Bitcoin – besseres Geld für eine bessere Welt

Wichtige Konzepte im Überblick

Leo Mattes

VORSTELLUNG – LEO MATTES

Technologiemanagement & meine Begeisterung:

- Vision für den technischen Fortschritt: Eine Infrastruktur mit „nahezu unendlicher“ Produktivität
- Entwicklung und Mitgestaltung einer dezentralen, vernetzten, intelligenten, automatisierten Energie-Informations-Transport-Geld Infrastruktur
- Interesse für den technischen Fortschritt, Produktivitätswachstum und Disruptionen und damit einhergehende Chancen & Pfadabhängigkeiten
- Wissenschaft der Praxeologie/österreichische Schule der Nationalökonomie: Gesetzmäßigkeiten über das Handeln gelten heute und in Zukunft
- Geld als eine sich verändernde Technologie, die für die Arbeitsteilung, Kapitalakkumulation und eine fortschrittliche Gesellschaft extrem wichtig ist
- Betrachtung von komplexen, dynamischen und lebendigen Systemen bzgl. Fragilität und Antifragilität
- Endliche und unendliche Spiele als Framework zur Zielfindung und Beschreibung der Situation

Meine Erfahrungen mit Geldtheorie & Bitcoin:

- Buch über die Gesetzmäßigkeiten des Handelns: „Eine Revolution der Denkart“
- Blog über Geldtheorie, Geldgeschichte und deren Auswirkungen auf eine Gesellschaft
- Mitglied in der Einundzwanzig Community – Podcast, Meetups, Diskussionspanels, Vorträge
- Inhaber der Seite www.fixyourmoney.space
- Zusammenstellung der Pump it up! Bitcoin-Playlist
- Aktiv in der Bitcoin Community seit 2019

Leo Mattes
Kontakt:
info@leo-mattes.com
Website:
www.leo-mattes.com
Twitter:
@lemalive

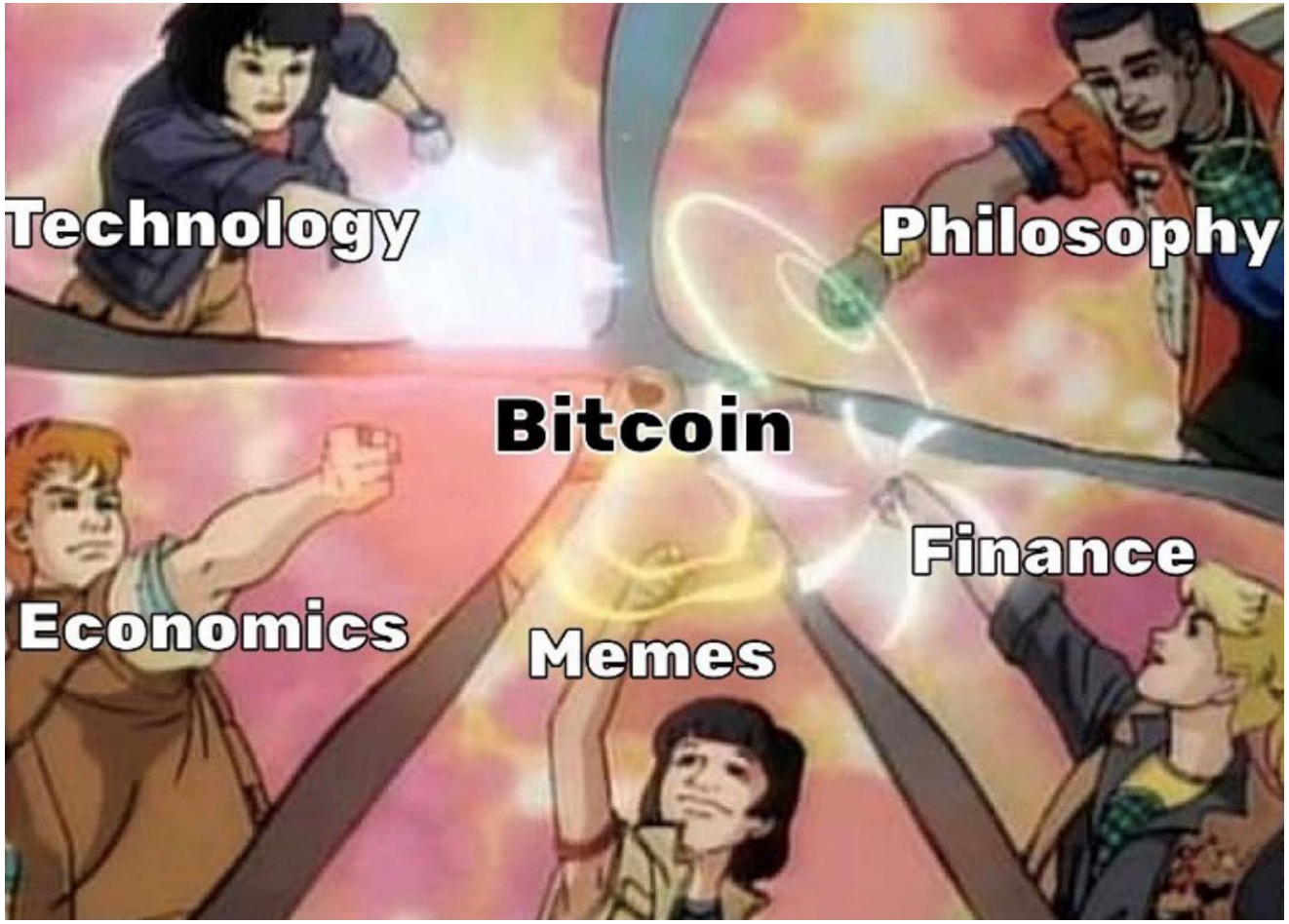
ZIEL FÜR DIESEN VORTRAG

Wie sieht die Welt aus, wenn wir das Individuum in den Mittelpunkt des Handelns stellen?

Was ist Geld? Was ist Bitcoin und wie funktioniert die Blockchain?

Was sind die wichtigsten Konzepte von Bitcoin?

Wie verändert eine fixe Geldmenge die Welt?



AGENDA

1 **DER MENSCH HANDELT**

2 **FUNKTIONEN UND EIGENSCHAFTEN VON GELD**

3 **WAS SIND DIE EIGENSCHAFTEN VON GOLD UND ZENTRALBANKGELD?**

4 **GRUNDLAGEN BITCOIN – WAS IST BITCOIN? WIE FUNKTIONIERT BITCOIN?**

5 **DAS ORACLE PROBLEM und DAS BLOCKCHAIN TRILEMMA und PROOF OF WORK**

6 **AUSWIRKUNGEN AUF DIE GESELLSCHAFT**

7 **FAZIT & WEITERFÜHRENDE INFORMATIONEN**

1. DER MENSCH HANDELT

Methode der Praxeologie/Österreichischen Schule:

- Das Individuum handelt nach seinen Ideen und zeigt Präferenzen, um mit Mitteln Ziele zu erreichen.
- Ein Bottom-up Ansatz: Vom Individuum aus baut sich die Gesellschaft auf

Das Handelsaxiom:

„Der Mensch handelt.“

Marktwirtschaftliches Vorgehen:

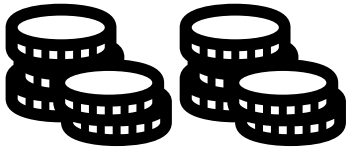
- Menschen respektieren Eigentum, sparen ist möglich
- Kooperationen bringen beiden Seiten einen Vorteil
- Es kommt zu Tauschvorgängen, Preisen und **Geld**
- Wirtschaftlichkeitsrechnungen werden ermöglicht
- Preise übertragen Informationen über Knappheit und setzen Anreize zur Produktion
- Wettbewerb ermöglicht Alternativen

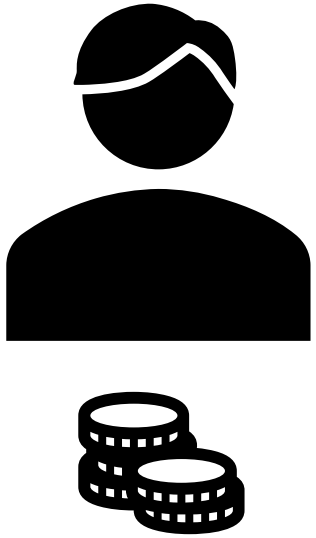
Planwirtschaftliches Vorgehen:

- Individuelle Werte und Eigentum werden nicht respektiert
- Sparen ist nicht möglich
- Es gibt keine Tauschvorgänge, sondern zentrale Ressourcenzuteilung, **keine Notwendigkeit für Geld**
- Wirtschaftlichkeitsrechnungen sind nicht möglich
- Kein Wettbewerb und Produktionsanreize

2. WAS SIND DIE HAUPTFUNKTIONEN VON GELD?

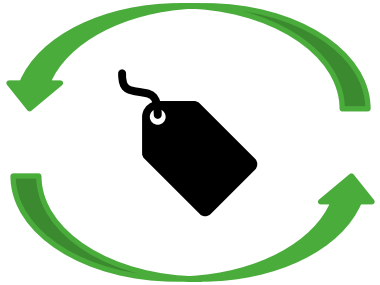
Wertspeicher

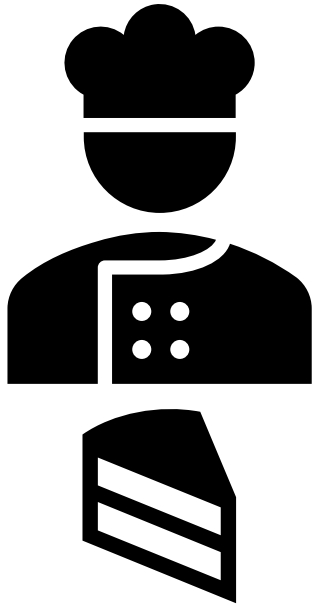


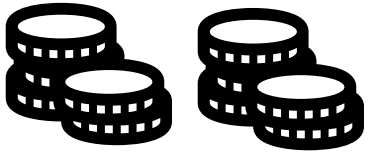


Tauschmittel

Recheneinheit







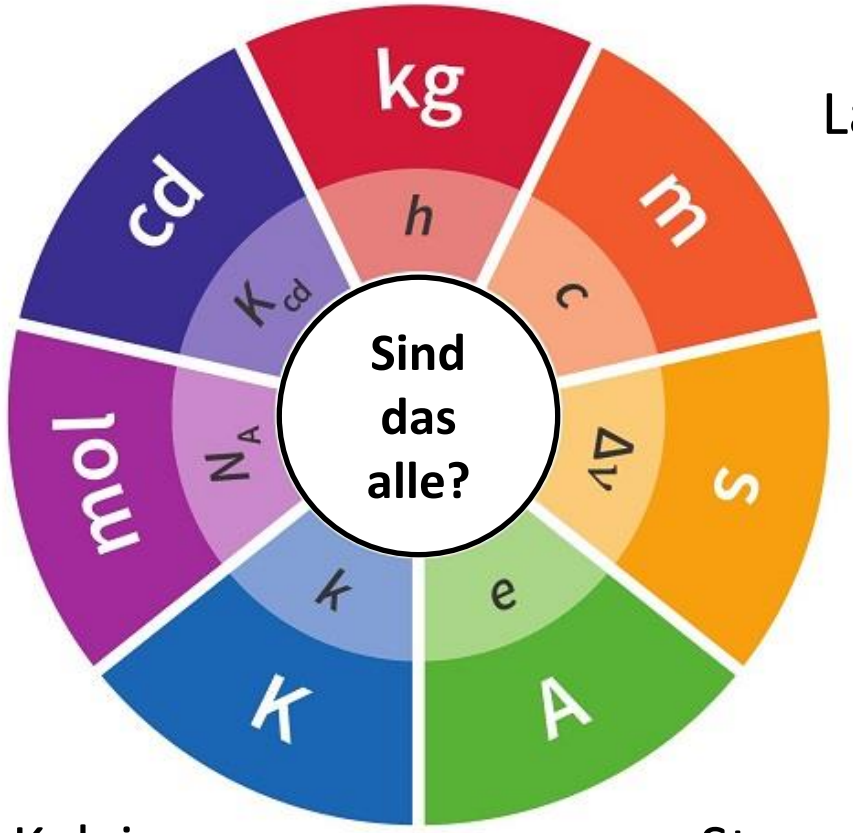
2. GELD: NICHT NUR SOZIALES KONSTRUKT - AUCH TECHNOLOGIE

2. INTERNATIONALES EINHEITENSYSTEM FÜR MESSUNGEN

Masse - Kilogramm

Lichtstärke - Candela

Länge - Meter



Stoffmenge - Mol

Zeit - Sekunde

Temperatur - Kelvin

Stromstärke - Ampere

2. ES GIBT VIELE WÄHRUNGEN - GELD IST WAS MENSCHEN NUTZEN

2. FUNKTIONEN UND EIGENSCHAFTEN VON GELD

Funktionen und Eigenschaften von Geld:

Funktionen:
- Tauschmittel (Raum)
- Wertspeicher (Zeit)
- Recheneinheit (Kalkulation)

Eigenschaften:
- Knappheit, Teilbarkeit, Transportierbarkeit, Haltbarkeit, Homogenität, …

Geldregressionstheorem:

- **Geld entsteht** nicht aus dem Nichts durch eine Regierung oder andere Entität, sondern entsteht **auf dem Markt**
- Die heutige Kaufkraft des Geldes hängt mit der Gestrigen zusammen, dies hilft uns zu verstehen, warum Geld ohne große Nachfrage für industrielle Zwecke dennoch nachgefragt wird → Tauschwert

Cantillon-Effekt:

- Die Ausweitung der Geldmenge ist nicht neutral und verteilt sich nicht gleichmäßig, sondern in Stufen über die verschiedenen Bereiche der Gesellschaft

Token/Ware oder Ledger/Datenbank:

Token/Ware:
- Physischer Gegenstand
- Dezentral gelagert
- Hardware IST das ‚Ding'
- Vertrauenswürdig, weil es real existiert
- Einzigartig
- Zeitlos

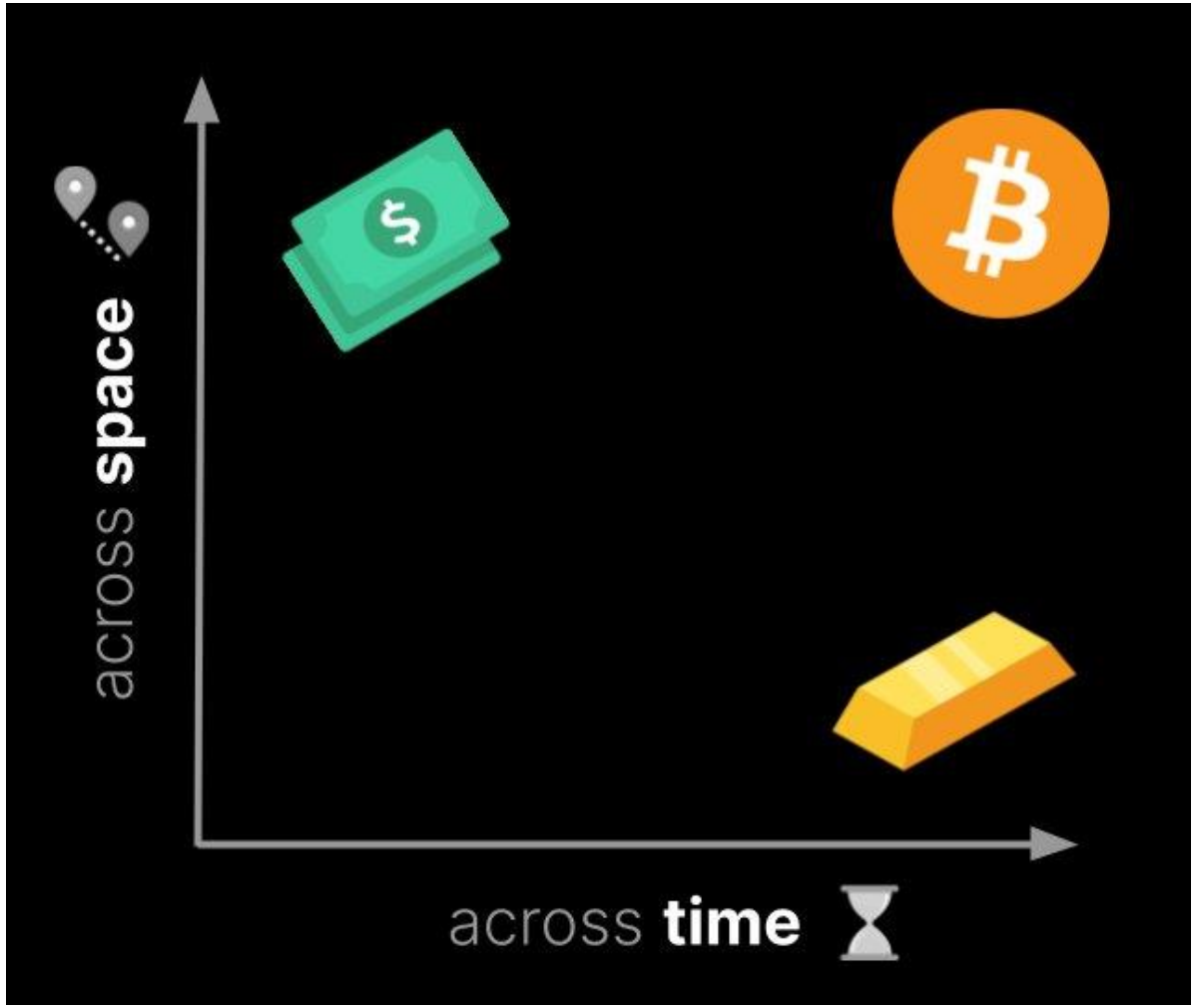
Ledger/Register:
- Datenbank aus Informationen
- Zentralisiert
- Software speichert das ‚Ding' ab
- Braucht Vertrauen
- Kopierbar
- Zeitstempel erforderlich

3. WAS SIND EIGENSCHAFTEN VON GOLD UND ZENTRALBANKGELD?

Eigenschaften von Geld	Gold	Fiat
Verifizierbarkeit	Mittel	Mittel
Homogenität	Hoch	Hoch
Transportierbarkeit	Niedrig	Hoch
Haltbarkeit	Hoch	Niedrig
Teilbarkeit	Niedrig	Mittel
Knappheit	Mittel	Niedrig
Etablierte Geschichte	Hoch	Niedrig
Zensurresistenz	Mittel	Niedrig
Transparenz	Niedrig	Niedrig
Dezentralität	Mittel	Niedrig

Zentrale Instanzen haben in der Vergangenheit immer das Geldmonopol für ihre Ziele verwendet. Die Ersparnisse und die Kaufkraft der Menschen wurde dadurch herabgesetzt.

4. BITCOIN ALS EVOLUTION : ABSOLUTE DIGITALE KNAPPHEIT



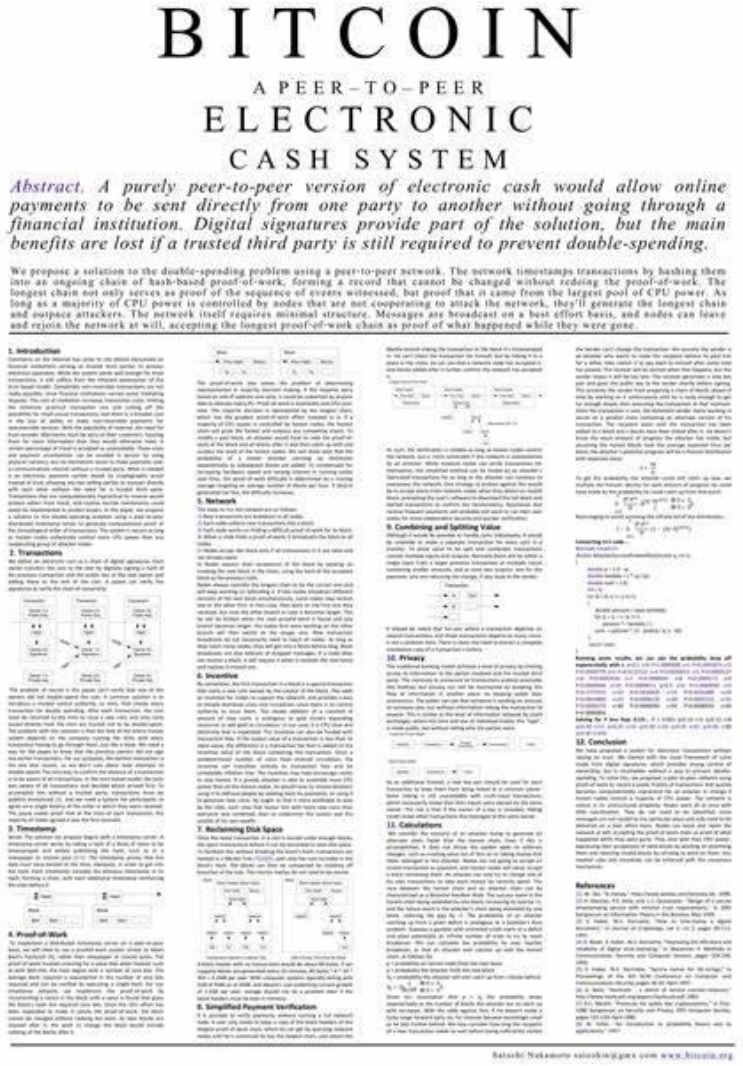
Was sind Anforderungen an “gutes Geld”?

- **absolute Knappheit**
- **digital**
- teilbar
- transportierbar
- grenzenunabhängig
- zugangsfrei
- dezentral
- open-source
- kryptographisch verschlüsselt
- kein Wechselgeld

4. GRUNDLAGEN BITCOIN – WAS IST BITCOIN?

Wer hat Bitcoin “erfunden” oder “entdeckt”?

- Die Ursprünge von Bitcoin liegen in der Cyberpunk Bewegung.
- Das so genannte White Paper von Satoshi Nakamoto (Anonym) wurde im Oktober 2008 veröffentlicht.
- Der erste „Genesis“- Block wurde am 3. Januar 2009 gemined.
- Der Amerikaner Laszlo Hanyecz kaufte am 22. Mai 2010 zwei Pizzen für 10.000 Bitcoin. Bitcoin hatte nun einen Preis.



BITCOIN

A PEER-TO-PEER ELECTRONIC CASH SYSTEM

Abstract. *A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending.*

We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

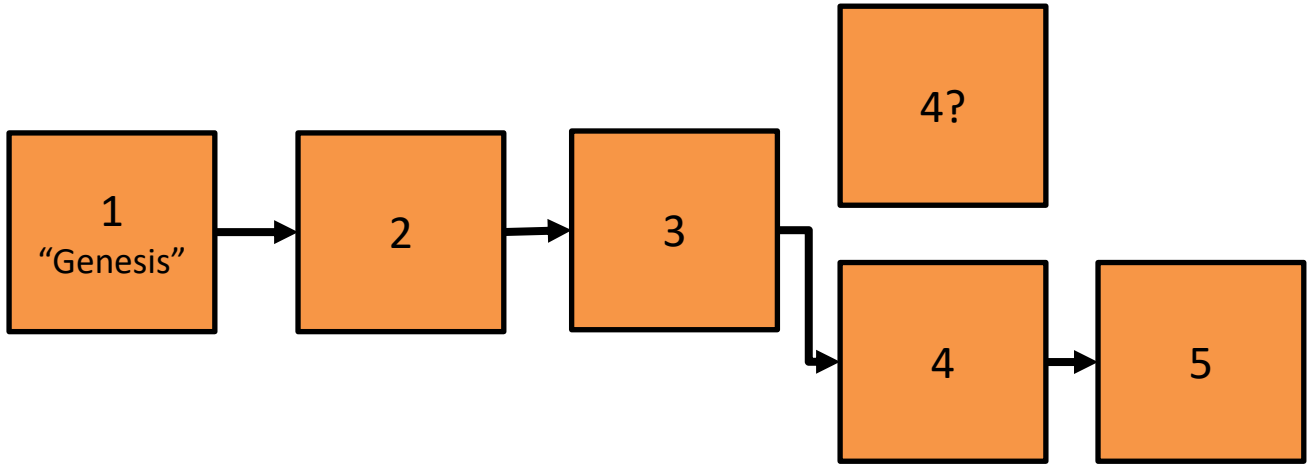
Welches Problem löst Bitcoin?

- Die Blockchain ermöglicht Peer-to-Peer Zahlungen zwischen den Teilnehmern im Netzwerk – ohne Mittelsmann
- Bitcoin löst das Double-Spend Problem
- Weil die Blöcke aufeinander aufbauen, ist es unmöglich, frühere Transaktionen zu manipulieren oder zu löschen
- Konsensmechanismus in einem dezentralen System

4. GRUNDLAGEN BITCOIN – WIE FUNKTIONIERT BITCOIN?

Block:

- Jeder Block enthält Transaktionen
- Jeder Block ist mit seinem Vorgänger kryptographisch verknüpft



Proof-Of-Work:

- Konsensmechanismus zur Verknüpfung der realen und digitalen Welt durch Energieaufwand
- Keine Kontrolle eines einzelnen durch probabilistische „Rätsel"

Blockchain/Timechain:

- Enthält alle vergangenen Transaktionen in Blöcken gebündelt
- ~alle 10 Minuten ein neuer Block

Node/Knoten:

- Speichert dezentral die Blockchain (aktuell ~400GB)
- Verifiziert alle Transaktionen
- Kann jeder von zuhause aus tun

Mining:

- Die Suche nach dem nächsten Block
- Verarbeitung der Transaktionen
- Wird mit Transaktionskosten und dem Blockreward belohnt

4. Node / Netzwerkknoten

Node:

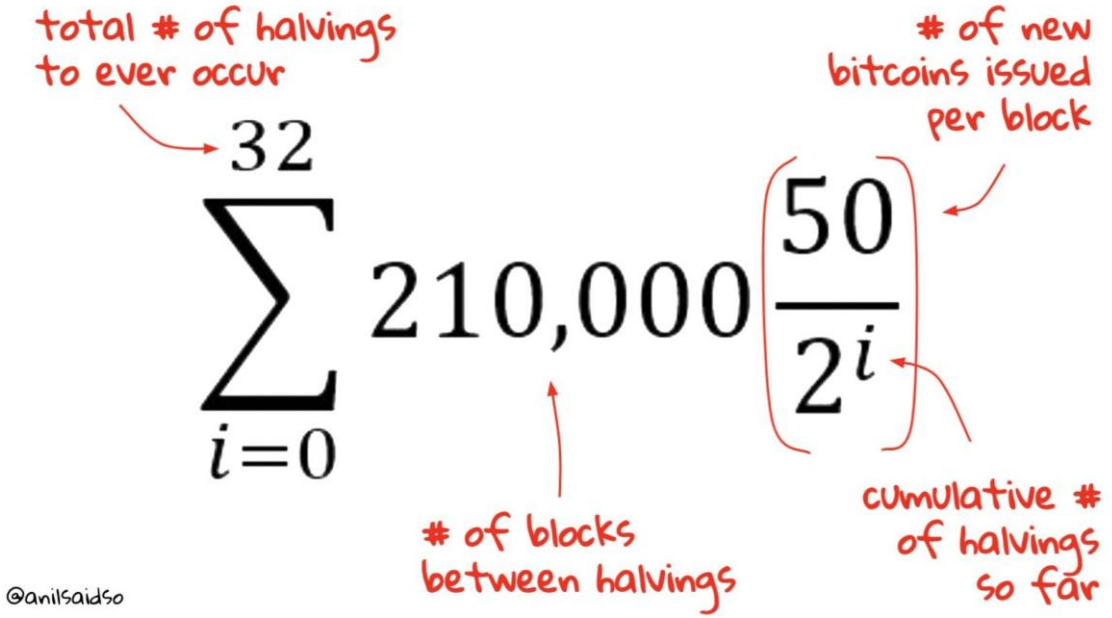
- Speichert dezentral die Blockchain (aktuell ~400GB)
- Verifiziert alle Transaktionen
- Kann jeder von zuhause mit Internetanschluss tun

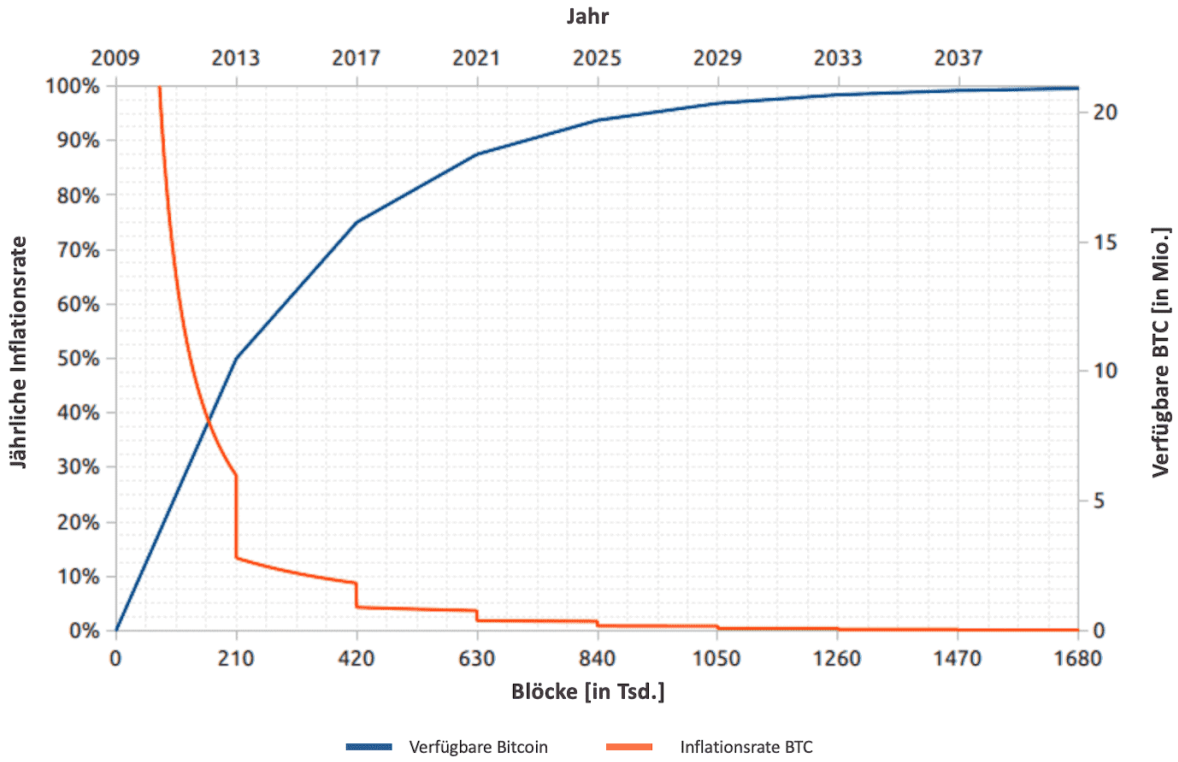
4. MINING – PROOF-OF-WORK KONSENSMECHANISMUS

Mining:

- Miner sichern das Netzwerk und eifern um den Blockreward und die Transaktionsgebühren
- Rechenzentren sind auf niedrige Energiekosten angewiesen

4. SEHR EINFACHE GELDPOLITIK – REGELN ANSTATT REGULIERER





4. GELD ALS REINE INFORMATION – DIGITALES EIGENTUM

Bitcoin Address

SHARE

1F2zD5ihusVNDFLsBueKsq3ZJ47Rvnfmds

Private Key

SECRET

L1yaxTsR8ndxghKUAtrf1dmHeo6p1zNRwXy3zyYdyABnVNVATJUv

4. WAS SIND EIGENSCHAFTEN VON GOLD, FIAT UND BITCOIN?

Eigenschaften von Geld	Gold	Fiat	Bitcoin
Verifizierbarkeit	Mittel	Mittel	Hoch
Homogenität	Hoch	Hoch	Hoch
Transportierbarkeit	Niedrig	Hoch	Hoch
Haltbarkeit	Hoch	Niedrig	Mittel
Teilbarkeit	Niedrig	Mittel	Hoch
Knappheit	Mittel	Niedrig	Hoch
Etablierte Geschichte	Hoch	Niedrig	Niedrig
Zensurresistenz	Mittel	Niedrig	Hoch
Transparenz	Niedrig	Niedrig	Hoch
Dezentralität	Mittel	Niedrig	Hoch

Jeder Mensch entscheidet für sich welches Tauschmittel, Wertspeicher und Recheneinheit er bevorzugt. Gutes Geld unterliegt der Knappheit und lässt die Preise tendenziell sinken.

5. BILD UND ABBILD – DAS ORACLE PROBLEM

Welche Eigenschaften haben Informationen?

- Sie brauchen einen Datenträger
- Die Form der Informationen/Gedanken/Ideen ist egal
- Es gibt nicht zwingend einen Bezug zur Realität

Welche Eigenschaften hat die physische Welt?

- Gegenstände, Dinge, Atome
- Form gibt Funktion vor
- Gegenstände sind die physische Realität

→ Was auf der Liste steht, muss nicht zwingen die Realität abbilden. Das Abbild ist nicht das Bild. „**The map is not the territory.“**

“The map is not the territory, the word is not the thing it describes. […].” – Alfred Korzybski

Wie macht es Bitcoin?

- Bitcoin ist ein geschlossenes System, welches nur mit den internen (on-chain) Daten arbeitet und ist somit ein unabhängiges System
- Geld als reine Information und braucht daher keine Abbild oder Verweis in die materiellen Welt
- Bitcoin bildet nicht die materielle Welt ab und möchte das auch nicht tun
- **„In Bitcoin the map is the territory.“ - Gigi**

5. GRUNDLAGEN BLOCKCHAIN – WAS IST DAS TRILEMMA?

Dezentralität:

- Blockchains werden nicht von einer einzigen Stelle verwaltet, sondern die Kontrolle über das Netzwerk wird gleichmäßig auf alle Teilnehmer verteilt/ jeder kontrolliert bei sich – **„Don‘t trust, verify.“**

Sicherheit:

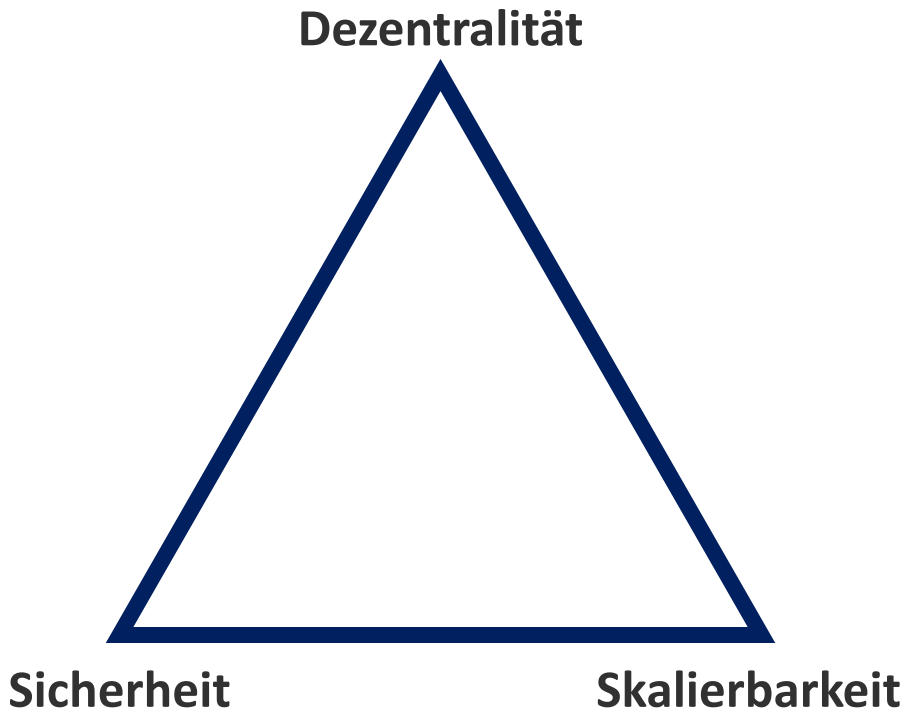
- Die Sicherheit ist das einzige grundlegende Element, das erforderlich ist, damit das Blockchain-Netzwerk tatsächlich funktioniert. Man kann mit Sicherheit sagen, dass Blockchain-Netzwerke ohne Sicherheit völlig unzuverlässig und unbrauchbar sind.

Skalierbarkeit:

- Blockchains sollten eine enorme Anzahl von Transaktionen und Nutzern unterstützen, ohne durch steigende Gebühren und Transaktionszeiten ins Stocken zu geraten.

→ Nur zwei der drei Eigenschaften können erfüllt werden

→ **Bei Bitcoin steht die Dezentralität und die Sicherheit im Fokus**

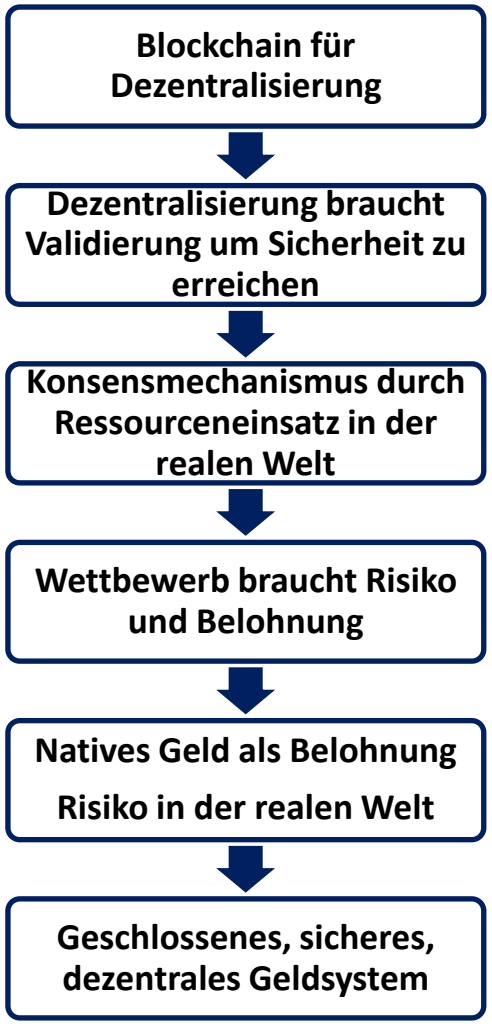


5. KONSENSMECHANISMUS: PROOF-OF-WORK

Proof-Of-Work:

- **Miner werden aus dem Netzwerk heraus bezahlt**. **Wenn ein Miner bezahlt werden will, muss er auch das fixierte Angebot der Währung von 21 Mio. durchsetzen, was das Netzwerk zusätzlich weiter in Einklang bringt**.
- Miner müssen **erhebliche Vorlaufkosten** für die Sicherung des Netzes tragen, werden aber nur bezahlt, wenn gültige Arbeit geleistet wird. Die Anreizstruktur der Währung ist so stark, dass jeder gezwungen ist sich an die Regeln zu halten, was der wichtigste Treiber des dezentralen Konsenses ist.
- **Wenn ein Miner ungültige Arbeit leistet, würde dies reale Kosten verursachen, der Miner aber im Gegenzug nicht kompensiert werden.**
- Dies ist der Grund wieso das Bitcoin Netzwerk mit steigenden Miningkosten sicherer wird. Je mehr Energie benötigt wird, um die Transaktionsgeschichte von Bitcoin zu schreiben oder neu zu schreiben, desto geringer ist die Wahrscheinlichkeit, dass ein einzelner Miner das Netzwerk untergraben könnte.

→ **Eine Blockchain muss sich aus sich selbst heraus finanzieren und somit stabilisieren. Der Wert der Währung schützt letztlich die Blockchain und die Unveränderlichkeit der Blockchain ist ein Hauptgrund für den Wert der Währung. Es ist eine sich von Natur aus selbst verstärkende Beziehung.**



6. EINE NEUE WELTSICHT DURCH DEN DREISATZ

6. AUSWIRKUNGEN FÜR DAS INDIVIDUUM UND DIE GESELLSCHAFT

Für Privatpersonen:

- Individuum steht im Mittelpunkt
- Sparen lohnt sich wieder
- Langfristige Orientierung wächst
- Alternative zu zunehmenden Zentralismus, Niedrigzins und Interventionismus
- Anlagemöglichkeit gegen Inflation
- Möglichkeit zur Altersvorsorge
- Enormes Chance-Risikoverhältnis durch Monetisierung und Netzwerkeffekte

Für Unternehmen:

- Bitcoin als Treasury Asset/Wertspeicher
- Bitcoin als Unit of Account/Recheneinheit
- Bitcoin als Medium of Exchange/Tauschmittel
- Wirtschaftlichkeitsrechnung und somit Kunden entscheiden über Fortbestehen (nicht Subventionen)
- Wettbewerb setzt Anreize für Qualität und Produktivität

Für Gesellschaft:

- Mögliche Disruption durch Trennung von Staat und Geld: Abwärtsspirale, Macht- und Einflussverlust der Institutionen & weniger Finanzierungsmöglichkeiten planwirtschaftlicher Modelle
- Wettbewerb als große regulierende Kraft bzgl. Geldmenge und Zins
- Mögliche Entwicklung hin zu dezentralen Organisationen
- Stärkung dezentraler Strukturen durch bottom-up Ansatz

Eine fixe Geldmenge, Deflation & Dezentralisierung als neues Paradigma

Was ist Geld für dich?
www.FixYourMoney.space

7. ZUSAMMENFASSUNG & AUSBLICK

Ökonomie:

- Nur das Individuum handelt; Wert ist subjektiv; Geld entsteht durch das Tun

Bitcoin:

- **Geschlossenes, dezentrales, digitales Geldsystem** mit einem glaubwürdigen Knappheitsversprechen von 21 Millionen Bitcoin mit je 100 000 000 Satoshi.
- Abgesichert über den Proof-Of-Work Konsensmechanismus über Energieeinsatz in der realen Welt
- **Teilnahme und Verifizierung für jedes Individuum** mit Internetverbindung möglich
- Uneingeschränkte **Eigentumsrechte durch Kryptographie** kommt mit großer Verantwortung
- Nur eine Blockchain ist langfristig lebensfähig und letztendlich notwendig. Jede andere Kryptowährung konkurriert um den gleichen Anwendungsfall wie Bitcoin, und zwar den des Geldes.

Neues Ökonomisches Paradigma:

- Eine fixe Geldmenge, Deflation und Dezentralisierung
- Renaissance von Eigentumsrechten, Individualität und „gutem Geld“

7. DIE KERNGEDANKEN

Geld als Technologie mit bestimmten Anforderungen

Absolute digitale Knappheit

Monetäre Recheneinheit an Konstante geknüpft

Digitales, uneingeschränktes Eigentum

Besseres Geld – bessere Welt

7. WEITERFÜHRENDE INFORMATIONEN

Bücher:

- „**Der Bitcoin Standard**“ von Saifedean Ammous
- „21 Lessons“ von Gigi
- „Alles, was Sie über die Österreichische Schule der Nationalökonomie wissen müssen“ – Rahim Taghizadegan
- Ökonomische Schriften von Ludwig von Mises, Friedrich Hayek, Murray Rothbard

Podcasts:

- „Einundzwanzig“: **Einundzwanzig, der Bitcoin Podcast**
- „Bitcoin verstehen“: **Startseite - Bitcoin verstehen**
- „Honigdachs“: **Honigdachs - Der Bitcoin-Podcast aus Leipzig | The Coinspondent**; „Mises Karma“: **Mises Karma – Der freiheitliche Podcast**
- Engl.: „What money did“, „The Bitcoin Standard podcast“

Mediatheken und Blogs:

- **Mediathek | Aprycot Media**
- **dergigi.com**
- **Blocktrainer - Bitcoin & Krypto Videos - Blockchain Wissen**
- **Ludwig von Mises Institut Deutschland (misesde.org)**
- **FixYourMoney - Mit dem Dreisatz in eine deflationäre Welt**
- **Buch: Eine Revolution der Denkart - Leo Mattes**

YouTube:

- Der Blocktrainer – Roman: **Blocktrainer - YouTube**
- Vorträge Ludwig von Mises Institut: **misesde – YouTube**
- Blockchainwelt: **Blockchainwelt – YouTube**
- **Einundzwanzig Tutorials**
- **Human B - Bitcoin Dokumentation**

Bitcoin – besseres Geld für eine bessere Welt!

Leo Mattes

www.leo-mattes.com
info@leo-mattes.com
@lemalive