

Patrick Rosenberger

Bitcoin und Blockchain

Vom Scheitern einer Ideologie
und dem Erfolg einer
revolutionären Technik

SACHBUCH



Springer

Bitcoin und Blockchain

Patrick Rosenberger

Bitcoin und Blockchain

Vom Scheitern einer Ideologie
und dem Erfolg einer
revolutionären Technik

2. Auflage

 Springer

Patrick Rosenberger
Münster, Deutschland

ISBN 978-3-662-66529-9 ISBN 978-3-662-66530-5 (eBook)
<https://doi.org/10.1007/978-3-662-66530-5>

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

© Springer-Verlag GmbH Deutschland, ein Teil von Springer Nature 2018, 2023, korrigierte Publikation 2023

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.

Planung/Lektorat: David Imgrund

Springer 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

In den 80er Jahren hatte ich einen Freund, der mit einem Commodore 64 kleine Computerspiele schrieb. Es war ein 64er mit einem selbstgelöteten Reset-Button, der von seinen Fans aufgrund seines eckigen Designs auch liebevoll „Brotkasten“ genannt wurde. Viele von Ihnen werden sowohl den Computer als auch diesen Typ Freund noch kennen.

Dieser Freund tauschte mit einem anderen Freund Programmdaten mithilfe eines Geräts namens Akustik-koppler – einer Art Adapter, auf den sich die damaligen Norm-Telefonhörer aufstecken ließen. Wie der Name schon sagt, funktionierte die Übertragung der Daten mittels akustischer Signale, was zu Übertragungsfehlern führte, wenn man beispielsweise einmal laut Niesen

Die Originalversion des Buchs wurde revidiert. Ein Erratum ist verfügbar unter https://doi.org/10.1007/978-3-662-66530-5_12

musste. Zudem war die Datenübertragung für heutige Verhältnisse mit durchschnittlich 800 Bits/s extrem langsam.

Dennoch bot diese Form der Datenübertragung entscheidende Vorteile. Zum einen konnte mein Freund mit Gleichgesinnten am anderen Ende der Leitung quasi in Echtzeit Daten austauschen, zum anderen hatte er diese Daten durch den Transfer am anderen Ende der Leitung dupliziert und somit gesichert.

Wer bereits von der Blockchain gehört hat, der weiß, worauf ich hinaus will. Im Gegensatz zur normalen Datenbank punktet die Blockchain mit einer dezentralen Datenspeicherung. Um beim Beispiel meines Freundes zu bleiben, würden seine Daten nicht nur bei ihm, sondern bei all seinen Freunden hinterlegt. Das schützt nicht nur vor dem Verlust, sondern sorgt auch dafür, dass diese Daten nicht manipuliert werden können.

Dieses so simple Prinzip der externen Datenspeicherung wird in Zukunft Einzug in nahezu jeden Bereich unseres Lebens halten und unseren Alltag revolutionieren. Banken, Versicherungen, die Industrie – sie alle sind dran an dieser revolutionären Technologie. Wer sich heute für die Thematik interessiert, der darf teilhaben an einer Entwicklung, die gerade erst am Anfang steht und in der derzeit noch Standards fehlen. Niemand ahnt, welche Auswirkungen die Umstellung auf die Blockchain auf die bestehende Infrastruktur hat. Neue Geschäftsmodelle werden entstehen und die entsprechenden Berufswelten nach sich ziehen.

Lizenzmodelle und -mechaniken bei der Rechteverwertung von Songs oder eine zeilengenaue Abrechnung in der Literatur werden in Zukunft neu erfunden werden. Genauso wie individuelle Versicherungsmodelle oder Autos, die nach dem Tanken selbst bezahlen. Identitäten

können fälschungssicher und weltumspannend hinterlegt werden, was bereits als Meilenstein in der Terrorismusbekämpfung interpretiert wird.

Das bekannteste Anwendungsbeispiel für eine Blockchain-Anwendung, die Kryptowährung Bitcoin, lässt schon heute erahnen, wie digitale Währungen den Zahlungstransfer der Zukunft verändern könnten. Denn in der Theorie machen sie Banken in ihrer Kernfunktion, der Verwaltung von Geld, überflüssig. In Zukunft könnte man direkt von A nach B überweisen, also ohne eine Instanz dazwischen.

Doch die Zeit scheint noch nicht reif zu sein. Ende 2022 berichten die Medien in einer Endlosschleife über die starken Kursschwankungen der Kryptowährung, wohl unwissend darüber, dass eben diese Berichterstattung maßgeblich zu diesen Kursschwankungen beiträgt, was Bitcoin wiederum als Zahlungsmittel vollkommen unbrauchbar macht.

Noch immer unterstellt man Bitcoin, eine Währung für das Darknet zu sein und so kriminelle Aktivitäten erst möglich zu machen. Es wird bereits laut über Regulierung diskutiert. Wohin sich Bitcoin entwickeln wird, das kann derzeit wohl niemand sagen. Der Kurs könnte sich in naher Zukunft vervielfältigen oder auch auf Null fallen. Die Meinungsmacher sind in diesem Punkt in zwei Lager gespalten.

Doch in einem Punkt, da ist man sich einig: Die Blockchain wird kommen und wir stehen gerade erst am Anfang.

Patrick Rosenberger

Inhaltsverzeichnis

1	Ein revolutionäres Konzept	1
2	Vom Tausch zur digitalen Münze	5
2.1	Geld, Grundlage unserer Gesellschaft	5
2.2	Naturalgeld	6
2.3	Münzgeld	7
2.4	Papiergeld	9
2.5	Giralgeld	10
2.6	Elektronisches Geld	11
2.7	Fiatgeld	12
2.8	Kryptowährungen	13
3	Zukunftswährung Bitcoin	15
3.1	Cypherpunks	15
3.2	Vertrauen	20
3.3	Das Bitcoin-Konzept	23
3.3.1	Digital und dezentral	23
3.3.2	Bitcoins technische Basis heißt Blockchain	25

X Inhaltsverzeichnis

3.3.3	Wie entstehen Bitcoins	26
3.3.4	Preisfindung Bitcoin	29
3.4	Das digitale Portemonnaie	33
3.4.1	Bitcoin als Summe aller Transaktionen	33
3.4.2	Hardware-Wallets	34
3.4.3	Desktop-Wallets	35
3.4.4	Paper-Wallets	35
3.4.5	Mobile Wallets	36
3.4.6	Online-Wallets	36
3.5	Alternative Kryptowährungen	37
3.5.1	Bitcoin Cash – Schneller als das Original	39
3.5.2	Ethereum – Die Mutter der Smart Contracts	42
3.5.3	NEO – Chinas Antwort auf Ethereum	49
3.5.4	IOTA – Wenn Maschinen Maschinen bezahlen	51
3.5.5	Ripple – Bindeglied zwischen alt und neu	54
3.5.6	Dash – Schnell und demokratisch	58
3.5.7	SpunkChain – Sex sells	60
4	Satoshi Nakamoto	63
4.1	Einzelperson oder Gruppe?	63
4.2	Spurlos verschwunden	65
4.3	Mitstreiter gesucht	68
4.4	Die Legende von Hal Finney	70
4.4.1	Alle jagen Nakamoto	70
4.4.2	Hal Finney	71
4.4.3	Dorian Prentice Satoshi Nakamoto	73

4.4.4	Ist Hal Finney selbst Satoshi Nakamoto?	75
4.4.5	Zu guter Letzt	77
5	Bitcoins dunkle Seite	81
5.1	Bitcoin beflügelt die kriminelle Fantasie	81
5.2	Das Darknet	82
5.2.1	Deep Web vs. Darknet	82
5.2.2	Maximal anonym	83
5.2.3	Eine Spielwiese für Kriminelle	83
5.2.4	Enttarnung nahezu unmöglich	85
5.3	Silk Road	85
5.3.1	Ein Marktplatz für Gauner	85
5.3.2	Ross William Ulbricht ist Dread Pirate Roberts	88
5.3.3	Ein abschreckendes Urteil	91
5.4	Bitcoin-Börse Mt.Gox	93
5.4.1	Jed McCaleb	94
5.4.2	Die einst größte Bitcoin-Börse der Welt	96
5.4.3	Mt.Gox am Ende	97
5.5	QuadrigaCX	100
5.5.1	Kanadas erfolgreichste Kryptobörse	100
5.5.2	Alles nur Betrug	101
6	Innovationstreiber Blockchain	105
6.1	Rai - die Mutter aller Blockchains	105
6.2	Die Bitcoin-Blockchain	108
6.2.1	Die Byzantinischen Generäle	108
6.2.2	Das digitale Journal	110

6.2.3	Rätselhaftes Bitcoin-Mining	112
6.2.4	Mehr Geld für die Miner	114
6.3	So revolutionär wie einst das Internet	115
6.3.1	Willkommen im Krypto-Zeitalter	115
6.3.2	Bahnbrechende Projekte auf Blockchain-Basis	117
6.3.3	Der dezentrale Marktplatz	119
6.3.4	Der kybernetische Wald	122
7	Die Blockchain kann die Welt verändern	125
7.1	Eine Bank für die Banklosen	125
7.1.1	Menschen ohne Bank	125
7.1.2	Ein Handy wird zur Bankfiliale	128
7.1.3	Internationaler Handel dank Kryptowährungen	129
7.2	Mehr Geld für die humanitäre Hilfe	131
8	Eine Ideologie wird Wirklichkeit	137
8.1	Bitcoin hat prominente Unterstützung	137
8.2	Die Krypto-Profiteure	140
8.3	Bitcoin als Kapitalanlage	146
8.3.1	Künstliche Verknappung als Kaufanreiz	146
8.3.2	Mogelpackung Bitcoin-ETF	147
8.3.3	Bitcoin versus Gold	150
8.4	Pizza for Bitcoins	153

9	Die Zukunft ist heute	157
9.1	ICO: Crowdfunding auf Kryptobasis	157
9.2	Smart Contracts	159
9.2.1	Eigentlich schon alter Tobak	159
9.2.2	Grenzenlose Anwendungsmöglichkeiten	161
9.2.3	Die Angst vor Plagiaten	164
9.2.4	Token-Economy	165
9.2.5	Non-fungible Tokens (NFT)	167
9.2.6	Tokenisierung von Immobilien	169
9.3	Wie die Blockchain den Arbeitsmarkt verändert	175
9.3.1	Wir werden dezentral	175
9.3.2	Alte Technologien neu erfunden	177
9.3.3	Neue Berufswelten entstehen	182
9.4	Internet of Things (IoT)	183
9.5	Metaverse	186
10	Tod einer Ideologie?	189
10.1	Bitcoin verkommt zur Kapitalanlage	189
10.1.1	Auf nach Clarion	189
10.1.2	Ist die Bitcoin-Ideologie gescheitert?	190
10.1.3	Bitcoin als Weltanschauung	193
10.1.4	Warum setzt sich Bitcoin nicht durch?	195
10.1.5	Spekulationsobjekt statt Zahlungsmittel	197

XIV	Inhaltsverzeichnis	
	10.1.6	Bitcoins Probleme sind hausgemacht 198
	10.1.7	So schlimm ist Fiat doch gar nicht 199
10.2		Technische Herausforderungen 201
	10.2.1	Zu hoher Stromverbrauch 201
	10.2.2	Schlecht für die Umwelt 204
	10.2.3	Proof-of-Stake 206
	10.2.4	Theoretisch denkbar: die 51 %-Attacke 207
	10.2.5	Lightning – Fluch und Segen 208
	10.2.6	Kryptografie versus Quantencomputing 210
11	Ausblick	213
	11.1	Die Blockchain-Realität 213
	11.2	Regulierung von Kryptowährungen 216
	11.2.1	Mit der Bekanntheit kommt die Kontrolle 216
	11.2.2	Die Bundesregierung setzt auf die Blockchain 221
	11.2.3	Digitales Zentralbankgeld (CBDC) 223
	11.3	Wird Bitcoin abgelöst? 227
	11.4	Erfolg fördert Kriminalität 230
	11.5	Typische Blockchain-Branchen der Zukunft 232
	11.6	Fazit 236
	Erratum zu: Bitcoin und Blockchain	E1
	Anmerkungen	241



1

Ein revolutionäres Konzept

„Ich glaube“, so Bill Miller, legendärer amerikanischer Investor und Fondsmanager, „es gibt eine nicht zu unterschätzende Wahrscheinlichkeit, dass der Bitcoin auf null fällt. Doch an jedem Tag, an dem es nicht passiert, wird diese Wahrscheinlichkeit geringer.“¹

Es ist der 31. Oktober 2008, als eine Gruppe kryptografiebegeisterter Informatiker eine E-Mail erhält.² Unterzeichnet ist diese E-Mail von Satoshi Nakamoto – einem bis zu diesem Zeitpunkt vollkommen unbekanntem Namen, der später als Erfinder von Bitcoin und Erzeuger des sogenannten Genesis-Blocks, des ersten Blocks in der Blockchain, in die Geschichte eingehen wird. Der Zeitpunkt ist perfekt gewählt: Nach der Konkursanmeldung der Investmentbank Lehman Brothers bahnt sich gerade der Höhepunkt der Finanzkrise an. Massive

Rettungsmaßnahmen werden eingeleitet. Das gesamte Finanzsystem, dem man bereits seit Jahren misstraute, entpuppt sich nun als reine Fiktion.

In seiner E-Mail berichtet Nakamoto sachlich über ein neues elektronisches Zahlungssystem, welches vollständig auf einem dezentralen Netzwerk gleichberechtigter Rechner-zu-Rechner-Verbindungen beruht. Eine Transaktion erfordert dabei keine Moderation eines Dritten.³ Das ist beachtlich, da zu dieser Zeit nahezu jeder Geldtransfer über eine Bank erfolgt.

Mithilfe von Bitcoin, wie Nakamoto seine Währung nennt, soll es von nun an möglich sein, den Transfer einer Währungseinheit direkt von Computer zu Computer und somit von einer Person zur nächsten zu ermöglichen. Die Anwendung gleicht den Eigenschaften von Bargeld, nur eben in digitaler Form. 2008 gleicht dies noch einer Revolution.

Laut Nakamoto bietet Bitcoin seinen Nutzern das in der Geldgeschichte höchste Maß an Freiheit. Von nun an müsse man sich nicht mehr auf die bestehende Infrastruktur der Finanzinstitute verlassen, die Unterstützung von Banken bei der Transaktion von Geld ist nicht länger notwendig. Vielmehr habe der Nutzer die zur Transaktion notwendige Technologie nun selbst in der Hand – ganz einfach in Form eines Computers oder Smartphones. Erstmals hatte man nun jederzeit unlimitierten Zugriff auf sein gesamtes Vermögen.

Seit es Banken gibt, haben wir uns immer mehr an sie gewöhnt. Der Mensch ist bequem und Banken arbeiten zuverlässig. Im Laufe der Jahrzehnte haben sich Banken dermaßen tief in unsere Gesellschaft integriert, dass ein Leben ohne sie undenkbar zu sein scheint. Doch haben wir jemals versucht, nach Alternativen zu suchen? Warum sollte man etwas verändern, das gut funktioniert? Never change a running system. Banken wickeln unseren gesamten Zahlungsverkehr ab, unsere Gehälter landen auf

unseren Konten. Daueraufträge und Lastschriftmandate vereinfachen unser Leben. Doch Bitcoin gibt einen ernsthaften Anstoß, das Bewährte zu überdenken. Die Kryptowährung könnte eine echte Alternative sein.

Bitcoins technische Basis ist die Bitcoin-Blockchain. In ihr werden sämtliche Kontobewegungen dezentral gespeichert und verbucht. Die Blockchain fungiert dabei wie ein öffentlich einsehbares Grundbuch, das jedoch die Absender und Adressaten der Transaktionen hinter Kontonummern verbirgt. Mithilfe der Blockchain-Technologie ist es so möglich, ein vollkommen transparentes Ökosystem im internationalen Handel zu schaffen.

Es gibt unterschiedliche Arten von Blockchains, die verschiedene Funktionen erfüllen können. Während die Bitcoin-Blockchain in erster Linie Transaktionen speichert, können andere Blockchains zusätzlich zu den Transaktionen beispielsweise auch Dateien oder Eigentumsverhältnisse speichern. Wieder andere helfen dabei, den Weg eines Produkts vom Produzenten zum Konsumenten unverfälscht zu dokumentieren. Das bekannteste Beispiel für eine solche „Multifunktions-Blockchain“ ist die Ethereum-Blockchain. Wir lernen ihr Potential gerade erst richtig kennen.

Die bekannteste Anwendung, die auf einer Blockchain läuft, ist bis heute Bitcoin. Dabei blickt die digitale Münze längst nicht nur auf rosige Zeiten zurück. Man kennt die Geschichten über den illegalen Online-Marktplatz Silk Road, das Darknet, Waffen- und Drogenhandel, alles bezahlt mit Bitcoin. Viele haben von Mt.Gox gehört. Die ehemals größte Börse, auf der man Bitcoins handeln konnte, wickelte zeitweise den größten Teil des Welthandels von Bitcoin nahezu alleine ab. 2011 wurde die Plattform medienwirksam gehackt und zahlreiche Anleger um ihr Vermögen gebracht. Diese Geschichten wurden von den Medien dankbar ausgeschlachtet. Leider

hat Bitcoin dadurch bis heute ein ernsthaftes Akzeptanzproblem. Über die eigentliche Ideologie von Bitcoin und die dahinterliegende Technik, die Blockchain, wissen hingegen nur die wenigsten Bescheid.

Wer sich mit Bitcoin beschäftigt, der kennt zudem die hohe Volatilität der Kryptowährung. Die enormen Kursschwankungen wecken das Interesse der Risikospekulanten und schrecken den normalen Nutzer ab. Der weitaus größte Teil der bislang erzeugten Bitcoins wird derzeit als Spekulationsobjekt gehortet, statt als Zahlungsmittel eingesetzt zu werden. Kryptowährungen sind im Mainstream ankommen. Mehr und mehr Anleger springen auf den Zug auf und spekulieren darauf, ihre Investition durch einen langfristig steigenden Kurs zu versilbern.

Inzwischen steht längst fest, dass sich Bitcoin nicht als Zahlungsmittel etablieren konnte. Zu starr scheint das technische Korsett, das die Kryptowährung mit zunehmender Nutzung immer leistungshungriger und träger werden lässt. Niemand weiß, ob der Kurs der Kryptowährung fällt oder steigt oder Bitcoin irgendwann vollständig vom Markt verschwindet. Denn es sind viele Einflüsse, die Bitcoin zu schaffen machen: In erster Linie ein Mangel an Akzeptanz, sein nach wie vor schlechter Ruf als Zahlungsmittel und dazu weltweite und uneinheitliche Regulierungen. All das lässt Bitcoins Kritiker ein schnelles Ende der digitalen Münzen prophezeien. Immer mehr sogenannte Altcoins, alternative digitale Währungen, wollen vom Hype profitieren und schießen bis heute wie Pilze aus dem Boden. Auch zahlreiche Zentralbanken arbeiten fieberhaft an digitalen Währungen. Werden sie Bitcoin eines Tages den Rang ablaufen?



2

Vom Tausch zur digitalen Münze

2.1 Geld, Grundlage unserer Gesellschaft

Vor einigen Tausend Jahren betrieben die Menschen Handel durch den Tausch von Waren oder Dienstleistungen. So wurde beispielsweise eine Kuh gegen Werkzeug getauscht, Kleidung gegen Reis oder auch eine Dienstleistung gegen einen entsprechenden Gegenwert. Doch was tun, wenn der, der die Kuh veräußern möchte, zum Zeitpunkt des Tauschs gar kein Werkzeug benötigt, da er bereits vollständig mit Werkzeug ausgestattet ist? Die Suche nach geeigneten Tauschpartnern stellte sich im Laufe der Geschichte als zu aufwendig und nicht praktikabel heraus. Ein Zwischentauschgut musste her, mit dessen Hilfe der Kaufprozess in zwei getrennte Vorgänge

zerlegt werden konnte. Das Prinzip von Kauf und Verkauf war geboren. Heute stellen die sogenannten arbeitsteiligen Wirtschaftsprozesse eine der Grundlagen unserer Gesellschaft dar und sind ohne Geld kaum mehr denkbar.

Seit es Geld gibt, gilt es als der Prototyp von Macht. Viel Geld führt zu Reichtum, Reichtum zu Macht. Geld war im Laufe der Geschichte Anlass für zahllose Kriege, hat unzählige Menschenleben gekostet und über alle Epochen hinweg Begehrlichkeiten geweckt. Gleichwohl ist Geld eine der wichtigsten Errungenschaften in der Geschichte der Menschheit.

In erster Linie aber ist Geld als Tauschmittel zu verstehen. Der Austausch von Gütern wird durch Geld vereinfacht. Dadurch, dass man diese nicht direkt gegeneinander tauscht, sondern Geld als Zwischentauschmittel verwendet, können Kauf und Verkauf auch zeitlich auseinanderliegen. Der Wert eines Gutes kann so festgehalten werden. Man spricht von der Wertaufbewahrungsfunktion von Geld. Generell aber schafft Geld erst die Möglichkeit, die unterschiedlichsten Güter und Dienstleistungen in ihrem Wert vergleichbar zu machen. Geld dient so also auch als Recheneinheit bzw. Wertmaßstab. Dabei spielt es keine Rolle, um welche Art von Geld es sich handelt. Ob Geld in Form von Banknoten und Münzen, digital auf dem Smartphone oder als Buchgeld auf dem Bankkonto – entscheidend ist, dass Geld von den Beteiligten als Zahlungsmittel akzeptiert wird.

2.2 Naturalgeld

Doch zunächst wieder einen Schritt zurück. Als Zwischentauschgüter etablierten sich im 6. Jahrtausend vor Christus eher nützliche Alltagsgegenstände wie Muscheln, Pfeilspitzen, Perlen, Felle oder auch Salz und Kakaobohnen.

Das Naturalgeld war geboren. Wichtig war, dass es leicht zu transportieren und zu zählen war. Überdies musste sein Gegenwert anerkannt sein, was in unterschiedlichen Regionen zur Herausforderung werden konnte. Zum Beispiel war das Angebot an Muscheln in Küstennähe naturgemäß höher als im Landesinneren. Ebenso verhielt es sich mit Salz, während der Kakaobohne eine Wertsteigerung in die umgekehrte Richtung bescheinigt werden konnte. In vielen Kulturen wurden auch Ziegen, Schafe oder Rinder als Tauschgut verwendet. Sie dienten gleichzeitig auch als Preisauszeichnung. So wurden militärische Ausrüstungsgegenstände wie eine Ritterrüstung bis ins Mittelalter gegen eine definierte Anzahl an Nutztieren getauscht.

Das Gesetz von Angebot und Nachfrage fand hier also bereits Anwendung. Ein Gesetz, das auch bei Bitcoin zum Tragen kommt, doch dazu später mehr. Als eine der ersten Formen von Naturalgeld, das sich überregional verbreitet hat, gilt die Kaurischnecke (auch Porzellanschnecke genannt). Das sehr harte und dadurch langlebige Schneckengehäuse kam in weiten Teilen Afrikas und Asiens über 3000 Jahre lang zum Einsatz und gilt daher bis heute als eines der erfolgreichsten und langlebigsten Zahlungsmittel der Welt. Schnecken und Muscheln brachten der Welt übrigens auch das erste Falschgeld. Statt der echten Muscheln brachten Fälscher aufwendig nachgemachte Exemplare aus Knochen oder sogar Steinen in den Umlauf.

2.3 Münzgeld

Den Durchbruch brachte die Erfindung der Waage. Sie schuf erst die Grundlage für die Entstehung der Münze, denn mit ihrer Hilfe konnten die damaligen Zwischentauschgüter vereinheitlicht werden. Die Münzen, deren

Wert zunächst exakt ihrem Materialwert entsprach, bestanden damals meist aus Elektron (auch Elektrum genannt), einer recht leicht zu gewinnenden Gold-/Silber-Legierung. Große und damit schwere Münzen waren seinerzeit also mehr wert als kleine, leichte Münzen. Im Gegensatz zum Naturalgeld waren Metallmünzen zudem praktischer, da sie sich aufgrund ihrer nahezu identischen Größe einfacher aufbewahren, zählen oder stapeln ließen.

Im 6. Jahrhundert vor Christus versah man Münzen erstmals mit einer Prägung. Die Prägung machte den Wert der Münze erst eindeutig und stellte gleichzeitig eine Art Echtheitszertifikat dar. Die neue Bezahlkultur breitete sich rasch über Asien und Europa aus, bis die ersten Herrscher der Antike begannen, ihre Konterfeis auf Münzen zu prägen. Eine frühzeitliche Form der Selbstvermarktung. Der prominenteste Vertreter der damaligen Münzprägung war sicherlich der Lyder-König Krösos (auch Kroisos genannt), der als einer der Ersten einheitliche Münzen mit Stier und Löwe prägte und dessen Name bis heute sinnbildlich für Reichtum und Wohlstand steht. Die Erfindung des Münzgeldes verhalf den Lydern so zu enormem wirtschaftlichen Aufschwung. In diesem Zusammenhang entstanden auch die ersten Handelsplätze. Wer etwas zu verkaufen hatte, der bot seine Waren auf dem Markt an und musste nicht mehr mühsam nach Abnehmern suchen.

Erst später bemerkte man, dass nicht das Gewicht einer Münze ausschlaggebend für deren Wert ist, sondern vielmehr ihre reine Anzahl und die Nachfrage danach. Dieses Prinzip, das eigentlich bereits vom Naturalgeld bekannt war, bei dem Muscheln in Küstennähe weniger wert waren als im Inland, wurde nun auf die Münzen übertragen. Eine definierte Menge sollte von nun an ihren Wert bestimmen. Auch die digitale Münze Bitcoin hat eine

per Skript definierte Menge von maximal 21 Mio. Stück. Auch ihr Wert steigt durch Angebot und Nachfrage.

Der oftmals umgangssprachlich verwendete Begriff „Moneten“ stammt übrigens von den Römern. Diese prägten ihre Münzen im Tempel der Göttin Juno, die den Beinamen „Moneta“ trug.

2.4 Papiergeld

Es sollte einige Jahrhunderte dauern, bis die Chinesen im 10. Jahrhundert die schweren Münzen gegen Papiergeld tauschten. Münzen waren aufgrund ihres hohen Gewichts im Alltag einfach unhandlich geworden. Als frühe Form des Papiergelds gilt dabei der Depotschein. Ihn erhielt man, wenn man Münzen an offizieller Stelle abgab und diese gegen eben diesen Schein tauschte. Da Depotscheine nicht personalisiert waren, konnten sie untereinander oder gegen Waren oder Dienstleistungen getauscht werden.

Noch länger trugen die Europäer ihre Münzen bei sich. Sie erkannten erst im 15. Jahrhundert die Vorteile des Papiergelds. Streng genommen mussten sie ihn erkennen, denn ihnen gingen im Laufe der Zeit die Münzen aus. Als Behelf versah man einen Zettel mit Wert und Siegel und funktionierte diesen so ganz einfach zu Papiergeld um.

Im Laufe der Zeit setzte sich das Papiergeld schließlich in ganz Europa durch und wurde nun auch von offizieller Stelle gedruckt. Doch trotz der praktischen Vorteile hatte Papiergeld ein Akzeptanzproblem. Denn die Herstellungskosten von Papiergeld waren deutlich geringer als der Wert der Münzen, die man dafür kaufen konnte. Banken mussten Überzeugungsarbeit leisten und glaubhaft versichern, für jede Papiernote den Gegenwert in Münzen bereit zu halten. Skeptiker sollten jederzeit auf das altbewährte Münzgeld wechseln können. Papiergeld stellt

im Grunde bis heute nichts anderes dar als das schriftliche Versprechen, den angegebenen Wert auch tatsächlich zu zahlen. Schaut man sich die englische Pfundnote einmal genauer an, so findet man auf ihr auch heute noch den Hinweis:

„I promise to pay the bearer on demand the sum of one pound.“ Zu Deutsch: „Ich verspreche, dem Überbringer auf Verlangen die Summe von einem Pfund zu zahlen.“

Erst die Bank of England schaffte es schließlich, Papiergeld dauerhaft in den Köpfen der Gesellschaft zu verankern. Sie erklärte 1833 Banknoten in der Form, wie wir sie noch heute kennen, zu einem offiziellen Zahlungsmittel. Die Einführung der Banknote gilt bis heute als Wegbereiter der schnell wachsenden Industrialisierung. Münzen wurden von nun an zu Kleingeld degradiert.

2.5 Giralgeld

Später waren auch Scheine und Münzen nicht mehr zeitgemäß. Stapelweise Geld für größere Investitionen zu organisieren, wurde auf Dauer einfach zu unpraktisch. Abhilfe schaffte das sogenannte Giralgeld, auch Buchgeld genannt. Geld, das keines ist – im physischen Sinne. Ab dem 14. Jahrhundert schufen Banken zunächst die Möglichkeit, Geld, ganz gleich, ob Scheine oder Münzgeld, auf einem Konto einzuzahlen und zu einem beliebigen Zeitpunkt wieder abzuholen. Die Verzinsung wurde erfunden, um die Einzahlung attraktiver zu machen und so den Banken die Möglichkeit zu verschaffen, mit größeren Geldmengen zu arbeiten. Im 19. Jahrhundert ersetzten Konten, Überweisungen sowie später auch Schecks zunehmend Münzen und Scheine und machten

eine neue Form der Wert-Transaktion attraktiv – den bargeldlosen Zahlungsverkehr. In der Nachkriegszeit gewann das Konto immer mehr an Bedeutung und ersetzte schließlich sogar die bis dahin übliche Gehaltsauszahlung per Lohntüte. Auch laufende Kosten für Wasser oder Gas wurden fortan per Überweisung ausgeglichen. Übrigens ist Giralgeld bis heute kein gesetzliches Zahlungsmittel, sondern lediglich der Auszahlungsanspruch eines Kontoinhabers gegenüber seinem Kreditinstitut. Die Zahlungsmethode wird aber von nahezu allen seriösen Unternehmen in Form von Überweisungen akzeptiert.

2.6 Elektronisches Geld

Mit der Digitalisierung im 20. Jahrhundert wurden die handschriftlichen Transaktionen schließlich elektronisch. Der Scheck, einst mit viel Mühe ausgefüllt und unterschrieben, musste der Elektronik ebenso weichen wie das Überweisungsformular. Die neuen Player am Markt hießen EC-, Kredit- oder Geldkarte. Mit der Verbreitung des Internets folgten schließlich das E-Payment und das Onlinebanking. Über Handy-Klingeltöne und -Logos hielt auch das Mobile Payment Einzug in die Wohn- und Kinderzimmer unserer Gesellschaft. Die Erfindung des Smartphones gilt als Durchbruch der Micro- und Macropayments, da es zumeist für den Transfer von geringen Beträgen genutzt wird. Gezahlt wird per App. Die Bedeutung von Bargeld nimmt seitdem von Jahr zu Jahr ab.

2.7 Fiatgeld

Fiatgeld ist eigentlich genau das, was die meisten Menschen heute als „Geld“ bezeichnen, dabei ist es eigentlich eine spezielle Kategorie von Geld. Als Fiatgeld oder Fiatwahrung bezeichnet man namlich Geld, das von den Zentralbanken in Form von Giralgeld oder Bargeld ausgegeben und als einziges gesetzliches Zahlungsmittel in den entsprechenden Wahrungsraumen akzeptiert wird. Die prominentesten Beispiele fur Fiatgeld sind der Euro, der US-Dollar oder der Yen. Fiatwahrungen sind bereits zu einer Zeit entstanden, als Munzen noch aus wertvollen Rohstoffen wie Gold oder Silber gepragt wurden und ihr Wert dem Gewicht ihres Materials entsprach. Heute hat Fiatgeld keinen entsprechenden Gegenwert mehr. Vielmehr bemisst sich der Wert am Vertrauen zum Herausgeber der Wahrung, also den Regierungen und Zentralbanken, und dem Verhaltnis von Angebot und Nachfrage. Der Wert beruht insofern ausschlielich auf Basis einer gesellschaftlichen Ubereinkunft. Verlieren die Menschen das Vertrauen in diese Wahrung, geht sie sogleich dorthin zuruck, woraus sie erzeugt wurde – ins Nichts. Fiatwahrungen haben fur sich betrachtet also keinen inneren (intrinsischen) Wert, so wie ihn Handelswahrungen wie beispielsweise Gold haben.

Eine der groten Starken von Fiatwahrungen ist zugleich auch ihre Schwache: Die Regierung eines Landes hat die volle Kontrolle uber die im Umlauf befindliche Menge der Fiatwahrung und reguliert damit ihren Wert. Dies setzt eine auerst verantwortungsvolle Geldpolitik und Regulierung der Regierung voraus. Eine schlechte Geldpolitik kann im schlimmsten Fall zur Hyperinflation einer Fiat-Wahrung fuhren, bei der Menschen ihr Geld

möglichst schnell ausgeben, um einer Geldentwertung zuvorzukommen.^{4,5}

2.8 Kryptowährungen

Der Begriff „Kryptowährung“ hat schon etwas Mystisches. Höchste Zeit, das komplexe Thema einmal zu entmystifizieren. Das Kofferwort aus „Kryptografie“, der Wissenschaft der Verschlüsselung von Informationen, und „Währung“ soll letztlich nichts anderes suggerieren, als dass zur Erschaffung der Währung das Prinzip der Verschlüsselung angewandt wird. Alle Kryptowährungen haben gemeinsam, dass sie von Menschen statt Institutionen hergestellt und verwaltet werden können. Außerdem beruhen sie in nahezu allen Fällen auf einem dezentralen System zur Verwaltung der digitalen Münzen.

Streng genommen sind Kryptowährungen keine Währungen, sondern digitale Werte, die getauscht und gehandelt werden können. Im Gegensatz zu Fiatwährungen sind Kryptowährungen jedoch weitgehend unreguliert. Sie werden bislang kaum durch staatliche Institutionen oder Regierungen kontrolliert, sondern durch das Netzwerk ihrer Nutzer demokratisiert (siehe Abschn. 11.2).

Die Mutter aller Kryptowährungen ist Bitcoin. Die Wortkomposition aus „Bit“, der Maßeinheit einer Datenmenge, und „Coin“, englisch für Münze, wurde bereits 2009 zum ersten Mal gehandelt. Seitdem wurden noch mehrere Tausend andere digitale Währungen entwickelt. Tendenz steigend. Sie alle wollen schneller, anonymer oder energiesparender als ihre Wettbewerber sein. Nahezu alle der sogenannten Altcoins (Alternate Coins) werben mit einer Verbesserung des Konzepts, einzigartigen Merkmalen oder Anwendungsbereichen. Manche versuchen ernst-

haft, die Idee weiterzuentwickeln, andere wollen nur den schwindelerregenden Höhenflug des Bitcoin-Kurses reproduzieren, ohne eigene Substanz einzubringen. Dabei sehen sich die meisten der Kryptowährungen selbst gar nicht als Währung. Die Begrifflichkeit führt hier in die Irre. Vielmehr dienen diese der Finanzierung eines Unternehmens oder stellen eine Unternehmensbeteiligung ähnlich einer Aktie dar. Nur die wenigsten von ihnen treten wirklich an, um Fiatwährungen zu ersetzen oder zu ergänzen.

Kryptowährungen werden über Kryptobörsen gehandelt. Das sind Plattformen, die je nach Größe einige wenige bis Hunderte Währungspaare für den Handel zur Verfügung stellen. Man kann dort Kryptowährungen gegen Fiatwährungen oder umgekehrt oder auch Kryptowährungen gegen andere Kryptowährungen tauschen. Diese Kryptobörsen verdienen ihr Geld mit jeder Transaktion, für die sie Gebühren erheben. Ironischerweise sind nahezu alle dieser Börsen vollständig zentralisiert. Obwohl Kryptowährungen theoretisch direkt von A nach B transferiert werden können, findet ihr Handel in der Praxis fast ausschließlich über zentralisierte Kryptobörsen, also einer dritten Instanz, statt.

An Kryptobörsen können Kryptowährungen rund um die Uhr und sieben Tage in der Woche gehandelt werden. An Börsen können Aktien oder Rohstoffe dagegen nur zu den üblichen Handelszeiten gekauft oder verkauft werden. Dieser Wettbewerbsvorteil von Kryptobörsen gegenüber Börsen ist so groß, dass die Handelszentren derzeit sogar darüber nachdenken, ob börsengehandelte Wertpapiere zukünftig auch außerhalb der Handelszeiten gehandelt werden sollen.