Daniel Hellwig
Goran Karlic
Arnd Huchzermeier

Entwickeln Sie Ihre eigene Blockchain

Ein praktischer Leitfaden zur Distributed-Ledger-Technologie

Springer Gabler

Entwickeln Sie Ihre eigene Blockchain

Daniel Hellwig • Goran Karlic
Arnd Huchzermeier

Entwickeln Sie Ihre eigene Blockchain

Ein praktischer Leitfaden zur Distributed-Ledger-Technologie

Springer Gabler

Daniel Hellwig
WHU – Otto Beisheim School of Management,
Vallendar, Deutschland

Goran Karlic
Kepler Cannon
New York, USA

Arnd Huchzermeier
WHU – Otto Beisheim School of Management,
Vallendar, Deutschland

ISBN 978-3-662-62965-9 ISBN 978-3-662-62966-6 (eBook)
https://doi.org/10.1007/978-3-662-62966-6

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Springer Gabler
Übersetzung der englischen Ausgabe: Build Your Own Blockchain by Daniel Hellwig, Goran Karlic, Arnd Huchzermeier, © Springer Nature Switzerland AG 2020. Herausgegeben von Springer International Publishing. Alle Rechte vorbehalten.
© Der/die Herausgeber bzw. der/die Autor(en), exklusiv lizenziert durch Springer-Verlag GmbH, DE, ein Teil von Springer Nature 2021
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 jedermann benutzt werden dürfen. Die Berechtigung zur Benutzung unterliegt, auch ohne gesonderten Hinweis hierzu, den Regeln des Markenrechts. Die Rechte des jeweiligen Zeicheninhabers sind zu beachten.
Der Verlag, die Autoren und die Herausgeber gehen davon aus, dass die Angaben und Informationen in diesem Werk zum Zeitpunkt der Veröffentlichung vollständig und korrekt sind. Weder der Verlag, noch die Autoren oder die Herausgeber 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.

Springer Gabler ist ein Imprint der eingetragenen Gesellschaft Springer-Verlag GmbH, DE und ist ein Teil von Springer Nature.
Die Anschrift der Gesellschaft ist: Heidelberger Platz 3, 14197 Berlin, Germany

Vorwort

Die Blockchain-Technologie gehört wohl zu den am häufigsten diskutierten Innovationen seit dem Aufkommen des Internets. Durch Nutzung der Konzepte der Dezentralisierung, Zuverlässigkeit und Fälschungssicherheit hat Blockchain das Potenzial, ein breites Feld innovativer Anwendungen und neuer Formen der Zusammenarbeit zu ermöglichen. Im Kern vermittelt Blockchain in Ermangelung einer offensichtlichen zentralisierten Autorität Daten und kann dazu beitragen, Vertrauen zwischen allen Netzwerkteilnehmern aufzubauen. Darüber hinaus können mithilfe der Blockchain-Technologie fast alle denkbaren Werte, Rechte und Pflichten von materiellen und immateriellen Gütern durch Token dargestellt werden, wodurch deren Handelbarkeit und Austauschbarkeit vereinfacht wird. Welche Auswirkungen diese Entwicklung weltweit haben wird, bleibt abzuwarten. Kryptowährungen wie Bitcoin und Ethereum haben die erste „Killer"-Anwendung dieser Technologie markiert; immer mehr Organisationen erforschen jedoch, wie sie Blockchain in ihre bestehenden Systeme integrieren können.

Zunehmend wird Blockchain nicht mehr nur als ausschließlich störend/schädigend, sondern als zukunftsweisendes Protokoll anerkannt. Natürlich ging dieser Bedeutungszuwachs mit einer Flut von öffentlichen Weißbüchern einher, die das Störungspotenzial von Blockchain auf die Probe stellten. Auch die Bücherregale füllten sich schnell mit akademisch orientierten Bänden über ihre theoretischen und mathematischen Grundlagen. Nichtsdestotrotz finden wir trotz der Flut des verfügbaren Materials, dass erstere stilisierte Diskussionen auf hohem Niveau liefern, während letztere sich für tief gehende Erklärungen der Technologie entscheiden. Keiner der beiden Ansätze stattet die Leserschaft mit den Werkzeugen aus, die für eine praktische Umsetzung von Blockchain erforderlich sind, und auch nicht mit dem Wissensumfang, der für die Einbindung Blockchain-fähiger Technologien in bestehende Unternehmensrahmen und die Steuerung organisatorischer Entscheidungen notwendig ist. Da sich die Blockchain-Technologie ihrem elften Geburtstag nähert, sind wir der Ansicht, dass die Trennung von Theorie und Anwendung schon zu lange andauert.

Dieses Buch verbindet Theorie und Praxis. Es richtet sich an ein nicht-technisches Publikum und stellt alle grundlegenden Bausteine zum Verständnis von Blockchain vor, gefolgt von praktischen Problemlösungsroutinen. So führen wir in jedem Kapitel die

Hauptideen konzeptionell und praktisch ein, wobei die nachfolgenden Kapitel auf dem in den vorhergehenden Abschnitten erworbenen Wissen und Können aufbauen. Um es unserer Leserschaft so einfach wie möglich zu machen, sich mit diesen Übungen zu beschäftigen, haben wir die Docker-Technologie unter Verwendung vorkonfigurierter Container eingesetzt, bei denen es sich um eine Software-Standardeinheit handelt, die den Code und all seine Abhängigkeiten bündelt. Dieser Aufbau ermöglicht es, dass Anwendungen schnell und zuverlässig von einer Computerumgebung zur anderen laufen, und stellt sicher, dass alle unsere Leser – sowohl Windows- als auch MacOS-Benutzer – die Übungen mit minimalen technischen Schwierigkeiten absolvieren können.

Das Buch ist in drei Abschnitte unterteilt.

Teil I, Blockchain-Grundlagen, gibt einen Überblick über die wichtigsten, für praktische Anwendungen relevanten Blockchain-Komponenten und umfasst die ersten fünf Kapitel:

1. Blockchain-Grundlagen
2. Kryptowährungen
3. Konsensmechanismen
4. Smart Contracts
5. Privatsphäre und Anonymität

Teil II, Grundlagen der Kryptografie, bietet eine detaillierte Einführung in die zugrunde liegenden technologischen Grundlagen der in Teil I untersuchten Konzepte, vor allem, was die Kryptografie-Rahmenwerke und -Mechanismen betrifft.

6. Verschlüsselungsmethoden
7. Bereitstellung digitaler Signaturen

Teil III, Anwendungen aus der realen Welt, bietet eine Zusammenfassung vergangener und laufender realer Anwendungsfälle, kategorisiert nach Industriezweigen, die Gründe für die Wahl der Blockchain-Technologie sowie die Herausforderungen, denen man sich in jedem Fall stellen muss.

Wie die meisten im Entstehen begriffenen Technologien war auch Blockchain nicht immun gegen den traditionellen Zyklus von Hype, Enttäuschung und Aufklärung. Der globale Markt ist der Technologie heute wohl immer noch voraus, was viele dazu veranlasst, die angebliche Bedeutung und das Potenzial von Blockchain angesichts der großen Versprechungen und des derzeitigen Mangels an erfolgreichen und wirkungsvollen Implementierungen in Frage zu stellen. Während wir jedoch weiterhin neue Einsichten in diese neue Technologie gewinnen und immer konkretere Anwendungen auf dem Markt auftauchen (z. B. Geldbewegung über die JPM-Münze von JP Morgan und erweiterte Datenschutzkontrollen, die über Zero-Knowledge-Beweise ermöglicht werden), hat Blockchain begonnen, den „Berg der Erleuchtung“ hinaufzusteigen.

Dieses Buch zielt darauf ab, Sie mit den Fähigkeiten auszustatten, die notwendig sind, um das Potenzial dieser Technologie bei ihrer Entfaltung voll auszuschöpfen. Daher hoffen wir, dass Ihnen dieses Buch dabei helfen wird, ein grundlegendes Verständnis der wichtigsten Implementierungskomponenten von Blockchains zu erlangen. Ferner ist es unser Ziel, Ihnen das praktische Wissen, das für die Einbindung Blockchain-fähiger Module in bestehende und zukünftige Geschäftssysteme erforderlich ist, zu vermitteln. Nicht zuletzt hoffen wir, dass Ihnen die Ausführungen in diesem Buch auch einen Überblick hinsichtlich der potenziellen Auswirkungen der Blockchain auf Volkswirtschaften und globale Finanzstrukturen verschaffen wird.

Vallendar, Deutschland — Daniel Hellwig
New York, USA — Goran Karlic
Vallendar, Deutschland — Arnd Huchzermeier

Danksagungen

Dieses Buch wurde weitgehend von zwei Kursen inspiriert (Einführung in Blockchain und Blockchain-Programmierung), die wir an der WHU – Otto Beisheim School of Management unterrichtet haben und die darauf abzielten, ein vertieftes Verständnis der grundlegenden Bausteine einer Blockchain, ihres Ökosystems und der Funktionalität von Smart Contracts zu vermitteln. Obwohl die Kurse erst in den letzten zwei Jahren stattgefunden haben und sich noch in ihren Anfängen befinden, waren unsere Studenten eine unschätzbare Ressource bei der Gestaltung der theoretischen Inhalte und Programmieraufgaben des Kurses und damit auch des Buches. Wir haben viel aus ihrem Feedback gelernt, wofür wir dankbar sind, und haben versucht, alle Anregungen und Vorschläge so weit wie möglich einzubeziehen.

Wir danken Max Mäckler und Farhan Javed für ihre redaktionellen Kommentare und richten unseren tiefsten Dank an Dr. Jasmin Imran Alsous (Princeton, MIT) für ihr detailliertes und substanzielles Feedback zu mehreren Entwürfen dieses Buches. Unser Dank gilt auch Sonny Ajmani von Kepler Cannon für seine Unterstützung bei diesem Unterfangen, die für den Abschluss des Projekts von unschätzbarem Wert war. Für Hilfe bei der Übersetzung und Überarbeitung der deutschen Version des Buches danken wir außerdem Kornelia Schwaben-Beicht (ABC-Lektorat.Korrektur).

Und schließlich freuen wir uns, dass Springer uns die Möglichkeit gegeben hat, an diesem Projekt mitzuarbeiten. Blockchain und ihre potenzielle Rolle in unserer heutigen und zukünftigen Gesellschaft ist ein Thema, das mit Sicherheit Reaktionen hervorrufen wird. Deshalb hoffen wir, dass dieses Buch unsere Leserinnen und Leser mit dem theoretischen und praktischen Wissen ausstatten kann, das erforderlich ist, um das Potenzial dieser Technologie zu verstehen, zu nutzen und Anwendungen für unsere Gesellschaft sinnvoll zu gestalten.

Inhaltsverzeichnis

Teil I Blockchain-Grundlagen

1 Blockchain-Grundlagen 3
1.1 Einführung 3
1.1.1 Terminologie 4
1.1.2 Die erste Blockchain-Anwendung 5
1.1.3 Währungen: Traditionell und Krypto 7
1.1.4 Eigentum 8
1.2 Kryptowährungen 9
1.2.1 Kontrollmechanismen 9
1.2.2 Kryptografie 10
1.2.3 Kryptografisches Hashing 10
1.2.4 Asymmetrische Kryptografie 11
1.2.5 Digitale Signaturen 12
1.3 Grundlagen der Netzwerkarchitektur 12
1.4 Die Blockchain 13
1.4.1 Funktionsprinzipien 13
1.4.2 Blöcke 14
1.5 Datenintegrität 16
1.5.1 Ledger-Propagation 16
1.5.2 Transaktionsvalidierung 17
1.5.3 Merkle-Bäume 19
1.6 Arten von Blockchains 19
1.6.1 Öffentliche Blockchains 20
1.6.2 Private Blockchains 20
1.6.3 Konsortium-kontrollierte Blockchains 21
1.6.4 Auswahlprozess 21
1.7 Übungen 21
1.7.1 Einleitung 21
1.7.2 Umgebungssetup 22
1.7.3 Ihre eigene Blockchain 23

1.7.4 Erstellen Sie ein neues Verzeichnis 23
1.7.5 Tool-Download 23
1.7.6 Tool-Installation 24
1.7.7 Anlegen eines Accounts 24
1.7.8 Einrichtung des Genesis-Blocks 26
1.7.9 Bildung eines neuen Netzwerks 28
1.7.10 Start des Netzwerks 28
Literatur 30

2 Kryptowährungen 31
2.1 Einführung 31
2.1.1 Übersicht 32
2.1.2 Krypto-Eigenschaften 33
2.1.3 Transaktionen 34
2.1.4 Die doppelte Ausgabe 35
2.2 Die Miner 36
2.2.1 Übersicht über den Prozess 36
2.2.2 Transaktionsbestätigung 36
2.2.3 Mining-Prozess 38
2.2.4 Die Nonce 39
2.3 Coins und Token 40
2.3.1 Einführung 40
2.3.2 Altcoins 40
2.3.3 Token 41
2.3.4 ERC-20-Standard 42
2.4 Handelsplätze/Börsen 44
2.4.1 Einführung 44
2.4.2 Broker 45
2.4.3 Traditionelle Börsen 45
2.4.4 Dezentralisierte Börsen 45
2.4.5 Handelsplattformen 46
2.4.6 Offline-Börsen 46
2.5 Wallets 46
2.5.1 Einführung 46
2.5.2 Hardware-Wallets 47
2.5.3 Software-Wallets 48
2.5.4 Online-E-Wallets 48
2.6 Übungen 49
2.6.1 Einführung 49
2.6.2 Standardtransfer: Herstellung der Verbindung 49
2.6.3 Interaktion mit der Blockchain 50
2.6.4 Konten und Salden 51

2.6.5 Ihre erste Transaktion . . . 51
2.6.6 Validierung von Transaktionen . . . 54
Literatur . . . 55

3 Konsensmechanismen . . . 57
3.1 Einführung . . . 57
3.1.1 Definition . . . 57
3.1.2 Zielsetzungen . . . 58
3.1.3 Variationen . . . 59
3.2 Das CAP-Theorem . . . 59
3.2.1 Das Trilemma . . . 59
3.2.2 CAP-Theorem und Blockchains . . . 60
3.2.3 Das CAP-Theorem in der Praxis . . . 61
3.3 Byzantinischer Fehler . . . 63
3.3.1 Hintergrund . . . 63
3.3.2 Das Problem des byzantinischen Generals . . . 64
3.3.3 Ein Beispiel . . . 65
3.4 Verbreitete Konsensprotokolle . . . 66
3.4.1 Proof-of-Work (PoW) . . . 66
3.4.2 Proof-of-Stake (PoS) . . . 68
3.4.3 Proof-of-Capacity/Proof-of-Space . . . 69
3.4.4 Delegated-Proof-of-Stake (DPoS) . . . 71
3.4.5 Proof-of-Authority (PoA) . . . 72
3.4.6 Praktische byzantinische Fehlertoleranz (PBFT) . . . 72
3.4.7 Proof-of-Elapsed-Time (PoET) . . . 73
3.4.8 Andere Mechanismen . . . 74
3.5 Übungen . . . 75
3.5.1 Einführung . . . 75
3.5.2 Einrichtung des PoA-Genesis-Blocks . . . 75
3.5.3 Erstellen eines Proof-of-Authority-Netzwerks . . . 79
Literatur . . . 80

4 Smart Contracts . . . 81
4.1 Einführung . . . 81
4.2 Ethereum – eine Alternative zu Bitcoin . . . 83
4.2.1 Einführung . . . 83
4.2.2 Ethereum versus Bitcoin-Anwendungen . . . 84
4.2.3 Ethereum-Ansatz . . . 86
4.2.4 Gas . . . 86
4.2.5 Der Gaspreis . . . 88
4.3 Solidity-Programmiersprache . . . 88
4.3.1 Syntax . . . 88
4.3.2 Münzwurf-Beispiel . . . 89

4.4 Oracles . . . 89
4.4.1 Einführung . . . 89
4.4.2 Integration von Smart Contracts . . . 91
4.4.3 Oracles und Sicherheit . . . 91
4.4.4 Arten von Oracles . . . 91
4.4.5 Vertragsbeispiel für Oracles . . . 93
4.5 Dezentralisierte Anwendungen (dApps) . . . 93
4.5.1 Einführung . . . 93
4.5.2 dApp-Beispiel: Dezentralisierte Autonome Organisation (DAO) . . . 94
4.6 Turing-Vollständigkeit . . . 95
4.6.1 Hintergrund . . . 95
4.6.2 Turing-Vollständigkeit und Ethereum . . . 95
4.7 Rechtliche Perspektive . . . 96
4.7.1 Interpretation von Smart Contracts . . . 96
4.7.2 Offene Fragen . . . 97
4.7.3 Fazit . . . 98
4.8 Übung („Sparschwein“) . . . 98
4.8.1 Einführung . . . 98
4.8.2 Opcode . . . 99
4.8.3 Bytecode . . . 99
4.8.4 Application Binary Interface (ABI) . . . 100
4.8.5 Einsatz des Sparschweins . . . 101
4.8.6 Erneutes Verbinden . . . 101
4.8.7 ABI-Erstellung . . . 102
4.8.8 Start des Vertrags . . . 103
4.8.9 Interaktion . . . 104
Literatur . . . 105

5 Privatsphäre und Anonymität . . . 107
5.1 Einführung . . . 107
5.1.1 Anonymität . . . 108
5.1.2 Unverkettbarkeit . . . 108
5.1.3 Anonymität versus Pseudonymität . . . 109
5.1.4 Taint-Analyse . . . 110
5.2 Deanonymisierung . . . 111
5.2.1 Einführung . . . 111
5.2.2 Transaktionsgraphen-Analyse . . . 111
5.2.3 Deanonymisierung auf Netzwerkebene . . . 112
5.3 „The-Onion-Router“-Netzwerk (TOR) . . . 112
5.3.1 Hintergrund . . . 112
5.3.2 TOR-Methode . . . 113

5.3.3 Anwendung von TOR . . . 115
5.3.4 Einschränkungen . . . 116
5.4 Mixing-Modelle . . . 116
5.5 Dezentralisiertes Mixing . . . 117
5.5.1 Motivation . . . 117
5.5.2 Coinjoin-Modell . . . 117
5.5.3 Coinjoin-Anonymität . . . 118
5.6 Zero-Knowledge-Beweise . . . 119
5.6.1 Einführung . . . 119
5.7 Privatsphäre und Sicherheitsprotokolle . . . 120
5.7.1 Einführung . . . 120
5.8 Privacy Coins . . . 121
5.8.1 Einführung . . . 121
5.8.2 Die Nullwährungen . . . 123
5.8.3 Zerocoin . . . 123
5.8.4 Zerocash . . . 125
5.9 Übung . . . 127
5.9.1 Einführung . . . 127
5.9.2 Vorbereitung der Umgebung . . . 127
5.9.3 Bestimmung eines Blocks . . . 128
5.9.4 Block-Analyse . . . 130
5.9.5 Transaktionen finden . . . 131
Literatur . . . 132

Teil II Grundlagen der Kryptografie

6 Blockchain-Kryptografie: Teil 1 . . . 135
6.1 Einführung . . . 135
6.1.1 Grundlagen der Kryptografie . . . 135
6.1.2 Voraussetzungen der Geheimhaltung . . . 136
6.1.3 Blockchain und Kryptografie . . . 136
6.2 Klassische Chiffren . . . 137
6.2.1 Substitution . . . 138
6.2.2 Transposition . . . 138
6.3 Moderne kryptografische Algorithmen . . . 140
6.3.1 Einführung . . . 140
6.3.2 Schwachstellen . . . 142
6.4 Hashing . . . 142
6.4.1 Einführung . . . 142
6.4.2 Hash-Kollisionen . . . 143
6.4.3 Merkle-Damgård-Konstruktion . . . 144

6.4.4 Längenerweiterungsangriff . . . 145
6.5 Secure Hash Algorithmus (SHA) . . . 146
6.5.1 Einführung . . . 146
6.5.2 Hash-Beispiel . . . 146
6.6 Symmetrische Verschlüsselung . . . 148
6.6.1 Einzelentschlüsselungsschlüssel . . . 148
6.6.2 Die Hill-Chiffre . . . 149
6.6.3 Die Pohlig-Hellman Chiffre . . . 153
6.7 Übung . . . 156
6.7.1 Einführung . . . 156
6.7.2 Vorbereitung der Nachricht . . . 157
6.7.3 OpenSSL-Setup . . . 157
6.7.4 Verschlüsselung der Nachricht . . . 157
6.7.5 Entschlüsselung der Nachricht . . . 159
Literatur . . . 160

7 Blockchain-Kryptografie: Teil 2 . . . 161
7.1 Asymmetrische Schlüsselschemata . . . 161
7.1.1 Einführung . . . 161
7.1.2 Ein Beispiel . . . 162
7.2 Die Diffie-Hellman-Merkle-Schlüsselvereinbarung . . . 163
7.2.1 Einführung . . . 163
7.2.2 Ein Beispiel . . . 164
7.2.3 Einschränkungen . . . 166
7.3 Rivest, Shamir und Adleman (RSA) . . . 167
7.3.1 Einführung . . . 167
7.3.2 Schlüsselpaare . . . 168
7.3.3 Intuition . . . 170
7.3.4 Ein Beispiel . . . 171
7.4 Digitale Signaturen . . . 172
7.4.1 Einführung . . . 172
7.4.2 Motivation . . . 172
7.4.3 Anwendung . . . 173
7.4.4 Signaturen . . . 174
7.4.5 Ein Beispiel . . . 175
7.5 Quantenresistente Kryptografie . . . 176
7.5.1 Einführung . . . 176
7.5.2 Mechanismus . . . 177
7.5.3 Shor-Algorithmus . . . 177
7.5.4 Grover-Algorithmus . . . 177
7.5.5 Bedrohung . . . 179

7.5.6 Sicherheitsüberlegungen 179
7.5.7 Quantenwiderstand 179
7.6 Übungen 180
7.6.1 Einführung 180
7.6.2 Vorbereitung der Nachricht 181
7.6.3 Erstellung des Schlüssels (RSA) 181
7.6.4 Digitale Signaturen (RSA) 183
7.6.5 Generierung des Schlüssels (Elliptische Kurven) 184
7.6.6 Digitale Signaturen (Elliptische Kurven) 185
Literatur 186

Teil III Anwendungen aus der realen Welt

8 Blockchain in Aktion: Praxisanwendungen 189
8.1 Einführung 189
8.2 Währungen 190
8.3 Grenzüberschreitende Transfers 191
8.4 Tokenisierung 193
8.5 Verfolgung von Vermögenswerten 194
8.6 Güterhandel 195
8.7 Blick in die Zukunft 196
8.7.1 Bescheidene Anfänge 196
8.7.2 Warnhinweis 197
8.7.3 Das letzte Wort ist noch nicht gesprochen 198
Literatur 200

Stichwortverzeichnis 201

Teil I

Blockchain-Grundlagen

Blockchain-Grundlagen

1

1.1 Einführung

Eine Blockchain ist ein Verzeichnis von Informationsblöcken (z. B. Transaktionen, Verträge, etc.), die aufeinander aufbauend über ein Computernetzwerk verteilt gespeichert werden. Sie ist nicht einfach nur ein Algorithmus, sondern ein komplexes technologisches Konstrukt und Freigabeprotokoll, das eine dezentralisierte Vermittlung von Daten zwischen den Teilnehmern ermöglicht. Die revolutionären Eigenschaften der Blockchain ergeben sich daraus, dass sie Daten auf einzigartige Weise sicher speichern kann – sofern sie entsprechend implementiert und verwendet wird –, nämlich dezentralisiert und ohne darauf angewiesen zu sein, dass die Netzwerkteilnehmer sich gegenseitig vertrauen müssen (im Folgenden wird das englische Wort „trustless“ mit „vertrauensfrei“ übersetzt). So wie das Transmission Control Protocol und das Internet Protocol (TCP-IP), in den 1970er-Jahren an der DARPA (Held 2003) erfunden, erstmals den dezentralen Austausch von Informationen (d. h. das Internet) möglich machten, so ermöglicht eine Blockchain die dezentralisierte Übertragung von Vermögenswerten. Die aus der Blockchain resultierende Innovation ergibt sich nicht aus einem grundlegend neuen Technologieansatz, sondern aus der Anwendung etablierter Methoden der Informationstechnologie auf das Problem der Informationsübertragung, wie kryptografisches Hashing, asymmetrische Verschlüsselung und Peer-to-Peer-Netzwerkarchitektur.

Die Blockchain erlaubt die Erstellung eines digitalen Kontobuchs (das „Ledger“) und die gemeinsame Nutzung der darin enthaltenen Daten durch ein Netzwerk unabhängiger Parteien (die „Nodes“), die über die zugrunde liegende Internetinfrastruktur verbunden sind (Abb. 1.1). Jeder Knoten („Node“) verfügt zu jedem Zeitpunkt über eine exakte Kopie des Ledgers, was permanente, mit Zeitstempel versehene Transaktionsaufzeichnungen, die aus den zugrunde liegenden Blockchain-Knoten bestehen, sicherstellt. Um einen

© Der/die Autor(en), exklusiv lizenziert durch Springer-Verlag GmbH, DE, ein Teil von Springer Nature 2021

D. Hellwig et al., *Entwickeln Sie Ihre eigene Blockchain*,
https://doi.org/10.1007/978-3-662-62966-6_1

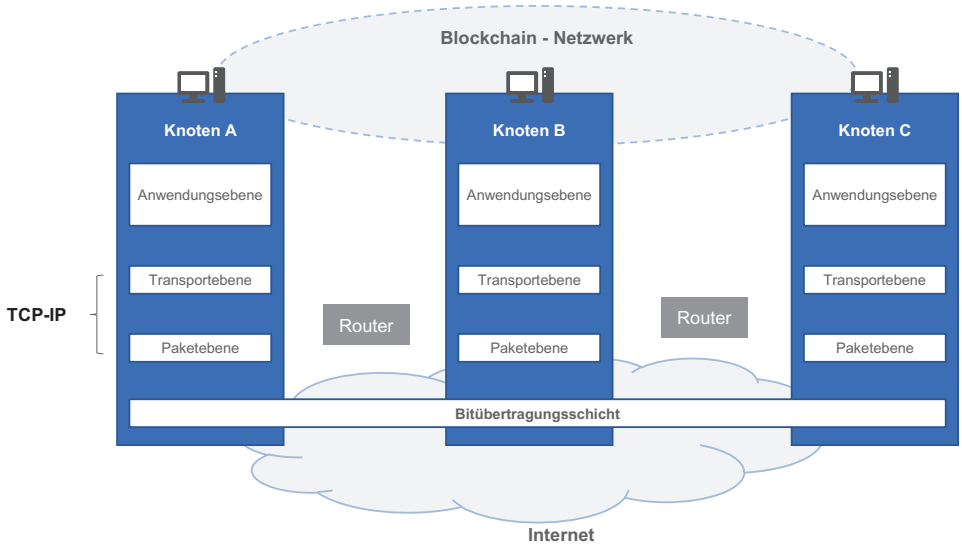

Abb. 1.1 Übersicht der Blockchain-Netzwerkinfrastruktur

Datensatz zu ändern, muss ein großer Teil der Blockchain-Netzwerkteilnehmer gleichzeitig der Änderung der Informationen zustimmen, und es müssen mehrere zusätzliche Sicherheitsvorkehrungen überwunden werden: Sobald ein Knoten Informationen in der Blockchain-Datenbank speichert, ist es nahezu unmöglich, diese zu entfernen.

In diesem Kapitel werden die relevante Terminologie und die grundlegenden Funktionen von Blockchains, die sie für solche Operationen prädisponieren, am Beispiel von Bitcoin vorgestellt.

1.1.1 Terminologie

Zunächst einmal gilt es, zwischen der *Blockchain*- und der *Distributed-Ledger-Technologie (DLT)* zu unterscheiden: „Blockchain“ beschreibt eine Datenstruktur, die eine permanente Chronik von Transaktionen speichert, während „Distributed-Ledger- Technology“ (DLT) eine Datenstruktur bezeichnet, die sich über mehrere Computer erstreckt und für gewöhnlich über viele verschiedene Standorte und Regionen verteilt ist.

Blockchain, einer breiteren Öffentlichkeit als die Technologie hinter Bitcoin, Ethereum sowie anderen Kryptowährungen bekannt, ist somit eine Untergruppe von DLT. Der Begriff Blockchain wird aber manchmal auch für Transaktionen und andere Datensätze verwendet, die in Blöcken zusammengefasst und an eine Reihung bereits verifizierter Blöcke angehängt werden.

„Bitcoin“ ist die erste und am häufigsten verwendete Kryptowährung und beschreibt sowohl das Netzwerk als auch die Software und die Community; „Bitcoin“ bezeichnet auch die eigentliche Währung (d. h. eine Einheit).

Das „Token“ ist eine digitale Repräsentation eines Vermögenswertes. Bitcoins sind also keine Token, da sie selbst einen Wert darstellen (d. h. gemäß ihrem de facto begrenzten Angebot).

Der Begriff „Fiat-Währung“ bezieht sich auf eine Währung ohne inneren Wert. Eine solche wird in der Regel durch staatliche Regulierung als Geld festgelegt (z. B. USD oder EUR).

1.1.2 Die erste Blockchain-Anwendung

Die Bitcoin-Kryptowährung war die erste Blockchain-Anwendung, die einen sicheren, digitalen und dezentralen Geldtransfer zwischen zwei Personen bieten sollte. Das auf der Blockchain basierende Bitcoin-Netzwerk ermöglicht Werttransfers, welche völlig unabhängig von externen Parteien wie beispielsweise Banken oder Kreditkartenanbieter sind. Mittels Bitcoins können Händler Zahlungen von überall auf der Welt annehmen, ohne technischen oder rechtlichen Einschränkungen zu unterliegen, die häufig durch die bestehende Zahlungsinfrastruktur auferlegt werden (z. B. Wechselkurse, Verzögerungen bei der Abwicklung, regulatorische Beschränkungen). Allerdings muss der Empfänger einer Überweisung von Bitcoins diese wieder in eine Fiat-Währung umtauschen, um damit Waren kaufen zu können, es sei denn, der Verkäufer der Waren akzeptiert bereits Bitcoins als Zahlungsmittel.

Da Blockchains Transaktionen überwachen können, die digital in Datensätzen dargestellt werden, sind die Anwendungen, für die sich Blockchains am besten eignen, vertrauensfreie Asset-Transfers (z. B. Kryptowährungen). Diese wurden erst möglich, als mithilfe von Blockchain herkömmliche Methoden wie Rechnungen oder Aktien durch digitale Token ersetzt wurden.

Kryptowährungen sind nur eine von vielen möglichen Anwendungen, die sich die Blockchain-Infrastruktur zunutze machen können (Abb. 1.2). Der Bereich der denkbaren Blockchain-Anwendungen ist sehr groß und geht über den primären Anwendungsfall des

Abb. 1.2 Blockchain ist eine Basistechnologie

Werttransfers mittels Token hinaus: Es kann im Prinzip jedes reale physikalische Gut auf einer Blockchain nachverfolgt („tracked“) werden, da das zugrunde liegende Netzwerk als Vermittler und Buchhaltung fungiert.

Zu solchen Anwendungen gehören fehlersicheres Datenmanagement und Identitätsverfolgung, da Blockchains eine exakte Chronik erzeugen können, die zeigt, wer wann welche Daten gespeichert hat. Der Zugang dazu eröffnet eine Vielzahl von Möglichkeiten für Anwendungen sowohl im öffentlichen (z. B. bei vertrauensfreien Grundbuchämtern) als auch im privaten (z. B. bei grenzüberschreitenden Geldtransfers) Bereich.

Blockchains bieten ein Datensystem, das niemandem gehört, an dem jeder teilnehmen kann und welches über einen Pay-to-Play-Mechanismus verfügt (d. h. für das Hinzufügen von Daten entstehen Kosten). Damit eignet sich die Technologie gut für Szenarios, in denen es darauf ankommt, dass alle Netzwerkteilnehmer den darin enthaltenen Informationen vertrauen, und zwar ohne zentralisierte Autorität, welche diese Angaben bestätigen oder legitimieren könnte.

Der Hauptunterschied zwischen herkömmlichen zentralisierten Systemen wie denen, die von Banken verwendet werden, und dezentralisierten Blockchain-Systemen besteht darin, dass erstere auf einen Vermittler angewiesen sind. So wird beispielsweise bei einer traditionellen Banküberweisung eine Clearingstelle mit dem Saldieren der Transaktion zwischen den Banken beauftragt (Choudhry 2012) (Abb. 1.3). Blockchains benötigen dies nicht, da Sender und Empfänger Transaktionen direkt miteinander ausmachen.

Lassen Sie uns als Nächstes die Funktionen und Merkmale unseres traditionellen Währungssystems sowie herkömmlicher Zahlungsmittel begutachten, um dann am Beispiel

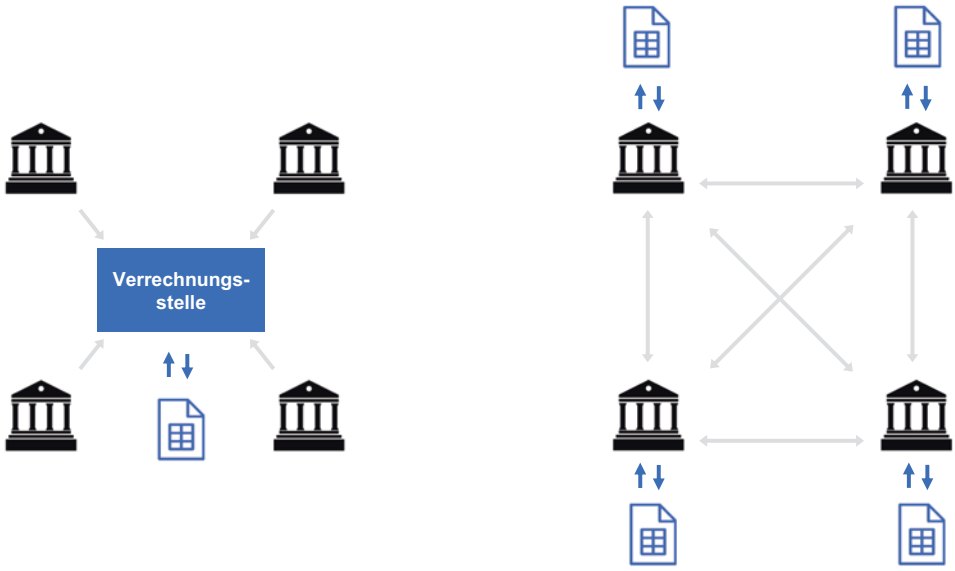

Abb. 1.3 Blockchain und das Konzept der Dezentralisierung

von Bitcoin die Mechanismen, die den Kryptowährungen und der Blockchain-Technologie zugrunde liegen, zu verdeutlichen.

1.1.3 Währungen: Traditionell und Krypto

Herkömmliches Geld, wie Banknoten und Münzen, muss drei Funktionen erfüllen (Martin 2015):

- Zahlungsmittel zur Erleichterung von Transaktionen
- Werterhalt über die Zeit
- Rechnungseinheit, die zum Beispiel für die Wertberechnung oder den Vergleich von Waren oder Dienstleistungen verwendet werden kann

Um diesen Anforderungen gerecht zu werden, muss Geld folgende Merkmale aufweisen:

- Schutz gegen Vervielfältigung
- Physische Sicherheit, sodass der physische Besitz des Geldes Eigentümerschaft bedeutet

Unser traditionelles Währungssystem beruht auf Fiat-Währungen, d. h. Währungen, die an sich wertlose Objekte sind (Münzen und Geldscheine), ihren Wert jedoch fast vollständig aus der staatlichen Unterstützung beziehen (Graeber 2014). Ein solches System hat sowohl Vor- als auch Nachteile: Wenn die Regierung, die eine Währung stützt, stabil ist, dann ist auch die Währung tendenziell stabil, und es gibt Mechanismen, mit denen inflationären Schwankungen begegnet werden kann. Immer wieder versagen Regierungen im Hinblick auf diese wichtige volkswirtschaftliche Funktion. Dabei verlieren Währungen oft einen großen Teil ihres Wertes, wie jüngst am Beispiel Venezuelas zu beobachten war.

Kryptowährungen wie Bitcoin erfüllen sowohl die funktionalen Anforderungen (Zahlungsmittel, Werterhalt und Rechnungseinheit) als auch die Sicherheitsmerkmale (Schutz gegen Vervielfältigung und physische Sicherheit) eines herkömmlichen Währungssystems.

Bitcoin etwa ermöglicht den direkten und diskreten Token-Transfer von einer Person zur anderen und funktioniert damit per definitionem als Zahlungsmittel, ohne dabei auf einen Vermittler angewiesen zu sein. In der Praxis muss jede Transaktion dieser Art eine Herkunfts- und eine Zieladresse sowie die Anzahl der zu übertragenden Wertmarken benennen. Kap. 3 gibt einen detaillierten Überblick über alle Daten, die in einer Bitcoin-Transaktion enthalten sind.

Was den Werterhalt betrifft, kann man Bitcoin am ehesten mit Rohstoffressourcen wie Silber und Gold vergleichen, die einen bestimmten Preis pro Einheit haben. Die Marktkräfte (d. h. Angebot und Nachfrage) bestimmen den Preis dieser Rohstoffe ebenso, wie sie den Preis von Bitcoin beeinflussen. Daher erfüllt Bitcoin die Werterhaltsanforderung auf der Grundlage seiner aktuellen marktbestimmten Bewertung. Bitcoin ist so gegen die

meisten Faktoren immun, die den Wertverlust einer traditionellen Währung verursachen können, wie etwa Regierungsversagen.

Schließlich hat Bitcoin, wie herkömmliche Währungen, eine Rechnungseinheit. Die Währungseinheit des Bitcoin-Netzwerks ist der „Bitcoin“ mit der Abkürzung BTC. Die kleinste Einheit ist ein Satoshi, benannt nach dem Pseudonym Satoshi Nakamoto, dem anonymen Erfinder des Bitcoin-Netzwerkprotokolls (siehe Kap. 3). Ein Bitcoin entspricht 100.000.000 Satoshis.

1.1.4 Eigentum

In blockchainbasierten Systemen werden individuelle Transaktionen nicht einzeln versandt. Stattdessen führen die Netzwerkknoten Transaktionen in sogenannten Blöcken durch und fügen diese Blöcke dann an ein dezentralisiertes Ledger (d. h. die Blockchain) an. Wenn ein Benutzer Bitcoins besitzt, zeigt das Ledger jederzeit an, wie viele Bitcoins er auf seinem Konto, also der Bitcoin-Adresse, hat. Der Benutzer kann Bitcoins nur dann auf einen anderen übertragen, wenn er sie tatsächlich besitzt. Eine gültige Transaktionsanweisung aktualisiert das Ledger entsprechend (Abb. 1.4).

Als einfaches Beispiel können wir annehmen, dass die Summe aller traditionellen Münzen und Scheine, die eine Person besitzt, den aktuellen Nettowert darstellt: Wenn ich Dollarscheine in meiner Tasche habe, dann gehören diese Dollars mir, und es gibt keine Unklarheit bezüglich der Frage des Eigentums daran.

Bei traditionellen Bankkonten werden umfangreiche Datenbanken eingesetzt, um zu überblicken, über wie viel Geld ein Kunde dort verfügt. Wir können diese Systeme als zentralisierte, ständig aktualisierte Ledger betrachten, die das Guthaben eines jeden Kontoinhabers nachverfolgen.

Im Hinblick auf Bitcoin funktioniert das System anders. Anstatt eine zentrale Stelle zu haben, die ein großes Ledger kontrolliert, unterhält jeder Teilnehmer („Node“) des Blockchain-Netzwerks eine kryptografisch verifizierte Kopie des neuesten dezentralen Ledgers, das alle jemals stattgefundenen Transaktionen enthält. Dieses Ledger ist öffent-

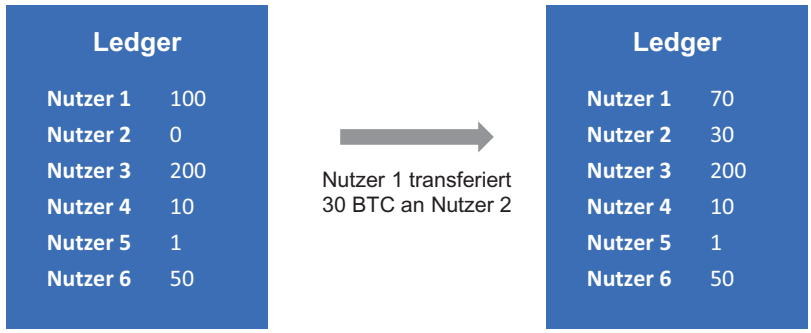

Abb. 1.4 Übertragung von Positionen mithilfe eines blockchainbasierten Kontobuchsystems