IN DIESEM KAPITEL

- Die Geschichte der digitalen Währungen entdecken
- Mehr über die Anfänge von Bitcoin und seinen Urheber erfahren
- Verstehen, was Geld (und Bitcoin) ist und was nicht
- Die Vorteile von Bitcoin ergründen

Kapitel 1
Bitcoin in aller Kürze

Für einen Teenager hat das Bitcoin-Netzwerk zweifellos bereits einen großen Einfluss auf die Welt genommen. Allein im Jahr 2021 fanden Transaktionen im Wert von über 12,4 Milliarden US-Dollar statt. Während wir diese Zeilen schreiben, beträgt die *Marktkapitalisierung* (der Gesamtwert) von Bitcoin 918.705.395.133, also fast eine Billion US-Dollar. (Die Marktkapitalisierung entspricht der Gesamtzahl der im Umlauf befindlichen Bitcoins multipliziert mit dem aktuellen Marktpreis eines einzelnen Bitcoins.)

Aber das ist ein momentaner Tiefstand; nur wenige Wochen zuvor betrug der Gesamtwert noch fast 1,3 Billionen Dollar. Wenn Sie dies lesen, kann der Wert höher, niedriger oder gleich sein. Das ist eine der Besonderheiten von Bitcoin: Sein Marktpreis kann sehr volatil sein. Das werden Sie bald auch selbst feststellen, wenn Sie etwas Zeit mit der Beobachtung der Märkte verbringen.

Aber der Einfluss, von dem wir hier sprechen, bezieht sich nicht nur auf den aktuellen Bitcoin-Preis. Tatsächlich ist die Marktkapitalisierung von Apple über dreimal so groß wie die des Bitcoin-Netzwerks. Trotzdem könnte gerade jetzt ein Vergleich mit Apple angebracht sein. Abbildung 1.1 zeigt, wie viele Bitcoins notwendig gewesen wäre, um im Zeitraum von 2010 bis 2021 eine einzelne Aktie von Apple zu kaufen. Der Wert eines einzelnen Bitcoins ist im Verhältnis zur Apple-Aktie gestiegen (wie natürlich auch im Verhältnis zum US-Dollar und zu anderen staatlichen Währungen).

Der Start des Bitcoin-Netzwerks löste eine wahre Blockchain- und Kryptowährungsrevolution aus. Inzwischen gibt es über 13.000 verschiedene Kryptowährungen. (Achtung, die meisten davon sind im Wesentlichen wertlos und werden es auch bleiben!) Zum gegenwärtigen Zeitpunkt haben die fünf wichtigsten Kryptowährungen zusammen eine Marktkapitalisierung von knapp 1,7 Billionen Dollar, und eine Reihe von Kryptowährungen bieten

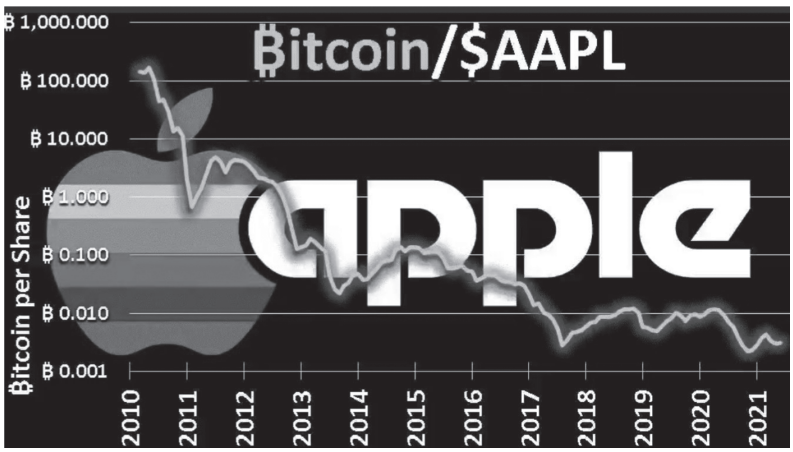

Abbildung 1.1: Was kostet eine Apple-Aktie in Bitcoins?

nützliche Funktionen, die über die reine Nutzung als Geld oder Wertaufbewahrungsmittel hinausgehen. Wahrscheinlich werden einige dieser Kryptowährungen überleben, auch wenn dies auf die meisten nicht zutreffen wird.

Aber wir wollen hier ja über Bitcoin sprechen, also fangen wir mit ein wenig Geschichte an. Woher kommt der Bitcoin und wie entwickelte er sich?

Am Anfang waren … digitale Währungen?

Blockchainbasierte Kryptowährungen sind ziemlich neu, aber digitale, für den Einsatz im Internet konzipierte Währungen, gibt es schon eine ganze Weile. (Zerbrechen Sie sich über das Thema *Blockchain* erst einmal nicht den Kopf; wir erklären das detaillierter in Kapitel 2 und ohne Sie dabei zu überfordern. Vorerst genügt es zu verstehen, dass eine Blockchain eine besondere Art von Datenbank ist, ein Speicherungssystem für digitale Daten).

Als die Menschen in immer größerer Zahl das Internet benutzten – diese Entwicklung begann in den frühen 1980er-Jahren, nahm aber erst 1994 mit dem Aufkommen des kommerziellen Internets richtig Fahrt auf – wurde klar, dass sie eine Möglichkeit brauchten, um im Cyberspace Geld auszugeben (die ersten Onlineshops wurden in diesem Jahr eröffnet). Natürlich werden heute die meisten Onlinetransaktionen über Kredit- und Debitkarten abgewickelt – auch PayPal und Venmo setzen im Wesentlichen (neben Banküberweisungen) auf solche Transaktionen –, aber das war in der Anfangszeit nicht der Fall. Viele Leute fürchteten den Diebstahl ihrer Kreditkartendaten und scheuten sich daher, die Nummern online zu verwenden. (Als Mitautor Peter 1997 einen Onlineshop eröffnete, verfügte er zwar über ein funktionierendes Zahlungssystem für Kreditkarten, aber viele Kundinnen und Kunden druckten sich lieber einen Bestellschein auf Papier aus und schickten einen Scheck mit der Post!)

Dann gab es da noch das Problem der *Mikrotransaktionen*. In der digitalen Welt sollte es natürlich auch möglich sein, jemandem beispielsweise fünf oder zehn Cent für etwas zu bezahlen, etwa für den Zugang zu einem Video oder Artikel. Diese Aufgabenstellung

ist immer noch nicht gelöst (obwohl man argumentieren könnte, dass das in Kapitel 4 besprochene Bitcoin Lightning Network dies fast geschafft hat). Nichtsdestotrotz ist dies einer der Gedanken, die die Entwicklung digitaler Währungen vorangetrieben haben.

Und sie entwickelten sich tatsächlich: 1983 schrieb David Chaum ein wissenschaftliches Paper über das Konzept einer digitalen Währung (*Blind Signatures for Untraceable Payments*), in dem er den Einsatz von Kryptografie zur Erstellung und Verwaltung einer digitalen Währung vorschlug. Schon damals spielte die Kryptografie eine Rolle bei digitalen Währungen, auch wenn diese noch nicht als Kryptowährungen bezeichnet wurden. Wenn heute von Kryptowährungen die Rede ist, bezieht sich dies in der Regel auf die neue Generation der Blockchainbasierten Kryptowährungen, die ihren Ursprung in Bitcoins haben. (Mehr über Kryptografie und ihre Bedeutung für Kryptowährungen erfahren Sie in Kapitel 2.)

Chaum brachte 1990 mit *DigiCash* tatsächlich eine digitale, auf Kryptografie basierende Währung auf den Markt, aber das war damals wirklich alles noch sehr am Anfang. 1990 waren nur sehr wenig Menschen online, und die Währung starb um das Jahr 1998 herum aus. Was den digitalen Währungen Ende der 1990er Jahre schadete, war vermutlich die Tatsache, dass die Kreditkartenunternehmen ein Stück vom Onlinegeschäft abhaben wollten und daher alles daran setzten, den Verbrauchern die Angst vor dem Kreditkarteneinsatz im Internet zu nehmen.

Trotzdem tauchten noch andere digitale Währungen auf. Es gab E-Gold, eine Währung, die durch echtes Gold gedeckt war, und Millicent, die von einem großen Computerunternehmen, der Digital Equipment Corporation (DEC), entwickelt wurde. (Wenn Sie jünger als, sagen wir, Mitte dreißig, werden Sie sich wahrscheinlich nicht mehr an DEC erinnern, aber das war damals ein großes Ding. Sogar IBM hatte damals eine Micropaymentsabteilung, die sich mit digitalen Währungen beschäftigte).

Dann gab es noch NetBill, ein Projekt der Carnegie Mellon University, das später in einem weiteren System, CyberCash, aufging, welches wiederum in den Fängen von PayPal landete. Es gab Beenz, das zwischenzeitlich eine Partnerschaft mit MasterCard einging, First Virtual, CyberCoin, Flooz (von Whoopi Goldberg beworben!) und diverse andere.

Aber es konnte sich nichts wirklich *durchsetzen*. Es gab viele tolle Ideen, aber niemand konnte alles richtig *umsetzen*. Anfang der 2000er-Jahre gingen die meisten dieser Unternehmungen zugrunde (wahrscheinlich ausgelöst durch den Dotcom-Crash vom Jahresende 2000). Es gab aber auch Ausnahmen. Liberty Reserve mit Sitz in Costa Rica war von 2006 bis 2013 in Betrieb, wurde aber nach Geldwäschevorwürfen in Milliardenhöhe aufgelöst. Und geschlossene Systeme zur Nutzung in bestimmten Netzwerken, wie etwa die chinesischen QQ Coins, werden überwiegend über den QQ-Messaging-Dienst von Tencent genutzt.

Aber dann kam Satoshi Nakamoto mit seiner oder ihrer magischen Blockchain.

Die Geburtsstunde von Bitcoin

Am 1. November 2008 postete eine Person (oder Gruppe) namens Satoshi Nakamoto eine Nachricht mit dem Titel *Bitcoin P2P e-cash paper* (archiviert unter `https://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html`) in einem Kryptografieforum. In dieser Nachricht kündigte Nakamoto an, dass er oder sie »an einem neuen

elektronischen Bargeldsystem arbeitet, dessen Nutzer ausschließlich in direktem Kontakt zueinanderstehen, ohne dabei eine Drittpartei einzuschalten, der man vertrauen müsste«.

Mit anderen Worten: Nakamoto schuf ein Währungssystem, das auf einem Peer-to-Peer-Netzwerk beruhte, also auf gleichberechtigt zusammengeschalteten Computern. Da dieses ohne zentrale Instanz auskommt, braucht es dabei auch keine Bank oder Regierung als »vertrauenswürdige Drittpartei«.

Eine Bemerkung in dem Beitrag verdeutlicht, worin Nakamoto das Problem mit den früheren Kryptowährungen sah: »Viele Menschen betrachten E-Währungen von vorneherein als aussichtslos, weil seit den 1990er-Jahren so viele Unternehmen damit gescheitert sind«. Für Nakamoto hatten all diese anderen digitalen Geldsysteme demnach eine gemeinsame Achillesferse oder kritische Schwäche. »Es ist doch hoffentlich klar, dass diese Systeme nur aufgrund ihrer zentralen Steuerung zum Scheitern verurteilt waren. Ich denke, hier probieren wir zum ersten Mal ein dezentrales, nicht auf Vertrauen gestütztes System aus.«

Nakamoto hatte zuvor unter `bitcoin.org` einen Domainnamen und eine einfache Website eingerichtet und dort ein Dokument veröffentlicht, in dem erklärt wurde, wie das alles funktionieren würde: `https://bitcoin.org/bitcoin.pdf`. Vielleicht möchten Sie einen kurzen Blick darauf werfen, auch wenn es zum Verständnis von Bitcoin nicht unbedingt notwendig ist (es handelt sich dabei um ziemlich technischen Kram).

Nakamotos Whitepaper beschreibt, wie eine *Blockchain* (eine besondere Form der Datenbank) zur Verwaltung der Währung eingesetzt werden könnte. Im Wesentlichen speichert die Blockchain ein Hauptbuch, also eine Aufzeichnung sämtlicher Währungstransaktionen, und da die Blockchain über zahlreiche Computer (die *Peers*) dupliziert wird und diese alle gleichberechtigt sind, ist kein Vertrauen in eine zentrale Instanz erforderlich. Sie haben vielleicht schon gehört, dass Bitcoin als ein vertrauensfreies (engl: trustless) System bezeichnet wird. Das heißt nicht, dass es nicht vertrauenswürdig ist, sondern dass dafür keine vertrauenswürdige Drittpartei intermediär erforderlich ist. Tatsächlich ist die Vertrauenswürdigkeit fest im System verankert. Die dem System zugrunde liegende Mathematik – oder Mathemagie, wie Peter sie gerne nennt – sorgt dafür, dass Bitcoin-Transaktionen auch ohne zentrale »Aufsichtsbehörde« vertraut werden kann. In Kapitel 2 erklären wir Ihnen die Gründe.)

Satoshi Nakamoto (wer auch immer er, sie oder es ist) hat die Worte *Kryptowährung, Blockchain* oder *vertrauensfrei* an keiner Stelle im Whitepaper verwendet. Das sind Begriffe, die später von anderen zur Beschreibung des Systems verwendet wurden.

Die Blockchain-Idee gab es eigentlich schon länger – mindestens seit 1991. Erinnern Sie sich noch an David Chaum, der mit DigiCash berühmt wurde? Er hatte seit den frühen 1990er-Jahren am Konzept einer Blockchain gearbeitet.

Wie auch immer, Nakamoto hat es nicht dabei belassen. Im Januar 2009 startete er/sie/es das Bitcoin-Netzwerk. Nakamoto veröffentlichte etwa dreißigtausend Codezeilen, die

die für den Betrieb dieses dezentralen Peer-to-Peer-Geldsystems Netzwerkprotokolle und Abläufe definierten. Und damit war Bitcoin geboren.

Natürlich war der Bitcoin im Januar 2009 praktisch wertlos. Dennoch enthielten der von Nakamoto erstellte *Genesis-Block* (der allererste Datenblock in der Blockchain, mit dem zugleich die ersten 50 Bitcoins entstanden), zusammen mit den nachfolgend von Nakamoto »geschürften« Datenblöcken (siehe Kapitel 7), rund eine Million Bitcoins: Zum derzeitigen Preis wären dies 47,369,000,000 US-Dollar. Ja, fast 50 Milliarden US-Dollar!

Aber wer ist Nakamoto?

Wer ist also Satoshi Nakamoto? Das weiß niemand. Na ja, irgendjemand muss es wissen, aber entweder sagt er es nicht, oder er hat niemanden überzeugen können. Tatsächlich ist nicht einmal klar, was Satoshi Nakamoto ist. Ein Mann? Eine Frau? Eine Gruppe? Eine Organisation oder Firma? Wir wissen es nicht mit Sicherheit, obwohl die meisten Annahmen darauf hinauslaufen, dass es sich um einen einzelnen Menschen oder eine Gruppe aus zwei bis drei Personen handelt. Es ist vielleicht wenig überraschend, dass am häufigsten Kryptografen und Mathematiker hinter Nakamoto vermutet werden.

Da gibt es natürlich den realen Satoshi Nakamoto – eine offensichtliche Wahl. Ein japanisch-amerikanischer Einwohner Kaliforniens, der als Satoshi Nakamoto geboren wurde und heute den Namen Dorian Prentice Satoshi Nakamoto trägt, scheint einige der erforderlichen Kompetenzen zu besitzen, um *der* Nakamoto zu sein, aber er bestreitet, der Begründer von Bitcoin zu sein.

Dann ist da Nick Szabo, ein begeisterter Anhänger digitaler Währungen, der bereits als Nakamoto gehandelt wurde, dies aber bestreitet. Auch Elon Musk wurde »bezichtigt«, aber er streitet es ab (und wir selbst glauben, dass er wahrscheinlich zu beschäftigt war, um Zeit dafür zu finden!). Da wären noch der japanische Mathematiker Shinichi Mochizuki (er streitet es ab), der finnischen Wirtschaftssoziologe Dr. Vili Lehdonvirta (er streitet es ab) und der irische Kryptografie-Student Michael Clear (ja, auch er bestreitet es).

Zu den lautesten Kandidaten gehört Craig Wright, ein australischer Informatiker. Er behauptet zwar, Nakamoto zu sein, wird aber von vielen Seiten beschuldigt, einen ausgeklügelten Betrug durchzuführen. Während wir diese Zeilen schreiben, hat ein Geschworenengericht Wright dazu verurteilt, dem Nachlass von David Kleiman, einem verstorbenen Freund und Kollegen, wegen Veruntreuung von Geldern aus einem gemeinsamen Unternehmen 100 Millionen US-Dollar zu zahlen. Unabhängig davon befanden die Geschworenen jedoch auch, dass David Kleiman nicht an der Entwicklung von Bitcoin beteiligt war.

Die Geschworenen haben jedoch nicht festgestellt, dass Craig Wright Nakamoto *ist* — nur, dass er, *falls* er es ist, seine 50 Milliarden Dollar nicht mit Kleimans Nachlass teilen muss. Kein schlechter Deal. Der Deal ist sogar so gut, dass Wright erklärte, er sei *erleichtert*, dass er nur 100 Millionen Dollar zahlen müsse! Der Fall ist damit jedoch noch nicht geklärt. Es ist unklar, ob Kleimans Nachlass tatsächlich an dem Joint Venture beteiligt ist, und Wright könnte auch seiner Ex-Frau 100 Millionen Dollar schulden. Das Geheimnis, ob Wright tatsächlich Nakamoto ist oder nicht, wird dadurch nicht gelüftet. Wright behauptet, die

Geschworenen hätten festgestellt, dass er Nakamoto *sei*; das haben sie nicht.) Das wird erst dann geklärt sein, wenn Wright – oder der *echte Satoshi Nakamoto* – einige der Bitcoins aus Nakamotos Blockchain-Adressen verschiebt.

Unabhängig davon funktionierte das Bitcoin-Netzwerk wie geplant weiter, auch lange nachdem Satoshi Nakamoto sich auf mysteriöse Weise aus dem Netzwerk ausgeklinkt hatte. Kurz zuvor hatte er verkündet, Julian Assange und Wikileaks hätten »den Stein ins Rollen gebracht«, als sie 2010 begannen, fortan Bitcoin-Spenden für ihre kontroverse Berichterstattung zu akzeptieren.

Verstehen, was Bitcoin eigentlich ist

Was also ist Bitcoin? Also, wir können Ihnen recht schnell sagen, was es nicht ist. Es ist nichts Greifbares – es gibt nichts, was Sie anfassen oder in der Hand halten können. Sie können es nicht schmecken oder riechen. Sie können es nicht einmal sehen. Tatsächlich – und das erklären wir in Kapitel 2 ausführlicher – *gibt es eigentlich gar keine Bitcoins*.

Was es allerdings gibt – und was Sie sehen können – ist der sogenannte Bitcoin-*Ledger* (noch so ein Wort, das Satoshi Nakamoto in dem berühmten Bitcoin-Whitepaper übrigens gar nicht verwendet hat, aber als das die in der Bitcoin-Blockchain gespeicherten Daten inzwischen allgemein bekannt sind). Ein Ledger oder auf Deutsch *Hauptbuch*, *Kassenbuch* oder *Register* ist die schriftliche Aufzeichnung aller Transaktionen; das kleine Kontoregister Ihres Scheckbuchs ist zum Beispiel eine Art Hauptbuch. (Für alle unter 30: Ein Scheck ist ein Stück Papier, auf das man eine Zahl schreiben, es mit seiner Unterschrift versehen und dann jemandem geben kann, der es dann bei seiner Bank einreicht, und die Bank zahlt ihm dann das Geld aus … ein erstaunlich effizientes System.) Oder denken Sie an einen Kontoauszug, der die ein- und ausgehenden Zahlungen auf Ihrem Konto ausweist. (Nur allzu oft sind es *ausgehende* Zahlungen.) Auch das ist eine Art von Hauptbuch.

Und wie hat Satoshi Nakamoto dann also die allerersten Bitcoins erschaffen? Nun, wenn wir davon sprechen, dass Bitcoins »erschaffen« wurden, dann ist das eigentlich nur eine Vereinfachung. Es wurde keine Bitcoin-*Sache* erschaffen. Als Nakamoto Bitcoin erstmals »erschuf«, erstellte er in Wirklichkeit eine Reihe von Regeln für ein Hauptbuch, in dem er die Erzeugung von Bitcoins *festhielt*. Tatsächlich steht auf der ersten Seite dieses Hauptbuchs: »Heute wurden 50 neue Bitcoins geschaffen«. Und siehe da, schon gibt es Bitcoin.

Mit der Erstellung dieses ersten »Genesis-Blocks« durch Nakamoto war das Wesen des Netzwerks mathematisch in Stein gemeißelt. Im ersten Datenblock befand sich noch ein kleiner Zusatztext, der von der Titelseite von *The Times* vom 3. Januar 2009 zitiert: »Chancellor on Brink of Second Bailout for Banks.« (Schatzkanzler steht kurz vor zweitem Bankenrettungspaket). Vielleicht war dies ein Hinweis auf Nakamotos Motivation für die Gründung des Netzwerks, als Alternative zu den seiner Meinung nach korrupten, von den Regierungen gesteuerten Geldsystemen.

Das Hauptbuch hält im Wesentlichen zwei Dinge fest. Zum einen die *Schaffung* neuer Bitcoins durch einen Prozess namens »Mining«. Nakamoto »schürfte« diese ursprünglichen 50 Bitcoins (wobei die allerersten 50 Bitcoins aufgrund der Beschaffenheit des Codes nicht ausgegeben werden können). Das Mining geht weiter, und tatsächlich werden mit jedem neuen Transaktionsblock, der an die Bitcoin-Blockchain angehängt wird (dies geschieht etwa alle

zehn Minuten), neue Bitcoins erzeugt. (In Kapitel 7 wird erklärt, wie dieser »Mining«-Prozess funktioniert.)

Das Ganze beruht jedoch auf einem mathematisch festgeschriebenen Schema: Bitcoins werden nach einem festen Zeitplan erzeugt, und etwa alle vier Jahre wird die Anzahl der alle zehn Minuten erzeugten Bitcoins (im Rahmen eines Ereignisses, das originellerweise »*Halving*« genannt wird) halbiert. Momentan entstehen alle zehn Minuten 6,25 neue Bitcoins, aber irgendwann im Jahr 2024 wird diese Zahl auf 3,125 reduziert, vier Jahre später dann erneut halbiert und so weiter (alle vier Jahre) bis etwa zum Jahr 2140, wenn schließlich die größtmögliche Anzahl von Bitcoins im Umlauf sein wird.

Die zweite Sache, die das Hauptbuch aufzeichnet, ist, was mit den Bitcoins geschieht, nachdem sie einmal erstellt wurden. Wie wir in Kapitel 2 besprechen werden, sind alle Bitcoins mit »Adressen« in der Blockchain verknüpft, und wenn Menschen Bitcoins kaufen und verkaufen oder sie verwenden, um etwas damit zu bezahlen (was im Grunde dasselbe ist wie ein Bitcoin-Verkauf), werden die Coins von einer Adresse in der Blockchain zu einer anderen geschickt. Das Bitcoin-Hauptbuch zeichnet auf, wohin die Bitcoins fließen, und zwar von Adresse zu Adresse zu Adresse. Jede Adresse wird von jemandem kontrolliert, sodass die Blockchain letztlich festhält, wem was gehört. Wenn das Bitcoin-Blockchain-Ledger sagt, dass die von Ihnen kontrollierte Adresse mit 2 Bitcoins verknüpft ist, dann haben Sie die Kontrolle über diese 2 Bitcoins. (In den Kapiteln 3 und 4 erklären wir, wie Sie diese Verfügungsgewalt ausüben können – d. h., wie Sie Ihre Bitcoins – beispielsweise im Gegenzug für staatliche Fiat-Währung oder für Waren und Dienstleistungen – an eine andere Adresse übertragen können).

Fiat-Währung?

Wenn Sie lange genug in der Bitcoin-Community unterwegs sind, werden Sie früher oder später auch den Begriff »*Fiat*-Währung« hören, und zwar meistens in abschätzigem Ton. Eine Fiat-Währung ist eine Währung, die per Dekret, per offizieller Verfügung ausgegeben wird. Eine Fiat-Währung wird von einer Regierung herausgegeben, ohne durch einen Sachwert wie etwa Gold abgesichert zu sein. (Um den Wirtschaftsnobelpreisträger Paul Krugman zu zitieren: »Fiat-Währungen liegt ein Wert zugrunde, weil Männer mit Gewehren dies behaupten«). Die meisten der heutigen Währungen sind Fiat-Währungen; der »Goldstandard« wurde in den 1930er-Jahren, während der Großen Depression, weitgehend abgeschafft. (Großbritannien schaffte ihn 1931 ab.) Der US-Dollar war ursprünglich an Silber gekoppelt, aber im Jahr 1900 wurde ein Gesetz verabschiedet, das ihn an Gold band. Die Bindung an Gold blieb fast das ganze Jahrhundert über bestehen, bis sie 1971 vollständig aufgehoben und der Dollar zu einer Fiat-Währung wurde. (Allerdings werteten die USA den Dollar bereits 1934 gegenüber Gold ab, d. h. sie verringerten das Goldgewicht pro Dollar).

Der Vorteil von Fiat-Währungen ist, dass sie den Regierungen mehr Kontrolle über die Geldmenge geben. Viele Ökonomen, wahrscheinlich die meisten, glauben, dass die Weltwirtschaftskrise durch das Festhalten am Goldstandard in die Länge gezogen wurde, weil die Regierungen nicht in der Lage waren, ihre Volkswirtschaften durch eine Ausweitung der Geldmenge zu stimulieren. Der Nachteil ist nach Ansicht vieler treuer Bitcoin-Anhänger, dass sie den Regierungen zu viel Kontrolle über die Geldmenge geben!

Wenn sich das alles jetzt ein wenig fadenscheinig anhört, ein wenig wie ein Schwindel – und es gibt mit Sicherheit genug Leute, die Ihnen sagen werden, dass Bitcoin ein Schwindel *ist* –, dann werden wir Ihnen in wenigen Augenblicken erklären, was *Geld* ist. Sie denken vielleicht, Sie wüssten das bereits, aber das tun Sie wahrscheinlich nicht, und ohne zu wissen, was Geld ist, ist es schwer zu verstehen, wie Bitcoin Geld sein *kann*. Aber erst einmal noch ein bisschen mehr über Bitcoin.

Bitcoin-Einheiten verstehen

Zunächst einmal müssen Sie sich im Klaren darüber sein, dass Bitcoins unterteilt und in Bruchteilen gekauft und verkauft werden können. Ein Bitcoin ist keine Goldmünze, die Sie im Ganzen kaufen müssen, wie zum Beispiel eine 10-Dollar-Liberty-Goldmünze (zum Preis von rund 1.000 Dollar, nebenbei bemerkt). Von dieser Münze kauft man nicht die Hälfte oder ein Viertel.

Aber bei Bitcoin, der 50.000 oder 60.000 US-Dollar oder was auch immer *pro Coin* kosten kann, könnten es sich die meisten Leute gar nicht leisten, einen kompletten Coin zu kaufen. Und es gibt ja sowieso keinen *Coin*, keine *Münze*. Es existiert nur ein Buchungseintrag im Hauptbuch.

Dieser Eintrag im Hauptbuch kann also ganz beliebig ausfallen. Er kann besagen, dass Sie einen halben Bitcoin gekauft haben, ein Zehntel, ein Hundertstel oder ein Zehntausendstel, bis hin zu einem einzigen Hundertmillionstel. Das heißt, Sie können Bruchteile eines Bitcoins erwerben. Tabelle 1.1 bietet einen kurzen Überblick über die Bitcoin-Einheiten.

Einheit	Bezeichnung
1; ein	Bitcoin, BTC, ₿
1/10; ein Zehntel	deci-Bitcoin, dBTC
1/1,000; ein Tausendstel	milli-Bitcoin, millibit
1/1,000,000; ein Millionstel	micro-Bitcoin, µBTC, bit
1/100,000,000; ein Hundertmillionstel	Satoshi, sat

Tabelle 1.1: Bitcoin-Einheiten

Die Tabelle zeigt nicht alle Einheiten, aber das sind die wichtigsten Einheiten, die Sie vermutlich einmal sehen und von denen Sie hören werden. Da Bitcoins in Satoshis unterteilt sind – hundert Millionen Satoshis pro Bitcoin –, können Sie einen Bitcoin problemlos mehrfach durch Zehn teilen: Dezi-Bitcoin, Centi-Bitcoin, Milli-Bitcoin, Micro-Bitcoin und so weiter. (Tatsächlich gibt es theoretisch sogar die Möglichkeit, einen Bitcoin unterhalb der Satoshi-Ebene noch weiter in *milliSatoshi* zu unterteilen. Dies funktioniert über ein spezielles Zusatznetzwerk namens Lightning Network, das wir in Kapitel 4 besprechen).

Gibt es von der kleinsten Bitcoin-Einheit genug für alle? Lassen Sie uns einmal einen Blick darauf werfen. Es wird niemals mehr als 21 Millionen Bitcoins geben; das bedeutet, dass maximal 2.100.000.000.000.000 Satoshis im Umlauf sein können.

Heute sind jedoch rund 19 Millionen Bitcoins im Umlauf und damit etwa 1.900.000.000.000.000 Satoshis.

Bei einer Erdbevölkerung von etwa acht Milliarden Menschen sind heute rund 237.500 Satoshis pro Person im Umlauf (die Zahl schwankt; siehe die Satoshi-Uhr unter `https://satoshisperperson.com/`). Das entspricht einem heutigen Wert von etwa 110 US-Dollar.

Im Verhältnis dazu sind heute etwa 2.500 US-Dollar pro Person auf der Erde im Umlauf (»M1«-Geldmenge) (gemäß der Website der Federal Reserve unter `https://fred.stlouisfed.org/series/M1SL`). Das sind 250.000 Cent pro Person, ähnlich der Anzahl an Satoshis.

Das alles bedeutet, dass Sie keine große Geldsumme für den Einstieg in Bitcoin benötigen. Sie können kleine Teile eines Bitcoins kaufen, aber achten Sie auf die Gebühren. Der Kauf kleiner Mengen an einer normalen Börse (siehe Kapitel 3) kann teuer sein; in manchen Fällen zahlen Sie wahrscheinlich mehr an Gebühren als für den Bitcoinpreis. Einige Börsen bieten jetzt auch gebührenfreie Transaktionen an.

Kryptowährung oder Kryptovermögenswert?

Bitcoin wird gemeinhin als Kryptowährung bezeichnet. Aber ist es wirklich eine Währung? Wir sind anderer Meinung. In Kapitel 3 gehen wir näher darauf ein, aber zumindest im Moment können Sie sich Bitcoin eher als Vermögenswert denn als Währung vorstellen. Es ist mehr Gold als Geldschein. Es ist schwer, Bitcoin auszugeben, genau wie es schwer ist, Gold auszugeben. Natürlich geht das, aber es ist nicht immer einfach, und die meisten Einrichtungen, wo Sie vielleicht Ihre Bitcoins ausgeben möchten, akzeptieren sie nicht.

Und warum sollten Sie Ihre Bitcoins überhaupt ausgeben wollen, wenn sie sich in den nächsten Monaten verdoppeln oder verdreifachen könnten? Nein, Bitcoin ist keine echte Währung, auch wenn er ursprünglich als solche gedacht war (und vielleicht in Zukunft auch eine werden wird).

Google und das Oxford-Wörterbuch beschreiben *Währung* als »ein Geldsystem, das in einem bestimmten Land in allgemeiner Verwendung ist«. Bitcoin ist in, sagen wir, Europa oder Nordamerika sicherlich keine Währung. Das vielleicht einzige Land, in dem er auch nur annähernd eine Währung ist, ist El Salvador, dessen Regierung Bitcoin als zweites Zahlungsmittel eingeführt hat. Aber für die meisten von uns ist Bitcoin ein *Wertaufbewahrungsmittel* und nichts, womit wir unseren Lebensmitteleinkauf bezahlen würden.

Dennoch besprechen wir in Kapitel 3, wie Sie Bitcoins kaufen und verkaufen können – und Bitcoins zu verkaufen ist natürlich im Wesentlichen dasselbe, wie sie umzutauschen (Sie tauschen sie gegen Waren oder Dienstleistungen ein).

Wie können Bitcoins wertvoll sein, wenn es doch gar keine gibt?

Während wir dies schreiben, kann jeder, der einen Bitcoin besitzt, diesen für rund 48.000 US-Dollar verkaufen. Aber wir haben Ihnen gerade gesagt, dass *es keine Bitcoins gibt …*, dass alles, was es gibt, ein Hauptbuch ist, das festhält, dass die Bitcoins existieren und wer (welche Adresse in der Blockchain) sie besitzt. Wie kann das überhaupt einen Wert haben!?

Um das zu verstehen, müssen wir etwas mehr über Geld erfahren und verstehen, wie es funktioniert. Wie bei *jeder* Form von Geld geht es auch bei Bitcoin um den *Glauben*. Wenn genügend Menschen glauben, dass eine bestimmte Ausprägung von Geld einen Wert hat, dann hat sie auch einen Wert. Es kann mit anderen Menschen, die ebenfalls glauben, dass es einen Wert hat, gegen Waren und Dienstleistungen getauscht werden. Sobald die Menschen jedoch nicht mehr daran glauben, hat das Geld keinen Wert mehr. Und das kommt tatsächlich manchmal vor. In der Geschichte der Menschheit hat es etwa 60 Fälle von *Hyperinflation* gegeben, bei denen die Menschen das Vertrauen in die Währung verloren haben und der Wert des Gelds rapide gesunken ist, bis es praktisch wertlos war. Zuletzt geschah dies in Simbabwe; im Jahr 2008 gab das Land tatsächlich seine Währung zugunsten von Fremdwährungen auf. (Ironischerweise stiegen die simbabwischen Dollarnoten daraufhin im Wert, da sie von Sammlern in aller Welt aufgekauft wurden.)

Also noch einmal: Solange Menschen an eine bestimmte Art von Geld *glauben*, hat dieses Geld einen Wert. Nehmen wir an, Sie besitzen einen halben Bitcoin; mit anderen Worten sagt die Bitcoin-Blockchain aus, dass Sie einen halben Bitcoin besitzen. (Denken Sie daran, dass es keine physischen Bitcoins gibt, sondern nur die Aufzeichnung von Bitcoin-Transaktionen.) Nun möchten Sie sich auszahlen lassen und diesen Bitcoin-Betrag in Ihre Landeswährung umwandeln. Die Bitcoin-Blockchain besagt, dass Sie die Blockchain-Adresse besitzen, die mit diesem (halben) Coin verknüpft ist (wie das funktioniert, erklären wir in Kapitel 2). Dadurch können Sie den Betrag auf die Adresse *einer anderen Person* übertragen.

Gegenwärtig ist es kein Problem, jemanden zu finden, der einen Wert in der Verknüpfung dieses Bitcoins mit seiner eigenen Blockchain-Adresse sieht. Warum? Weil die Menschen an diese Form des Gelds glauben und potenzielle Käufer daher wissen, dass, wenn sie ihrerseits zum Verkauf bereit sind, es *wieder jemanden* geben wird, der genug daran glaubt, um dafür zu bezahlen oder Waren und Dienstleistungen dafür einzutauschen. (Außerdem hoffen sie, dass der Wert des Gelds steigt, worauf wir in Kapitel 6 näher eingehen.)

Bitcoin funktioniert also durch Überzeugung. Das klingt vielleicht etwas hanebüchen oder schwach. Sie denken vielleicht, dass das nicht gerade sehr viel ist, um darauf ein Geldsystem zu begründen, aber in Wahrheit basiert so ziemlich *jede* Form von Geld genau darauf. Wir möchten Ihnen dazu gerne eine Geschichte erzählen.

Milton Friedman und die Rai-Steine

Der renommierte Wirtschaftswissenschaftler und Nobelpreisträger Milton Friedman schrieb in den 1990er-Jahren eine Veröffentlichung über *Rai-Steine* – eine Geldform, die

einst auf den Yap-Inseln verwendet wurde – und verglich darin dieses System mit dem Einsatz von Gold zur Besicherung von Währungen in den westlichen Ländern.

Die Yap-Inseln sind eine Gruppe aus vier kleinen Inseln mitten im Pazifischen Ozean, etwa 800 Meilen östlich der Philippinen. Mit einer Bevölkerung von etwa 12.000 Einwohnern hat Yap nicht viel von sich reden gemacht, außer vielleicht durch eine ungewöhnliche Form des Geldes, die als *Rai-* (oder *Fei*)-Steine bekannt wurde.

Das Rai-Steingeld besteht aus »Münzen« aus Kalkstein. Diese Münzen konnte man sich nicht in die Tasche stecken, denn sie waren groß, manchmal sehr groß. Die Steine hatten in der Mitte Löcher, durch die ein Baumstamm gesteckt werden konnte, um sie besser tragen zu können! (Wenn Sie sehen möchten, wovon wir hier sprechen, führen Sie eine kurze Bildersuche im Internet nach »Rai Steingeld« durch).

In den meisten Fällen wurden sie aber gar nicht transportiert, sondern verblieben so lange an Ort und Stelle, bis sie vom Moos überwachsen waren. Und so funktionierte es: Nehmen wir an, Sie wollten einen Haufen Kokosnuss-Kopra (das getrocknete Nährgewebe, aus dem das Kokosnussöl gewonnen wird, was auf den Yap-Inseln ein großes Geschäft ist) kaufen. Sie würden den Verkäufer ansprechen und so etwas sagen wie: »Sie kennen doch meinen Rai-Stein im Wald am Fluss? Nun, ich gebe Ihnen den Rai-Stein im Tausch gegen die Kopra.« Vorausgesetzt, der Preis stimmt, würden Sie und die andere Partei dann allen erzählen, dass der betreffende Rai-Stein nun nicht mehr Ihnen gehört, sondern dass er in den Besitz des Verkäufers übergegangen ist.

Nebenbei bemerkt, waren diese Steine ein relativ rares Gut. Man konnte nicht einfach ein Stück Kalkstein nehmen und sein eigenes Geld machen. Abgesehen von dem hohen Arbeitsaufwand für die Herstellung eines solchen Steins gab es ein weiteres Problem: Auf den Yap-Inseln gibt es keinen Kalkstein! Stattdessen muss der Kalkstein in Palau abgebaut und dann auf die Inseln gebracht werden, eine Reise von circa 900 Kilometern. (In Währungsfachkreisen ist dies als *Proof of Work* (deutsch: Arbeitsnachweis) bekannt, worüber Sie in Kapitel 7 mehr erfahren können.)

Es gibt sogar eine wohlbekannte Geschichte (nun ja, wohlbekannt für Menschen, die sich mit Rai-Steinen auskennen!) über einen großen Rai-Stein, der auf der Rückreise von Palau über Bord ging. Man kann sich diese Unterhaltung gut vorstellen:

Seemann 1: »Oh, nein, wir haben diesen riesigen Stein verloren! Der war so wertvoll!«

Seemann 2: »Oh, Mann, das gibt Ärger! Aber warte mal, wir wissen doch ungefähr, wo er *liegt*, oder?«

Und so blieb dieser besondere Rai-Stein so lange im Umlauf, wie der Besitzer sagen konnte: »Du kennst doch meinen Rai-Stein, den, der vom Schiff gefallen und gesunken ist?«

Nun zurück zu Milton Friedman. In seiner Abhandlung über diese Form der Währung erörtert er, was geschah, als die Inseln von Deutschland besetzt wurden. (Rai-Steine wurden bis ins frühe 20. Jahrhundert verwendet.) Den deutschen Besatzer gelang es, wie er schreibt, wenig überraschend nicht, die einheimische Bevölkerung dazu zu bewegen, Arbeitskräfte zur Verfügung zu stellen (um zum Beispiel die Straßen und Wege auf den Inseln zu verbessern).

Aber die deutschen Verwalter hatten eine Idee. Sie schickten jemanden los, um schwarze Kreuze auf die Steine zu malen und den Einheimischen mitzuteilen, dass die Steine nun ihnen – den Deutschen – gehörten! Damit bestraften sie die lokale Bevölkerung dafür, dass sie keine Arbeitskraft zur Verfügung stellte.

Das hat tatsächlich funktioniert, was zeigt, dass die Menschen von Yap – wie vielleicht auch einige Leser dieses Buches – nicht richtig verstanden haben, was Geld ist (ein Glaube) und wie es funktioniert (es hat nur so lange einen Wert, wie Menschen an diesen Wert glauben). Die einheimische Bevölkerung leistete Arbeit, um ihr Geld zurückzubekommen (die Kreuze wurden beseitigt).

Friedman führte die Geschichte noch weiter aus. Er erörterte ein Ereignis, das sich 1932 weit entfernt von den Yap-Inseln ereignete. Frankreich bat die Federal Reserve Bank von New York, einen Teil seines Dollarvermögens in Gold umzuwandeln. Anstatt das Gold nach Frankreich zu verschiffen, gingen die Bankangestellten einfach in die Tresorräume und räumten das Gold ein wenig um, indem sie die entsprechende Menge an Goldbarren in bestimmte Fächer legten und diese Fächer markierten, um zu zeigen, dass die Barren Eigentum Frankreichs waren. (Dieses Ereignis führte in den USA zu einer Bankenpanik, da die Zeitungen den Verlust von Gold an Frankreich beklagten.)

Friedman verglich die Kennzeichnung der Rai-Steine mit der Kennzeichnung des Golds; er erklärt, dass Beamte der Federal Reserve die erforderliche Goldmenge abtrennten und das Gold kennzeichneten, um zu verdeutlichen, dass es Frankreich gehörte. Friedman erklärt: »Sie hätten das ebenso gut mit einem Kreuz in schwarzer Farbe tun können, so wie es die Deutschen mit den Steinen gemacht hatten«.

Sie können dieses Paper unter `https://miltonfriedman.hoover.org/internal/media/dispatcher/215061/full` lesen. Es ist wirklich sehr hilfreich und bietet eine Möglichkeit, Ihre Denkweise über Geld und seine wahre Natur zu hinterfragen. Sehen wir uns einfach an, wie Friedman sein Dokument beendet hat:

> Beide Beispiele – und es ließen sich noch zahlreiche weitere anführen – zeigen, wie wichtig der »Mythos«, der unhinterfragte Glaube, in Geldangelegenheiten ist. Unser eigenes Geld, das Geld, mit dem wir aufgewachsen sind, das System, von dem es kontrolliert wird, das alles erscheint uns »real« und »rational«. Das Geld anderer Länder erscheint uns oft wie Papier oder wertloses Metall, selbst wenn die einzelnen Währungseinheiten eine hohe Kaufkraft aufweisen.

Geld existiert eigentlich gar nicht. Es ist lediglich ein Konzept. Ja, wir haben Münzen und Scheine, die Geld *verkörpern*, aber sie sind nicht das eigentliche Geld, und sie haben wenig bis gar keinen inneren Wert. Ohne den Glauben an das Versprechen, das dem Geld zugrunde liegt, hat seine physische Ausprägung keinerlei Wert, so wie es die Menschen in Simbabwe im Jahr 2008 feststellen mussten.

Geld ist Glauben

Beim Geld geht es also nur um den Glauben. Die physischen Ausprägungen von Geld, mit denen wir aufwachsen, erscheinen uns vollkommen selbstverständlich. Andere Varianten fühlen sich wie »Spielgeld« an.

Marco Polo war verblüfft, als er auf seiner Reise nach China entdeckte, dass der Großkhan Alchemie – also Zauberei – einsetzte, um (wie es in einer Kapitelüberschrift in Polos Buch heißt) »*die Rinde von Bäumen, die zu etwas wie Papier gemacht wurde, in seinem ganzen Land als Geld durchgehen zu lassen*«. Richtig, nur Zauberei konnte Papier in Geld verwandeln!

Tatsächlich besteht sogar der größte Teil Ihrer eigenen Fiat-Währung aus nichts weiter als einer Idee. Der Historiker Yuval Noah Harari erklärt in seinem Buch *Sapiens*, dass Geld lediglich eine Vorstellung ist, ein menschliches Konzept und kein realer Gegenstand, den man sehen oder anfassen kann.

Er sagt: »Der Gesamtwert des weltweiten Gelds liegt bei 60 Billionen Dollar, wovon nur 6 Billionen Dollar in Bargeld oder Münzen vorliegen. 90 Prozent des Gelds sind nichts weiter als Buchungen auf einem Computerserver. Geld ist ein auf dem Glauben basierendes Objekt, dessen Wert sich aus der gemeinsamen Vorstellung von seinem Wert ergibt«.

Davon können Sie sich selbst überzeugen. Wenn Sie im Internet nach »Geldmenge« oder »Money Supply« suchen und ein wenig herumstöbern, finden Sie verschiedene Maße für die Geldmenge: M0, M1, M2 und so weiter. M0 ist Bargeld – Münzen und Scheine. M1 umfasst auch Einlagen auf Girokonten. M2 beinhaltet all das, aber auch Sparkonten, Anlagefonds und so weiter. Wenn Sie noch etwas tiefer graben, werden Sie feststellen, dass das, was Sie für Geld halten – die Münzen und Scheine – in Wahrheit nur maximal 10 Prozent des gesamten im Umlauf befindlichen Gelds ausmacht!

Hier also eine kurze Frage an Sie: Was ist der Unterschied zwischen Bitcoin und US-Dollar, Pfund Sterling oder Euro? Bei diesen Fiat-Währungen sind 90 Prozent des Gelds »nichts weiter als Buchungen auf einem Computerserver«. Bei Bitcoin sind es 100 Prozent!

Es gibt natürlich noch weitere Unterschiede (einige davon behandeln wir in Kapitel 2). Aber unser Ziel hier ist es, Ihnen zu zeigen, dass Bitcoin und Fiat-Währungen eine wichtige Gemeinsamkeit haben: Sie sind alle auf den Glauben angewiesen, um zu funktionieren. Solange die Menschen an eine *beliebige* Währung glauben, behält sie ihren Wert.

Das soll nicht heißen, dass eine bestimmte Währung – einschließlich Bitcoin – sich für immer den Glauben der Menschen bewahren wird. Was wir hier zu erklären versuchen, ist, dass etwas so Flüchtiges wie Bitcoin wertvoll sein kann.

Die Vorteile von Bitcoin verstehen

Nun, da Sie verstehen, inwiefern Bitcoin einen Wert haben *kann* – und das hat er offensichtlich im Moment, da Millionen von Menschen bereit sind, dafür zu bezahlen –, lassen Sie uns einen Blick auf einige seiner Vorteile werfen, auf Eigenschaften, die ihn von anderen Geldformen abheben.

Betrachten wir zunächst die Funktionen von Geld:

- ✔ Geld kann als **Tauschmittel** dienen. Man kann es also verwenden, um Dinge zu kaufen. Bitcoin schneidet in dieser Hinsicht derzeit nicht besonders gut ab, weil er nicht

weithin akzeptiert wird, Transaktionen meist langsam und teuer sind und die meisten Menschen Bitcoin immer noch zu spekulativen Zwecken kaufen und anhäufen, um zu sehen, ob der Wert steigt.

- ✔ Geld kann auch als **Maß für den Wert** oder als **Verrechnungseinheit** dienen. Wir verwenden es, um Dingen einen Wert zuzuschreiben, von Zucker bis zu Autos. Auch in diesem Bereich macht sich Bitcoin aktuell nicht sehr gut, weil sein Preis so stark schwankt.
- ✔ Geld kann auch als **Wertspeicher** fungieren, als eine Möglichkeit, gesparte Werte sicher aufzubewahren. Sie sollten hierzu die Möglichkeit haben, Bitcoins zu kaufen und Ihr Vermögen darin zu speichern, um es dann bei Bedarf wieder abrufen zu können. Bitcoin hat sich in dieser Hinsicht auf lange Sicht sehr gut gemacht. Natürlich gibt es kurzfristige Schwankungen, aber auf lange Sicht hat er sich aufgrund der erheblichen Wertsteigerung sehr gut als Wertaufbewahrungsmittel behauptet.

Nachfolgend finden Sie einige Merkmale und Vorteile, die Bitcoin von anderen Geldsystemen abhebt.

Transportfähigkeit

Geld muss leicht zu transportieren sein. Wenn Sie es nicht bewegen können, wie sollen Sie es dann verwenden? Es mag den Anschein haben, dass die Rai-Steine aus unserem vorangegangenen Beispiel in diesem Kapitel physisch nicht besonders portabel waren, aber ihr Wert war in der Tat sehr portabel. Die Bewohner von Yap kommunizierten und übertrugen den Besitz mündlich. Bitcoin ist ebenfalls sehr gut übertragbar, wie Sie in diesem Buch feststellen werden. Sie können ihn über das Internet fast mit Lichtgeschwindigkeit an jeden Ort der Welt transferieren.

Überprüfbarkeit

Wie Sie in Kapitel 2 sehen, lässt sich Ihr Anspruch auf Ihre Bitcoins auf jeden Fall nachweisen. Da eine vollständige Kopie der Transaktionshistorie in der Bitcoin-Blockchain auf jedem Computer, der die Bitcoin-Software ausführt, gespeichert ist, müssen die Tausende von Netzwerkknoten jede einzelne Transaktion und jeden Block nach den Bitcoin-Regeln überprüfen. Diese Regeln müssen von allen Teilnehmern befolgt werden, sonst können sie nicht mehr erfolgreich am Netzwerk mitwirken. Die Struktur der Bitcoin-Blockchain stellt sicher, dass Sie den Besitz Ihrer Bitcoins nachweisen können und Sie dies tatsächlich auch müssen, bevor Sie sie weiterversenden können (vorausgesetzt, Sie verlieren Ihre privaten Schlüssel nicht; siehe Kapitel 2).

Fungibilität

Eine wichtige Eigenschaft von Geld ist, dass es fungibel sein muss. Das heißt, ein Dollar ist genauso viel wert wie ein anderer, mein Dollar hat denselben Wert wie Ihr Dollar. Wie jede gute Form von Geld ist auch Bitcoin fungibel; jeder Bitcoin hat im Allgemeinen den gleichen Wert wie ein anderer Bitcoin. (Okay, das stimmt nicht zu 100 Prozent. Manche Menschen

möchten Bitcoins besitzen, die über die Blockchain nicht zu einem bestimmten Besitzer zurückverfolgt werden können. Sie sind bereit, einen gewissen Aufpreis für Bitcoins zu bezahlen, die erstellt und transferiert werden, ohne dass sie den in Kapitel 3 besprochenen »Know Your Customer«-Bankregeln unterliegen).

Beständigkeit

Bitcoin vermodert nicht, wenn man ihn der Witterung aussetzt, und er verbrennt auch nicht, wenn Ihr Haus abbrennt. Bitcoin ist nur Information, reines Geld ohne das verletzliche, greifbare Material. Solange die Bitcoin-Blockchain und das Bitcoin-Netzwerk Bestand haben, wird Ihr Bitcoin dort bleiben, wo er schon immer war: in der Blockchain. Sie müssen nur wissen, wie Sie Ihren Zugang zur Blockchain-Adresse, die mit Ihrem Bitcoin verknüpft ist, schützen können, worauf wir in Kapitel 5 eingehen.

Teilbarkeit

Bitcoins lassen sich in winzig kleine Teile unterteilen – in Hundertmillionstel, die sogenannten Satoshis. Das heißt, dass Sie einen Bitcoin oder einen beliebigen Bruchteil eines Bitcoins ausgeben können. Beim aktuellen Preis ist der kleinste Bruchteil eines Bitcoins etwa ein Zwanzigstel eines US-Cents wert.

Offener Zugang

Das Bitcoin-Netzwerk ist, wie die früheren Rai-Steine, ein offen zugängliches Netzwerk, das nicht zensiert werden kann. Auch wenn Bitcoin nicht für jeden geeignet ist, so steht es doch jedem zur Verfügung, der es nutzen möchte; niemand kann den Zugang eines anderen zum Netzwerk beschränken.

Unwiderrufliche Abwicklung

Monetäre Netzwerke der Vergangenheit haben die Abwicklung gut bewerkstelligt; selbst im Fall des versunkenen Rai-Steins wurde das Hauptbuch aktualisiert und die Abwicklung erfolgte – wenn auch nur mündlich. Mit Bitcoin werden Transaktionen nach sechs Bestätigungen (siehe Kapitel 3) mathematisch unumkehrbar, was etwa eine Stunde dauert. Im Vergleich zu anderen Verfahren bietet das Bitcoin-Netzwerk relativ schnell endgültige Zahlungsabschlüsse, die nicht rückbelastet werden können.

Grenzen- und staatenlos

Bitcoin ist international. Jeder Mensch aus jedem Land, das einen offenen Zugang zum Internet hat, kann Bitcoins besitzen und handeln. Selbst wenn ein Land versucht, Bitcoin zu verbieten, wird die Kryptowährung anderswo weiter existieren und sachkundige Bürgerinnen und Bürger wären wahrscheinlich in der Lage, die Beschränkungen zu umgehen und ihre Spuren zu verwischen. Eine Bitcoin-Transaktion kann sogar über Amateurfunk, lokale Mesh-Netzwerke und über Satelliten übertragen werden.

Pseudonym

Im Gegensatz zur landläufigen Meinung ist Bitcoin nicht anonym. Aber er ist *pseudonym*. Die Blockchain selbst kennt beispielsweise keine Kontonamen. Ihr Bitcoin ist dort weder mit Ihrem Namen noch mit anderen identifizierenden Informationen versehen. (Wie die Blockchain funktioniert, erfahren Sie in Kapitel 2.) Aber die Blockchain ist öffentlich einsehbar. Jeder kann sie aufrufen, darin herumstöbern und Transaktionen von einer Adresse zur nächsten verfolgen. Das bedeutet, dass, wenn es Informationen gibt, die Ihren »Eintrag« in die Blockchain identifizieren – zum Beispiel, wenn Sie Bitcoins von einer Handelsplattform kaufen, die den KYC-Bestimmungen (Know Your Customer) folgt – Ihre Transaktionen zurückverfolgt werden können.

Beständig gegen Monopole

Bitcoin basiert auf der Peer-to-Peer-Bitcoin-Blockchain, die von Zehntausenden von Menschen betrieben wird. Keine einzelne Person oder Personengruppe kann die Kontrolle an sich reißen.

Entwertungssicher

Entwerten bedeutet: »etwas in seiner Qualität oder seinem Wert herabsetzen; verschlechtern«. Im Zusammenhang mit Währungen bedeutete es ursprünglich, den Wert des zur Prägung von Münzen verwendeten Metalls zu verringern. Heute spricht man meist dann von Geldentwertung, wenn die Regierung immer mehr Geld druckt, sodass jeder Schein oder jede Münze weniger wert ist.

In der Bitcoin-Gemeinschaft herrscht eine gewisse libertäre Grundströmung vor. Echte Bitcoiner sehen es als einen großen Vorteil an, dass Bitcoin *nicht* unter der Kontrolle einer bestimmten Regierung steht. Es handelt sich um Geld für die Menschen von den Menschen.

Das bedeutet, dass keine Regierung – oder eine andere Form von Autorität – mehr Bitcoins »drucken« kann. Tatsächlich ist die Emissionskurve von Bitcoin in den mathematischen Formeln, die seine Funktionsweise definieren, fest eingeschrieben (derzeit sind es 6,25 Bitcoins alle zehn Minuten); alle vier Jahre wird diese Rate um die Hälfte absinken, bis schließlich der Zustrom neuer Bitcoins nur noch tröpfchenweise erfolgt und letztlich sogar auf null heruntergeht. Bitcoin kann nicht »entwertet“ werden, indem der Markt mit mehr Bitcoins überschwemmt wird.