ENÉE BUSSAC

Bitcoin, Ethereum & Co.

Praxiswissen Kryptowährungen und Blockchain

ESV ERICH SCHMIDT VERLAG

ERICH
SCHMIDT
VERLAG

Bitcoin, Ethereum & Co.

Praxiswissen Kryptowährungen und Blockchain

Von

Enée Bussac

ERICH SCHMIDT VERLAG

Weitere Informationen zu diesem Titel finden Sie im Internet unter
ESV.info/978-978-3-503-18700-3

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

Ergeben sich zwischen der Version dieses eBooks
und dem gedruckten Werk Abweichungen,
ist der Inhalt des gedruckten Werkes verbindlich.

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

Vorwort 5

1 Währung und Kryptographie 13

1.1 Was ist eine Währung? 13
1.2 Was erteilt einer Währung ihren Wert? 13
1.3 Die Entwicklung der Währungen 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

2 Das Kryptowährungsökosystem 17

2.1 Was ist eine Kryptowährung? 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 Währung? 21
2.2.5 Das Lightning-Network 21
2.2.6 Warum ist Bitcoin bei weitem die wichtigste Kryptowährung? 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 Gebühren auf Ethereum 30
2.3.5 NFT 30
2.4 Stablecoins 32
2.5 Der Wert der Kryptowährungen 35
2.5.1 Der Aufschwung 35
2.5.2 Was sind momentan die wesentlichen Vor- und Nachteile der Kryptowährungen im Vergleich zu Fiatwährungen? 36
2.6 Warum gibt es so viele Kryptowährungen? 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

3 Konsens und Transaktionen 65

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

4 Der Markt der Kryptowährungen 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

5 In Kryptowährungen anlegen 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

6 Vorschläge für Anlagestrategien 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

7 Die Bezahlarten der Zukunft 139

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

8 Das neue Wertmanagement 165

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

9 Schlusswort . . . 193

Anhang . . . 195

Der Autor . . . 221

1 Währung und Kryptographie

Bevor wir die Welt der Kryptowährungen erkunden, werden wir drei grundlegende Elemente erläutern, auf denen sie beruht: Währung, Wert und Kryptographie.

1.1 Was ist eine Währung?

Eine Währung ist ein vom Menschen erzeugtes Werkzeug, das drei Funktionen hat: Währung fungiert als Wertaufbewahrungsmittel. Wenn ich eine Münze oder einen Geldschein besitze, habe ich etwas Wertvolles, was ich leicht verkaufen oder tauschen kann. Eine Währung ist außerdem eine Recheneinheit für die wirtschaftliche Kalkulation oder Buchhaltung. Zum Beispiel ist eine Zeitung 2 Euro wert oder eine Fachzeitschrift kostet 1.000 Yen. Eine Währung ist ein Zahlungsmittel. Mit ihr können Waren und Dienstleistungen getauscht sowie Schulden beglichen werden.

Fiatwährungen (Euro, Dollar etc.), wie wir sie heute kennen, sind eine konstitutionelle Institution, die einem Handelsgebiet angegliedert sind, das in der Wirtschaft als nationaler Markt bezeichnet wird. Die Währung ist das Zahlungsmittel, das in diesem Gebiet zu einem bestimmten Zeitpunkt aufgrund von Gesetz und Praxis rechtsgültig ist.

1.2 Was erteilt einer Währung ihren Wert?

An sich hat eine Währung keinen Wert: Sie besteht aus (immer weniger) Metallteilen, den Münzen, und Papierstücken, den Geldscheinen, und (immer mehr) aus Nullen und Einsen. Erst das Vertrauen gibt einer Währung ihren Wert; es ist ein untrennbarer Bestandteil davon. Beispielsweise erkenne ich an, dass eine Währung einen gewissen Wert hat, weil ich und viele andere Menschen dem Emittenten dieser Währung vertrauen. Anders gesagt, weiß ich, dass ich sie einfach gegen eine Ware, eine Dienstleistung oder eine andere Währung eintauschen könnte. Früher wurde die Währung durch wertvolles Material gestützt. Der Wert einer Währung beruht auf dem Vertrauen, das wir in die öffentliche Behörde haben, welche die jeweilige Währung ausgibt, ihren Namen, ihre Unterschrift und ihr Akronym bestimmt. Seit dem Ende des Bretton-Woods-Systems sind es nur noch die Staaten, die Vertrauen geben und daher Währungen Wert verleihen.

1.3 Die Entwicklung der Währungen in den letzten Jahrzehnten

Die Währung erfuhr im 20. Jahrhundert drei große Veränderungen: Sie wurde nicht mehr an wertvollen Materialien indexiert, ihre Menge stieg explosionsartig an und sie erlebte eine große Welle der Dematerialisierung. Bargeld, selbst wenn Sie es wahrscheinlich immer noch häufig benutzen, stellt nur noch einen sehr kleinen Teil der Geldmenge dar und verschwindet allmählich in einigen Ländern. In Schweden, einem sehr fortschrittlichen Land, wird beispielsweise kaum noch Bargeld verwendet. Bargeld ist außerdem das „teuerste“ Geld, weil es durch menschliche Arbeitskraft geschützt, bewegt und gelagert werden muss.

Der Aufschwung des Internets und der Smartphones hat die Dematerialisierung der Währung beschleunigt und den Weg für neue Zahlungsmethoden wie Paypal, Apple Pay, Online-Transfers und andere entmaterialisierte Zahlungslösungen geebnet. Das derzeitige System der Fiatwährungen mit der Angliederung an ein gewisses Handelsgebiet passt immer weniger in unsere globalisierte und digitalisierte Welt. Die Fließfähigkeit des Handels ist ein Schlüsselfaktor für die Entwicklung der Menschheit, und Geld ist zusammen mit Kommunikation und Transport eines der grundlegenden Instrumente, die diese ermöglicht.

1.4 Die latente Krise des Treuhandsystems

Gleichzeitig wurde 2008 wegen der Subprime-Krise Vertrauen und damit Wert in den Fiatwährungen untergraben, die aus Staaten und dem System der Zentral- und Geschäftsbanken stammten. Die jüngsten Bankrotte von Staaten wie Griechenland oder Venezuela haben uns gezeigt, dass das System ins Wanken geraten und sich sogar gegen die Bevölkerung wenden kann. In Zypern beispielsweise haben die Banken das Geld der Vermögenden ohne deren Zustimmung verwendet, um Schulden 2013 abzuzahlen. Die Zentralbanken stecken so viel Geld in das System im Rahmen des sogenannten Quantitative Easing (QE) und die Staaten sind dermaßen verschuldet, dass unser Geldsystem mehr und mehr wie eine Flucht nach vorne aussieht, die langsam aber sicher das Vertrauen und damit auch den Wert von Fiatwährungen schwächt. Es stellt sich langsam die Frage, wer von diesen massiven Geldspritzen profitiert, da es anscheinend nicht der Großteil der Bevölkerung ist und die Staaten immer mehr sparen müssen und sich immer mehr verschulden.

Aber solange es keine Alternative gab, konnten wir uns nur auf das System der Fiatwährungen verlassen, das von Staaten und Banken gestaltet und verwaltet wird.

1.5 Was ist Kryptographie?

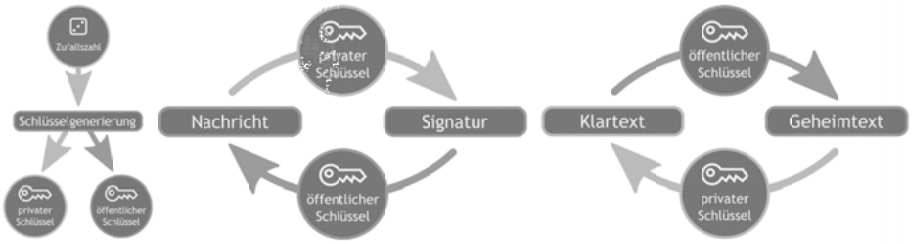
1.5.1 Kryptographie

Kryptographie ist eine Technik, die Botschaften anhand von Zeichen (Ziffern, Buchstaben usw.) schützen kann, indem sie sie durch eine bestimmte Verschlüsselung unverständlich macht. Das Wort „Kryptographie“ kommt von den altgriechischen Wörtern „kryptós“ (verborgen) und „gráphein“ (schreiben). In der klassischen Kryptographie, auch symmetrische Kryptographie genannt, ist die Verschlüsselung die Umwandlung einer verständlichen Botschaft („Klartext“) in eine unverständliche Nachricht („Geheimtext“) für diejenigen, die den Entschlüsselungsschlüssel nicht besitzen. In der symmetrischen Kryptographie wird mit demselben Schlüssel eine Botschaft verschlüsselt und entschlüsselt. Dies ist die Schwäche des Systems: Der Entschlüsselungsschlüssel muss zugleich streng geheim bleiben und einem Korrespondenten auf sichere Weise übermittelt werden.

1.5.2 Asymmetrische Kryptographie

Um dieses Problem zu lösen, wurde Ende des 20. Jahrhunderts die asymmetrische Kryptographie ins Leben gerufen. In der asymmetrischen Kryptographie hat jeder seinen Schlüssel, sodass dem Korrespondenten keiner übermittelt werden muss. Die allermeisten Kryptowährungen benutzen diese asymmetrische Kryptographie, um die Sicherheit des Systems zu gewährleisten. Die Kernidee dahinter ist, dass die Verschlüsselung einer Botschaft sehr einfach ist und es so gut wie unmöglich ist, diese ohne den passenden Schlüssel zu entziffern.

Bei den Einwegfunktionen, die für die asymmetrische Kryptographie charakteristisch sind, handelt es sich um mathematische Funktionen, die es extrem schwierig machen, an die ursprüngliche Botschaft zu gelangen. Die asymmetrische Kryptographie basiert auf der Unterscheidung von öffentlichen und privaten Daten. Sie verwendet zwei Schlüssel: den öffentlichen Schlüssel, auch Public Key genannt, der die Botschaft unverständlich macht, sie also verschlüsselt; dieser Schlüssel kann allen zugänglich gemacht werden. Der private Schlüssel hingegen, auch Private Key genannt, dient der Entschlüsselung und muss daher absolut geheim bleiben. Dieses Public-Key-Verschlüsselungsverfahren ist genau das, was fast alle Kryptowährungen verwenden. Dieses Verfahren hat zwei Hauptvorteile: Die Vertraulichkeit der Nachricht wird durch den Einsatz des öffentlichen Schlüssels für die Verschlüsselung und des privaten Schlüssels für die Entschlüsselung gewährleistet. Ein weiterer Vorteil ist, dass die Echtheit des Absenders sichergestellt wird. Zum Verschlüsseln der Nachricht verwendet der Absender den öffentlichen Schlüssel des Empfängers. Um die Nachricht zu entschlüsseln, benötigt der Empfänger seinen privaten Schlüssel; diesen privaten Schlüssel besitzt nur er, wodurch wiederum sicherstellt ist, dass nur er die verschlüsselten Daten lesen kann. Asymmetrische Kryptographie wird seit langem von Banken und im Internet zur Verschlüsselung von Daten und Nachrichten wie z.B. Passwörtern verwendet.



Quelle: Wikipedia

Zusammenfassung

- Eine Währung im klassischen Sinne erfüllt drei Hauptaufgaben: Sie ist ein Wertaufbewahrungsmittel, eine Recheneinheit und ein Zahlungsmittel.
- 2008 sind die Grenzen des aktuellen monetären und finanziellen Systems sichtbar geworden, was einen Platz für ein alternatives System geschafft hat.
- Die Kryptographie ist eine Technik, die Botschaften anhand von Zeichen schützen kann, indem sie sie durch eine bestimmte Verschlüsselung unverständlich macht.
- Die asymmetrische Kryptographie unterscheidet sich dadurch von der normalen bzw. symmetrischen Kryptographie, dass es einen Verschlüsselungs- und einen Entschlüsselungsschlüssel gibt, wodurch das System deutlich sicherer wird.

2 Das Kryptowährungsökosystem

In diesem Kapitel werde ich Ihnen zeigen, was Kryptowährungen sind und wie sie sich von den Fiatwährungen unterscheiden. Außerdem werden wir wichtige Komponenten aus dem Ökosystem der Kryptowährungen entdecken: z.B. Blockchain, Mining, Forks, Smart Contracts usw. Am Ende dieses Buches befindet sich ein Glossar mit den wichtigsten Begriffen zum Thema Kryptowährungen, damit Sie sich möglichst schnell in der für Sie vielleicht noch neuen Welt zurechtfinden.

2.1 Was ist eine Kryptowährung?

Eine Kryptowährung, auch kryptographische, digitale oder virtuelle Währung genannt, ist eine Währung, deren Funktionsweise und Sicherheit auf Kryptographie basiert und völlig digital ist.

Sie erfüllt die drei wesentlichen Funktionen einer Währung: Kryptowährungen fungieren als Wertaufbewahrungsmittel. Wenn ich einen Bitcoin besitze, habe ich etwas Wertvolles, was ich leicht verkaufen oder tauschen kann. Außerdem sind Kryptowährungen eine Recheneinheit für die wirtschaftliche Kalkulation oder Buchhaltung. Sie können bereits einige Produkte und Dienstleistungen mithilfe von Kryptowährungen kaufen; dies ist vor allem mit Bitcoins möglich. Zusätzlich dazu sind Kryptowährungen ein Zahlungsmittel. Sie sind immer an ein Zahlungssystem angeschlossen, um Austausch zu ermöglichen, der momentan hauptsächlich zu Spekulationszwecken und auf bestimmten Marktplätzen stattfindet. Kryptowährungen haben sogar noch eine weitere Funktion, die ich Ihnen im Laufe des Buches vorstellen werde.

Das Funktionieren einer Kryptowährung und ihre Sicherheit basieren auf der asymmetrischen Kryptographie (mit ein paar Ausnahmen, z.B. Stellar Lumens). Kryptowährungen werden mithilfe eines Protokolls durchgeführt, das kryptographische Funktionen für den Währungsaustausch auf einem sicheren globalen Netzwerk bereitstellt, ohne dass eine zentrale Kontrollinstanz (wie z.B. eine Bank) benötigt wird. Im Gegenteil zu Fiatwährungen (Euro, Dollar, Won usw.) wird eine Kryptowährung nicht unbedingt auf Veranlassung eines Staates oder einer Gruppe von Staaten durch eine Zentralbank kreiert. Sie kann von einer oder mehreren Personen, einer Organisation oder einem Unternehmen erstellt werden; sie existiert nur in elektronischer Form und ist nicht an ein Territorium gebunden.

Die erste Kryptowährung, der Bitcoin, entstand im Januar 2009; mit ihr wurde die Technologie der Blockchain ins Leben gerufen. Der Bitcoin ist zugleich die bekannteste und auch die bedeutendste Kryptowährung, die wir kennen. Alle Kryptowährungen funktionieren auf einer Blockchain und unterscheiden sich vor allem durch ihren Wert, den Rhythmus der Schöpfung von neuen Blöcken und Coins, die Funktionsweise ihrer Blockchain sowie ihre Geschäftsidee voneinander. Ihr Wert ist relativ volatil und wird durch Angebot und Nachfrage bestimmt. Es existiert eine vordefinierte Frequenz für die Schaffung neuer Blöcke bzw. Geldeinheiten.

Jede Kryptowährung läuft auf einem Computernetzwerk. Sie wird wie Aktien durch ein Symbol gekennzeichnet, das Ticker genannt wird, und in der Regel aus drei Buchstaben besteht (z.B. LTC für Litecoin). Eine Kryptowährung ist immer an ein Zahlungssystem angeschlossen, das es ermöglicht, Transaktionen durchzuführen. Diese Transaktionen finden zwischen zwei Entitäten (z.B. zwei Personen) statt, ohne dass es eines Zwischenhändlers (z.B. einer Bank) bedarf. Kryptowährungen unterliegen einem Protokoll, das den Rhythmus und die Regeln für die Erstellung der neuen Blöcke sowie die Zuweisung der Geldeinheiten (Coins oder Token genannt) festlegt.

Der englische Begriff „Crypto Asset“ wird Ihnen regelmäßig als Bezeichnung für Kryptowährungen begegnen. Dieser Begriff ist sinnvoll und sollte mehr und mehr verwendet werden, weil dadurch Kryptowährungen eine größere Dimension verliehen wird. Denn die meisten Kryptowährungen wollen nicht nur eine Währung sein, sondern gleichzeitig einen finanziellen Vermögenswert darstellen. Dieser Vermögenswert soll den Wert des emittierenden Unternehmens, ihres Vorhabens und ihrer Aussichten, wie bei einer Aktie, widerspiegeln. Außerdem können Kryptowährungen ein Werkzeug sein, um einen Dienst wie ein Computernetzwerk zu verwenden oder um Smart Contracts auszuführen. Im weiteren Verlauf dieses Buches werde ich der Einfachheit halber weiterhin den Begriff „Kryptowährung“ verwenden.

Zusammenfassung

- Kryptowährungen sind dematerialisierte Währungen, deren Betrieb in der Regel dezentral ist und auf asymmetrischer Kryptographie beruht.
- Sie brauchen keinen Staat oder irgendeine zentrale Kontrollinstanz, um kreiert zu werden bzw. zu funktionieren; sie werden momentan von keinem bedeutenden Staat als legales Zahlungsmittel anerkannt.
- Ihr Wert wird lediglich durch Angebot und Nachfrage auf besonderen Märkten, die Exchanges genannt werden, bestimmt.
- Sie erfüllen die Funktionen einer Währung und sind immer an ein Zahlungssystem angeschlossen.

2.2 Der Bitcoin

2.2.1 Kleine Geschichte

Wie wir es bereits gesehen haben, sind Kryptowährungen Währungen, die immer ein Zahlungssystem bieten, das Transaktionen zwischen zwei Public Adresses (Kontonummern) der Währung ermöglicht. Der Bitcoin ist die erste und bekannteste Kryptowährung. Er weist die mit Abstand größte Marktkapitalisierung auf, d.h. er stellt alleine mehr als die Hälfte der Marktkapitalisierung des gesamten Kryptowährungsmarktes dar (Stand: Oktober 2018). Der Bitcoin führte das Prinzip der Peer-to-Peer-Zahlung ohne zentralisiertes Kontrollsystem, d.h. ohne Bank bzw. Bankkonto, ein. Aber auch die Blockchain-Technologie und der Konsensalgorithmus „Proof-of-Work“, zu dem wir in einem späteren

Teil des Buches kommen werden und der von vielen Kryptowährungen übernommen wurde, sind auf Bitcoin zurückzuführen. Ursprünglich wollte der Bitcoin eine digitale Währung (digital cash) mit einem schnellen, kostengünstigen, effizienten, anonymen, dezentralen sowie flexiblen Zahlungssystem sein; er hat mittlerweile auch eine neue Berufung gefunden, nämlich als sogenannter „Marketmaker".

Der Bitcoin wurde Ende 2008 von einer Person, einer Gruppe von Menschen oder einer Entität namens „Satoshi Nakamoto" geschaffen. Selbst wenn es viele Gerüchte über die wahre Identität von diesem Satoshi Nakamoto gibt, weiß niemand oder kaum jemand, wer hinter diesem geheimnisvollen Namen steckt, ob es eine oder mehrere Personen sind, ob sie noch lebt usw. Der Erfolg des Bitcoins und der Kryptowährungen im Allgemeinen in Japan ist vielleicht auf die Tatsache zurückzuführen, dass Satoshi Nakamoto typisch japanisch klingt. Wir wissen allerdings, dass Satoshi Nakamoto die ersten Bitcoins fast zwei Jahre lang selber gemined hat und ungefähr eine Million davon besitzt; er ist also ein sehr reicher Mann. Die Aktivität des Bitcoin Wallets von Satoshi Nakamoto wird von vielen Menschen verfolgt. Es wird angeblich weiterhin mit Bitcoins gefüttert, aber es kommen keine heraus.

2.2.2 Die Vorteile des Bitcoins

Der Erfolg des Bitcoins ist teilweise darauf zurückzuführen, dass es die erste Kryptowährung ist, die die Technologie der Blockchain und das Konzept der Kryptowährung überhaupt hervorgebracht hat. Heutzutage ist Bitcoin die Kryptowährung schlechthin: Alle anderen Kryptowährungen (auch Altcoins genannt) sind in Bitcoins notiert. Auch Sie werden einmal Bitcoins besitzen, wenn Sie beispielsweise traden wollen. Bitcoins sind somit das Tor zum Kryptowährungshandel. Alle Investoren schauen sich den Kurs des Bitcoins an; er ist also die Währung, die den Markttrend bestimmt. Schließlich ist Bitcoin die Kryptowährung, die heute am häufigsten von Online- und Offline-Händlern angenommen wird. Vielleicht haben Sie auch schon einmal Bitcoin-Geldmaschinen, vor allem in Asien und Nordamerika, gesehen. Wenn Sie mittels eines Geldscheines oder Ihrer Kreditkarte einen gewissen Betrag einzahlen, erhalten Sie einen privaten Schlüssel, der Ihnen Zugriff auf den entsprechenden Betrag in Bitcoins ermöglicht. Die drei Probleme dieses Systems sind, dass die Geldmaschine selber den Tauschkurs zwischen Euro und Bitcoin bestimmt, dass sie sich theoretisch den privaten Schlüssel merken könnte und dass die umgewandelten Bitcoins deswegen umgehend an eine andere Public Address gesendet werden müssen.

Durch den „Proof-of-Work" wird immer wieder ein Konsens auf der Blockchain des Bitcoins erreicht oder anders gesagt: Die Realität dieser Blockchain wird in regelmäßigen Abständen (durchschnittlich jede zehn Minuten) bestimmt und von allen Teilen des Netzwerkes als richtig anerkannt, was riesige Investitionen in Hardware und einen enormen Stromverbrauch verursacht. Bitcoin wird u.a. aus diesem Grund stark kritisiert. Ende 2018 wird schätzungsweise genauso viel Strom verbraucht, um Bitcoin zu schürfen, wie in Dänemark (mit ungefähr sechs Millionen Einwohnern) verbraucht wird. Dieser Verbrauch hat eine schnell steigende Tendenz, denn je mehr in Computerhardware investiert und somit Strom verbraucht wird, desto wahrscheinlicher erhalten Miner Bitcoins für ihren Systembeitrag, den Sie durch das „Mining" leisten.

2.2.3 Die Grenzen des Bitcoin-Systems

Wie wir noch sehen werden, ist der Bitcoin keine Währung, die im täglichen Leben verwendet wird bzw. ist er noch weit davon entfernt. Dafür liegen verschiedene Gründen vor:

- Momentan kann er noch in keinem Land als legales Zahlungsmittel benutzt werden, sondern wird nur geduldet. In Berlin akzeptieren mehrere Kneipen und in Japan viele Geschäfte Bitcoins als Zahlungsmittel.
- Das Bitcoin-System ist nicht besonders benutzerfreundlich und verursacht einen enormen Stromverbrauch wegen des PoW-Konsensalgorithmus.
- Es dauert manchmal mehrere Minuten, bis eine Transaktion abgeschlossen ist. Ende 2017 belief sich die Wartezeit sogar auf mehr als zehn Minuten.
- Die Transaktionskosten sind relativ hoch.
- Zentrale Systeme wie Banken, Kreditkarten oder Paypal sind immer noch die Norm. Sie bieten effektive Schutz- und Widerspruchssysteme sowie praktische und angenehme Schnittstellen. Außerdem verfügen sie über Mittel für Innovationen und sind damit den dezentralisierten Systemen wie Bitcoin einen Schritt voraus.
- Unternehmen und Händler brauchen Zeit, Motivationshebel und einen rechtlichen Rahmen, um das System zu verstehen und anzunehmen.

Darüber hinaus sind Bitcoins im Vergleich zu anderen Kryptowährungen:

- ziemlich teuer aufgrund hoher Transaktionskosten, sodass er nicht für Produkte oder Dienstleistungen des Alltags verwendet werden kann,
- ziemlich langsam, da die Anzahl der Transaktionen auf etwa 7 pro Sekunde begrenzt ist, was natürlich nicht reicht, um aus Bitcoins ein weit verbreitetes Zahlungssystem zu machen,
- schlecht skalierbar, d.h. die Anzahl der Transaktionen und die Größe der Blöcke sind begrenzt und die Bitcoin-Community hat nicht vor, dies in naher Zukunft zu ändern,
- nicht automatisch anonym, vor allem nicht, wenn Sie Ihre Bitcoins in einem Exchange Wallet lagern.

Die Beschränkungen des Bitcoin-Systems sind jedoch ein Segen für andere Währungen, die Lösungen bieten und einen Teil der Defekte dieses Systems korrigieren. Litecoin oder Zcash bieten z.B. schnelle Transaktionen zu einem sehr günstigen Preis und wollen an der Stelle von Bitcoin die Rolle des weltweiten „Digital Cash“ spielen. Der Hauptvorteil der Kryptowährung Monero ist die Anonymität der Transaktionen. Wir werden später noch sehen, dass das Hauptziel der meisten Kryptowährungen nicht darin besteht, lediglich eine Währung zu sein. Viele Kryptowährungen sind innovativ in ihren Projekten, der Funktionsweise ihrer Blockchain, ihrem Konsensalgorithmus und dem Grad der Dezentralisierung.

2.2.4 Ist Bitcoin eine anonyme Währung?

Im Gegensatz zu dem, was man in den Medien manchmal lesen kann, ist der Bitcoin nicht automatisch anonym. Es würde sonst keinen Sinn ergeben, dass viele Kryptowährungen die Anonymität als Angebotsmittelpunkt wählen. Jeder kann den Verlauf jeder Bitcoin-Transaktion verfolgen (z.B. auf blockchain.info), wenn eine Transaction-ID (TxID) oder Public Address vorhanden sind; dann kann man Daten wie die Menge der ausgetauschten Bitcoins, die Public Address von Absender und Empfänger, den Zeitpunkt der Transaktion und einige andere technische Informationen erhalten.

Wenn Sie allerdings herausfinden, dass eine Public Address einen gewissen Betrag von Bitcoins (oder einer anderen Währung) mit einer anderen Public Address getauscht hat, wird Ihnen das nicht viel nutzen, wenn Sie nicht wissen, wer sich hinter den Adressen verbirgt. Aus diesem Grund ist die Identifizierung der Inhaber von Public Addresses unerlässlich, um die Rückverfolgbarkeit von Bitcoin-Transaktionen zu gewährleisten. In diesem Bereich spielen die Exchanges eine wesentliche Rolle, da sie von ihren Mitgliedern verlangen können, dass sie sich identifizieren, um ein Konto zu eröffnen. Die bedeutendsten Exchanges wie Kraken oder Coinbase verlangen bereits eine Identifizierung durch das KYC-Verfahren (KYC steht für „Know your customer“). Zusammenfassend kann man sagen, dass Kryptowährungen außer der anonymen Kryptowährungen (siehe „Die Coin-Familien“) eine transparente Funktionsweise haben, da alle Transaktionen auf einer bestimmten Blockchain jedem zur Verfügung stehen. Wichtige Kryptowährungen sind also auch nur solange anonym, bis man herausgefunden hat, wer der Inhaber einer gewissen Public Address ist. Diese Information wird vom Wallet verwaltet, sei es ein Exchange Wallet, ein Desktop Wallet oder ein Hardware Wallet. Privatleute können nicht einfach bei einem Exchange erfragen, wer die Adresse xyz besitzt, eine Behörde könnte dies schon eher.

2.2.5 Das Lightning-Network

Das Lightning-Network ist ein Zahlungsprotokoll, das parallel zu einer Blockchain auf einer zweiten Ebene abläuft und den Nutzern somit bei Transaktionen die Sicherheit und Effizienz der Blockchain bietet, ohne diese zu belasten. Es ermöglicht durch eine Treuhandvereinbarung sofortige Transaktionen zwischen Teilnehmern und wird als potenzielle Lösung für das Problem der Skalierbarkeit des Bitcoin-Netzwerkes präsentiert. Tatsächlich ist das Lightning-Network ein Peer-to-Peer-System, das es Nutzern ermöglicht, kleine Beträge in Kryptowährungen über ein Netz von bilateralen Zahlungskanälen zu überweisen, ohne dieses Geld dem Netzwerk anvertrauen zu müssen. Zwei Teilnehmer, die sich nicht kennen, können einen sicheren Geldtransfer durchführen, indem sie ihr Vertrauen in das System setzen. Das Lightning-Network wird derzeit auf der Bitcoin-Blockchain getestet und scheint seine Versprechen zu halten. Mitte Mai 2018 waren ungefähr 1000 Teilnehmer und ungefähr 15 Bitcoins auf diesem parallelen Netzwerk aktiv. Wenn das System funktioniert, könnten es sich schnell andere Kryptowährungen zunutze machen.

2.2.6 Warum ist Bitcoin bei weitem die wichtigste Kryptowährung?

Der Bitcoin unterscheidet sich in mehreren Punkten, die von Maximalisten (Bitcoin-Anhänger) und professionellen Anlegern sehr geschätzt werden, wesentlich von anderen Kryptowährungen:

- Der Bitcoin bietet ein sehr zuverlässiges digitales Währungssystem, aus drei Hauptgründen. Die extrem hohe Zuverlässigkeit dieses Systems stammt einerseits daher, dass der Bitcoin dank des PoW-Algorithmus und des derzeitigen Kurses technisch sehr schwierig aufgebaut und schwer zu produzieren ist (siehe „Warum wird so viel Energie verbraucht?“). Es ist außerdem ein zuverlässiges monetäres System, weil die Entwicklung der Geldmenge zu 100 % vorhersehbar ist: Es besteht daher kein Risiko von Manipulation, Quantative Easing oder ungezügelter Inflation, wie es in Ländern wie Venezuela oder Zimbabwe regelmäßig zu beobachten ist. Aus diesem Grund meinen einige Beobachter, dass Kryptowährungen am meisten Chancen haben, sich als Zahlungsmittel in Ländern durchzusetzen, deren Währung keine globale Bedeutung hat, wie in den zwei hier erwähnten Ländern oder im Iran beispielsweise. Eine Fiatwährung wird durch eine Zentralbank verwaltet, die souverän über Nacht entscheiden kann, die Währung aus geopolitischen oder wirtschaftlichen Gründen anzupassen. Es ist außerdem ein zuverlässiges System, weil niemand mehr Bitcoins erstellen kann, als es im System vorgesehen ist (zurzeit 12,5 jede zehn Minuten), was zur Folge hätte, dass diejenigen, die ich besitze, an Wert verlieren würden. Andererseits kann auch niemand die Schaffung neuer Bitcoins abstellen und dadurch den Wert wie im Falle einiger Edelsteine künstlich erhöhen. Falls die Zuverlässigkeit des Bitcoins in Frage gestellt wäre, würde sein Kurs sofort um fast 100 % sinken. Aktuell beträgt der Bitcoin-Markt um die 100 Milliarden Euro (dies ist aber eine Hochrechnung!).
- Bitcoin ist die einzige (Krypto-)Währung, die wirklich dezentralisiert ist: Es besteht keine identifizierbare Einheit hinter Bitcoin, seitdem Satoshi Nakamoto sich 2011 in Luft aufgelöst hat, sodass Bitcoin nicht „angegriffen“ oder „zerstört“ werden kann. Bitcoin braucht keine spezielle Person, um zu funktionieren, und niemand kann den Bitcoin manipulieren, um reicher zu werden oder einer anderen Partei zu schaden. Der Bitcoin wird also von niemandem verwaltet, und es ist die einzige Währung dieser Welt, die so etwas kann. Infolgedessen kann niemand eine gültige Transaktion blockieren oder annullieren, und vergangene Transaktionen sind unveränderlich. Sogar bei Ethereum, der zweitwichtigsten Kryptowährung, wurde die Blockchain nach dem DAO-Skandal 2016 verändert, um Betrugsopfer zu entschädigen und die Blockchain wieder „sauber“ zu machen. Über anderen Währungen hängt daher ein Manipulationsverdacht, obwohl scheinbar keiner stattgefunden hat. Manipulationen sind einerseits möglich aufgrund des derzeitigen Mangels an Regulierung und andererseits, weil all diese Währungen von einem identifizierbaren Team gesteuert werden, das eines Tages beschließen könnte, die Sachen in eine bestimmte Richtung zu lenken, die für sie von Vorteil wäre.
- Der Bitcoin beruht auf verschiedenen kryptographischen Verfahren, die allen bekannt sind und sich über die Jahre als sehr solide und stabil erwiesen haben, da seine Blockchain von keinem Ausfall und keinem Hacking betroffen war. Darüber hinaus ist der