

FLASH-
CARDS
INSIDE

Filip Balonis
Alex von Frankenberg

Bitcoin Durchblick

Wirtschaftliche, gesellschaftliche
und technische Zusammenhänge
verstehen

SACHBUCH

 Springer

Bitcoin Durchblick

SPRINGER NATURE

FLASH-
CARDS
INSIDE

SN Flashcards Microlearning

Schnelles und effizientes Lernen mit digitalen Karteikarten – für Arbeit oder Schule!

Diese Möglichkeiten bieten Ihnen die SN Flashcards:

- Jederzeit und überall auf Ihrem Smartphone, Tablet oder Computer **lernen**
- Den Inhalt des Buches lernen und Ihr Wissen **testen**
- Sich durch verschiedene Fragetypen **motivieren lassen** und zwischen 3 Lernalgorithmen **wählen**
- Ihre eigenen Fragen-Sets **erstellen**, um Ihre Lernerfahrung zu **personalisieren**

So greifen Sie auf Ihre SN Flashcards zu:

1. Gehen Sie auf die **1. Seite des 1. Kapitels** und folgen Sie den Anweisungen in der Box.
2. Laden Sie die SN Flashcards App aus dem Apple App Store oder Google Play Store herunter und folgen Sie den Anweisungen in der App.
3. Wählen Sie die Lernkarten für dieses Buch aus und beginnen Sie zu lernen!

Probleme? Schreiben Sie bitte eine E-Mail an

customerservice@springernature.com und geben Sie in der Betreffzeile „**SN Flashcards**“ und den Buchtitel an.

Filip Balonis •
Alex von Frankenberg

Bitcoin Durchblick

Wirtschaftliche,
gesellschaftliche und
technische Zusammenhänge
verstehen

 Springer

Filip Balonis
Köln, Deutschland

Alex von Frankenberg
Bonn, Deutschland

ISBN 978-3-658-47405-8 ISBN 978-3-658-47406-5 (eBook)
<https://doi.org/10.1007/978-3-658-47406-5>

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <https://portal.dnb.de> abrufbar.

© Der/die Herausgeber bzw. der/die Autor(en), exklusiv lizenziert an Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2025

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsgesetz zugelassen ist, bedarf der vorherigen Zustimmung des Verlags. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Die Wiedergabe von allgemein beschreibenden Bezeichnungen, Marken, Unternehmensnamen etc. in diesem Werk bedeutet nicht, dass diese frei durch jede Person benutzt werden dürfen. Die Berechtigung zur Benutzung unterliegt, auch ohne gesonderten Hinweis hierzu, den Regeln des Markenrechts. Die Rechte des/der jeweiligen Zeicheninhaber*in sind zu beachten.

Der Verlag, die Autor*innen und die Herausgeber*innen gehen davon aus, dass die Angaben und Informationen in diesem Werk zum Zeitpunkt der Veröffentlichung vollständig und korrekt sind. Weder der Verlag noch die Autor*innen oder die Herausgeber*innen übernehmen, ausdrücklich oder implizit, Gewähr für den Inhalt des Werkes, etwaige Fehler oder Äußerungen. Der Verlag bleibt im Hinblick auf geografische Zuordnungen und Gebietsbezeichnungen in veröffentlichten Karten und Institutionsadressen neutral.

Planung/Lektorat: Catarina Gomes de Almeida

Springer ist ein Imprint der eingetragenen Gesellschaft Springer Fachmedien Wiesbaden GmbH und ist ein Teil von Springer Nature.

Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

Wenn Sie dieses Produkt entsorgen, geben Sie das Papier bitte zum Recycling.

Vorwort

Bitcoin ist einfach nur eine neue Technologie mit bestimmten Eigenschaften. Im Grunde ist Bitcoin eine Datenbank, die anders als heutige Hochleistungsdatenbanken, sehr langsam und umständlich neue Einträge hinzufügt. Vier Eigenschaften machen Bitcoin so besonders:

Eine wesentliche Eigenschaft dieser Datenbank ist Dezentralität: Es gibt nicht einen Ort, sondern tausende, an denen sich Kopien der Datenbank befinden und niemand, keine zentrale Entität, hat die Kontrolle über das System, die Datenbank und insbesondere die Einträge in die Datenbank. Die zweite Eigenschaft ist der Bitcoin, der Teil der Datenbank ist, die dritte ist die Limitierung der möglichen Anzahl aller Bitcoin auf 21 Mio. und die vierte ist die Offenlegung und Nachvollziehbarkeit der Software, die das ganze System steuert. Sie ist OpenSource und damit ist transparent, wie das System funktioniert. Das Vertrauen in das System ergibt sich nicht aus einer zentralen Stelle, sondern der Dezentralität und Transparenz des Systems.

Aus diesen vier Eigenschaften ergibt sich etwas ganz Besonderes: Bitcoin ist ein digitales Gut, das nicht kopiert

oder vermehrt, aber sehr leicht transferiert werden kann. Das ist etwas fundamental Neues in der Menschheitsgeschichte: Bisher konnten digitale Güter nur kopiert werden: Eine Information, die an einen neuen Ort gebracht wurde, existiert am alten Ort weiter. Ein Geheimnis, das geteilt wird, existiert an zwei Orten. Es ist kein Geheimnis mehr.

Der weltverändernde Erfolg von Gutenbergs Buchdruck liegt in der schnellen und kostengünstigen Vervielfältigung von Informationen. Plötzlich stand Wissen grundsätzlich allen Menschen zu Verfügung. Das Internet beschleunigte die Verbreitung von digitalen Gütern noch viel mehr. Mit dem Smartphone haben wir heute Zugang zu dem fast vollständigen Weltwissen. Wir können von fast allen Orten der Welt miteinander kommunizieren, arbeiten und lernen.

Zweifellos hat die Vervielfältigung von Informationen die Welt und unsere Gesellschaften mehr verändert als fast alle anderen Innovationen zuvor.

Bitcoin hat das Potenzial, durch die Nicht-Vervielfältigung von Informationen ebenfalls die Welt fundamental zu verändern. Die Begrenztheit des Bitcoin auf 21 Mio. führt nicht nur zu einem eindeutig begrenzten Gut, sondern zu einem begrenzten *digitalen* Gut. Bitcoin ist digitale Knappheit, *digital scarcity*. Die *eindeutige* Begrenztheit von Bitcoin ist einzigartig: Beispielsweise glauben wir, dass Gold begrenzt ist, wir wissen aber nicht, wieviel sich noch in der Erdkruste verbirgt. Ganz im Gegenteil: Wir wissen, dass es Asteroiden aus purem Gold gibt, deren Menge jeden Menschen zum Multimilliardär machen würde. Noch sind solche Asteroiden unerreichbar. Sobald sich das ändert, ist Gold fast so verfügbar, wie Sand am Meer. Es ist völlig offensichtlich, was dann mit der Wertentwicklung von Gold passieren würde! Der Wert von Gold ginge gegen Null!

Die absolute und damit einzigartige Knappheit von Bitcoin verspricht, Bitcoin zu einem einzigartigen Wert-

speicher zu machen. Bitcoin könnte ein neues Geld werden, dass dem bisherigen Geld, den sogenannten *Fiatwährungen*, wie US-Dollar, Euro oder Yuan, oder auch Gold, einem ehemaligen Geld, in vielen Aspekten überlegen ist. Fiatwährungen sind sehr gut für den täglichen Gebrauch geeignet. Wir können bar oder bargeldlos beim Bäcker unsere Brötchen bezahlen. Fast überall auf der Welt kann man via VISA oder Mastercard in unterschiedlichsten Währungen bezahlen. Die Fiatwährungen sind tief integriert in Gesellschaft und Staat. Banken sorgen für einen effizienten und effektiven Transfer von Sparern zu Kreditnehmern. Über die Geldschöpfung (= Geldschaffung oder auch *Geld drucken*) generieren Banken Kredite für Unternehmen, Häuserbauer, Konsumenten aber auch Staaten. Zentralbanken stellen die Geldversorgung und hin und wieder die Stabilität des Finanzsystems sicher. Ab und zu finanzieren sich die Staaten, in dem die Zentralbanken deren Anleihen mit neu geschaffenem Geld kaufen. Die Wirtschaft funktioniert. Einigermmaßen.

Das Fiat-Geldsystem hat ein großes Problem: Der Wert des Geldes verfällt. Manchmal langsam, manchmal schnell. Die westlichen Zentralbanken streben eine Inflation, oder anders ausgedrückt einen Verfall des Geldes, von 2 % pro Jahr gemessen am durchschnittlichen Warenkorb (Verbraucherpreisindex) an. Manchmal liegt die offizielle Geldentwertung darunter, zuletzt auch deutlich darüber. Die Kaufkraft des Fiatgeldes verringert sich kontinuierlich. Selbst bei 2 % Inflation halbiert sich die Kaufkraft des Geldes in ungefähr 35 Jahren. Die Österreichische Schule der Nationalökonomie dagegen definiert die Inflation als die Ausweitung der Geldmenge. Seit der Einführung des Euros hat sich die M2-Geldmenge jährlich um 6 % erhöht. Das würde bedeuten, dass sich der Geldwert in ungefähr 12 Jahren halbiert. Nach 36 Jahren wäre von einem Euro nur noch die Kaufkraft von rund 12,5 Cent übrig. Wenn sich

die Preise des täglichen Bedarfs im Vergleich zur Ausweitung der Geldmenge nur unterdurchschnittlich erhöhen, so gibt es andere Güter, deren Preise weit überdurchschnittlich steigen. Zum Beispiel deutsche Aktien rund 8 % p.a. (DAX 1987–2023) oder Immobilien rund 7 % pro Jahr in deutschen Großstädten von 2015 bis 2023, Gold übrigens auch 8 % pro Jahr. Der Preisanstieg von Aktien führt dazu, dass es immer schwerer wird, Aktienvermögen aufzubauen, der Preisanstieg von Immobilien führt dazu, dass diese immer unerschwinglicher werden, insbesondere für junge Menschen und Familien. Denn die Lohn- und Gehaltsentwicklung orientiert sich an der Entwicklung des Verbraucherpreisindex. Das heißt Löhne und Gehälter steigen unterdurchschnittlich im Vergleich zu Aktien, Immobilien und Gold.

Der typische Deutsche legt sein Geld auf das Sparkonto. Weniger als 20 % der Haushalte in Deutschland besitzen Aktien, die Wohneigentumsquote liegt unter 50 %. Sehr wahrscheinlich schaffen es die allermeisten Deutschen nicht, ihr Ersparnis vor dem Wertverfall durch Inflation zu schützen. Wird die Inflation mit der Ausweitung der Geldmenge beziffert, schafft auch kaum jemand ihre oder seine Entlohnung entsprechend zu steigern. Inflation enteignet die breite Masse der Bevölkerung. Weltweit.

Die weltweite M2-Geldmenge entspricht rund 80 Billionen US-Dollar. Wenn die durchschnittliche Inflation weltweit 5 % betragen würde (sehr wahrscheinlich ist sie höher), dann würden jedes Jahr 4 Billionen Dollar an Werten vernichtet. Das entspricht ungefähr dem Bruttosozialprodukt von Deutschland. Genau genommen werden die Werte nicht vernichtet, sondern umverteilt: Von denen, die Geld halten, zu denen, die das neu geschaffene Geld bekommen. Dieser Prozess wird mit dem Cantillon-Effekt beschrieben: Nicht alle in einer Gesellschaft bekommen gleichmäßig neu geschaffenes Geld, sondern nur wenige. Diejenigen,

die es zuerst bekommen, profitieren davon. Diejenigen, die gar kein neues Geld bekommen, leiden unter gestiegenen Preisen. Typischerweise verteilt Inflation Kaufkraft von unten nach oben. Vermögende profitieren von steigenden Vermögens-Preisen, können vielleicht unternehmerische Gewinne überproportional oder die Entlohnung überproportional steigern. Die Bürgerin oder der Bürger verlieren Kaufkraft. Regelmäßig wird Inflation nicht nur zu einem sozialen, sondern auch zu einem gesellschaftlichen und politischen Problem. Wenn eine hohe Inflation breite Bevölkerungsschichten enteignet, werden Gesellschaften und politische Systeme regelmäßig destabilisiert.

Bitcoin ist eine Lösung für das weltweit sehr große Problem der Geldentwertung. Bitcoin, durch die Eigenschaften der Dezentralität und Limitierung auf 21 Mio., ist langfristig nicht inflationär. Damit eröffnet Bitcoin die Chance, Werte über einen langen Zeitraum in die Zukunft zu transportieren. Die bisher gut 15-jährige Geschichte von Bitcoin hat gezeigt, dass sich der Wert des Bitcoin durch zunehmende Akzeptanz ganz erheblich steigern kann. Als am 3. Januar 2009 der erste Bitcoin-Block, das heißt der erste Eintrag in die Bitcoin-Datenbank, geschrieben wurde, war der Wert Null. Im Februar 2025 bewegte sich der Bitcoin-Preis zwischen 80.000 und 100.000 US-Dollar. Wenn die Akzeptanz, das heißt die Nachfrage, von Bitcoin ähnlich wie in den letzten Jahren fortschreitet, besteht die Möglichkeit, dass sich der Preis von Bitcoin weiter, vielleicht sehr deutlich, erhöht.

Bitcoin verspricht nicht nur einen überlegenen Wertespeicher und potenziell in Fiatgeld gemessen attraktive Renditen. Bitcoin ist auch ein System außerhalb des etablierten Finanzsystems. In der Finanzkrise 2008/2009 stand das Finanzsystem vor einem Kollaps. 2013 wurden in Zypern die dortigen Banken durch Beschlagnahmung („Bail-in“) der Einlagen, die 100.000 € überstiegen, ge-

rettet. Der Wertspeicher Bitcoin funktioniert unabhängig vom etablierten Finanzsystem. Nicht inflationierendes, das heißt stabiles oder auch *hartes* Geld kann vielfältige positive Effekte haben: Es lohnt sich zu sparen. Der damit einhergehende Verzicht auf Konsum schont die Ressourcen und die Erde. Es incentiviert zu langfristigem Denken und vermeidet kurzfristig lohnende, aber langfristig schädliche Entscheidungen.

Bitcoin und die dahinter liegende Technologie sind neu und komplex. Genauso sind beispielsweise der Verbrennermotor und das Internet komplex. Wir müssen die Details nicht unbedingt verstehen, um eine Technologie nutzen zu können. Dieses Buch gibt einen sehr guten und verständlichen Blick in die Entstehung, die Funktionsweise und die Effekte von Bitcoin. Wenn man Bitcoin einmal verstanden hat, ist es sehr einfach. Denn es ändert sich nicht oder nur minimal über die Zeit. Anders als Unternehmen und deren Aktien, die permanentem technologischen Wandel, neuen Regulierungen, veränderten Märkten und neuem und verändertem Wettbewerb ausgesetzt sind, ist Bitcoin seit seiner Entstehung am 3. Januar 2009 nahezu unverändert.

Entscheidend sind die Dezentralität und die Begrenzung von Bitcoin auf 21 Mio. zu verstehen. Im Kontext einer fortwährenden Entwertung von Fiat-Währungen ermöglicht Bitcoin, geleistete Arbeitszeit, ein wesentlicher Teil des Lebens, in Form eines stabilen, nicht inflationierenden Geldes in die Zukunft zu transportieren. Inflation lässt unsere Kaufkraft und damit die Zeit, die wir aufgewendet haben, die Kaufkraft zu erarbeiten, zerrinnen. Bitcoin ist eine Lösung für dieses sehr große Problem. Dabei ist Bitcoin kein Gegner des Fiatgeldes. Er ergänzt das Fiat-Geldsystem mit Stärken, die dieses nicht hat. Möglicherweise weist Bitcoin heute noch Schwächen auf, die das bisherige Fiatgeld durchaus rechtfertigen. Ähnlich wie das Fiatgeld ursprüng-

lich mit Gold unterlegt war, könnte eine Bitcoin-Unterlegung zur dauerhaften Stabilität der Währungen und des Finanzsystems beitragen. Die Beziehung zwischen Bitcoin und Fiatwährungen könnte durchaus eine symbiotische sein.

Es mag sich für Einzelne, Unternehmen wie auch Staaten und Zentralbanken sehr lohnen, Bitcoin zu verstehen. Dieses Buch hilft dabei.

Dr. Alex von Frankenberg
(Wirkte unterstützend bei diesem Werk mit.)

Danksagung

An erster Stelle geht mein Dank an den Erfinder oder die Erfindergruppe von Bitcoin: Satoshi Nakamoto. Wer auch immer sich hinter diesem Pseudonym verbirgt, hat Großes erschaffen. Auch möchte ich mich bedanken bei dem mittlerweile leider verstorbenen Hal Finney. Er gilt als der erste Nutzer von Bitcoin nach Satoshi Nakamoto selbst und empfing überdies die erste Bitcoin-Transaktion. In diesem Zusammenhang ist auch Adam Back zu nennen, der mit seiner Technologie *Hashcash* die Basis für den Arbeitsnachweis im Bitcoin-Netzwerk legte. Bis heute spielt er als CEO von *Blockstream* eine bedeutende Rolle im Bitcoin-Ökosystem und gilt in den Augen vieler als wichtigster Einflussnehmer auf Bitcoin. Weiterhin geht mein Dank an alle, die an einer der zahlreichen Vorgänger- und Teiltechnologien, auf denen Bitcoin aufbaut, beteiligt waren.

Die zur heutigen Zeit wohl präsenteste Bitcoin-Persönlichkeit ist zweifelsfrei Michael Saylor. Kaum ein Zweiter thematisiert das Thema in der Öffentlichkeit mit einer solchen Präsenz und Überzeugung. Darüber hinaus kauft er mit seinem Unternehmen *Strategy* (ehem. *MicroStrategy*)

selbst Bitcoin in spektakulärem Ausmaß. In Deutschland gilt Roman Reher als bedeutendster Experte. Auf seinem YouTube-Kanal *Blocktrainer*, dem weltweit größten *Bitcoin only* YouTube-Kanal, klärt er umfangreich über das Thema auf und bezieht tagtäglich Stellung zu aktuellen Ereignissen rund um Bitcoin.

Darüber hinaus möchte ich mich bei der gesamten Bitcoin-Community in Deutschland bedanken, die sich für das Thema einsetzt und Kanäle zum Informationsaustausch schafft. Dabei vor Allem bei der *Einundzwanzig-Community*: Neben ihrem vielseitigen Podcast organisiert der Verein Events, Meetups und viele weitere Formate der gemeinschaftlichen Auseinandersetzung mit Bitcoin.

Bezogen auf dieses Buch hat mich in erster Linie mein Co-Autor Dr. Alex von Frankenberg (@Justdoitalex) begleitet. Sowohl die Konzeptentwicklung, Inhalte und Vermarktung sind durch seine umfangreiche Unterstützung geprägt und ich hätte dieses Projekt alleine so erfolgreich nicht auf die Beine stellen können. Auch Jan-Paul vom Podcast *Nodesignal* (@actionslave21) hat durch sein inhaltliches Lektorat eine relevante Rolle dabei gespielt, vor Allem die technischen Kapitel zu präzisieren. Das erste umfangreiche Lektorat führte Dr. Andreas Olmes durch und setzte damit in einem Frühstadium des Buches wichtige Impulse.

In meinem persönlichen Umfeld geht mein Dank hauptsächlich an meine Verlobte Jule, die mich seit Jahren bei diesem Projekt umfassend begleitet und mir stets allseitiges Feedback gibt. Auch bei meinen Eltern Mirek und Ewa möchte ich mich für die Unterstützung und Beratung bedanken.

Abschließend wäre das Buch in dieser Form nicht zustande gekommen, wenn unsere Lektorin Catarina Gomes

de Almeida nicht seit dem Erstkontakt, mit daran geglaubt hätte. Wir freuen uns sehr darüber, mit dem **Bitcoin Durchblick** ein Buch zu Bitcoin beim renommierten *Springer-Verlag* zu veröffentlichen, welches von *Bitcoinern* selbst verfasst wurde.

Danke an alle Beteiligten für diese vertrauensvolle Zusammenarbeit!

Filip Balonis

Inhaltsverzeichnis

1	Prolog	1
2	Geld	7
2.1	Evolution des Geldes	8
2.2	Das Fiat-Geldsystem	20
2.3	Aufgaben	42
3	Bitcoin	51
3.1	Entstehung von Bitcoin	52
3.2	Das Protokoll und die Nodes	59
3.3	Kryptografische Transaktionen und Wallets	74
3.4	Blockchain	94
3.5	Mining	110
3.6	Aufgaben	128
4	Bitcoin als Wirtschaftsgut	153
4.1	Bitcoins wirtschaftliche Eigenschaften	154
4.2	Bitcoin als neues Gold?	169
4.3	Bitcoin als neues Geld? – Das Lightning-Netzwerk	185

XVIII	Inhaltsverzeichnis	
4.4	Unterschied zu anderen Kryptowährungen	207
4.5	Aufgaben	220
5	Diskussion	237
5.1	Kritik	238
5.2	Idealismus	259
5.3	Regulatorik als Risiko?	269
5.4	Aufgaben	276
6	Praxisrelevante Hinweise	283
7	Epilog	301
	Lösungen zu Aufgaben	309
	Literatur	321
	Stichwortverzeichnis	333

Abkürzungen

ASIC	Application Specific Integrated Circuit
BIP	Bruttoinlandsprodukt
BIP32/39/141	Bitcoin Improvement Proposal 32/39/141
BNB	Binance Coin
BTC, ₿	Bitcoin-Währungseinheit
CBDC	Central Bank Digital Currency
CDO	Collateralized Debt Obligation
DCA	Dollar Cost Average
DOGE	Dogecoin
ECDSA	Elliptic Curve Digital Signature Algorithm
ETF	Exchange Traded Fund
ETH	Ether
EZB	Europäische Zentralbank
FED	Federal Reserve Bank
HNT	Helium Coin
ICO	Initial Coin Offering
J	Joule
KBV	Kurs-Buchwert-Verhältnis
kWh	Kilowattstunde
KYC	Know-Your-Customer-Vorschriften
LE	Little-Endian-Notation
MB	Megabyte
Mempool	Memory Pool

XX Abkürzungen

MH	Megahash
NFT	Non-Fungible Token
PBC	People's Bank of China
PH	Petahash
Sats	BTC-Untereinheit
SHA	Secure Hash Algorithm
TFR	Transfer of Fundings Regulation
TH	Terahash
USDT	Tether
UTXO	Unspent Transaction Output
W	Watt
WU	Weight Unit

Abbildungsverzeichnis

Abb. 2.1	Multilateraler Tauschhandel	11
Abb. 2.2	Kaurischneckengehäuse. (Metropolitan Museum: Hepy, String of cowrie shells, 2024b)	13
Abb. 2.3	Erste Münzen. (Metropolitan Museum: Gold stater, 2024a)	15
Abb. 2.4	Rai-Steingeld. (Nelson, 2013)	16
Abb. 2.5	Geldmengen	21
Abb. 2.6	Preiszunahme und Geldwertabnahme	35
Abb. 2.7	Rezession	36
Abb. 2.8	Vermögensentwicklung im Euroraum	39
Abb. 2.9	Handelsvolumen und Preisniveau im Euroraum	41
Abb. 3.1	Computer-Netzwerk	59
Abb. 3.2	Soft-Fork	64
Abb. 3.3	Hard-Fork	65
Abb. 3.4	Beispielhafter Transaktionsverlauf	66
Abb. 3.5	Exponentiell abnehmende Funktion	70
Abb. 3.6	Bitcoin-Geldmengenausweitung	73
Abb. 3.7	Elliptische Kurve	79
Abb. 3.8	Addition zweier Punkte	79

XXII **Abbildungsverzeichnis**

Abb. 3.9	Addition mit sich selbst	80
Abb. 3.10	Mehrmalige Addition eines Punktes	81
Abb. 3.11	Hash-Algorithmus	84
Abb. 3.12	Größendimension bei Schlüsselgenerierung	88
Abb. 3.13	Herleitung Seedphrase	91
Abb. 3.14	Deterministische Schlüsselableitung	93
Abb. 3.15	Stille Post	95
Abb. 3.16	Spieleraustausch	96
Abb. 3.17	Blockchain	97
Abb. 3.18	Blockaufbau	98
Abb. 3.19	Merkle-Tree	103
Abb. 3.20	Hinzufügen eines Wortes	104
Abb. 3.21	Verkettungsmechanismus	107
Abb. 3.22	Blockheader-Zeichenkette	109
Abb. 3.23	Goldabbau und -preis	111
Abb. 3.24	nBits-Validierung	115
Abb. 3.25	ASIC-Miner. (3d_molier International, 2024)	121
Abb. 3.26	Mining-Pool	122
Abb. 3.27	MSCI World	125
Abb. 3.28	Bitcoin-Transaktionskosten	127
Abb. 4.1	51-Prozent-Angriff	156
Abb. 4.2	BTC und MSCI World	162
Abb. 4.3	Goldverwendung	171
Abb. 4.4	Goldtresor der Deutschen Bundesbank. (Thies, 2024)	174
Abb. 4.5	Goldbarren. (Steinberg, 2017)	178
Abb. 4.6	Auszug aus niederländischem Bevölkerungsregister. (Gemeente Amsterdam Stadsarchief, 2024)	189
Abb. 4.7	Psychische Erkrankungen und BIP	191
Abb. 4.8	Isolierter Austausch	198
Abb. 4.9	Zahlungskanal	198
Abb. 4.10	Verwendung von Geheimnis	200
Abb. 4.11	Verbundene Zahlungskanäle	202
Abb. 4.12	Lightning-Transaktionen	203
Abb. 4.13	Blockchain-Trilemma	217

Abb. 5.1	Bitcoin-Energieverbrauch im Vergleich	241
Abb. 5.2	Bitcoin-Energieanteil regenerativ im Vergleich	243
Abb. 5.3	Pyramidensystem	248
Abb. 5.4	Bitcoin-Verteilung. (Vgl. Schultze-Kraft, 2021)	252
Abb. 5.5	Geografische Mining-Verteilung	254
Abb. 5.6	Pool-Verteilung	254
Abb. 5.7	Schrödingers Katze	256
Abb. 5.8	Stock-to-Flow-Modell. (BitboBTC, 2024)	268
Abb. 5.9	China-Mining-Restriktion	270
Abb. 6.1	Vermögensportfolio	285
Abb. 6.2	Monatliche Käufe	287
Abb. 6.3	Kosten bei BTC-Kauf	289
Abb. 6.4	BitBox02. (Shift Crypto, 2024)	292
Abb. 6.5	Genesis-Adresse	296
Abb. 6.6	Raspberry Pi 4 mit Gehäuse. (SparkFun Electronics, 2019)	300



1

Prolog

Flashcard

Als Käufer dieses Buches können Sie kostenlos unsere Flashcard-App „SN Flashcards“ mit Fragen zur Wissensüberprüfung und zum Lernen von Buchinhalten nutzen (siehe auch den untenstehenden Abschn. „Aufgaben“). Für die Nutzung folgen Sie bitte den folgenden Anweisungen:

1. Gehen Sie auf <https://flashcards.springernature.com/login>
2. Erstellen Sie ein Benutzerkonto, indem Sie Ihre Mailadresse angeben und ein Passwort vergeben.
3. Verwenden Sie den folgenden Link, um Zugang zu Ihrem SN Flashcards Set zu erhalten: ► <https://sn.pub/3owfsi>

Sollte der Link fehlen oder nicht funktionieren, senden Sie uns bitte eine E-Mail mit dem Betreff „SN Flashcards“ und dem Buchtitel an customerservice@springernature.com.

„Der Bitcoin ist wie Lottospielen – und allenfalls etwas für Profis“, Handelsblatt vom 16.03.2024.¹ „Die verrückte Bitcoin-Rally“, Frankfurter Allgemeine Zeitung vom 24.11.2024.² „Bitcoin verliert an Wert: Trump ordnet Kryptoreserve an – und enttäuscht die Branche“, Spiegel vom 07.03.2025.³ Drei Schlagzeilen etablierter deutscher Medienhäuser verdeutlichen die Verwirrung, die mit Bitcoin einhergeht.

Viele reden darüber, einige investieren und die wenigsten verstehen, was es damit auf sich hat. Im Internet kursieren haufenweise Geschichten von jungen Bitcoin-Investoren, die bereits mehr als ausgesorgt haben. Coole Typen mit Lamborghinis, Strandhäusern oder sogar Privatjets. Auf der anderen Seite hört man von Menschen, die ihr Passwort verloren haben und damit den Zugriff auf Bitcoin im Gegenwert von Millionen von Euros. Geschichten dieser Art schaffen für viele die ersten Berührungspunkte mit der dubios erscheinenden Thematik.

Den meisten fehlt der Zugang, um sich tiefergehend mit dem Ganzen auseinanderzusetzen. Nur Computer-Nerds hätten den Durchblick, wie das Internetgeld und die Kryptografie zu verstehen sind.

Bitcoin sei keine Investition, sondern reines Glücksspiel. Dabei steckt in letzterer These mehr Wahrheit als dem überzeugten Bitcoin-Enthusiasten lieb sein mag. Denn wenn die Kurse für einen Bitcoin, kurz *BTC* (Bitcoin-Währungseinheit), wieder zu Höchstpreisen ansetzen, stürzen sich haufenweise ahnungslose Spekulanten ins Verderben. Vor allem junge Männer neigen zu einem überstürzten Umgang mit den eigenen Finanzen. Die Angst etwas Bahnbrechendes zu verpassen, die *Fear of Missing out (FOMO)*, hat zur Folge, dass der Bezug zum Geld verloren geht. Diejenigen, die sich be-

¹ Hinterberger, 2024.

² Huemer, 2024.

³ Spiegel Wirtschaft, 2025.

sonders stark ihre Finger verbrannt haben, verbannen Bitcoin oftmals wieder aus ihrem Leben und drehen zu tatkräftiger Kritik auf.

Und dann ist da noch der immense Energieverbrauch des Bitcoin-Netzwerks, der Klimaaktivisten zum Verzweifeln bringt.

Ist Bitcoin also Spielcasino und Klimasünder oder doch die Lösung eines großen Problems, dem fortwährenden Verfall der Währungen, vielleicht sogar die Rettung unserer Welt?

Einordnung des Werkes Natürlich entsteht dieses Buch in der Überzeugung, Bitcoin sei etwas Gutes. In erster Linie geht es jedoch um Aufklärung und Diskussion – nicht nur der Thematik Bitcoin gegenüber, sondern dem Geld im Allgemeinen. Statt dem Einsatz von manipulativ wirkenden Adjektiven, wird sich bemüht saubere und faktenbasierte Argumentationen aufzubauen. An den Stellen, an denen auf die Erkenntnisse konkreter Arbeiten zurückgegriffen wird, dienen Quellenverweise der Anerkennung und Nachvollziehbarkeit. Auch ist dies hier weder eine Anlage- noch Steuerberatung – höchstens eine nüchterne Vorbereitung, in Zukunft eigene Investitionsentscheidungen zu treffen.

„Warum braucht es überhaupt noch ein weiteres Buch über Kryptowährungen?“, werden sich die Leser fragen, die bereits mit der Vielfalt ähnlicher Werke vertraut sind. Zum einen handelt es sich hierbei um eine Abhandlung zu Bitcoin und nicht zu Kryptowährungen im Allgemeinen. Darüber hinaus wird ein thematischer Rundumschlag gewagt, der die wirtschaftliche Perspektive einnimmt und dabei die Technologie hinter Bitcoin nicht zu kurz kommen lässt. Bitcoin zu verstehen bedeutet, sich in verschiedenen Disziplinen auszukennen. Von Ökonomie über Geschichte, Informatik, Mathematik, Physik, Psychologie hinzu Politik wird jedes Fach abgedeckt.

Dabei soll der Leser bei Null abgeholt und an die Hand genommen werden. Vor allem im technischen Teil wird es etwas anspruchsvoller, da wichtige Aspekte der Technologie nicht vernachlässigt werden sollen. Wem das Ganze zu trocken wird, kann diese Teile überspringen, ohne dadurch thematisch abgehängt zu werden.

Damit dient **Bitcoin Durchblick** als allumfänglicher Einstieg in die Thematik und setzt keinen expliziten Fokus. Aus didaktischen Gründen werden besonders komplexe Sachverhalte teilweise leicht vereinfacht dargestellt. Mit dem Thema bereits bewandte Leser kommen aufgrund der Vielfalt der Blickwinkel sicherlich auch auf ihre Kosten und können womöglich den ein oder anderen Denkanstoß mitnehmen.

Aufbau Vorab noch einige Worte zum Aufbau und den jeweiligen Lernzielen hinter den Kapiteln.

Bevor das Bitcoin-Netzwerk näher betrachtet wird, geht es zunächst allumfassend um das Thema Geld. Im Abschn. 2.1 **Evolution des Geldes** wird sich damit befasst, was Geld ist, welche Formen es historisch angenommen hat und wie sich mit der Zeit das heutige Geldsystem entwickelte. Dieses sogenannte Fiat-Geldsystem wird im Anschluss weiter unter die Lupe genommen. Es werden Antworten auf Fragen zu Organisation, Geldschöpfung und Möglichkeiten der staatlichen Einflussnahme gegeben. Darüber hinaus werden Probleme aufgezeigt und Grundsätze der Anwendung findenden Geldtheorie kritisch hinterfragt.

Darauffolgend wird auf die Entstehungsgeschichte hinter Bitcoin eingegangen, um das Ganze zu entmystifizieren und ein Verständnis für die Motivation hinter der Technologie zu schaffen. Die Abschnitte **Das Protokoll und die Nodes** (Abschn. 3.2), **Kryptografische Transaktionen und Wallets** (Abschn. 3.3), **Blockchain** (Abschn. 3.4) und **Mining** (Abschn. 3.5) schaffen technische Einblicke. Dabei werden detaillierte Erklärungen zu Netzwerkstruktur, -kommunikation, -regeln und -sicherheit angebracht.

In Kap. 4 werden aus der technischen Architektur wirtschaftliche Eigenschaften abgeleitet. Es wird die Frage danach behandelt, wem Bitcoin nützt und weswegen. Abschn. 4.2 kann als Vergleich zwischen Bitcoin und dem Edelmetall Gold verstanden werden. Woraufhin die Brücke zum Geld geschlagen wird, mit der Überlegung, worin sich Bitcoin von den alltäglich bekannten Währungen unterscheidet. In diesem Zuge wird das Lightning-Netzwerk als Ergänzung zum Bitcoin-Netzwerk eingeführt und es werden innovative Einsatzmöglichkeiten präsentiert. In **Unterschied zu anderen Kryptowährungen** (Abschn. 4.4) werden weitere Kryptowährungen vorgestellt. Ziel ist die Kategorisierung und Abgrenzung dieser gegenüber Bitcoin.

Die zwei darauffolgenden Abschnitte in Kap. 5 widmen sich vollständig der Diskussion. Zuerst werden die geläufigsten Kritikpunkte am Bitcoin besprochen. Danach werden einige idealistische Thesen der befürwortenden Seite relativiert. Zum Ende hin wird das mögliche Investitionsrisiko durch staatliche Regulierungsmaßnahmen behandelt. Bedeutende Wege der staatlichen Einflussnahme werden angebracht und deren Konsequenzen für Bitcoin durchdacht.

Das letzte thematische Kapitel (Kap. 6) dient denjenigen, die sich dazu entschließen, praktische Erfahrungen mit der Bitcoin-Technologie zu sammeln. Hier werden konkrete Handlungsvorschläge und -warnungen ausgesprochen.

Schlussendlich wird dieses Werk im **Epilog** (Kap. 7) mit einer Wiederholung und einem Ausklang abgerundet, und es werden verschiedene Quellen zur weiteren inhaltlichen Auseinandersetzung aufgezeigt.

Aufgaben Die Kapitel **Geld** (Kap. 2), **Bitcoin** (Kap. 3), **Bitcoin als Wirtschaftsgut** (Kap. 4) und **Diskussion** (Kap. 5) schließen jeweils mit umfangreichen Aufgabenkatalogen zu den jeweiligen Kapiteln ab. Diese können dazu genutzt werden, das gelernte Wissen auf die Probe zu stellen und zu ver-

tiefen. Mit den *Springer Nature Flashcards* können darüber hinaus dieselben Aufgaben bequem am PC oder Smartphone bearbeitet werden. Dieses interaktive Angebot bietet verschiedene Lernmodi, die dabei unterstützen, die Inhalte zu verinnerlichen. Für die Nutzung siehe den Kasten am Anfang dieses Kapitels.



2

Geld

Zusammenfassung Geld passte sich in der Menschheitsgeschichte den Anforderungen und Möglichkeiten fortlaufend an. In der Bronzezeit entwickelten sich verschiedene Formen von Zwischentauschmitteln. Der physische Nutzen solcher geriet mit der Zeit in den Hintergrund und seltene Güter wie Gold, bis zu Goldmünzen, wurden zum Geld der Wahl. Die Ausgabe von Münzen erfolgte durch Regierungen, die den Wert des Geldes vom Materialwert entkoppelten. Papiergeld finalisierte diese Entwicklung und eröffnete Staaten mächtige Möglichkeiten der Geldpolitik. Immer wieder wurden solche missbraucht, weswegen verschiedene Währungsräume sich am Goldstandard versuchten. Mit dem Scheitern des goldgedeckten US-Dollars 1971 breitete sich das Fiatgeld aus. Heutige Geldsysteme bauen auf staatsnahe Zentralbanken und private Geschäftsbanken. Geld entsteht durch Kredite oder im Austausch gegen Vermögenswerte.

Zentralbanken können durch Veränderung des Mindestreserve- oder Leitzinssatzes auf die Wirtschaft einwirken. Es lässt sich feststellen, dass Fiatwährungen aufgrund von Inflation keinen besonders langfristigen Wertspeicher darstellen. Geldpolitik nach Keynes versucht Wirtschaftswachstum durch neues Geld zu fördern und Phasen des Abschwungs abzufedern. Ziel ist es dabei, im Zuge der Steigerung des Handelsvolumens, die Kontrolle über das Preisniveau beizubehalten. Jedoch misslingt dieses Manöver regelmäßig. Außerdem konkurrieren die großen Währungsräume miteinander und versuchen immer wieder die eigene Währung im Vergleich zu den anderen abzuwerten, um die eigene Wirtschaft zu stärken.

2.1 Evolution des Geldes

Wer die Evolution des Geldes betrachtet, muss sich vorerst anschauen, was es mit dem Begriff *Geld* überhaupt auf sich hat. Auf der Webseite der Deutschen Bundesbank finden sich folgende drei Anforderungen an ein Wirtschaftsgut, deren Wahrnehmung es zu Geld macht: Die *Tauschmittelfunktion*, die *Funktion als Recheneinheit* und die *Funktion als Wertspeicher*.¹

Unter der Tauschmittelfunktion wird verstanden, dass ein solches Gut sich gegen jedes andere zu erwerbende Wirtschaftsgut tauschen lässt. Das setzt vollumfängliches gegenseitiges Vertrauen und Übereinkunft über den Wert des Gutes innerhalb einer Volkswirtschaft voraus. Des Weiteren muss die Natur des Gutes eine sein, die den Besitzübergang vor dem Hintergrund verschiedenster Anforderungen praktisch realisierbar macht.

¹ Vgl. Deutsche Bundesbank, 2019.