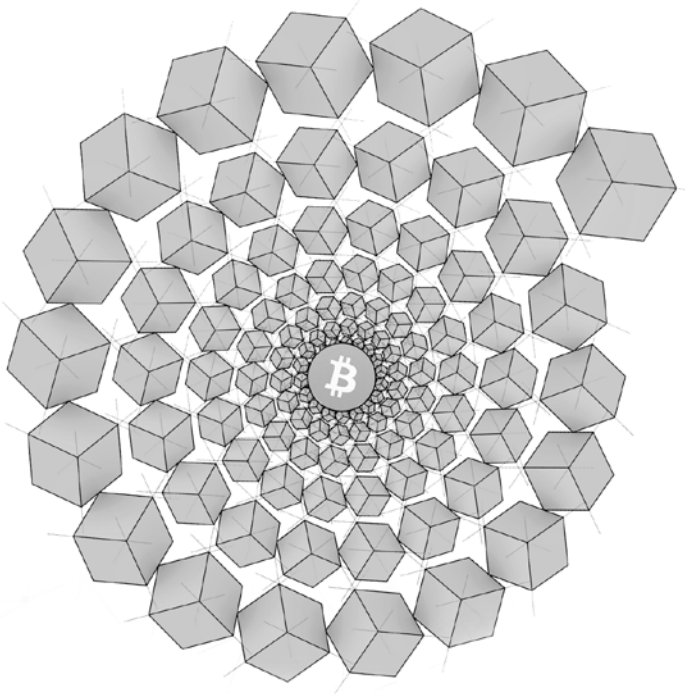
AARON KOENIG

DIE DEZENTRALE REVOLUTION

Wie Bitcoin und Blockchain-Technologie Wirtschaft und Gesellschaft verändern



FBV

Vorwort
von Andreas M. Antonopoulos

Als ich zum ersten Mal etwas über Bitcoin las, nahm ich es nicht weiter ernst. Ich hielt es für eine Art digitalen Jeton einer Website für Glücksspiele. Bitcoin zunächst ablehnend gegenüberzustehen war nicht besonders originell. Fast jeder, den ich kenne, zeigte anfangs die gleiche Reaktion. Als ich zum zweiten Mal auf Bitcoin stieß, irgendwann im Jahr 2012, fand ich auch einen Link zum *Whitepaper* von Satoshi Nakamoto und ich entschied mich, es zu lesen. An diesem Morgen änderte sich mein Leben für immer. Fast vier Monate lang ohne Unterbrechung, 16 bis 18 Stunden am Tag, verschlang ich alles, was es über Bitcoin zu lesen gab. Ich war mehr als nur besessen davon – es war für mich eine technologische *Epiphanie*.

Dieses aus dem Griechischen stammende Wort beschreibt einen Moment der plötzlichen Offenbarung, in dem man eine ganz neue Realität erkennt. Ich erinnere mich an mein erstes derartiges Offenbarungserlebnis, als ich mit elf Jahren meinen ersten Computer bekam. Damals verabschiedete ich mich von der Welt, völlig vertieft in die neuen Möglichkeiten, die sich mir dadurch auftaten. Zwischen meinem ersten Computer und Bitcoin hatte ich noch vier weitere solcher Epiphanie-Momente: mein

erstes Modem, den ersten Zugang zum Internet, die erste Website und das Linux-Betriebssystem. Jedes Mal erlebte ich eine Erweiterung der Realität. Jenseits der offensichtlichen Anwendungsfälle erkannte ich, dass diese Technologien die Welt verändern würden, und ich verlangte, dass die anderen mir zuhörten. Sie taten es natürlich nicht, denn niemand hört auf einen dummen Teenager. Aber mit der Zeit gewann ich mehr und mehr Vertrauen in meine Fähigkeit, Technologien zu erkennen, die die Welt verändern und starke Auswirkungen auf die Gesellschaft haben würden. Als ich Bitcoin für mich entdeckte, war ich nicht mehr länger bereit, die Zweifel der anderen ernst zu nehmen.

Bitcoin ist so viel mehr als nur Geld. Auf den ersten Blick kann man es als eine Form digitalen Geldes betrachten, aber entscheidend ist, wie es funktioniert. Bitcoin ermöglicht eine ganz neue Form von Vertrauensbildung. Es schafft einen Mechanismus, mit dem Menschen, ohne dass sie einander von vornherein vertrauen müssten, überall auf der Welt miteinander kooperieren können. Weil sie den Regeln folgen, die die Software vorgibt, vermögen sich all diese Leute auf eine gemeinsame Realität zu einigen, die aus dem System heraus entsteht.

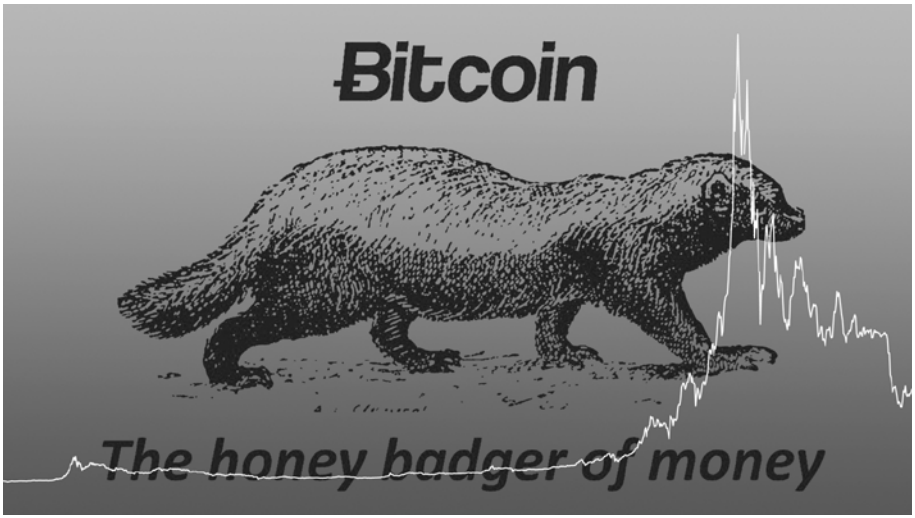
Einfache Tatsachen wie »diesem Konto gehören fünf Bitcoins« oder »von diesem Konto wurden zwei Bitcoins auf ein anderes überwiesen« können von jedem im Netzwerk gefunden und bestätigt werden. Man kann darauf vertrauen, dass alle den Regeln folgen, ohne dass es dazu

einer Autorität oder einer zentralen Kontrolle bedarf. Dieser neue Vertrauensmechanismus kann für viel mehr verwendet werden als für Zahlungen. Geld ist seine offensichtliche, mächtige und notwendige erste Anwendung. Doch darüber hinaus eröffnet sich durch Bitcoin und die Blockchain-Technologie eine ganze Welt weiterer Möglichkeiten. Als diese Erkenntnis in mir 2012 explodierte, konnte ich nicht anders, als ihr mit meiner ganzen Energie nachzugehen.

In diesem Buch über **die dezentrale Revolution** erforscht Aaron Koenig die neue Welt, die durch die Erfindung der dezentralen Vertrauensbildung möglich wird. Seine Lektüre könnte weitreichende Konsequenzen für Sie und die Menschen in Ihrer Umgebung haben. Es ist möglich, dass auch Sie eine Epiphanie erleben und die Welt nie wieder so sehen werden wie zuvor.

Andreas M. Antonopoulos ist einer der bekanntesten Bitcoin- und Blockchain-Experten. Aufgewachsen in Griechenland, hat er Computer Science in London studiert und als Experte für IT-Sicherheit in den USA gearbeitet. Er hält Vorträge in aller Welt und hat mehrere Bücher zum Thema geschrieben, darunter *Mastering Bitcoin, The Internet of Money* und *Mastering Ethereum*.

Mehr Info: **www.antonopoulos.com**



0. Einleitung

Als im September 2017 mein Buch *Cryptocoins – Investieren in digitale Währungen* erschien, erlebten Kryptowährungen gerade einen Boom. Der Bitcoin, der im Januar noch bei rund 1000 US-Dollar gestanden hatte, war zum Erscheinungstermin meines Buches auf über 4000 US-Dollar gestiegen. Bis zum 16. Dezember schnellte sein Kurs auf fast 20.000 US-Dollar hoch. Andere Cryptocoins wiesen sogar noch höhere Zuwachsraten auf. Doch im Jahr 2018 stürzten die Kurse auf breiter Front ab, der Bitcoin fiel auf knapp über 3000 US-Dollar. Während ich diese Zeilen schreibe (im April 2019), liegt der Bitcoin-Kurs bei rund 5000 US-Dollar. Wer im Dezember 2017 auf dem Höhepunkt des Hypes bei Bitcoin eingestiegen ist, hat somit eine Menge Geld verloren. Haben wir es hier also mit einer Blase zu tun? Keineswegs.

Ich beschäftige mich seit Mai 2011 mit dem Thema Bitcoin. Seitdem habe ich bereits vier solcher Hype-Zyklen

erlebt. Jedes Mal schnellte der Kurs in kurzer Zeit in ungeahnte Höhen, um dann wieder abzustürzen – allerdings auf ein deutlich höheres Niveau als vor dem Hype. Heftige Auf- und Abwärtsbewegungen sind bei einem so neuen Phänomen wie Kryptowährungen wohl nicht zu vermeiden. Ihr Handelsvolumen ist noch klein, jeder größere Kauf und Verkauf beeinflusst den Kurs sehr viel mehr als bei etablierten Anlageformen.

Auch die Psychologie spielt eine wichtige Rolle. Die meisten Menschen wissen bisher nur wenig über Bitcoin und die Blockchain-Technologie. Manche hören, dass man damit schnell Geld verdienen kann, und investieren, ohne sich ausreichend mit der Materie beschäftigt zu haben. Umso größer ist dann ihre Panik, wenn die Kurse fallen. Die Medien schrieben immer wieder vom »Ende des Bitcoins« – ob er von 30 auf 2 US-Dollar, von 200 auf 50 US-Dollar oder von 1000 auf 200 US-Dollar fiel. Die Website 99bitcoins.com zählte im April 2019 in der Rubrik »Bitcoin Obituaries« 351 Bitcoin-»Todesmeldungen«, davon allein 93 im Jahr 2018.[1]

Der Bitcoin-Preis 2011–2019 in logarithmischer Darstellung.

Doch Bitcoin, der »Honigdachs des Geldes«, hat sich stets als so zäh und hartnäckig erwiesen wie sein Maskottchen aus Afrika, das sich mutig mit Löwen anlegt und selbst Bisse von Giftschlangen übersteht. Nach einer dramatischen Talfahrt und einer Phase des Herumdümpelns folgte bisher jeweils eine neue, noch verrücktere Bitcoin-Rallye. Es gibt natürlich keine Garantie, dass dies immer so bleibt. Als Investor in Kryptowährungen braucht man starke Nerven. Doch es geht beim Thema Bitcoin um sehr viel mehr als um Spekulation. Davon handelt dieses Buch.

0.1 Technik, die die Welt verbessert

Bitcoin und die Blockchain-Technologie sind angetreten, die Welt zu verändern. Sie geben Milliarden von Menschen, die bisher über kein Bankkonto und keine Kreditkarte verfügen, Zugang zur weltweiten Wirtschaft. Sie ermöglichen direkte Zahlungen von Mensch zu Mensch, ohne dass man Mittelsmännern wie Banken oder Kreditkartenfirmen vertrauen müsste. Sie brechen die Macht der Regierungen, die Bürger durch Inflation, künstliche Niedrigzinsen und eingefrorene Bankkonten ihres Eigentums zu berauben.

Die Blockchain-Technologie kann jedoch nicht nur für digitale Bargeldsysteme wie Bitcoin genutzt werden, sondern für viele weitere Anwendungsfälle. Immer dann, wenn viele Menschen, die sich nicht kennen, einen

Konsens erreichen wollen, kann sie zum Einsatz kommen. Viele Dienstleistungen, die bisher von zentralen Autoritäten angeboten werden, lassen sich dezentral in der Blockchain abbilden – zum Beispiel Grundbücher, Personen- oder Firmenregister. Der große Vorteil: Man muss keine Macht an jemanden delegieren, der sie missbrauchen könnte.

Das Grundprinzip, auf dem Kryptowährungen und Blockchain-Technologie beruhen, ist die Dezentralität. In einem dezentralen Netzwerk gibt es keine zentralen Server. Jeder Computer kann Sender und Empfänger zugleich sein. Ein dezentrales Netzwerk ist daher wesentlich weniger anfällig für Zensur und Hackerangriffe, denn man müsste in sehr viele seiner Knotenpunkte eindringen, um es zu manipulieren oder abzuschalten. Doch es sind nicht allein technische Gründe, die für die Dezentralisierung sprechen. Die Vordenker der dezentralen Revolution wollen eine wirklich freie Gesellschaft ohne Machthaber und zentrale Autoritäten schaffen, in der freiwillige Vereinbarungen Hierarchien und Machtstrukturen ersetzen.

0.2 Die Kryptoserie

Schon in meinen Büchern *Bitcoin – Geld ohne Staat* (2015) und *Cryptocoins* (2017) habe ich mich mit der Dezentralisierung beschäftigt, wenn auch eher am Rande. Doch es gibt heute so viele spannende Entwicklungen, dass ich diesem Thema ein eigenes Buch widmen möchte. Es baut

auf meinen beiden vorigen Büchern auf. *Bitcoin – Geld ohne Staat* bietet einen allgemeinen Einstieg ins Thema Bitcoin und nutzt dabei die Erkenntnisse der Wiener Schule der Volkswirtschaft. Es geht vor allem um die Frage: Warum brauchen wir Bitcoin? *Cryptocoins* gibt einen Überblick über die verschiedenen Typen von Kryptowährungen. Es enthält viele praktische Tipps zum Umgang mit ihnen, etwa zur sicheren Speicherung, zum Handel und zur Vermeidung von Betrügereien. Dieses dritte Buch der Serie widmet sich nun ganz den möglichen Konsequenzen, die Bitcoin und die Blockchain-Technologie für unsere Wirtschaft und Gesellschaft haben.

In **Kapitel 1** und **2** gebe ich eine grundsätzliche Einführung in Kryptowährungen und beschreibe mögliche Einsatzgebiete der Blockchain-Technologie. In den **Kapiteln 3, 4 und 5** stelle ich Phänomene wie digitale Tokens, DApps (Dezentrale Anwendungsprogramme), DAOs (Dezentrale Autonome Organisationen) und ICOs (Initial Crypto Offerings) vor. In **Kapitel 6** geht es um die Dezentralisierung des Internets, das heutzutage von wenigen Großunternehmen beherrscht wird. Die **Kapitel 7** und **8** handeln von neuen Formen des menschlichen Zusammenlebens, die erst durch dezentrale Technologie möglich werden: Demokratie auf Blockchain-Basis, freie Privatstädte, »digitale Nationen« und andere scheinbar utopische Konzepte. **Kapitel 9** fasst die hoffentlich bei der Lektüre des Buches gewonnenen Einsichten zusammen und gibt einen Ausblick in die Zukunft.

0.3 Was bringt mir dieses Buch?

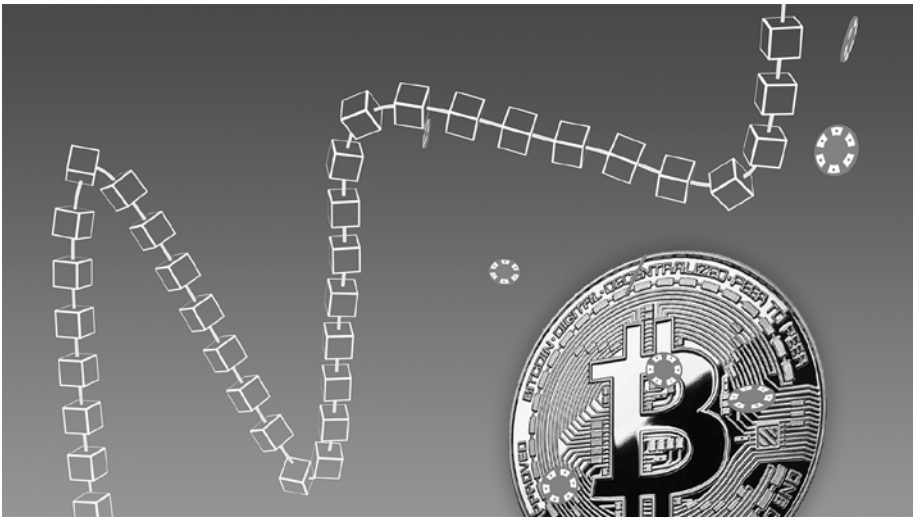
Sie fragen sich jetzt vielleicht, welchen konkreten Nutzen Sie persönlich aus diesem Buch ziehen können. Es ist sehr viel gesellschaftskritischer und politischer als meine ersten beiden, eher praxisnahen Bücher. Ich persönlich finde diese Dimension von Kryptowährungen am allerwichtigsten. Wer in ihnen lediglich ein Mittel sieht, um schnell viel Geld zu verdienen, verpasst das Wesentliche.

Doch selbst wenn Ihnen neue Gesellschaftsentwürfe egal sind und Sie sich für Cryptocoins vor allem als Geldanlage interessieren, werden Sie in diesem Buch nützliche Informationen finden. Denn auch die »Weltverbesserungsprojekte« der späteren Kapitel werden in der Regel von auf Gewinnmaximierung ausgerichteten Unternehmen betrieben. Ich halte es für durchaus möglich, dass sich ein aus heutiger Sicht utopisch wirkendes Projekt als hervorragende Geldanlage entpuppt. Wer hätte Anfang der 1970er-Jahre, als das Internet noch ein reines Forschungsprojekt des US-Militärs war, daran gedacht, durch Investitionen in Internetfirmen reich zu werden? Wer hätte Ende 2011, als der Bitcoin nach seinem ersten Höhenflug von 30 US-Dollar auf 2 US-Dollar abgestürzt war, jemals mit Kursen von mehreren Tausend US-Dollar gerechnet?

Die derzeitige Situation der Kryptowelt erinnert mich sehr an die Stimmung nach dem Platzen der Dotcom-Blase

Anfang der 2000er-Jahre. Damals wandten sich viele kurzfristig denkende Investoren enttäuscht vom Internet ab. Doch genau in dieser Zeit sind die Unternehmen groß geworden, die heute das Netz dominieren, wie Google, Facebook oder Amazon. Wer in schwierigen Zeiten investiert, in denen die Kurse am Boden sind, kann sehr viel mehr gewinnen, als derjenige, der bei steigenden Kursen auf den Zug aufspringt.

Es lohnt sich, bei Geldanlagen langfristig zu denken, radikale Veränderungen wahrzunehmen und rechtzeitig darauf zu setzen. Insofern ist dies nicht nur ein Buch für libertäre Revoluzzer. Es kann auch für den nüchtern kalkulierenden Investor interessant sein.



1. Bausteine einer neuen Welt
Was Sie zum Einstieg wissen sollten

Bevor wir tiefer ins eigentliche Thema einsteigen, wollen wir zunächst ein paar Grundbegriffe klären. Wenn Sie meine Bücher *Bitcoin – Geld ohne Staat* und *Cryptocoins* gelesen haben, können Sie diesen Teil getrost überspringen. Wenn Ihnen diese Einführung hingegen zu knapp ist, kann ich Ihnen die beiden ebenfalls beim FinanzBuch Verlag in München erschienenen Bücher durchaus empfehlen.

1.1 Was ist Bitcoin?

Bitcoin ist ein weltweites digitales Zahlungssystem, das ohne Banken und sonstige Mittelsmänner auskommt. Jeder kann an diesem dezentralen Netzwerk teilnehmen. Alles, was man dafür benötigt, ist eine frei verfügbare

Software, die *Wallet* heißt (siehe 1.3). Die digitale Währung, die man braucht, um dieses Zahlungssystem nutzen zu können, wird ebenfalls Bitcoin genannt. Ihre Gesamtmenge ist auf 21 Millionen begrenzt. Sie ist also im Gegensatz zu staatlichen Währungen wie Euro oder US-Dollar bewusst knapp gehalten. Darin ähnelt sie klassischen Geldarten wie Gold oder Silber.

Das Bitcoin-Konzept wurde 2008 von einem gewissen Satoshi Nakamoto veröffentlicht. Niemand weiß, wer sich hinter diesem Pseudonym verbirgt. Höchstwahrscheinlich steckt nicht eine Einzelperson, sondern eine Gruppe von Entwicklern dahinter. Am 3. Januar 2009 brachte das Satoshi-Nakamoto-Team die ersten Bitcoins in Umlauf. In den ersten Jahren fand es nur wenig Aufmerksamkeit für seine Arbeit. Nachdem sich allmählich eine Community von Software-Entwicklern gebildet hatte, zog sich »Satoshi« Ende 2010 überraschend aus dem Projekt zurück. Seitdem wird die Bitcoin-Software von einem weltweit verteilten Team freier Programmierer weiterentwickelt.

Die Grundidee bei Bitcoin ist, dass man keinen zentralen Autoritäten mehr vertrauen muss. Bitcoin-Anhänger misstrauen Zentralbanken oder Regierungen, die in der Vergangenheit immer wieder das Geld der Bürger durch Hyperinflationen und Währungsreformen entwertet haben. Bitcoin ersetzt alle bisher nötigen Mittelsmänner wie Banken und Kreditkartenfirmen durch Software, die auf Kryptographie beruht. Deshalb werden Bitcoin

und alle anderen Währungen, die nach ähnlichen Prinzipien funktionieren, unter den Begriffen *Kryptowährungen* oder *Cryptocoins* zusammengefasst.

1.2 Was sind öffentlicher und privater Schlüssel?

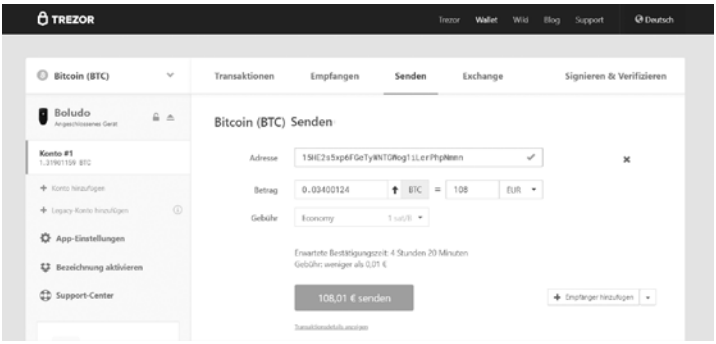
Bitcoin setzt Verschlüsselungstechnologie ein, um Eigentum nachzuweisen oder zu übertragen. Man benötigt dafür digitale Schlüsselpaare, die jeweils aus einem öffentlichen und einem privaten Schlüssel bestehen. Die *Wallet* genannte Software (siehe 1.3) kann unendlich viele solcher Schlüsselpaare erzeugen. Den öffentlichen Schlüssel, oder genauer, die daraus erzeugte Bitcoin-Adresse, braucht man, um jemandem Bitcoins zu schicken oder selbst welche zu erhalten. Eine Bitcoin-Adresse funktioniert gewissermaßen wie eine Kontonummer, mit dem Unterschied, dass man nicht eine Nummer, sondern unendlich viele davon hat. Man kann sie bedenkenlos über das Internet schicken, denn man kann damit nichts weiter tun, als jemandem Geld zu überweisen.

Ganz anders sieht es mit dem dazugehörigen privaten Schlüssel aus. Den braucht man, um an sein Geld heranzukommen und es auszugeben. Man sollte ihn daher auf keinen Fall jemand anderem verraten. Der private Schlüssel sollte mindestens so geheim bleiben wie der PIN-Code der eigenen Bankkarte. Auch private Schlüssel werden von der Wallet automatisch und in

unbegrenzter Zahl erzeugt. Sehr wichtig: Vertrauen Sie Ihre privaten Schlüssel niemals einem internetbasierten Dienst an! Speichern Sie sie nur auf Geräten, die Ihnen gehören, entweder auf Ihrem eigenen Computer oder Handy – oder noch besser: auf einer sogenannten Hardware Wallet (siehe 1.3), die größtmögliche Sicherheit vor Hackern bietet.

1.3 Die digitale Brieftasche

Die kostenlose Wallet-Software, die man zur Nutzung von Bitcoin und anderen Cryptocoins benötigt, kann man sich einfach auf seinen Computer oder sein Handy herunterladen. Man muss dafür keinen Antrag stellen und braucht von niemandem eine Erlaubnis. Bitcoin-Wallets gibt es für alle gängigen Betriebssysteme, wie etwa Windows, Mac, Linux, iOS oder Android. Andere Kryptowährungen bieten in der Regel eigene Wallets an. Es gibt außerdem sogenannte Multi-Wallets wie beispielsweise Jaxx, Coinomi oder Exodus, mit denen sich unterschiedliche Coins verwalten lassen. Zusätzlich empfiehlt sich die Anschaffung einer Hardware Wallet wie Trezor, Ledger oder Keepkey. Das sind kleine Geräte, die man an den USB-Port seines Computers anschließt und auf denen die privaten Schlüssel (siehe 1.2) so gespeichert werden, dass Hacker sie nicht stehlen können.



Geld senden per Bitcoin-Wallet

Die wichtigsten Funktionen einer Wallet sind das Empfangen und Verschicken digitaler Währungen. Dafür werden digitale Adressen verwendet, die aus vielen Zahlen sowie Klein- und Großbuchstaben bestehen und bei Bitcoin zum Beispiel so aussehen: 15HE2s5xp6FGeTyWNTGWog1iLerPhpNmmn. Sie werden aus dem öffentlichen Schlüssel (siehe 1.2) erzeugt und beginnen bei Bitcoin mit einer 1 oder einer 3. Man kann sich die Adresse auch in Form eines QR-Codes anzeigen lassen, den man per Handy einscannt – wie man es mittlerweile von Fahrkarten und Flugtickets kennt.

Jeder Nutzer kann über unendlich viele solcher Adressen verfügen. Wenn man jemandem Geld schicken möchte, benötigt man dafür lediglich dessen digitale Adresse. Die gibt man zusammen mit dem zu schickenden Betrag in das entsprechende Feld der Wallet ein. Wenn der Empfänger an das Geld herankommen möchte, benötigt er den zu dieser Adresse passenden privaten Schlüssel, der ebenfalls aus vielen Zahlen und Buchstaben besteht.

Der Umgang mit den langen kryptographischen Adressen mag zunächst etwas abschreckend wirken. Man muss jedoch nichts von dieser komplizierten Form der Mathematik verstehen, um Bitcoins zu benutzen. Oder haben Sie schon einmal etwas vom SMTP-Protokoll gehört? Wahrscheinlich nicht, und doch benutzen Sie es jedes Mal, wenn Sie eine E-Mail verschicken.

Ähnlich ist es bei Bitcoin. Ihre Wallet nimmt Ihnen den Umgang mit den Schlüsseln weitestgehend ab. Zudem arbeiten mehrere Unternehmen daran, die kryptischen Adressen durch Benutzernamen zu ersetzen, die für Menschen leichter verständlich sind.

1.4 Mit Bitcoin bezahlen

Man kann zwar bereits in mehreren Hunderttausend Onlineshops und in ein paar Tausend Geschäften in der realen Welt mit Bitcoins zahlen, doch von einer breiten Akzeptanz ist der Bitcoin noch weit entfernt. Ein Grund dafür: Die Zahl der technisch möglichen Transaktionen des Bitcoin-Netzwerks liegt zurzeit nur bei etwa fünf pro Sekunde – deutlich weniger als die mehreren Tausend Zahlungsvorgänge pro Sekunde, die Kreditkartenunternehmen wie *Visa* oder *Mastercard* abwickeln können. Durch diese technische Limitierung und das starke Wachstum der Anzahl der Bitcoin-Überweisungen ist