.
  - BTC kann es einfach und sofort überall hin übertragen werden, auch in den größten Mengen, ohne dass ein Transport oder der Aufwand von Ressourcen aufgrund von Gewicht, Diebstahlrisiko, Versicherung usw. erforderlich ist.
  - Allerdings ist der bisherige Track Record von BTC und das Image der Krypto-Assets allgemein durch unzählige Betrugsfälle, Verwendung für kriminelle Aktivitäten, Marktmanipulationen, usw. so, dass Vertrauen nicht wirklich begründet wäret. Das ist für eine Wertspeicherfunktion nicht angemessen.
  - BTCs Zukunft ist auch vom Verhalten und von den Entscheidungen von Regulierungsbehörden abhängig. Auch diese Unsicherheit trübt die Vorstellung der Nutzung von BTC als Wertspeicher, das eine langfristige Sicherheit voraussetzt.

Bitcoin ist ein bemerkenswertes Phänomen

1. Als Vorreiter und wegen seiner Resilienz.
2. Es stellte das Verständnis von Geld in Frage und zwingt uns, unsere Definition von Geld zu überdenken.
3. Es ist sicher kein Geld, was es werden wird, ist noch ungewiss.
4. Die Fehler und Mängel in seinem Design sind wichtige Erkenntnisse für zukünftige Entwicklungen.
5. Es machte es möglich, dass Initiativen wie Libra / Diem und CDBCs jetzt wie realistische Bemühungen erscheinen.
6. Kryptowährungen werden bei der Entwicklung von NFT, SBT, dem Metaverse (virtuelle Ökonomien) an Relevanz gewinnen werden.

ENDE