



# Politik Aspekte zu Zukunftspolitik | Bitcoin Bitcoin und Kryptowährungen als Innovationstreiber



■ Grundsätze ● Positionen ► Aussagen





- **Aspekte** Zukunftspolitik

# Bitcoin | Kryptowährungen

(Version Juli 2023 V1)



© Bildquelle: Bidcoin.de / format 2

• ludwiglorenz.ch • llorenz@bluewin.ch



# Zukunftspolitik

■ „you've got mail!“

*“How does everyone feel about the B symbol with the two lines through the outside? Can we live with that as our logo?”*

**„Was haltet ihr von einem Symbol mit einem B mit zwei Linien an der Aussenseite?**

**Können wir das als unser Logo akzeptieren? “**

*Satoshi Nakamoto*

*24. Februar 2010 / Bitcoin Forum*







## ■ Ursprung

- Bitcoin hat den Ursprung in der **Cypherpunk- Bewegung**, der kleinen Bewegung aus San Francisco, die sich unter anderem für den **Schutz** der **Privatsphäre** der Menschen im Bereich des Digitalen einsetzen.
- Dabei setzen sie mitunter auf den Einsatz von **Kryptographie**.
- Das Pseudonym „ **Satoshi Nakamoto**“ veröffentlichte sein **Bitcoin White Paper** zuerst auf der Mailing-Liste der „Cypherpunks“.
- Begünstigt wurde diese Bewegung durch die Entdeckung der **asymmetrischen Kryptographie**.
- Die Asymmetrie bedeutet, dass man nicht mehr dasselbe Passwort für das Ver- und Entschlüsseln von Daten nutzt, sondern **zwei Passwörter** hat.
- Eines wird nur zum Verschlüsseln genutzt, den „**Public Key**“. Das andere wird nur zum Entschlüsseln verwendet, auch „**Private Key**“ genannt.

▶ **Dezentral und gleichberechtigt: Bitcoin als Gamechanger von Finanzsystem und Weltwirtschaft.**



# Zukunftspolitik | Bitcoin ₿

## ■ Entstehung

- Am **3. Januar 2009** drückte „Satoshi Nakamoto“ eine Taste und startete damit ein Projekt, das die Welt verändern sollte: **Bitcoin**, das erste rein **digitale Geld**, das **nicht durch Staaten und Banken verwaltet** und organisiert wird, sondern durch Mathematik, Kryptografie und Algorithmen.
  - Ziel des Projekts war ein **freies, offenes und dezentrales Geldsystem** als Alternative zu einem zentralisierten, undurchsichtigen und krisenanfälligen Finanzsystem durch Banken. (*Finanzkrise 2008 !!*)
  - Das herkömmliche **Fiat-Finanzsystem** zwang die Regierungen der Welt, Banken mit dem **Geld der Steuerzahler** zu retten.
  - Mitten in dieser Finanzkrise begann also **ein einzelner Computer** zu arbeiten – öffentlich, aber von der Öffentlichkeit unbeachtet.
  - Von Computern wurden **Bitcoins** gutgeschrieben und dieses Guthaben in einer eigens dafür geschaffenen Datenbank vermerkt: der **Blockchain**.
- ▶ **Mit Bitcoin wurde ein innovatives Zahlungsnetzwerk und eine neue Art von Geld geschaffen.**





# Zukunftspolitik | Bitcoin ₿

## ■ "White Paper" by Satoshi Nakamoto

- Satoshi hat in einer Mail in der Cryptographie-Mailing-List am 1. November 2008 ein **Whitepaper** mit dem schlichten Titel "**Bitcoin: A Peer-to-Peer Electronic Cash System**" veröffentlicht.
- Auf gerade mal 8 Seiten skizziert Satoshi Nakamoto in diesem Whitepaper die technische **Grundlage für Bitcoin**, Kryptowährungen und die **Blockchain-Technologie**.
- In extrem verdichteter Form beschreibt der Gründer von Bitcoin, das kryptografisch Konzept einer praktisch **unveränderbare Transaktion**.
- **Satoshi** leitete die Entwicklung von Bitcoin bis **Ende 2010**. Dann hörte er plötzlich auf, in Online-Foren zu posten. **Er verschwand einfach**.
- Es dürfte nur wenige Schriftstücke des 21. Jahrhunderts geben, die mit so wenig Seiten einen so **grossen Einfluss** hatten wie das Bitcoin-Whitepaper von Satoshi Nakamoto.

▶ **Das Whitepaper gilt als zurecht **Gründungsdocument** der **virtuellen Währungen**.**



# Zukunftspolitik

## ■ Aussage

«Die Zukunft unserer Gesellschaft wird von Technologie geprägt sein. Wir müssen uns deshalb schon heute anstrengen, Aspekte wie den Bitcoin zu verstehen, um uns auf den Wandel vorzubereiten und gute Entscheidungen zu fällen.»





## ■ Bitcoin

- **Bitcoin** (BTC) ist eine **seit 2009 gehandelte digitale Währung**, oder auch Kryptowährung, die als sicheres, internationales und dezentrales Zahlungsmittel gilt.
- Bitcoin ist die erste öffentlich gehandelte und bis heute die bekannteste und **wichtigste Kryptowährung**. (1 BTC = 25'416.- Fr. / 28.07.2023)
- Bitcoin existiert ausschliesslich **virtuell** in Form einer digitalen Zeichenfolge und unterscheidet sich von traditionellen Währungen, da sie **unabhängig** von Staaten und Banken ist.
- Ein weiterer Vorteil von Bitcoin (BTC) ist seine **Inflationssicherheit**, da die **Gesamtmenge auf 21 Millionen begrenzt** ist.
- Das war auch das Ziel des unbekanntes Software-Entwicklers oder -Teams, bekannt unter dem Pseudonym Satoshi Nakamoto.
- Nach der Weltwirtschaftskrise im Jahr 2007 wollte dieses Kollektiv oder diese Person ein **unabhängiges Transaktionssystem** schaffen, das kryptografisch gesichert, **verifizierbar und unveränderlich** ist.





## ■ Bitcoin

- Die **Verwaltung von Guthaben und Zahlungen** erfolgt in einem dezentralen Netzwerk – die sogenannte **Blockchain**.
- Jede **Transaktion** wird als **Datenblock** abgebildet, welcher sämtliche Bitcoin-Transaktionen aus einem bestimmten Zeitraum enthält.
- Die **Richtigkeit** des Datenblocks wird vom **Blockchain-Netzwerk** überprüft und die Transaktion wird genehmigt, falls der Block korrekt ist.
- Anschliessend wird der Datenblock in die Blockchain-Kette integriert. Dadurch enthält die Blockchain eine **vollständige Aufzeichnung** aller Bitcoin-Transaktionen, die jemals durchgeführt wurden.
- Seit dem Bitcoin wurden zahlreiche **weitere Kryptowährungen** eingeführt, unter anderem **Ethereum**, Ripple und Litecoin.
- Der 2009 erschaffene Bitcoin ist die bekannteste von heute mehr als **23'000 Kryptowährungen**.
- Die **Marktkapitalisierung** der ältesten Kryptowährung **Bitcoin** beträgt derzeit rund **604 Milliarden Dollar**.



# Zukunftspolitik | Bitcoin



## ■ Bitcoin Kursentwicklung

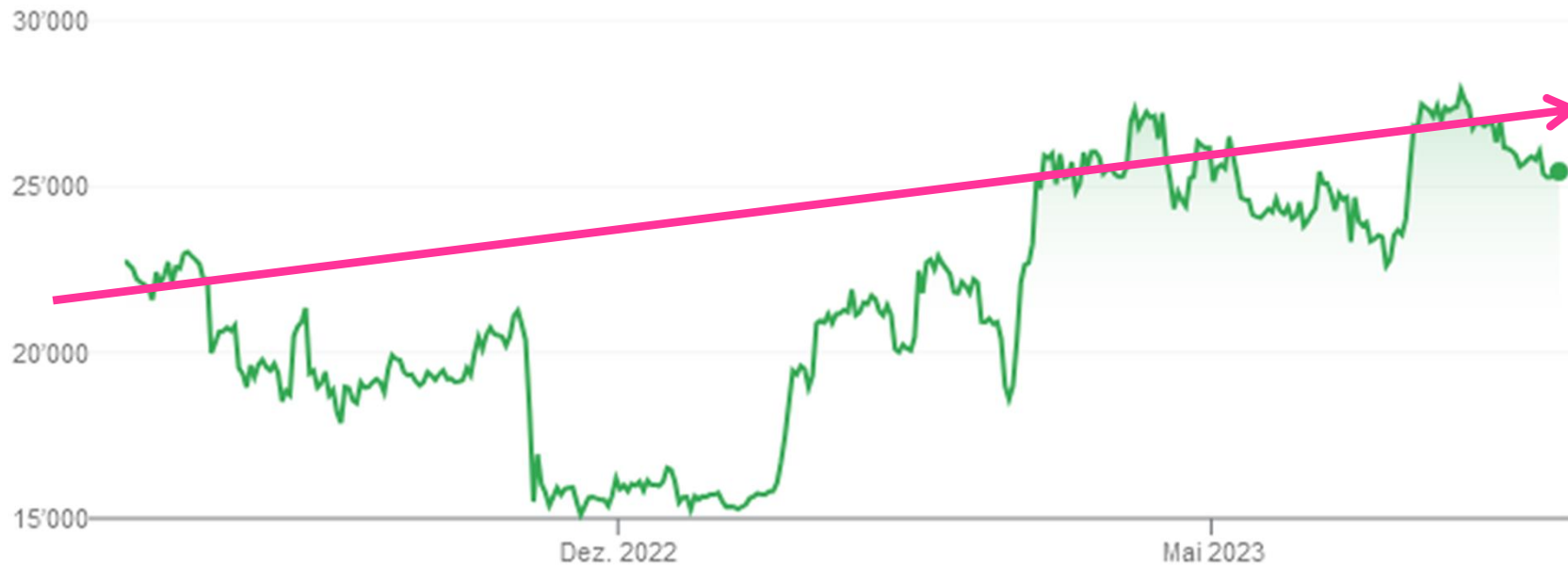
- Kursentwicklung **Bitcoin** zum **Schweizer Franken**: Juli 22 – Juli 23

25'406.43 CHF

+2'639.51 (11.59%) ↑ im letzten Jahr

28. Juli, 12:32 UTC · [Haftungsausschluss](#)

1 T. | 5 T. | 1 M. | 6 M. | YTD | 1 J. | 5 J. | Max.





# Zukunftspolitik | Bitcoin ₿

## ■ Die EZB

- Die Europäische Zentralbank führt **Marketing-Kampagnen** durch.
- Zwar ist die EZB mit einem **Monopol** ausgestattet, doch hat ihr **Produkt €** – chronisch bedingt – mit **Imageproblemen** zu kämpfen.
- Das **Vertrauen der Kunden** muss daher stets bestärkt oder **zurückgewonnen** werden.
- Auf der anderen Seite bedeutet das auch, **Konkurrenzprodukte** zu **diskreditieren**. Ein solches Konkurrenzprodukt ist Bitcoin.
- Bitcoin ist Teufelszeug! Mag albern klingen, doch so lesen sich die neuen **Twitter- Postings der Europäischen Zentralbank** (EZB), die eindringlich vor Kryptowährungen warnen.
- Dass Bitcoin gegenüber dem Euro sowie allen anderen Fiat-Währungen über Jahre an Wert **hinzugewonnen** hat, wird als Instabilität ausgelegt.



▶ **Statt zu diskreditieren sollte die EZB besser an den eigenen Qualitätsversprechen zum € (Geldwertstabilität!) arbeiten.**



# Zukunftspolitik | Bitcoin ₿

## ■ Bitcoin-Mining & Klima

- Zur Absicherung von Bitcoin ist viel **Energie für die Rechenleistung** der Computer nötig – das sogenannte **Mining** steht deshalb oft in der Kritik.
- Selbst wenn das **Bitcoin-Mining** heute vollständig verboten würde, wäre der Planet immer noch auf dem Weg, die Erwärmungsschwelle von 1,5 Grad Celsius innerhalb des nächsten Jahrzehnts zu überschreiten.
- Bitcoin-Mining spielt auch eine Rolle bei der **Förderung** der Einführung **erneuerbarer Energien**, seine Auswirkungen können jedoch je nach Szenario unterschiedlich sein. Es ist nicht der einzige **Katalysator**, aber es trägt zum Wachstum erneuerbarer Energien bei.
- Bitcoin verfügt über **einzigartige Eigenschaften**, die es ermöglichen, Abwärme an z.B. Gewächshäuser zu verkaufen oder sie für kommunale Heizzwecke zu nutzen.



► **Laut Schätzungen\* ist Bitcoin-Mining für etwa 0,14 % der gesamten globalen CO2-Emissionen verantwortlich.**

*\* Cambridge Bitcoin Electricity Consumption Index (CBECI)*



# Zukunftspolitik | Bitcoin

## ■ Fazit

- Bitcoin ist eine **neue Form von Geld**, eine revolutionäre Art und Weise, Wert(e) über das Internet auszudrücken und zu teilen.
- Bitcoin ist **rein digital** und wird nicht durch Regierungen geprägt oder ausgegeben.
- Jeder weitere **Teilnehmer** verschafft den Bitcoin-Regeln mehr Geltung und trägt dazu bei, eine **berechenbare** und faire **Plattform** für das Geld aller zu erschaffen.
- Für Millionen von Menschen weltweit ist das digitale Geld oftmals die **einzige Chance**, Handel zu betreiben oder Angehörigen zu helfen.
- **Bitcoin** ist kein Unternehmen, keine Organisation. Es gibt keinen zentralen Akteur, keine zuständige Behörde, keinen Geschäftsführer – das System wird ohne Machtzentrum von den Teilnehmern selbst gepflegt und verwaltet.
- ▶ **Bitcoin** ist offen, auf Kooperation beruhend, **überstaatlich**, neutral, unveränderlich, knapp, vorhersehbar, zulassungsfrei und unzensurierbar.







# Zukunftspolitik | Bitcoin ₿

## ■ Open Source

- Bitcoin ist **Open-Source**, das Design ist öffentlich, Bitcoin gehört niemandem und wird von niemandem kontrolliert.
  - **Jeder kann mitmachen!**
  - Durch viele seiner einzigartigen Eigenschaften eröffnet Bitcoin **aufregende Nutzungsmöglichkeiten**, die durch keines der bisherigen Zahlungssysteme abgedeckt sind.
  - Bitcoin weist verschiedene **Eigenschaften** auf, die es von herkömmlichen Währungen **unterscheiden**. So können weltweit Transaktionen ohne Zwischenhändler durchgeführt werden. *(Keine Banken, etc. nötig)*
  - Kryptowährungen haben bereits eine **grosse Revolution** in der **Finanzindustrie** ausgelöst und werden auch in Zukunft viele bedeutende Veränderungen im Finanzsektor bewirken.
- ▶ **Bitcoin ist von unabhängigen Unternehmen transparent und kooperativ entwickelt worden.**





## Zukunftspolitik | Bitcoin ₿

■ 20'999'999,97690000

- Der maximale **Bestand** des Bitcoins ist **fest definiert** und wird niemals die Grenze von knapp 21 Millionen Coins überschreiten.
- Es werden **maximal 20'999'999,97690000** Bitcoin existieren.
- **Aktuell** befinden sich laut dem Analysehaus Coinmarketcap knapp über **19,3 Millionen** Bitcoin im Umlauf. *(91.9% des Bestandes)*
- Durch die **Halvings** wird der letzte Bitcoin erst um das **Jahr 2140** herum geschürft werden.
- Die Anzahl der 21 Millionen BTC ist auch eine **mathematische Konsequenz**. Sie ergibt sich, wenn man die Zahl der produzierten Blöcke (210'000 pro Jahr) mit der Summe der sich halbierenden Belohnungen ( $50 + 25 + 12,5 + 6.25 + \dots + 0 \approx 100$ ) multipliziert.
- Im Gegensatz zum **unbegrenzten „Druckgeld“** der **FIAT-Währungen** ist BTC begrenzt und somit eher **vor Inflation geschützt**.

▶ **Der Bitcoin-Bestand kann also nicht ausgeweitet werden.**



## ■ Peer-to-Peer

- Bitcoin nutzt **Peer-To-Peer-Technologie**, um **ohne zentrale Autorität** auszukommen. (*Zentrale Autorität = ZB / Staat = Vertrauen*)
  - Peer-to-Peer oder kurz P2P wird auch als „Kommunikation unter Gleichen“ bezeichnet.
  - Gemeint ist damit ein Netzwerk, in dem **alle Rechner gleichberechtigt** sind und über dieselben Funktionen verfügen.
  - Peer-to-Peer-Systeme bieten zahlreiche Vorteile, weshalb viele Unternehmen und Communitys Zeit und Ressourcen in die Entwicklung und **Weiterentwicklung der P2P-Netzwerke** stecken.
  - Die **Bearbeitung** von Transaktionen und die Ausgabe neuer Bitcoins wird **kollektiv** durch das Netzwerk übernommen.
  - Das System verbindet mehrere kryptographische Konzepte, um erstmals ein **dezentrales Transaktionssystem** für digitales Bargeld zu schaffen.
- ▶ **Die Das System ist dezentral und kommt ohne Vertrauen aus.**



## ■ Nodes & Miner

- **Nodes** übernehmen im Bitcoin-Netzwerk die Rolle der “**Wächter**” und sind daher unerlässlich. (*Teilnehmer*)
- Ein Node ist in Bitcoin oder anderen Blockchain-Netzwerken ein **Knotenpunkt**, der eine Kopie der Blockchain hat und damit das Netzwerk aufrechterhält.
- Jeder Node **verifiziert** Transaktionen und kontrolliert, ob die **Netzwerkregeln** von allen **Teilnehmern eingehalten** werden. Je mehr Nodes ein Netzwerk hat, desto dezentraler ist es.
- Jedoch gibt es nicht nur eine Art von Nodes, sondern verschiedene Typen, die **jeweils andere Funktionen** im Netzwerk wahrnehmen.
- Es gibt Archival Full Nodes, **Light Nodes**, Mining Nodes, Masternodes und Lightning Nodes.
- Um die **Dezentralisierung** zu gewährleisten, ist es notwendig das Netzwerk auf viele dieser Knotenpunkte zu verteilen.

▶ **Nodes gehören zu den Schlüsselementen der Blockchain.**



## ■ Nodes & Miner

- Unter dem Begriff **Bitcoin Mining** versteht man das Erzeugen – oder das „Schürfen“ – neuer Bitcoin.
- Dies geschieht über sogenannte **Miner**, die im Falle des Bitcoins der Bitcoin-Blockchain den nächsten Block anhängen und dafür eine **Belohnung** einstreichen.
- Nur der erste Miner (oder **Mining Pool**), der einen neuen Prüfwert erzeugt, bekommt eine Entlohnung in Form von Bitcoin.
- Dabei wird nach 210'000 gelösten Blöcken bzw. etwa alle vier Jahre die **Entlohnung pro Block halbiert**. (*Halving* / 4. Halving ca. April 2024)
- Inzwischen gibt es mehr als 770'000 geknackte Blöcke – pro Block winken gegenwärtig **6,25 Bitcoins**. (*entspricht ca. Fr. 158'790.- / 28.07.2023*)
- Der übergeordnete Zweck von **Bitcoin-Mining** ist nicht das Finden neuer Bitcoin, sondern die **Sicherheit des Netzwerks**.
- ▶ **Das Fortschreiben und Sichern der Blockchain funktioniert über einen Mechanismus, der als „Mining“ bezeichnet wird.**





## ■ Hashrate

- Zum **Schürfen neuer Bitcoin** – im Fachjargon Mining genannt – wird viel **Rechenleistung** benötigt.
  - Die weltweit genutzte Rechenleistung zu einem bestimmten Zeitpunkt wird als **Hashrate** bezeichnet.
  - Sie ist damit eine **entscheidende Messgrösse** für die Rechenleistung im Bitcoin-Netzwerk und dessen Sicherheit gegenüber Angriffen von aussen.
  - Eine **höhere Hashrate** bedeutet eine grössere Leistungsfähigkeit. Mittelbar führt eine hohe Hashrate auch dazu, dass das **Bitcoin-Netzwerk sicherer** wird. Das liegt daran, dass mit einer höheren Hashrate die **Kosten steigen**, um sich am Mining zu beteiligen.
  - Eine **wachsende Hashrate** zeigt an, dass das Bitcoin-Netzwerk an Stärke gewinnt und immer mehr **Menschen Interesse** daran haben, in Bitcoin zu investieren.
- ▶ **Mit dem Anstieg der Bitcoin-Hashrate steigt der Energiebedarf und die Sicherheit des Netzwerks.**



# Zukunftspolitik | Kryptowährungen

## ■ Blockchain

- Die **Verwaltung** von Guthaben und Zahlungen erfolgt in einem dezentralen Netzwerk – die sogenannte **Blockchain**.
- Die Teilnehmer bleiben anonym und dennoch sind alle **Transaktionen transparent** und nachvollziehbar.
- Blockchain ermöglicht **Peer-to-Peer-Transaktionen** ohne jede Zwischenstelle wie eine Bank.
- Jeder Vorgang **fälschungssicher**. Das Vertrauen wird durch das System als Ganzes hergestellt.
- Und digitale Währungen wie Bitcoins sind nur **ein Anwendungsgebiet** der Blockchain-Revolution.
- In der Blockchain kann **jedes wichtige Dokument** gespeichert werden: Urkunden von Universitäten, Geburts- und Heiratsurkunden und vieles mehr.



▶ **Die Blockchain ist ein sicheres weltweites Register für alles.**



# Zukunftspolitik | Bitcoin



## ■ Von Twitter zu X

- **Elon Musk**, bekannt für seine bahnbrechenden Vorhaben in den Bereichen Raumfahrt, Elektrofahrzeuge und Künstliche Intelligenz, hat jetzt seine ehrgeizigen Augen auf das beliebte Mikroblogging-Netzwerk **Twitter** gerichtet.
- Durch die **Umbenennung des Netzwerks** in “X” zielt Musk auf die Verwirklichung einer visionären Vorstellung ab – die Schaffung einer **“Alles-in-einem-App”**.
- Die Umbenennung könnte mit dem Fokus verbunden sein, dass sich das Netzwerks auf die **Bereitstellung von Zahlungs- und Bankfunktionen** verlagert.
- Dies deutet darauf hin, dass “X” beabsichtigt, nicht nur ein Social-Media-Netzwerk zu bleiben, sondern zu einem umfassenden Finanzdienstleister zu werden.



## ► Transformation von Twitter zu X - von Tweets zu Transaktionen ???



# Zukunftspolitik | Bitcoin ₿

## ■ Szenario

- **Erstens:** Staaten rufen **zentralisierte Formen** von Kryptowährungen wie CBDC oder den Digitalen Yuan ins Leben.
- **Zweitens:** Staaten machen die Welt **bargeldlos**.
- **Drittens:** Alle Erdenbürger werden nur noch **digitale Zahlungsformen** verwenden und begreifen, dass sie ihre **Anonymität** durch die Nutzung dieser zentralisierten Kryptowährungen völlig **verloren** haben.
- **Viertens:** Die Menschen werden sich nach privatsphärefreundlichen und **dezentralisierten Währungen** umsehen und sich gegen die staatlich verordnete zentralisierte Kryptowährung wenden.
- **Fünftens:** Sie verstehen nun das **Potenzial** von Bitcoin, DASH, XMR, LTC und allen anderen **Kryptowährungen**, die ihnen die **Anonymität** bieten, die sie vom Bargeld gewöhnt waren.

▶ **Ja, es wird eine Weile dauern, aber jede grosse Veränderung in der Welt braucht ihre Zeit.**



# Zukunftspolitik

## ■ À propos: ₿

„Bitcoin ist wie die frühe Elektrizität. Roh, gefährlich, scheint sehr flüchtig und schwer zu verwenden zu sein. Mit der Zeit wird es sich sicherer, einfacher und normaler anfühlen. Wie Elektrizität wird sie neue, unvorstellbare Industrien inspirieren und antreiben. Und eines Tages werden wir uns fragen, wie wir ohne sie leben konnten.“

*Obi-Wan Kenobi*







Zukunftspolitik

▶ Bitcoin & Krypto: **Game-Changer** im Währungssystem!



© Bildquelle: Coin United.io

• ludwiglorenz.ch • llorenz@bluewin.ch

**LUDWIG LORETTZ**  
FÖRDERUNG FÜR DIE WIRTSCHAFT



Empfehlung:

## Der Bitcoin-Standard: Die dezentrale Alternative zum Zentralbankensystem

Saifedean Ammous

ISBN 978-3982109503

im Buchhandel erhältlich





*It might make sense to get some,  
just in case it catches on.*

*Satoshi Nakamoto*



# Politik

## ■ Impressum

### ■ Verantwortlich für den redaktionellen Inhalt:

Ludwig Loretz  
Gotthardstrasse  
6490 Andermatt



### ■ Kontakt

lloretz(at)bluewin.ch

### ■ Copyright ©

Der Inhalt ist für den privaten Gebrauch sowie zur persönliche Meinungsbildung und zur Reflektion bestimmt.

Vor einer Weiterveröffentlichung ist der Autor zu kontaktieren und in Kenntnis zu setzen.

Die Bilder sind eventuell urheberrechtlich geschützt und dienen ausschliesslich der privaten Illustration.

Sämtliche Bildrechte liegen bei den Urhebern.

### ■ Bildernachweis: © *Bildquelle, pixabay, pixnio.com, Wikimedia Commons, etc.*

### ■ Literaturquellen

Eigene Literatur- und Internetrecherche. Die Aussagen und Inhalte stützen sich, sofern nicht anderweitig erwähnt, vornehmlich auf Grundgedanken mit liberaler und neoliberaler Ausrichtung ab, sowie themenspezifische Fachbücher und Fachliteratur.

### ■ Literatur Themenspezifisch: *Eigene Recherche, Internetrecherche, Bitcoin.de. Saifedan Ammous: Der Bitcoin Standart*

### ■ Versionen: *Version V1*

### ▶ Genderhinweis

#### **Gleichberechtigung als Anliegen**

Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) verzichtet.

Sämtliche Personenbezeichnungen gelten gleichermassen für alle Geschlechter.

*Der Inhalt stellt die persönliche Meinung des Verfassers dar. Die Aussagen und Positionen sind in der Folge ebenso von persönlicher Natur und müssen nicht einheitlich mit denjenigen von politischen Parteien oder politischen Gruppierungen, Vereinen etc. übereinstimmen. Die Inhalte sind als indikativ und rechtlich unverbindlich zu verstehen. Die Sachverhalte unterliegen Veränderungen der Zeit und können auch örtlich unterschiedlich sein.*