Bitcoin, not Blockchain

Einführung in Bitcoin & Blockchain

Leo Mattes

EIN UND ZWAN ZIG

AGENDA

1 **VORSTELLUNG – LEO MATTES**
Wer bin ich und mit welchen Fragestellungen habe ich mich beschäftigt?

2 **WAS IST EINE BLOCKCHAIN? WAS IST BITCOIN?**
Ein Peer-to-Peer Electronic Cash System - Geld als dezentraler Ledger

3 **BILD UND ABBILD – DAS ORACLE PROBLEM**
„The map is not the territory“

4 **WARUM BRAUCHT EINE BLOCKCHAIN NATIVES GELD?**
Was ist der Anreiz das Netzwerk zu stabilisieren?

5 **WIE STABILISIERT PROOF-OF-WORK DIE BLOCKCHAIN?**
Belohnung innerhalb des Netzwerks, Risiko in der realen Welt

6 **WARUM KANN ES LANGFRISTIG NUR EIN GELD/EINE BLOCKCHAIN GEBEN?**
Geldsysteme konvergieren – „the winner takes it all“

7 **ZUSAMMENFASSUNG & WEITERE INFORMATIONEN**
Bücher, Webseiten, Podcast, Blogs, YouTube

1. VORSTELLUNG – LEO MATTES

Technologiemanagement & meine Begeisterung:

- Die Wissenschaft der Praxeologie, die Logik des menschlichen Handelns
- Das Leben aus der Sicht der Spieltheorie
- Vision für den technischen Fortschritt: Eine Infrastruktur mit „unendlicher“ Produktivität: Vision der Null-Grenzkosten Gesellschaft (NGG)
- Technologiesprünge und Pfadabhängigkeiten
- Dezentrale, vernetzte, intelligente, automatisierte Energie-Informations-Transport-Geld Infrastruktur
- Antifragile Systeme: Dezentrale fragile Teilsysteme, die untereinander im Wettbewerb stehen und somit aber das Gesamtsystem stabilisieren und verbessern

→ Blog und Buch: www.leo-mattes.com und „Eine Revolution der Denkart“

Meine Erfahrungen mit Bitcoin:

- Aktiv in der Bitcoin Community seit 2019
- Mitglied in der Einundzwanzig Community – Podcast, Meet-Ups, Diskussionspanels, Vorträge
- Geld ist eine sich verändernde Technologie, die für die Arbeitsteilung, den Wohlstandsaufbau und eine fortschrittliche Gesellschaft extrem wichtig ist
- Inhaber der Seite www.fixyourmoney.space

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

ZIEL FÜR DIESEN VORTRAG

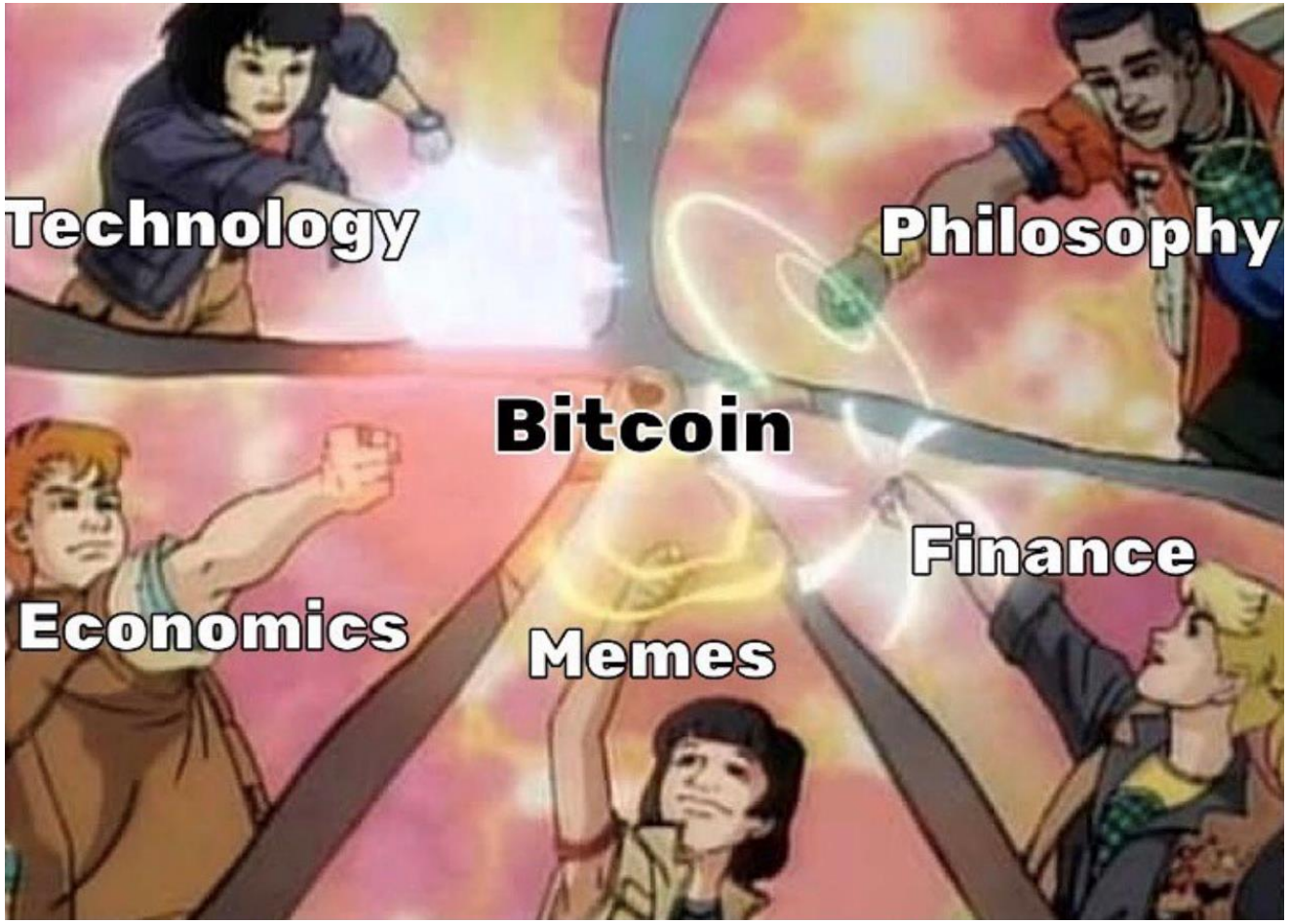
Was ist das Oracle Problem?

Wie kehrt Bitcoin dieses Problem um?

Warum ist Geld der einzige Anwendungsfall für eine Blockchain?

Warum benötigt eine Blockchain ihr eigenes Geld?

Warum benötigen wir nur ein Geld und somit nur eine Blockchain?



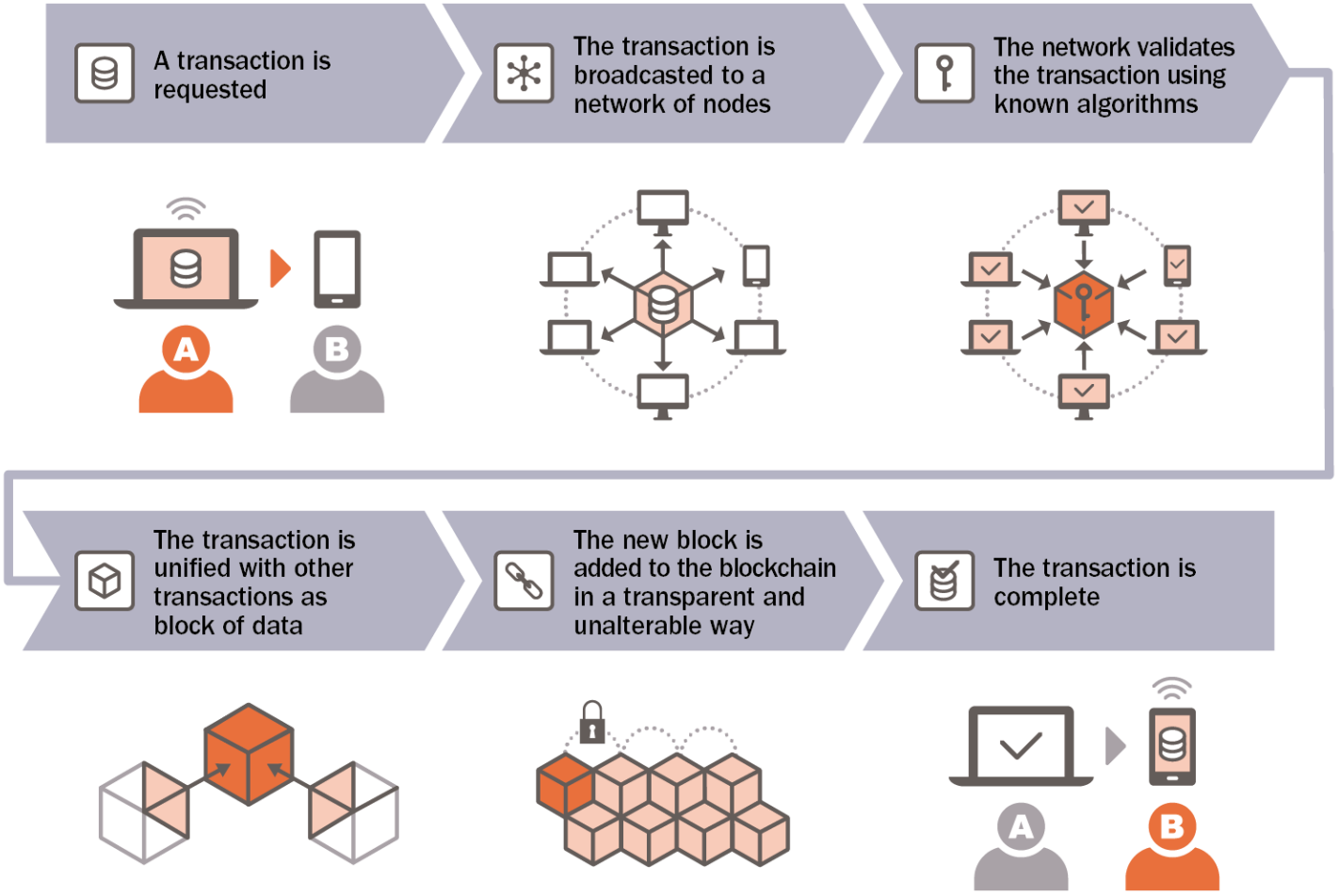
2. GRUNDLAGEN BLOCKCHAIN – WIE FUNKTIONIERT BITCOIN?

Timechain/Blockchain:

- Enthält alle vergangenen Transaktionen in Blöcken gebündelt
- Wird dezentral gespeichert

Node:

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



Mining:

- Die Suche nach dem nächsten Block wird mit Transaktionskosten und dem Blockreward belohnt
- Miner stabilisieren das Netzwerk

Proof-Of-Work:

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

2. GRUNDLAGEN BLOCKCHAIN – WAS IST DAS TRILEMMA?

Dezentralität:

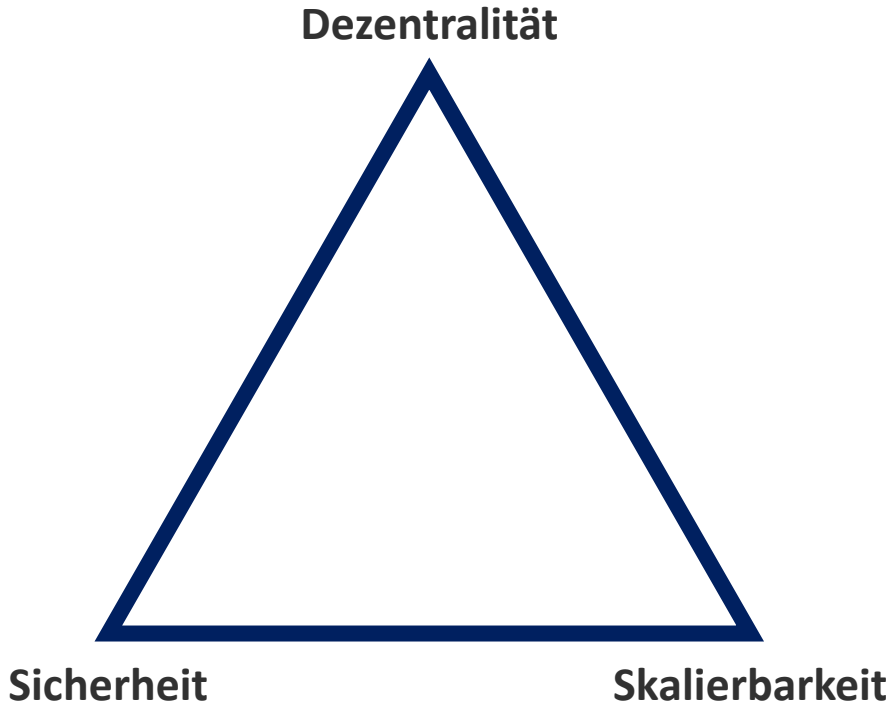
- Blockchains werden nicht von einer einzigen Stelle verwaltet, sondern die Kontrolle über das Netzwerk wird gleichmäßig auf alle Teilnehmer verteilt.

Sicherheit:

- Die Sicherheit ist das einzige grundlegende Element, das erforderlich ist, damit das Blockchain-Netzwerk tatsächlich funktioniert. Ohne Sicherheit können böswillige Akteure das Netzwerk stören, indem sie einen großen Teil der Knoten kontrollieren oder die Daten des Hauptbuchs manipulieren. 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.



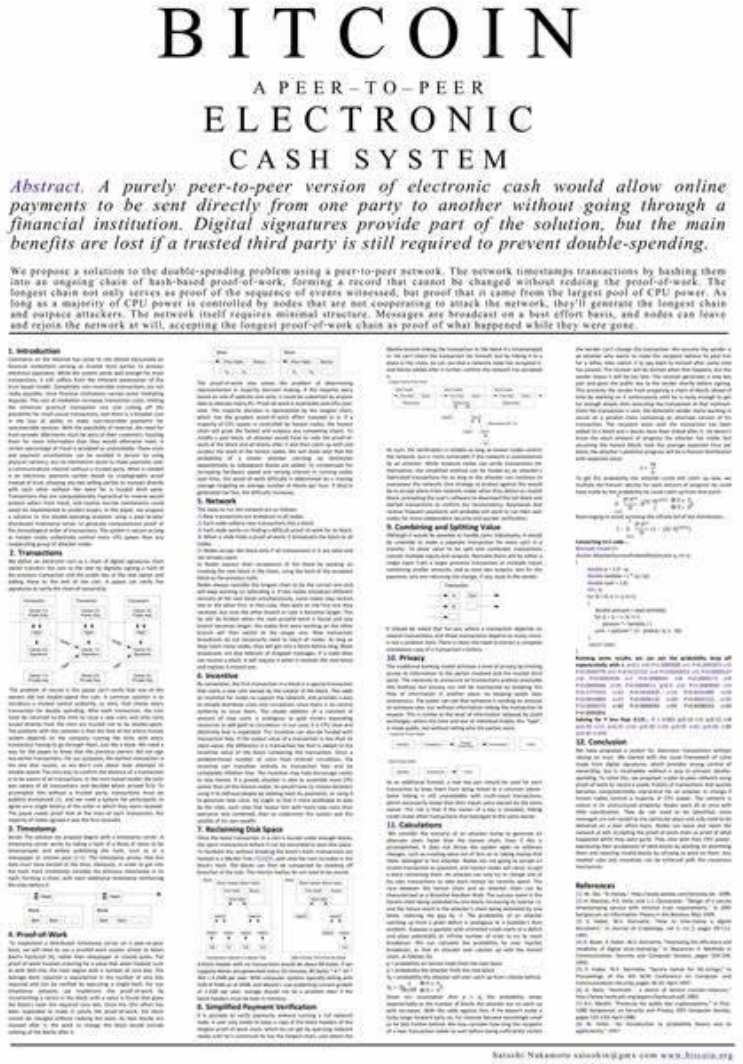
2. GRUNDLAGEN BITCOIN – WAS IST BITCOIN?

Wer hat Bitcoin “erfunden”?

- 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 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.

Welches Problem löst Bitcoin?

- Die Blockchain ermöglicht Peer-to-Peer Zahlungen zwischen den Teilnehmern im Netzwerk
- 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



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.

3. 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. Whenever the map is confused with the territory, a ‘semantic disturbance’ is set up in the organism. The disturbance continues until the limitation of the map is recognized.” – Alfred Korzybski

3. BILD UND ABBILD – DAS ORACLE PROBLEM

Was ist das allgemeine Problem?

- Echte Dinge auf eine Datenbank zu bringen ist schwer, weil es Vertrauen in eine Instanz braucht, welche die Geschehnisse in der physischen Welt verifiziert
- Computer können nichts über die materielle/echte Welt wissen, sie rechnen nur mit Informationen
- Im Kontext der Informatik bezeichnet der Begriff “Oracles” Datenquellen, welche Daten und Informationen aus der realen Welt zur Verfügung stellen.
- Die Schnittstelle ist eine zentrale Instanz
- Es gibt keine Möglichkeit mit externen Datenquellen sicher zu interagieren, da es für die Datenqualität und Durchsetzung der Eigentumsrechte keine Garantie gibt
- Die Verwendung von einzelnen Oracles, APIs, etc. würde ein signifikantes Risiko in die Funktionsweise von Blockchains re-integrieren, welches gegen die grundlegendste Architektur und Sicherheitsversprechen von Blockchains und Smart Contracts verstößt.
- **Fazit:** Es ist in einem dezentralen Kontext ein unlösbares Problem, ein digitales Gut mit einem physischen Gut zu verknüpfen, egal ob es sich um Obst, Autos oder Häuser handelt. Selbst digitale Güter wie E-Books, Krankenakten oder Filme leiden unter demselben Problem. Die "Rechte" an diesen digitalen Vermögenswerten werden letztlich von einer anderen Instanz festgelegt und durchgesetzt, und es braucht Vertrauen in ein Oracle.

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 ist reine Information und braucht daher keine Verknüpfung in die materielle Welt
- Bitcoin bildet nicht die materielle Welt ab und möchte das auch nicht tun
- Bitcoin kehrt die Logik um: Es wird nicht von der materiellen Realität auf Informationen geschlossen, sondern von Informationen wird auf die Realität geschlossen und es werden Anreize für Handlungen in der materiellen Welt gesetzt.
- **„In Bitcoin the map is the territory.“ - Gigi**

4. WARUM BRAUCHT EINE BLOCKCHAIN NATIVES GELD?

- In der Praxis sind **Bitcoin (die Währung) und seine Blockchain voneinander abhängig**. Das eine existiert nicht ohne das andere; Bitcoin braucht seine Blockchain, um zu funktionieren. Es gäbe keine funktionierende Blockchain ohne eine native Währung (Bitcoin), um Ressourcen zum Schutz der Blockchain (Mining) richtig zu incentivieren. Diese native Währung (Bitcoin) muss als Geldmittel überlebensfähig sein, denn **die Währung ist es, die ausschließlich und alleine für die Sicherheit des Netzwerks bezahlt**. Zudem muss diese Währung glaubwürdige **monetäre Eigenschaften** haben, um lebensfähig zu sein. Ohne Geld gibt es keine Sicherheit und ohne die Sicherheit brechen der Wert der Währung und die Integrität der Blockchain zusammen. Aus diesem Grund ist eine Blockchain nur bei der Anwendung von Geld nützlich.
- **Eine Blockchain kann nichts durchsetzen, was außerhalb des Netzwerks passiert**. Während eine Blockchain in der Lage zu sein scheint, das Eigentum außerhalb des Netzwerks zu verfolgen, kann sie nur das Eigentum an der **Währung durchsetzen**, welche in ihrem Netzwerk nativ ist. **Bitcoin erfasst Eigentum und setzt es durch**. Wenn eine Blockchain nicht beides tun kann, sind alle Datensätze, die sie aufbewahrt von Natur aus unsicher und unterliegen letztendlich möglichen Änderungen.
- Und wenn eine Blockchain nicht unveränderlich ist, wird ihre Währung nie als Geld lebensfähig sein, denn Transfer und Begleichung (Settlement) sind nie zuverlässig möglich. Ohne zuverlässiges Settlement ist ein Geldsystem nicht funktionsfähig und zieht keine Liquidität an. Ohne eine native Währung muss sich die Blockchain auf Vertrauen als Sicherheitsmodell verlassen, wodurch die Notwendigkeit einer Blockchain von vornherein entfällt. Im Wesentlichen muss das, wofür die Miner bezahlt werden (Bitcoin), eine zuverlässige Geldform sein um überhaupt Investitionen in dessen Sicherheit anzuregen. Wenn Bitcoin nicht als Geld bewertet werden würde, gäbe es keine Miner, und ohne Miner gäbe es keine schützenswerte Blockchain.
- **Fazit:** Wenn die Liquidität/Finanzierung für eine Blockchain außerhalb des Systems passiert, dann ist die Blockchain fragil und von einer zentralen Instanz abhängig. **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.** Bitcoin, Not Blockchain - Unchained Capital

4. WARUM BRAUCHT EINE BLOCKCHAIN NATIVES GELD?

"Why do blockchains not work without bitcoin, or rather why do blockchains not work without an intrinsic, valuable asset that is the basis for a game theoretical model of security? The reason is simple.

A blockchain, as a data structure, is a fairly inefficient data structure. The reason we use a blockchain is to achieve decentralization. In order to achieve decentralization, you have to be able to validate transactions without giving anyone the power of veto, or the power to control the network. You have to decentralize the process of validation. The best mechanism we've found so far for decentralizing the process of validation is by having a consensus algorithm that depends on competition […]. In order to have competition, you need risk and reward. In order to have a reward that is meaningful, you need an intrinsic token. You need something of value that people are trying to get, which keeps them playing fair.

If you don't have something of value, you don't have a basis for that competition. Without a basis for that competition, you don't have security. Without security, you have to control validation centrally. Without decentralization, there's no point in doing a blockchain. You might as well use a replicated database. It's going to be far more efficient. The purpose of blockchain technology and a consensus algorithm is to decentralize control, to provide censorship resistance and neutrality in a global open platform; in order to do those things, you need some mechanism to decentralize validation." – Andreas Antonopoulos

(Bitcoin Q&A: "Blockchain, not Bitcoin" - YouTube)

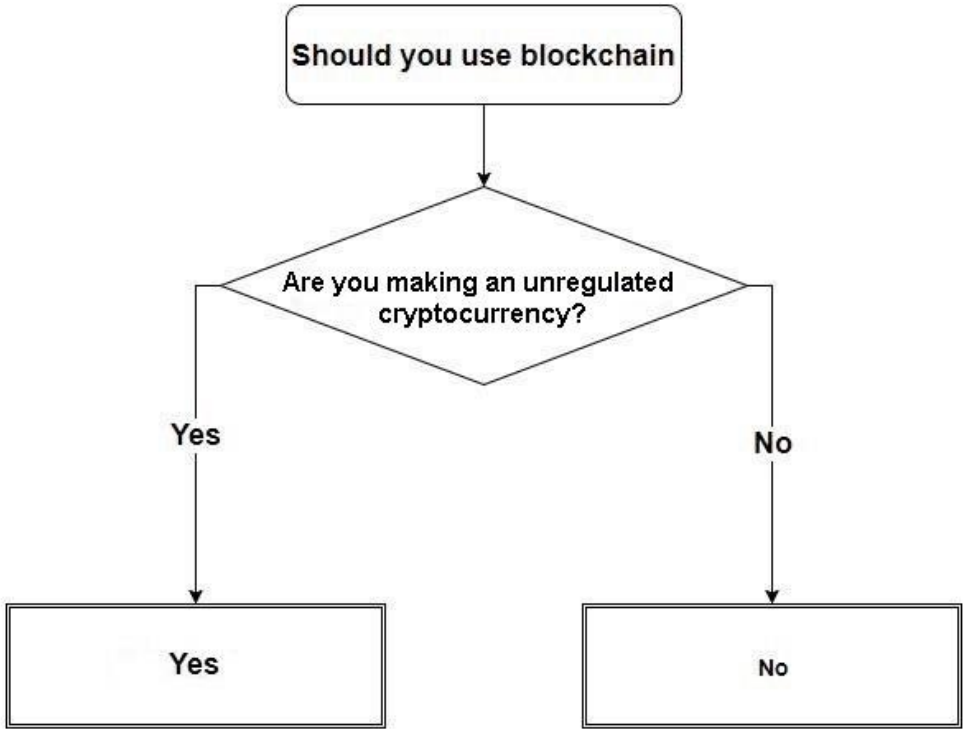
5. WIE STABILISIERT PROOF-OF-WORK DIE BLOCKCHAIN?

- Miner müssen **erhebliche Vorlaufkosten** für die Sicherung des Netzes tragen, werden aber nur bezahlt, wenn gültige Arbeit geleistet wird. **Miner werden aus dem Netzwerk heraus bezahlt**. Das finden eines Blocks belohnt Miner mit neu ausgegebenen Bitcoins als Gegenleistung für die Sicherung des Netzwerks, ist aber nur gültig, wenn die Arbeit gültig ist. **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**. 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.**
- Durch diesen Mechanismus werden die Miner maximal motiviert, ehrliche und gültige Arbeit zu leisten und jederzeit im Konsens der Kette zu arbeiten. Entweder sie werden bezahlt oder erhalten nichts. **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 (oder würde).** Der Anreiz zur Zusammenarbeit nimmt zu, wenn es teurer wird Arbeiten zu produzieren, welche sonst vom Rest des Netzwerks als ungültig abgelehnt würden. Mit zunehmender Netzwerksicherheit wird Bitcoin immer wertvoller. Wenn der Wert von Bitcoin steigt und die Kosten für die Lösung von Blöcken steigen, erhöht sich der Anreiz gültige Arbeit zu produzieren (mehr Umsatz, aber mehr Kosten) und die Bestrafung für das Ausführen ungültiger Arbeit wird dadurch auch höher (keine Einnahmen und höhere Kosten).
- Keine dieser dezentralen Abstimmungen wäre ohne Bitcoin, der Währung, möglich. Das gesamte Bitcoin-Netzwerk muss die Miner im Gegenzug für die Sicherheit entschädigen. Würde die an die Miner gezahlten Entschädigungen nicht als eine zuverlässige Form von Geld angesehen werden, wäre der Anreiz nicht gegeben Investitionen in das Lösen der Arbeit zu tätigen.

6. WARUM ES LANGFRISTIG NUR EIN GELD/EINE BLOCKCHAIN GIBT

- Letztendlich **konvergieren Geldsysteme auf ein Medium**, weil der Nutzen Liquidität vor Konsum oder Produktion steht. Die Liquidität konsolidiert sich **um den sichersten, langfristigsten Wertspeicher**; es wäre irrational, Vermögen in einem weniger sicheren, weniger liquiden monetären Netzwerk zu speichern, wenn ein sichereres, liquideres Netzwerk als erreichbare Option existiert. Die aggregierte Schlussfolgerung ist, dass **nur EINE Blockchain lebensfähig und letztendlich notwendig** ist. **Jede andere Kryptowährung konkurriert um den gleichen Anwendungsfall** wie Bitcoin, und zwar den des Geldes.
- Das Netzwerk ist nur zu einer einzigen aggregierten Funktion fähig: der Überprüfung, ob ein Bitcoin ein Bitcoin ist und die Erfassung des Eigentums.
- Letztendlich ist eine **Blockchain nur bei der Anwendung für Geld nützlich**, da sie aus Sicherheitsgründen von einer nativen Währung (Bitcoin) abhängig ist und es aufgrund des Oracle Problems ein geschlossenes System benötigt. Weil sich der Netzwerkeffekt von Bitcoin, die Sicherheits- und Liquiditätsvorteile gegenüber anderen Konkurrenten immer nur weiter erhöht, kann keine andere digitale Währung mit Bitcoin konkurrieren. **The winner takes it all.**
- Bitcoin ist das einzige geschlossene Geldsystem, das wir kennen. Aufgrund der absoluten Knappheit von 21 Millionen gibt es keine Inflation, wie bei anderen Vermögenswerten. Bitcoin hat somit optimale Wertspeichereigenschaften. Hinzu kommt eine Verifizierbarkeit, Teilbarkeit, Transportierbarkeit, und Haltbarkeit, die wir so von anderen Geldsystemen nicht kennen.
- **„There is no second best crypto asset.“ – Michael Saylor, Microstrategy**

6. BLOCKCHAIN ENTSCHEIDUNGSBÄUME



[When do you need blockchain? Decision models. | by Sebastien Meunier | Medium]

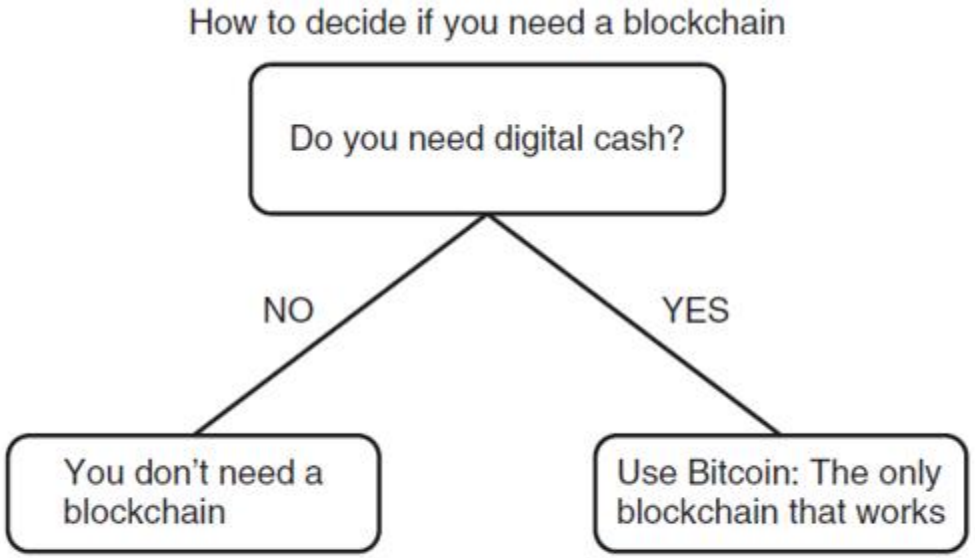


Figure 22 Blockchain decision chart.

[Der Bitcoin-Standard: Die dezentrale Alternative zum Zentralbankensystem - Ammous, Saifedean - Amazon.de: Bücher]

7. ZUSAMMENFASSUNG – BITCOIN, NOT BLOCKCHAIN

- Ein Abbild ist nicht die Realität und eine Schnittstelle enthält immer das Oracle Problem. Bitcoin kehrt dies um, denn **„in Bitcoin the map ist the territory**“.
- Jede Blockchain, die im Gegenzug für Sicherheit angeboten wird, ist ein geschlossenes System und benötigt somit ein im Netzwerk nativer monetärer Vermögenswert. Es gibt keine durchsetzbaren Ansprüche außerhalb des Netzwerks, weshalb **eine Blockchain nur im Zusammenhang mit der Verwendung von Geld nützlich sein kann**.
- Alles was Bitcoin weiß, ist wie es Währung ausgibt und diese validieren kann (ist der Bitcoin wirklich ein Bitcoin). Bitcoin ist **nicht in der Lage durchzusetzen, was außerhalb des Netzwerkes geschieht** (das gilt für jede Blockchain). Es ist ein völlig in sich **geschlossenes System** und das Bitcoin-Netzwerk kann immer nur eine Seite einer zweiseitigen Wertübertragung validieren. Wenn Bitcoin-Übertragungen nicht zuverlässig und endgültig angesehen werden würden, wäre es unmöglich jemals etwas von Wert gegen Bitcoin zu handeln. Deshalb ist die **Unveränderlichkeit** der Bitcoin-Blockchain untrennbar mit dem Wert von Bitcoin als Währung verbunden.
- Diese multidimensionale Anreizstruktur ist kompliziert, aber es ist entscheidend für das Verständnis, wie Bitcoin funktioniert und warum **Bitcoin und seine Blockchain voneinander abhängig sind** und warum jedes ein Werkzeug ist, welches auf das andere angewiesen ist. Bitcoin als Wirtschaftsgut ist nur als eine Form des Geldes wertvoll, weil es keinen anderen Nutzen hat. Dies gilt für alle möglichen Vermögensanlagen, die in einer Blockchain vorkommen. Der einzige Wert den Bitcoin letztendlich bieten kann, ist der gegenwärtige oder zukünftige Austausch gegen Waren oder Dienstleistungen. **Das Netzwerk ist nur zu einer einzigen aggregierten Funktion fähig: der Überprüfung, ob ein Bitcoin ein Bitcoin ist und die Erfassung des Eigentums.**
- Eine Blockchain ist eine Erfindung, die es ermöglicht Dritte, welchen vertraut werden müsste, zu entfernen. Die Blockchain dient keinem anderen Zweck. **Sie ist nur in Bitcoin als Teil eines größeren Puzzles wertvoll und sie wäre nutzlos, wenn sie nicht in Übereinstimmung mit der Währung funktioniert**. Die Integrität der fixierten Menge und die Unveränderlichkeit der Blockchain hängen letztlich vom Wert der Währung selbst ab.

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**
- Englisch: „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)**
- **Pump it up! - Best Bitcoin Songs Playlist - Leo Mattes (leo-mattes.com)**

YouTube:

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

Bitcoin, not Blockchain.

Leo Mattes

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