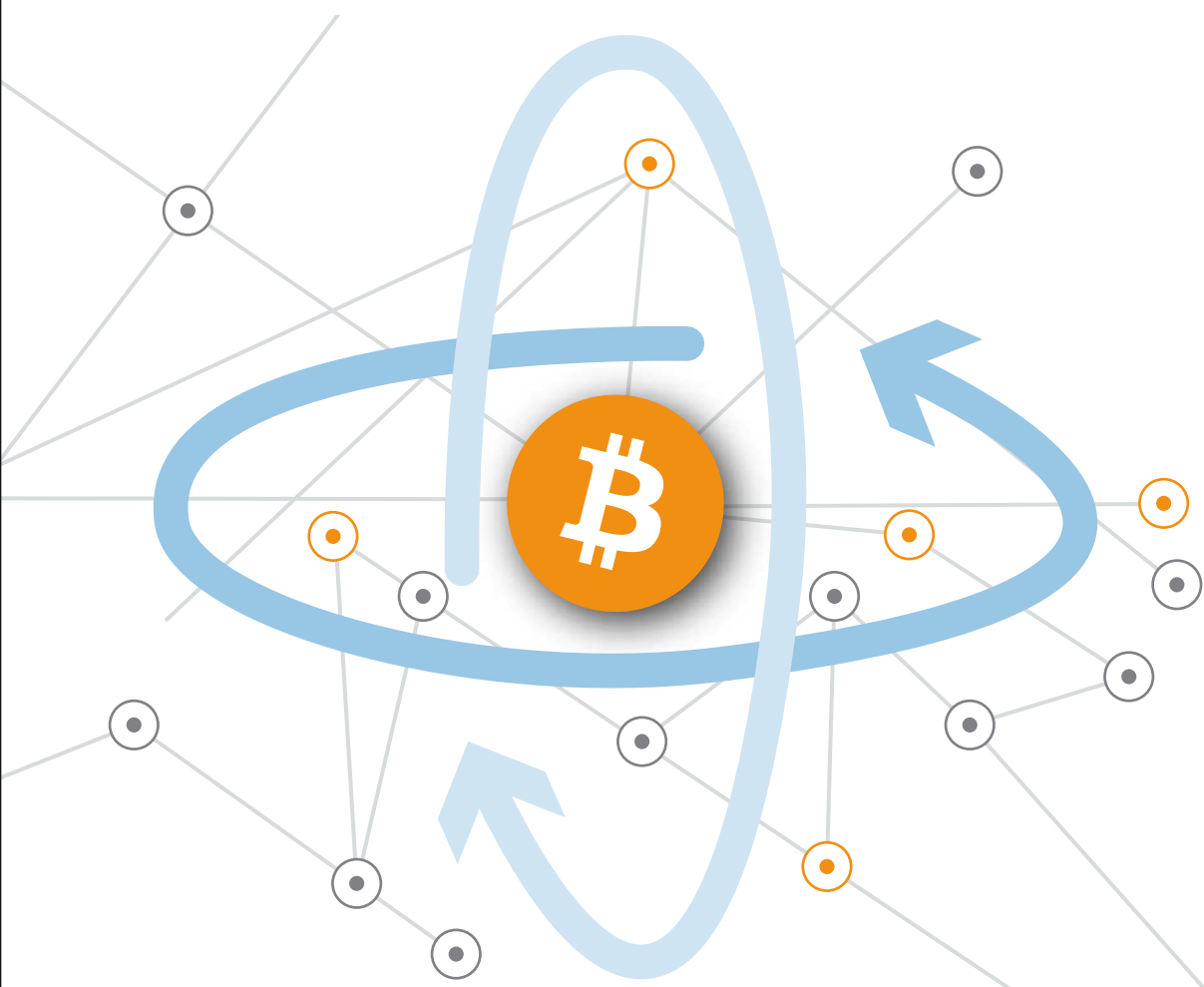


HWZ-Wissen

Pascal Hügli, Costantino Lanni (Mitautor)

Bitcoin verständlich erklärt

Für Beruf und Alltag



HWZ

VERLAG SKV

Pascal Hügli, Costantino Lanni (Mitautor)

Bitcoin verständlich erklärt

VERLAG:SKV

1. Auflage 2022

Pascal Hügli, Costantino Lanni (Mitautor)

Bitcoin verständlich erklärt

Für Beruf und Alltag

ISBN 978-3-286-51541-3

Das Werk erscheint als E-Book unter der ISBN 978-3-286-11788-4 (PDF)
und ISBN 978-3-286-11789-1 (EPUB)

© Verlag SKV AG, Zürich

www.verlagskv.ch

Alle Rechte vorbehalten.

Ohne Genehmigung des Verlags ist es nicht gestattet, das Buch
oder Teile daraus in irgendeiner Form zu reproduzieren.

Umschlagbild: Gianni Cocchiarella, Verlag SKV, Zürich

Haben Sie Fragen, Anregungen oder Rückmeldungen?

Wir nehmen diese sehr gerne per E-Mail an feedback@verlagskv.ch entgegen.

Danksagung

Mit der Publikation eines Buches rückt stets der Autor in den Vordergrund. Ein Buch – allen voran ein Lehrbuch – ist aber stets ein Gemeinschaftsprojekt. Mein Dank richtet sich zunächst an die HWZ Hochschule für Wirtschaft Zürich, welche mir dieses Lehrbuchprojekt überhaupt ermöglicht hat. Speziell bedanken möchte ich mich bei Dr. Daniel C. Schmid, Prof. Dr. Claude Meier sowie Dr. Stefan Joller, die mich nicht nur zur Publikation dieses Lehrbuches ermutigt, sondern mich bei der Ausarbeitung auch unterstützt haben.

Für seine Unterstützung als Mitautor bedeutender Inhalte in Kapitel 6 möchte ich Costantino Lanni herzlich danken. Auch seine technischen Kenntnisse zur Erarbeitung unterschiedlicher Statistiken und quantitativer Analysen waren mir eine grosse Hilfe.

Einen weiteren Dank möchte ich Gianni Cocchiarella aussprechen, der mich in allen verlagstechnischen Angelegenheiten tatkräftig unterstützt hat. Gleichzeitig bedanke ich mich auch beim gesamten Verlag, welcher die Umsetzung dieses Lehrbuch in Zusammenarbeit mit der HWZ überhaupt erst ermöglicht hat.

Was die geistigen Ergüsse und Erkenntnisse dieses Buches anbelangt, so möchte ich mich bei meinem Freund und Lektor Daniel Jungen bedanken. Die zahlreichen Marathon-Diskussionen mit ihm sowie die unzähligen Inputs und Gedankenanstösse seinerseits haben das Lehrbuch stark aufgewertet. Innigen Dank also, lieber Daniel. Im gleichen Atemzug möchte ich natürlich auch meiner Korrektorin Regula Walser danken.

Keinen geringen Anteil an der Fertigstellung des Lehrbuches hat Adrian Fritz von 21Shares, der mich für spezifische Kapitel mit Datenreihen versorgt hat. Dankbar bin ich auch für die zahlreichen sporadischen Unterstützungen von verschiedenen Krypto-Enthusiasten und Bitcoin-Kennern. Sie alle haben sich stets meinen offenen Fragen angenommen und wertvolle Antworten geliefert.

Und selbstverständlich geht der Dank auch an meine Liebsten und Engsten – an meine Frau, an meine Eltern und Schwiegereltern sowie an meine erweiterte Familie. Ihr habt mir alle stets die Kraft und die Zeit gegeben, mich meinem Lehrbuchprojekt zu widmen. Ohne euch hätte ich das niemals geschafft.

Damit bleibt mir, den Dank an alle noch ein letztes Mal zu wiederholen – ich weiss das sehr zu schätzen.

Der Autor

Nach mehreren Jahren im Finanzjournalismus, arbeitet Pascal Hügli heute als selbstständiger Moderator, Debattierer, Ghostwriter und Dozent an der HWZ. Zusätzlich publiziert er noch immer hin und wieder journalistische Texte in den Medien der traditionellen als auch der neuen Welt. Als Analyst befasst er sich hauptsächlich mit den aufstrebenden Kryptoassets und deren Auswirkungen auf Finanzmarkt, Wirtschaft und Gesellschaft. Über den deutschsprachigen Newsletter Insight DeFi klärt er die breitere Masse zweimal monatlich kompetent und prägnant über die Ereignisse, Chancen und Risiken der neuen dezentralen Welt von Bitcoin und Co. auf. Neben dem hier vorliegenden Lehrbuch ist er auch Autor eines weiteren Buches mit dem Titel «Ignorieren auf eigene Gefahr: Die neue dezentrale Welt von Bitcoin und Blockchain».

Links:

Insight DeFi: <https://insightdefi.substack.com/>

Ignorieren auf eigene Gefahr:

<https://www.amazon.com/Ignorieren-auf-eigene-Gefahr-dezentrale/dp/3952510807>

Der Mitautor:

Costantino Lanni, Betriebsökonom FH, begann seine berufliche Tätigkeit als Portfoliomanager bei der Credit Suisse Fides, Zürich. Nach Absolvierung der International Banker's School, New York, erwarb er das Finanzanalystendiplom CFA und später das Diplom zum Financial Risk Manager (FRM). Seit 1996 ist Lanni als selbständiger Vermögensverwalter tätig und amtiert als Anlageexperte bei einer grossen Schweizer Pensionkasse. Costantino Lanni ist seit vielen Jahren Studienleiter im Center for Financial Studies an der HWZ tätig. In dieser Funktion ist Costantino Lanni auch Mitglied der erweiterten Schulleitung der HWZ.

Inhaltsverzeichnis

Danksagung	VII
Der Autor	VII
Einleitung	1
Des Menschen Wunderwaffe	1
Zeitenwende: Auftakt der digitalen Ära	2
Digitales Inhaberinstrument	3
Absicht und Ziel	4
Aufbau und Inhalt	5
Praktische Lesehilfe	6
1 Eine digitale Renaissance	9
1.1 Zur Geburtsstunde von Bitcoin	9
1.1.1 Bitcoins umfangreiche Vorgeschichte	10
1.1.2 Perfektes Timing: Eine Idee, deren Zeit gekommen war	11
1.1.3 Dezentral auf allen Ebenen	12
1.2 Durchbruch von epochaler Tragweite	13
1.2.1 Lösung für das Double-Spend-Problem	13
1.2.2 Entdeckung digitaler Knappheit	16
1.2.3 Knapp, aber programmierbar	18
2 Ein Blick in den Maschinenraum	21
2.1 Das Ganze ist mehr als die Summe seiner Teile	21
2.1.1 Warum eigentlich Blockchain?	22
2.1.2 Über Blöcke und das Hashing	23
2.1.3 Zur Aufgabe der Miner	25
2.1.4 Von der Wichtigkeit des Arbeitsnachweises	25
2.1.5 Block-Belohnung und Transaktionsgebühren	27
2.1.6 Mining: Eine faire Art der Seigniorage?	30
2.1.7 Ein Mechanismus zur Schwierigkeitsgradanpassung	31
2.1.8 Das Resultat: Eine dezentrale, weltweit verteilte Datenbank	33
2.1.9 Digitales Eigentum dank digitaler Signaturen	34
2.1.10 Über die dezentralen Buchhalter und Revisoren des Netzwerkes ..	37

2.2	Blockchain ist nicht gleich Blockchain	40
2.2.1	Das Blockchain-Spektrum	40
2.2.2	Erlaubnisfrei und Open-Source	44
2.2.3	Forks: Die Kraft der Abspaltung	45
2.2.4	Verschiedene Arten der Konsens-Findung	47
2.2.5	Herausforderung Skalierung	49
3	Eine monetäre Revolution	55
3.1	Geld, Gold oder gar Garant der Zeit?	55
3.1.1	Ist Bitcoin Geld?	55
3.1.2	Bitcoin: Eine volatile Angelegenheit	59
3.1.3	Preisstabilität: Eine Frage der Liquidität	60
3.2	Zur Knappheit von Bitcoin	63
3.2.1	Ein Modell zur Bemessung der Knappheit?	65
3.2.2	Eine Versicherung gegen Geldentwertung	68
3.2.3	Zäsur in der Geldtheorie: Bitcoin als monetarisierte Zeit	70
3.2.4	Antwort auf die Geldfrage: Bitcoin als neues Basisgeld	71
4	Ein Upgrade auf Institutionenebene	77
4.1	Das Internet des Geldes	77
4.1.1	Ein Protokoll schafft Internet-eigene Werte	78
4.1.2	Der Wert von Institutionen	79
4.1.3	Grundbausteine des Vertrauens	80
4.1.4	Eine Institution mit beispiellosen Garantien	81
4.2	Öffentliche Blockchains als Grundlage für eine Finanzordnung	84
4.2.1	Die Hierarchie des Finanzsystems	84
4.2.2	Bitcoin als mehrschichtige Finanzordnung	87
4.2.3	Blockchain-Basis-Layer: Eine globale Settlement-Infrastruktur	87
4.2.4	Das Lightning-Netzwerk und andere Skalierungsunterfangen	90
4.2.5	Gleiches mit Gleichem vergleichen	93
4.2.6	Für eine Finanzordnung aus einem Guss	94
4.2.7	Unübertroffene soziale Skalierbarkeit	96
5	Kambrische Explosion: Schöne bunte Kryptowelt	99
5.1	Ethereums Aufstieg	99
5.1.1	Smart Contracts und der Weltcomputer	101
5.1.2	Die Turing-Vollständigkeit macht's möglich	102
5.1.3	Treibstoff für die Blockchain	103
5.1.4	Neue Welt der dezentralisierten Finanzen	104
5.1.5	Wallet: Das Tor zur Blockchain-Welt	106

5.1.6	Grundelemente der Finanzwelt	107
5.1.7	Herausforderungen in der DeFi-Welt	113
5.1.8	Der Wunsch nach einer besseren Finanzwelt	117
5.2	Coins und Token	123
5.2.1	Zur klaren Unterscheidung zwischen Coin und Token	124
5.2.2	Vom Schlagwort der Tokenisierung	126
5.2.3	Über die Daseinsberechtigung von Coins	130
5.2.4	Ein Token zur Anreizschaffung	132
5.2.5	Über den Netzwerkinhabereffekt	134
5.3	Ein Kampf, der keiner sein muss	136
5.3.1	Nichts geht über Kompromisse	136
5.3.2	Blockchain-Trilemma: Noch ist alles beim Alten	137
5.3.3	Interoperabilität: Wird alles dereinst eins?	140
5.3.4	Web3: Für ein neues Internet	142
5.3.5	Selbstverwaltete Identität im Blockchain-Zeitalter	144
5.3.6	Dezentralisierung des Internet-Hardware-Stacks	146
5.3.7	Metaverse: Die Entstehung einer neuen Welt	147
6	Krypto als Anlage	151
6.1	Kryptoassets im Portfoliokontext	151
6.1.1	Bitcoins historische Preise-Performance	152
6.1.2	Zur Korrelation von Bitcoin	156
6.1.3	Alles eine Frage des Risikos	158
6.1.4	Auswirkungen von Krypto auf ein diversifiziertes Portfolio	159
6.1.5	Rebalancing oder nicht?	163
6.1.6	Wie viel Bitcoin soll es sein?	166
6.1.7	Diversifikation innerhalb von Krypto	167
6.1.8	Bitcoins Marktdominanz bewegt Altcoins	169
6.1.9	Vergangenheitsgedöns oder Zukunftsmusik?	171
6.2	Krypto: Ein neues Anlageuniversum	172
6.2.1	Jenseits von Kryptowährungen	172
6.2.2	Kryptoassets: Ein Kategorisierungsversuch	173
6.2.3	Zahlungscoin/Kryptowährung	175
6.2.4	Nutzungscoins	176
6.2.5	Nutzungstoken	176
6.2.6	Zahlungstoken	177
6.2.7	Anlagetoken	177
6.2.8	Equity-Token	178

6.2.9	Governance-Token	179
6.2.10	Synthetische Token	180
6.2.11	Non-Fungible Token (NFT)	181
6.3	Bewertungsversuche von Kryptoassets	183
6.3.1	Woher stammt der Wert einer Sache?	183
6.3.2	Worin liegt der Wert von Bitcoin?	185
6.3.3	Angebot und Nachfrage als Ausgangspunkt	186
6.3.4	Kryptoassets und ihre Netzwerkeffekte	188
6.3.5	Quantitätsgleichung: Makroökonomischer Bewertungsansatz	193
6.3.6	Produktionskosten als Bewertungsgrundlage	194
6.3.7	Knappheit messen: Stock-to-Flow als Bewertungsmodell	

7.3.4	Algorithmische Stablecoins	236
7.3.5	Libra: Ein Weckruf für die Welt	239
7.3.6	Die Idee von Multi-CBDC-Vereinbarungen	240
7.3.7	Zur Relevanz von privaten Stablecoins	241
7.3.8	Private Stablecoins: Bedrohung für die Finanzstabilität?	244
7.3.9	Vollgedeckte oder fraktional besicherte Stablecoins	245
7.3.10	Handelsvolumen dank Umlaufgeschwindigkeit	248
8	Die brennende Energiefrage	251
8.1	Energieverbrauch unter Generalverdacht?	251
8.1.1	Der malthusianische Fehlschluss	251
8.1.2	Der Nutzen legitimiert den Verbrauch	252
8.1.3	Energie-gedecktes Geld: Eine Idee, deren Zeit gekommen ist	2

Einleitung

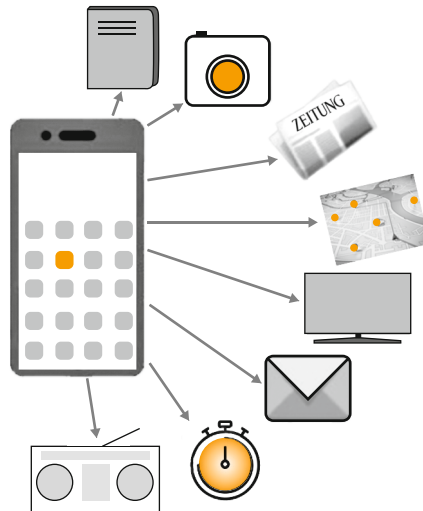
Sie lernen:

- dass Technologie dem Menschen seit jeher dazu verholfen hat, gegenseitige Vertrauensbeziehungen zu skalieren.
- dass Grundlagentechnologien aufeinander aufbauen und gemeinsam Potenzial für neue Innovation schaffen.
- dass mit der Lancierung des Bitcoin-Thesenpapiers am 31. Oktober 2008 eine neue Grundlagentechnologie angestossen worden ist, welche das Konzept echter digitaler Eigentumsrechte geschaffen hat.
- weshalb sich die digitale Ära nach Bitcoin grundlegend von dem unterscheidet, was gewöhnlich unter dem Begriff «Digitalisierung» verstanden wird.
- warum Digitalisiertes in Tat und Wahrheit nicht eigentlich (nativ) digital ist.
- dass Bitcoin und öffentliche Blockchains neue Eigentumssysteme abseits und unabhängig von Nationalstaaten im Cyberspace geschaffen haben.

Des Menschen Wunderwaffe

Die Geschichte

Die Revolution rund um den Personal Computer hat schliesslich zur Feststellung geführt, dass Software unsere Welt [verschlingt](#).⁴ Software gewinnt gegenüber Hardware immer mehr an Relevanz – in vielerlei Hinsicht substituiert Erstere die Letztere sogar. Physikalische Dinge werden zu Software-Applikationen komprimiert. So ist das bereits erwähnte Smartphone heute Telefonbuch, Kamera, Briefpost, Musikhörgerät, Bibliothek, DVD-Sammlung sowie Notizblock [in einem](#).



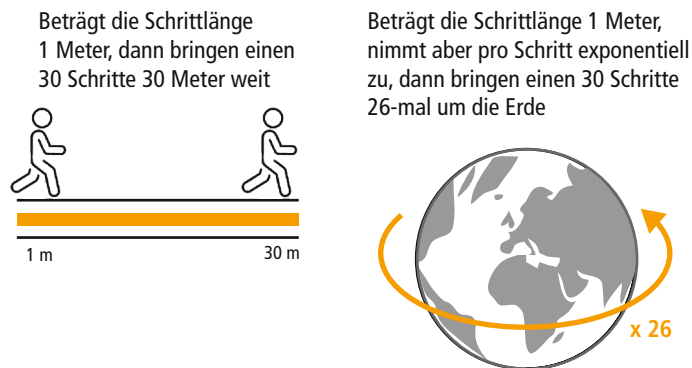
Bis heute ist Bitcoin gemeinhin als Mutter aller Kryptowährungen bekannt. Immer offensichtlicher wird, dass es sich bei Bitcoin nicht nur um eine neue Online-Währung handelt, sondern Bitcoin die organische Entstehung einer mehrschichtigen Geld- und Finanzordnung repräsentiert. Gerade wird die Menschheit Zeuge einer weiteren digitalen Transformation, die uns in eine neue digitale Ära katapultiert.

An der Schwelle zu dieser neuen Epoche können wir bereits erkennen, dass das digitale Zeitalter mit dem Erscheinen von Bitcoin unter neuen Vorzeichen gestellt worden ist. Die digitale Ära nach Bitcoin unterscheidet sich grundlegend von dem, was gegenwärtig unter dem Begriff «Digitalisierung» zusammengefasst wird. Bitcoin hat erstmals echte digitale Eigentumsrechte geschaffen.

Bis zur Ankunft von Bitcoin war das Digitale bloss in eine elektronische Form gegossen. Was im Frontend digital daherkommt, verläuft in Tat und Wahrheit in analogen

Beobachter mitunter verstörend. Der Ruf nach Regulierung oder gar Verboten ist daher unüberhörbar. Unterschiedliche Regulierungsvorhaben sind daher auf dem Weg oder werden angestrebt.

Aufgrund ihrer digitalen Natur grenzt es allerdings an ein Ding der Unmöglichkeit, Kryptoassets verbieten zu wollen. Deren Reich ist das Internet und dieses, obschon heute durch Techgiganten wie Google oder Facebook dominiert, ist im Kern offen und durch keinen Souverän regiert, ähnlich wie das für die Weltmeere [gilt](#).



Dieses Lehrbuch soll eine edukative und gesamtheitliche Sicht auf das Thema von Bitcoin, Blockchain und Kryptoassets geben. Dabei geht es darum, Unwissen zu mindern, indem Missdeutungen korrigiert, Halbwahrheiten entlarvt und Zusammenhänge aufgezeigt werden.

Aufbau und Inhalt

Das Lehrbuch ist in eine Einleitung, 8 Kapitel und eine Schlussfolgerung aufgeteilt. Die Einleitung trägt den Titel «Des Menschen Wunderwaffe» und thematisiert, welche Rolle die Technologie und deren Entwicklung bei der Koordination von Menschen spielt. Kapitel 1 ist der digitalen Renaissance gewidmet, die durch die technologische Entwicklung eingeläutet worden ist. Wir beleuchten die Geburtsstunde von Bitcoin und erklären, weshalb die Entdeckung von Bitcoin im historischen Kontext als Durchbruch epochaler Tragweite zu werten ist. Im Fokus steht das Double-Spend-Problem, für das Bitcoin eine Lösung dar

Als Auftakt von Kapitel 6 widmen wir uns den Kryptoassets im Portfoliokontext. Wir setzen uns damit auseinander, welche konkreten Auswirkungen die Beimischung von Kryptoassets – hauptsächlich Bitcoin – auf ein klassisches Portfolio hat. In einem weiteren Teil führen wir die zahlreichen Kryptoassets als verschiedene Kategorien eines neuen Anlageuniversums ein. Im Anschluss befassen wir uns mit den unterschiedlichen Bewertungsversuchen, mit denen man unterschiedliche Kryptoassets zum heutigen Zeitpunkt zu bewerten versucht.

Kapitel 7 soll eine makroökonomische Einordnung des Krypto-Phänomens bieten. Die Welt der Kryptoassets hat mittlerweile eine Marktkapitalisierung von mehr als einer Billion US-Dollar längst **überschritten**. Bitcoin hat nicht nur das Interesse von Finanzinstituten und anderen Unternehmen gewonnen, auch Zentralbanken scheinen durch die neuen Innovationen angeregt worden zu sein. Wir schildern die möglichen Arten zur Einführung von digitalem Zentralbankgeld, diskutieren deren mögliche Auswirkungen auf die Wirtschaft und spekulieren, wie CBDCs

gegenwärtig unter dem Begriff «Digitalisierung» zusammengefasst wird. Bitcoin hat erstmals echte digitale Eigentumsrechte geschaffen.

- In Wirklichkeit ist Digitalisiertes (jeglicher Art) gegenwärtig nicht an und für sich digital. Es existiert bloss als binäre Buchungseinträge in unterschiedlichen elektronischen Hauptbüchern, zum Beispiel den Datenbanken von Finanzinstitutionen.
- Bitcoin stellt ein digitales Inhaberinstrument dar. Dieser etwas umständliche Begriff meint, dass Bitcoin als Finanzwert mittels kryptografischer Verschlüsselungsmethoden beherrschbar ist.
- Bitcoin und öffentliche Blockchains haben neue Eigentumssysteme abseits und unabhängig von Nationalstaaten im Cyberspace begründet.

8 Die brennende Energiefrage

Sie lernen:

- und wissen Bescheid, dass die Idee eines globalen, nicht-staatlichen Geldes, das mit Energie unterlegt ist, bereits vor Bitcoin thematisiert worden ist.
- dass Bitcoin mit steigendem Energieaufwand als Netzwerk grundsätzlich sicherer wird.
- dass Bitcoins Energieverbrauch stets in Relation zu seinem Nutzen gesetzt werden muss.
- dass sich der Energieverbrauch von Bitcoin in der langen Frist mehr an den Transaktionsgebühren orientieren und die Kosteneffizienz von Bitcoins Sicherheits- und damit Energieaufwand relativ zur Marktkapitalisierung hoch sein könnte.
- weshalb Bitcoin-Mining gestrandete Energiequellen monetarisieren kann.

8.1 Energieverbrauch unter Generalverdacht?

Energie ist die Grundlage allen Lebens. Was keine Energiezufuhr erlebt, stirbt schnell ab. Diese unumstössliche Tatsache auf die Wirtschaftswelt angewendet bedeutet, dass Energie **aufgewendet** werden muss, um Arbeit zu verrichten, welche den Wohlstand steigern kann. Dass der Lebensstandard der westlichen Welt in materieller Hinsicht heute so hoch ist, ist auch unserem verhältnismässig hohen Energieverbrauch zu **verdanken**. Die Bedeutung des Energieverbrauchs im Zusammenhang mit zivilisatorischem Fortschritt und Wohlstand lässt sich eigentlich nicht **leugnen**.

Nichtsdestotrotz scheint das Verbrechen von Energie von gewissen politischen Gruppen immer stärker unter Generalverdacht gestellt zu werden. Deren Credo ist es: Als Gesellschaft sollten wir nicht mehr, sondern weniger Energie verwenden. Während derartige **Aufrufe** zu würdigen und auf individueller Ebene sinnvoll sind, besteht die Gefahr, dem sogenannten **malthusianischen Fehlschluss zu unterliegen**.

8.1.1 Der malthusianische Fehlschluss

Dessen Annahme besteht darin, dass der Mensch ein Nettoenergieverbraucher ist. Wie die Geschichte bislang eindrücklich **zeigt**, ist das Gegenteil der Fall. Bereits etliche Male in der Geschichte der Menschheit wurde eine Ressourcenknappheit prognostiziert. Eine der berühmtesten Publikationen stammt vom Club of Rome und trägt den Titel «**Die Grenzen des Wachstums**». Darin wird vor Überbevölkerung und Umweltkatastrophen gewarnt. Seit der Veröffentlichung dieses Werkes hat sich die Weltbevölkerung beinahe verdoppelt. Die Untergangsszenarien sind nicht eingetroffen und die Ressourcenknappheit ebenso wenig.

Dass dürfte vor allem damit zu tun haben, dass der Mensch eine denkende Spezies ist, die erfinderisch immer wieder neue Möglichkeiten der Energieaufbereitung entdeckt. So brauchen wir Menschen zwar immer mehr Energie, doch **tun** wir das immer effizienter und produktiver, wie das Vaclav Smil in einem Buch «**Energy and Civilization**» eindrücklich zeigt. Das führt dazu,

dass sich die These des Menschen als Nettoenergieverbraucher bislang nicht als richtig erwiesen hat.

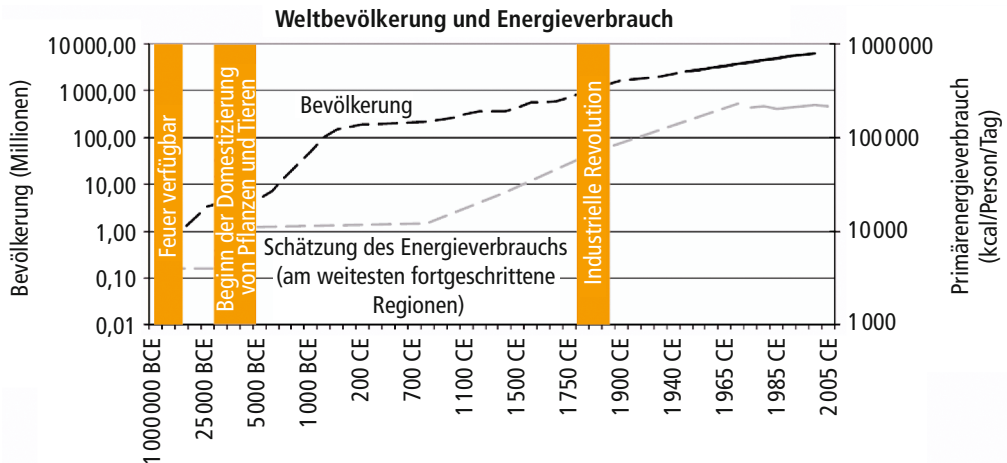


Abbildung 105: Diese Grafik zeigt in groben Zügen die historische Bevölkerungsentwicklung im Vergleich zum täglichen Energieverbrauch pro Person.

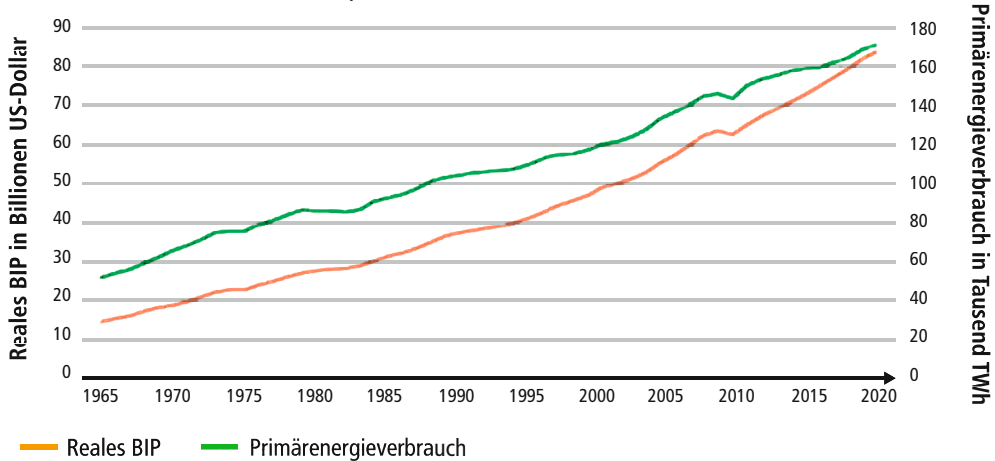
Quelle: *Historical Trends in Global Energy Consumption* von Mattick, Williams & Allenby

Angesichts des hohen Lebensstandards, den sich die Menschheit dank immer effizienterer Nutzung von Energie erarbeitet hat, dürfte weniger Energieverbrauch vor allem materieller Rückschritt bedeuten, weshalb diese malthusianische Auffassung gemeinhin kaum ernsthaft Beachtung findet. Allgemein anerkannter ist die Überzeugung, dass insbesondere der Energieverbrauch fossiler Brennstoffe ein grosses Problem unserer Zeit darstellt. Darüber scheinen sich mehr und mehr Menschen einig zu werden.

Genauso wie der Konsens über die Schattenseiten des fossilen Energieverbrauchs wächst, so sollte auch Einigkeit darüber bestehen, dass die Menschheit

anlagen, Ventilatoren, Transportmittel sowie Computer oder das Internet, welche eine riesige Menge an Energie verbrauchen, gleichzeitig aber die Lebensqualität erheblich erhöht haben.

Chart 2:
Globales reales BIP und Primärenergieverbrauch in
Billionen US-Dollar & Tsd. TWh, 1965–2019



Quellen: BP Statistical Review of Global Energy, The World Bank

Abbildung 106: In der langen Sicht betrachtet, ist der globale Energieverbrauch eng mit dem globalen Bruttoinlandprodukt korreliert.

Quelle: Bitcoin Net Zero, NYDIG

Der Nutzen, den diese Innovationen stiften, rechtfertigt schliesslich deren Energieverbrauch, so dass es kaum gesellschaftliche Diskussionen darüber gibt, ob man den Gebrauch von Kühlschränken oder Computern einschränken sollte. So sind es diese technologischen Durchbrüche, die das Leben in den unterschiedlichen Jahreszeiten erträglicher und lebenswerter, die Hausarbeit einfacher und bequemer und die Weltwirtschaft funktionaler und effizienter machen.

In derselben Frage des Nutzens liegt auch der Umstand begründet, weshalb Bitcoin als neue Technologie in der brennenden Energiefrage bislang einen schweren Stand hat. Wie in Kapitel 3 und 4 aufgezeigt, handelt es sich bei Bitcoin um eine Innovation in Form eines neuartigen Basisgeldes, das ein globales, nicht-staatliches Geld- und Finanzsystem ermöglicht und auf der Grundlage dezentral durchgesetzter Konsens-Regeln und wirtschaftlicher Anreizmechanismen funktioniert. Als solches bietet Bitcoin ein einzigartiges System von kryptografisch verankerten digitalen Eigentumsrechten.

Wie in den Anfängen bahnbrechender Technologien üblich, werden die Vorzüge, Chancen und Möglichkeiten von Bitcoin kaum durch den gesamten potenziell adressierbaren Markt vollumfänglich wahrgenommen geschweige

Wo aber liegt der Nutzen. Wie in Kapitel 6 gelernt, ist dieser subjektiv begründet: Für alle jene, die Bitcoin nutzen, schafft das Kryptoasset einen Mehrwert, sonst würden sie es nicht nutzen. Jede TWh-Energie, welche zur Sicherung der Bitcoin-Blockchain aufgewendet wird, ist es in den Augen der Nutzer wert, konsumiert zu werden. Ob [russische Oppositionelle](#) oder [nigerianische Geschäftsleute](#), diese und andere Menschen weltweit profitieren von Bitcoins Existenz als sicherem und unaufhaltsamem Wertübertragungsmittel.

Wer in Bitcoin demnach einen Nutzen sieht, für den relativiert sich die Energiefrage etwas. Es kommt dann nicht darauf an, ob Bitcoin Energie verbraucht, sondern vielmehr ist die Frage entscheidend: Wie viel Energie und welche Art von Energie verbraucht Bitcoin.

8.1.3 Energie-gedecktes Geld: Eine Idee, deren Zeit gekommen ist

Wer in Bitcoin gegenwärtig keinerlei Sinn, Funktion oder Nutzen sehen kann, dem fällt es nicht schwer, dessen Energieverbrauch als totale Verschwendung abzutun. Warum sollte man Energie zur Schaffung eines Basisgeldes aufwenden? Im Verständnis der meisten Menschen muss Geld doch durch den Staat geschaffen, rechtlich institutionalisiert und somit offiziell legitimiert werden.

Historisch spannend ist, dass die Idee eines globalen, nicht-staatlichen Geldes, das mit Energie unterlegt ist, schon lange Zeit vor der Ankunft Bitcoins von klugen Menschen angedacht worden ist. Kein Geringerer als Henry Ford, der Anfang des 20. Jahrhunderts dem Auto zum Durchbruch verhalf, plädierte für eine Energiewährung. Sein [Argument](#): Ein derartiges Geld würde nicht so leicht kontrolliert werden können wie beispielsweise Gold. Stattdessen würde jedes Land dieses Geld basierend auf seinen Energieressourcen mit emittieren können. Der Prozess der Geldschöpfung wäre auf diese Weise global verteilt und würde nicht einem einzigen Staat zufallen, so wie das heute mit dem US-Dollar der Fall ist. Dieser verleiht den Vereinigten Staaten gegenwärtig das sogenannte [exorbitante Privileg](#) und macht es möglich, dass die USA ihre US-Dollar als Leit- und Reservewährung in die gesamte Welt exportieren können.

Ebenfalls [aufgegriffen](#) hat diese Idee der Universalgelehrte Richard Buckminster Fuller, als er Vermögen und Wohlstand als Energie definierte und prognostizierte, dass wir dereinst ein wissenschaftliches Buchhaltungssystem (eine Blockchain vielleicht?) haben würden, das über dieses Vermögen Buch führt.

Tischgespräch: Mit Vulkanenergie Bitcoin schürfen

Bitcoin-Mining-Maschinen werden in einer geothermischen Anlage am Fuss eines Vulkans in El Salvador [betrieben](#). Diese Art der geothermischen Energie ist nicht nur rund um die Uhr verfügbar, sie gilt auch als eine der saubersten Energiequellen, welche die Natur zu bieten hat. Durch den Anschluss an das Bitcoin-Mining kann ein aufstrebendes Land wie El Salvador am globalen Aufstieg eines neuen globalen Basisgeldes teilhaben. Die Geldschöpfung (Seigniorage) ist nicht mehr auf einige wenige Institutionen beschränkt, sondern steht allen offen. Gut möglich also, dass die Energieerzeuger von heute die Banken von morgen sind.

Wie von diesen grossen Denkern angedacht, existiert ein solches Energiegeld seit 2009. Bitcoin erfüllt Henry Fords Definition ziemlich exakt: So schlug er eine Währung vor, die durch Kilowattstunden (kWh) gedeckt ist – genauso wie es bei Bitcoin [heute der Fall](#) ist: Die Kryptowährung ist durch Energieeinsatz, auch Proof-of-Work genannt, gedeckt. Neue Bitcoin-Einheiten werden nur gegen geleistete Arbeit, das heisst durch die Bereitstellung von Rechenleistung, ausgegeben. Je mehr Energie ein Miner aufwendet, desto höher die Wahrscheinlichkeit, dass er dafür Bitcoin erhält. Mit steigendem Aufwand durch alle Miner wird es für den einzelnen Miner allerdings auch immer schwieriger und teurer, neue Bitcoin zu minen. So sieht es das Bitcoin-Protokoll vor.

Letztlich folgt das Netzwerk einer einfachen Gleichung: Je mehr Energie Bitcoin absorbiert und auf sich vereint, desto sicherer und zuverlässiger wird das Netzwerk als Settlement-Infrastruktur. Aus der Sicht eines Netzwerknutzers bedeutet der stetig steigende Energieaufwand von Bitcoin, dass das Netzwerk und somit die durch den Nutzer getätigten Transaktionen sicherer werden, da es auch mehr Energie benötigen würde, das System erfolgreich zu attackieren. Wo genau die Schwelle liegt, ab der Bitcoin als unsicher gelten würde, ist kaum auszumachen. Es ist aber davon auszugehen, dass das Bitcoin-Netzwerk auch Ende 2021 für seine eigene Sicherheit zu viel bezahlt und daher mehr Energie als eigentlich nötig verbraucht. Wie viel Energie das Bitcoin-System konsumiert, ist eine spontane Marktentscheidung global verteilter Akteure.

Gut zu wissen: Energieeffizienterer Konsens-Mechanismus?

Von einigen Vertretern der Kryptoszene werden andere Konsens-Mechanismen als umweltfreundlicher angepriesen. Allen voran Proof-of-Stake, wo beinahe keine externe Energie mehr aufgewendet wird, sondern die Blockchain-eigenen Coins «gestakt», also aufs Spiel gesetzt werden. Auf den ersten Blick stimmt es, dass dieser Konsens-Mechanismus weniger Energie konsumiert. Die Frage ist aber: Zu welchem Preis? Der Proof-of-Stake ist als Konsens-Mechanismus grundsätzlich komplexer, was mehr Angriffsvektoren schafft, weshalb seine ökonomischen Garantien zum heutigen Zeitpunkt weniger erprobt sind – zumindest in einem Ausmass, wie das für ein Netzwerk der Grösse Bitcoins der Fall ist. Erst die Zukunft wird zeigen können, ob Proof-of-Stake für einen Anwendungsfall eines globalen, nicht-staatlichen Basisgeldes auch geeignet ist.

8.1.4 Bitcoins Energieverbrauch: Eine Frage der Perspektive

Dass Bitcoins Energieverbrauch den für das Bitcoin-Netzwerk so essenziellen Nutzen der Sicherheitsbereitstellung gewährleistet, geht häufig vergessen. In den Medien wird oftmals einzig und allein auf den Bitcoin-Preis und somit auf die Kosten des Bitcoin-Energieverbrauchs fokussiert.

Wie emotional und überrissen die Berichterstattung zu diesem Thema ist, führt ein Beispiel aus dem Jahr 2017 vor Augen. Dazumal haben mehrere Medien davon [gewarnt](#), dass das Mining für die Kryptowährung im Jahr 2020 voraussichtlich die gesamte Energieproduktion unseres Planeten beanspruchen würde. Heute, wo wir dieses Jahr bereits passiert haben, können wir schliessen: Diese Warnrufe waren mächtig übertrieben.

9 Schlussfolgerung

Sie lernen:

- und kennen die verschiedenen Varianten von zukünftigen Basisgeldern.
- dass öffentliche Blockchains den neutralen Boden in einer sich zuspitzenden geopolitischen Auseinandersetzung zwischen China und den USA darstellen könnten.
- dass währenddem die Chinesen auf ein zentralisiertes digitales Zentralbankengeld setzen, sich die durch die USA angeführte westliche Achse auf die Innovationen rund um private Stablecoin-Projekte einlassen wird.
- dass eine CBDC per Definition nicht nativ-digital sein kann.
- wie Bitcoin das Verständnis von Eigentum neu definiert hat.

9.1 Zur Zukunft von Geld und der Welt

In der Einleitung zu diesem Lehrbuch wurde davon gesprochen, dass wir uns gegenwärtig an der Schwelle einer neuen Ära befinden. Ausgangspunkt ist das Hervortreten einer neuen Grundlagentechnologie in der Gestalt öffentlicher Blockchains. Diese haben unseren Umgang mit dem Digitalen für immer verändert. So ist Digitales in der Form digitaler Inhaberinstrumente exklusiv kontrollier- und beherrschbar geworden. In Verbindung mit der Blockchain-Technologie können digitale Daten nicht-kopierbar gemacht werden. Dank der Blockchain erhalten Bits and Bytes einen digitalen Sachcharakter. Aufgrund dieser digitalen Körperlichkeit und der Möglichkeit der exklusiven Beherrschbarkeit werden digitale Daten so zu digitalen Werten. Diese Art von virtuellem Wert haben wir mit dem neuartigen Begriff «nativ-digital» zu erfassen versucht.

Das Ausmass und die Tragweite dieser Zäsur ist zum heutigen Zeitpunkt kaum abschliessend zu fassen. Auszumachen ist, dass unsere Vorstellung und die Konzeption von Geld nachhaltig und weitreichend auf den Kopf gestellt wird. Die schrittweise Etablierung von Bitcoin als neues digitales Basisgeld veranschaulicht diesen Umstand treffend.

Bitcoin ist allerdings weniger ein direktes Update unseres gegenwärtigen Fiatgeldes, sondern vielmehr eine neuartige Alternative dazu. Als digitales Basisgeld ist mit Bitcoin das Fundament für eine neue Finanzordnung geschaffen worden. Diese basiert auf einer nicht-staatlichen, unabhängigen und dezentralisierten Settlement-Infrastruktur.

In Grundzügen ist diese gegenwärtig vor allem auf Ethereum, der zweitgrössten öffentlichen Blockchain, auszumachen. Inwiefern es sich bei Ethereum langfristig um eine ernstzunehmende Alternative, vielleicht sogar um einen Kontrahenten unter diesen neuen Settlement-Infrastrukturen handelt, ist unklar. Nicht auszuschliessen ist, dass diese neuen öffentlichen Blockchains keine Gegenspieler sind, sondern symbiotische Systeme, die ihren jeweiligen Kompromissen gemäss neben- und miteinander gedeihen.

Sicher ist, dass diese neuen Systeme das traditionelle Geld- und Finanzwesen mitprägen, herausfordern und aus der Reserve locken. Als Folge der steigenden Relevanz von Bitcoin und Co.

sind die Mühlen von Regierungsinstitutionen und Zentralbanken in Bewegung gesetzt worden. Die Bestrebungen rund um CBDCs verdeutlichen dies.

9.1.1 Geopolitisches Hickhack: Digitales Geld in der Hauptrolle

Tatsache ist, dass die Anzahl möglicher Konzeptionen von Basisgeldern zugenommen hat. Ganz grob dürften sich in absehbarer Zukunft folgende Varianten vorfinden:

- CBDCs: Politisch, rechtlich orchestriertes Basisgeld in Form nationaler Währungen
- Gold: Durch die Natur im Angebot beschränktes Basisgeld
- Bitcoin: Im Angebot algorithmisch absolut beschränktes Basisgeld
- Ether: Algorithmisches Basisgeld mit an die Netzwerkauslastung angepasster Inflation

Basisgelder wie Bitcoin, Ether oder ähnliche werden den digitalen Raum beherrschen. Neue, sich über das global verteilte Internet formende Netzwerkstaaten werden derartige Basisgelder als monetären Standard adoptieren. Das schafft neue, unkonventionelle Währungsgebiete (hauptsächlich digitaler Natur), die mit anderen Währungsgebieten im Wettstreit stehen werden.

Selbst das allgemein für totgedachte Basisgeld Gold könnte dank fortschreitender Technologisierung eine Art Renaissance erleben. So gibt es Versuche, über den Weg der Tokenisierung das gelbe Edelmetall für das digitale Zeitalter fit zu machen. Andere Versuche bestehen darin, Geldscheine aus Gold [zu drucken](#). Beide Ansätze gehen dahin, Gold als transaktionsfähiges Medium aufzuwerten.

Mehr als Gold aber werden sich CBDCs als geeignete Basisgeldalternativen hervortun wollen. Diese haben die Rückendeckung von Staaten, und erste Zentralbanken sind bereits dabei, CBDCs nach Möglichkeit einzuführen. Einige kleinere Staaten haben ein digitales Zentralbankengeld auch schon lanciert. In den Bahamas wurde der digitale Bahama-Dollar, auch Sand-Dollar genannt, [gestartet](#).¹ Genauso wurde in den ostkaribischen Staaten die eigene Dollar-Währung in der Form einer CBDC unter dem Namen DCashEC² ins Leben [gerufen](#). Und auch Nigeria [verfügt](#) seit dem vierten Quartal von 2021 über eine CBDC. In Ländern wie Jamaika oder Uruguay hat man entweder bereits einen Pilotversuch absolviert oder stand Ende Oktober 2021 kurz davor, einen zu [beginnen](#).³

9.1.2 China macht vorwärts mit dem E-Yuan

In China zeichnet sich das neue (Geld-)System schon deutlich ab. Klar ist, dass man hier auf das CBDC-Konzept setzen wird. Offiziell eingeführt wurde dieser E-Yuan an den olympischen Winterspielen in Peking Anfang 2022. Auf nationaler Ebene haben die chinesischen Nationalspiele vom September 2021 bereits als Testbecken gedient. Lokalen Medien zufolge akzeptierten viele Offline-Verkäufer an den Austragungsorten den digitalen Yuan als Zahlungsmittel.

Als CBDC-Projekt soll der digitale Yuan in ein gesamtes System – auch [Digital Currency and Electronic Payment](#) (DCEP) genannt – eingebettet werden. Anders als andere CBDC-Vorhaben basiert dasjenige von China vollständig auf einer zentralisierten Datenbank. Obwohl eine Aus-

1 [Digital Bahamian Dollar Sand Dollar](#).

2 [ECCB Connects - DCash Launch](#)