

**ESV** ERICH  
SCHMIDT  
VERLAG

# **Bitcoin, Ethereum & Co.**

**Praxiswissen Kryptowährungen und Blockchain**

Von

**Enée Bussac**

**ERICH SCHMIDT VERLAG**

**Bibliografische Information der Deutschen Nationalbibliothek**

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

**Weitere Informationen zu diesem Titel finden Sie im Internet unter**

[ESV.info/978-3-503-18299-2](http://ESV.info/978-3-503-18299-2)

Titel der Originalausgabe:

»Bitcoin, ether & Cie«

© Dunod, 2018

Gedrucktes Werk: ISBN 978-3-503-18299-2

eBook: ISBN 978-3-503-18700-3

Alle Rechte für die deutschsprachige Ausgabe vorbehalten

© Erich Schmidt Verlag GmbH & Co. KG, Berlin 2019

[www.ESV.info](http://www.ESV.info)

Dieses Papier erfüllt die Frankfurter Forderungen der Deutschen Nationalbibliothek und der Gesellschaft für das Buch bezüglich der Alterungsbeständigkeit und entspricht sowohl den strengen Bestimmungen der US Norm Ansi/Niso Z 39.48-1992 als auch der ISO-Norm 9706.

Satz: schwarz auf weiss, Berlin

Druck und Bindung: Strauss, Mörlenbach

## Vorwort

Es ist nicht einfach, ein Buch über Kryptowährungen und die Blockchain zu schreiben, denn dieses Universum, das ein wahrer Dschungel ist, verändert sich jeden Tag, jede Stunde, jede Minute, jede Sekunde. Das Thema begeistert mich allerdings, und zwar hauptsächlich aus drei Gründen.

Erstens sind Kryptowährungen noch immer relativ unbekannt und werden von der Allgemeinheit schlecht angesehen. Es gibt also viel zu erklären und ein Zweck dieses Buches ist, dass Sie dieses neue Ökosystem zuerst verstehen, um sich dann zu entscheiden, ob Sie sich daran beteiligen möchten.

Der zweite Grund ist, dass Kryptowährungen nicht nur aus Bitcoin, dubiosen Transaktionen (die es übrigens auch schon vor Kryptowährungen gab) und zufälligen Preisschwankungen bestehen: Dahinter stecken Teams mit echten Projekten, Vorhaben, Ideen und neuen Modellen, wie Sie an einigen Beispielen dieses Buches sehen werden.

Drittens stehen wir am Anfang einer Revolution, die über die Neudefinition der Währung und das Aufkommen der Dezentralisierung hinausgeht. Die Entstehung dieses Buches ist einerseits auf meine Leidenschaft und mein Engagement in dieser relativ neuen, ereignisreichen und revolutionären Welt zurückzuführen, und andererseits auf meinen Wunsch, zu erklären, zu teilen, und zu strukturieren. Ich habe mich bemüht, diesen Leitfaden so nützlich, praxisnah und angenehm wie möglich zu gestalten, damit Sie diese neue Welt verstehen und Sie investieren und antizipieren können.

Ich danke meinen Korrektorinnen Katrin Bussac, Julia Politt und Nina Heck, die mich beim Schreiben dieses Buches unterstützt haben. Ohne sie hätte ich es sprachlich und zeitlich nicht geschafft.

München, im Dezember 2018

Enée Bussac

# Inhaltsverzeichnis

<b>Vorwort</b> .....	5
<b>1 Wahrung und Kryptographie</b> .....	13
1.1 Was ist eine Wahrung? .....	13
1.2 Was erteilt einer Wahrung ihren Wert? .....	13
1.3 Die Entwicklung der Wahrungen in den letzten Jahrzehnten .....	13
1.4 Die latente Krise des Treuhandsystems .....	14
1.5 Was ist Kryptographie? .....	14
1.5.1 Kryptographie .....	14
1.5.2 Asymmetrische Kryptographie .....	15
<b>2 Das Kryptowahrungssystem</b> .....	17
2.1 Was ist eine Kryptowahrung? .....	17
2.2 Der Bitcoin .....	18
2.2.1 Kleine Geschichte .....	18
2.2.2 Die Vorteile des Bitcoins .....	19
2.2.3 Die Grenzen des Bitcoin-Systems .....	20
2.2.4 Ist Bitcoin eine anonyme Wahrung? .....	21
2.2.5 Das Lightning-Network .....	21
2.2.6 Warum ist Bitcoin bei weitem die wichtigste Kryptowahrung? .....	22
2.2.7 Die Bitcoin-Maximalisten .....	23
2.2.8 Warum wird so viel Energie verbraucht? .....	24
2.3 Ethereum .....	26
2.3.1 Beschreibung .....	26
2.3.2 SWOT-Analyse von Ethereum .....	27
2.3.3 Ethereum vs. EOS .....	29
2.3.4 Gebuhren auf Ethereum .....	30
2.3.5 NFT .....	30
2.4 Stablecoins .....	32
2.5 Der Wert der Kryptowahrungen .....	35
2.5.1 Der Aufschwung .....	35
2.5.2 Was sind momentan die wesentlichen Vor- und Nachteile der Kryptowahrungen im Vergleich zu Fiatwahrungen? .....	36
2.6 Warum gibt es so viele Kryptowahrungen? .....	37
2.7 Die Coin-Familien .....	39
2.7.1 Reine Coins .....	41
2.7.2 Finanz-Coins .....	41
2.7.3 Technologie-Coins .....	41
2.7.4 Community-Coins .....	42

2.7.5	Reale-Welt-Coins . . . . .	42
2.8	Die Blockchain . . . . .	42
2.8.1	Definition und Funktionsweise . . . . .	42
2.8.2	Die Blockchain auf Kryptowährungen angewendet . . . . .	44
2.8.3	Die Lösung zur „Doppelausgabe“ (Double Spending) . . . . .	45
2.8.4	Warum ist dies bahnbrechend? . . . . .	46
2.8.5	Blockchain 1.0 und 2.0. . . . .	46
2.8.6	Die 51 %-Attacke . . . . .	47
2.8.7	Warum ist eine 51 %-Attacke auf den Bitcoin sehr unwahrscheinlich? . . . . .	47
2.8.8	Öffentliche und private Blockchains . . . . .	49
2.8.9	Das Trilemma der Blockchain . . . . .	50
2.8.10	Die Abschaffung der Zwischenhändler . . . . .	51
2.9	Die „Proof of“-Algorithmen . . . . .	52
2.9.1	Was ist ein Konsens? . . . . .	52
2.9.2	Was sind die Mechanismen, die einen Konsens ermöglichen? . . . . .	53
2.9.3	Eigenschaften der Konsensalgorithmen: . . . . .	53
2.9.4	Proof of . . . . .	54
2.9.5	Die zwei wesentlichsten „Proof of“. . . . .	54
2.10	Forks . . . . .	57
2.10.1	Soft Forks . . . . .	57
2.10.2	Hard Forks . . . . .	57
2.10.3	ETH und ETC . . . . .	58
2.10.4	Die Hard Forks des Bitcoins . . . . .	58
2.11	Smart Contracts . . . . .	60
2.11.1	Was ist ein Vertrag? . . . . .	60
2.11.2	Wie können digitale Technologien helfen? . . . . .	60
2.11.3	Anwendungsbereiche der Smart Contracts . . . . .	61
2.11.4	Die Risiken der Smart Contracts . . . . .	62
<b>3</b>	<b>Konsens und Transaktionen . . . . .</b>	<b>65</b>
3.1	Mining . . . . .	65
3.2	Abwicklung einer PoW-Transaktion . . . . .	67
3.2.1	Übermittlung des Auftrags an das Netzwerk (Benutzer) . . . . .	67
3.2.2	Identifikation und Verifikation von Aufträgen (Miner) . . . . .	67
3.2.3	Zusammenstellung von Blöcken (Miner) . . . . .	68
3.2.4	Erzeugung von Hashes (Miner) . . . . .	68
3.2.5	Beispiel der Bitcoin-Blockchain . . . . .	69
3.2.6	Zusammenstellung der Blockchain . . . . .	70
3.2.7	Verwaiste Blöcke . . . . .	70
3.2.8	Rückbehaltung von Blöcken . . . . .	71
3.3	Gas und Gas Price . . . . .	72

<b>4</b>	<b>Der Markt der Kryptowährungen</b>	77
4.1	2017	77
4.2	2018	78
4.3	Exchanges	79
4.3.1	Die Besonderheiten des Marktes der Kryptowährungen	80
4.3.2	Coin Market Cap	81
4.3.3	Anleger werden	81
4.3.4	Ein Tag bei Kraken in der guten alten Zeit (Ende 2017)	82
4.3.5	Exchanges vs. Zahlungslösungen	84
4.4	Die neuen Ponzi-Schemen	85
4.4.1	Was sind HYIP?	85
4.4.2	Wie funktionieren HYIP?	87
<b>5</b>	<b>In Kryptowährungen anlegen</b>	89
5.1	Wallets	89
5.1.1	Definition	89
5.1.2	Die verschiedenen Wallets	89
5.2	Public Address/Privater Schlüssel	92
5.3	Trading Bots	94
5.4	Arbitrage	95
5.5	Neue Währungen, neues Einkommen	97
5.5.1	Echtes Projekt oder Bitcoin-Sauger?	97
5.5.2	Neue Wege, um Geld zu verdienen	98
5.6	ICO	100
5.6.1	Definition	100
5.6.2	Ein neuer Weg, Start-ups und ... Betrüger zu finanzieren	100
5.6.3	Die wichtigsten Schritte eines ICO	102
5.6.4	Beispiel für einen ICO: Remme (REM)	103
5.7	Miner werden	113
5.7.1	Mining zu Hause	113
5.7.2	Ein paar Zahlen	115
5.7.3	Ist Mining eine profitable Tätigkeit?	117
5.8	Sich erkundigen	118
<b>6</b>	<b>Vorschläge für Anlagestrategien</b>	121
6.1	Trading	121
6.1.1	Strategie festlegen	121
6.1.2	In den Markt einsteigen	123
6.1.3	Geld auf sein Hauptkonto überweisen	124
6.1.4	In Kryptowährungen aus dem Hauptkonto anlegen	125
6.1.5	Ein paar Grundregeln	126
6.1.6	Empfehlungen je nach Budget	127
6.2	Risikoreiche Anlagestrategien	128

6.2.1	In Satcoins investieren . . . . .	128
6.2.2	In neue Coins investieren . . . . .	128
6.2.3	In die „biggest Losers“ investieren . . . . .	129
6.2.4	Die Yobit-Investbox . . . . .	129
6.2.5	Sich an einem ICO beteiligen . . . . .	131
6.2.6	In CFD investieren. . . . .	132
6.2.7	Zum Schluss . . . . .	132
6.3	Vorschlag einer Analysemethode, um die neue Perle der Kryptowährungen zu finden . . . . .	133
6.3.1	Voraussetzungen . . . . .	133
6.3.2	Die Kerneigenschaften . . . . .	134
6.3.3	Die Exchanges . . . . .	135
6.3.4	Der Block Explorer . . . . .	136
6.3.5	Die Community. . . . .	136
6.3.6	Die Innovation . . . . .	137
<b>7</b>	<b>Die Bezahlarten der Zukunft. . . . .</b>	<b>139</b>
7.1	Kryptowährungen überweisen, empfangen und benutzen . . . . .	139
7.1.1	Kryptowährungen empfangen. . . . .	139
7.1.2	Kryptowährungen überweisen . . . . .	140
7.1.3	Wo und wie kann man seine Coins ausgeben? . . . . .	141
7.2	Die neuen Anwendungsbereiche des Geldes . . . . .	143
7.2.1	Die Anpassung der Währung an die Entwicklung der Gesellschaft . . . . .	143
7.2.2	Die Herausforderung der Dezentralisierung . . . . .	144
7.2.3	Das Dogma der Dezentralisierung. . . . .	145
7.2.4	Die Markteffizienz. . . . .	146
7.2.5	Geld erobert sich ein neues Funktionsfeld . . . . .	147
7.2.6	Die Entstehung neuer Modelle . . . . .	148
7.2.7	Währungskontrolle . . . . .	149
7.3	Welche Auswirkung könnten Kryptowährungen auf unsere Zahlungsweisen haben? . . . . .	151
7.3.1	Die Rolle der Public Addresses. . . . .	151
7.3.2	Vereinfachung und Verbesserung von Zahlungen. . . . .	152
7.3.3	Rückverfolgbarkeit von Zahlungen . . . . .	154
7.3.4	Kryptowährungen und Steuerabzug. . . . .	156
7.3.5	Die neuen Treueprogramme . . . . .	157
7.4	Feststellen und vorhersagen . . . . .	158
7.4.1	Die Rolle des Orakels . . . . .	158
7.4.2	Ein Anwendungsbeispiel: prädiktive Märkte . . . . .	159
<b>8</b>	<b>Das neue Wertmanagement. . . . .</b>	<b>165</b>
8.1	Was bedeutet Wert? . . . . .	165
8.1.1	Definition . . . . .	165

8.1.2	Was hat Wert? . . . . .	165
8.1.3	Wer schafft Wert? . . . . .	166
8.1.4	Wie wird der Wert bestimmt? . . . . .	166
8.1.5	Wie werden Werte derzeit verwaltet? . . . . .	167
8.2	Die Blockchain als neues Werkzeug, um Eigentumsverhältnisse zu verwalten . . . . .	167
8.2.1	Von Werten zu Eigentumsverhältnissen . . . . .	167
8.2.2	Ein Beispiel: Das Grundbuch . . . . .	168
8.2.3	Die Inputs einer Blockchain . . . . .	169
8.3	Wird Uber überaltert? . . . . .	171
8.3.1	Was ist das Uber-Modell? . . . . .	171
8.3.2	Die Blockchain als neues Werkzeug, um Werte zu verwalten . . . . .	171
8.3.3	Ein Beispiel: Kurzzeitvermietung in Berlin . . . . .	171
8.3.4	Ein Beispiel aus der Musikindustrie . . . . .	173
8.3.5	Wiederholt sich die Geschichte? . . . . .	174
8.4	Das Web 3.0 . . . . .	176
8.4.1	Die Ursprünge des Webs . . . . .	176
8.4.2	Das neue Internet entsteht . . . . .	178
8.5	Neue Berufe . . . . .	179
8.5.1	Miner . . . . .	179
8.5.2	Ersteller von Blockchain-basierten Werteverwaltungssystemen. . . . .	180
8.5.3	Kryptowährung-Emittent . . . . .	180
8.5.4	Blockchain-Programmierer. . . . .	180
8.5.5	Smart-Contract-Programmierer. . . . .	181
8.5.6	Orakel. . . . .	181
8.5.7	Blockchain-Verwalter . . . . .	181
8.5.8	Spezialist für die Rückverfolgbarkeit von Blockchain- Transaktionen . . . . .	181
8.6	Werden Sie fit für die Blockchain! . . . . .	182
8.6.1	Die „Tokenisierung“ . . . . .	182
8.6.2	Die Inbetriebnahme der Blockchain . . . . .	184
8.6.3	Beispiel eines Unternehmens, das die Blockchain in die reale Welt einführt. . . . .	185
8.7	Zusammenfassende Diagramme . . . . .	186
8.7.1	Allgemeine Diagramme . . . . .	187
8.7.2	Beispiele für Blockchain-basierte Smart Contracts . . . . .	188
<b>9</b>	<b>Schlusswort</b> . . . . .	<b>193</b>
	<b>Anhang</b> . . . . .	<b>195</b>
	<b>Der Autor</b> . . . . .	<b>221</b>