LERNEN EINFACH GEMACHT

Bitcoin

für dummies®

Die Technik hinter Bitcoin verstehen

Bitcoin kaufen, verwenden und sicher verwalten

In Bitcoin investieren

Peter Kent
Tyler Bain

Bitcoin für Dummies

Schummelseite

DIE BITCOIN-SPRACHE LERNEN

Eigentlich gibt es gar keinen Bitcoin – zumindest ist da nichts, das sie greifen können. Vielmehr wird Bitcoin durch Aufzeichnungen von Bitcoin-Transaktionen im Bitcoin-»Ledger« repräsentiert, das in einer »Blockchain« gespeichert ist – das ist wirklich mal etwas anderes, und nur wenige Menschen verstehen es.

Das kann alles etwas verwirrend sein, deshalb ist hier ein kurzer Überblick über einige wichtige Begriffe.

- **Blockchain:** Eine *Blockchain* ist eine bestimmte Art von Datenbank, die Daten auf strukturierte Weise speichert. Im Fall der Blockchain ist die Datenbank verteilt; Kopien der Bitcoin-Blockchain liegen auf Tausenden von Computern auf der ganzen Welt. Da all diese Kopien identisch sein müssen, kann diese Kombination von Blockchain-Kopien nicht so ohne Weiteres manipuliert werden.
- Der **Bitcoin-Ledger:** Ein *Ledger* oder *Hauptbuch* ist eine Aufzeichnung von Finanztransaktionen. Hauptbücher wurden früher handschriftlich in Büchern geführt. Heute speichert das Bitcoin-Hauptbuch digitale Informationen über Bitcoin-Transaktionen in der Bitcoin-Blockchain. Übrigens ist das Bitcoin-Hauptbuch nicht verschlüsselt; es ist ein öffentlich einsehbares und zugängliches System, das es jedem erlaubt, mit einem »Blockchain-Explorer« in die Blockchain zu schauen und zu sehen, was dort vor sich geht.
- **Bitcoin:** Das ist zunächst verwirrend für viele Menschen, aber im Gegensatz zu Euro, Dollar, Kronen oder Pfund gibt es nicht nur keinen physischen Bitcoin, sondern auch keinen digitalen Bitcoin – nichts, auf das man zeigen und sagen könnte: »Seht her, da ist ein Bitcoin.« Stattdessen wird der Bitcoin nur durch das Hauptbuch repräsentiert, welches *besagt*, dass der Bitcoin existiert. Im Januar 2009 wurde im Bitcoin-Hauptbuch ein Eintrag vorgenommen – der sogenannte Genesis-Block –, welcher letztlich aussagt: »50 Bitcoins wurden zum Hauptbuch hinzugefügt.« Von da an gab es den Bitcoin, weil das Hauptbuch dies besagte!
- **Das Bitcoin-Netzwerk:** Das Internet beherbergt beispielsweise ein E-Mail-Netzwerk und das World Wide Web – ein Netzwerk aus Webseiten. Und dann gibt es da auch das Bitcoin-Netzwerk. Dieses besteht aus Tausenden von Computern, die alle über das Internet

miteinander kommunizieren. Einige dieser Computer sind Knotenpunkte, die eine vollständige oder teilweise Kopie der Blockchain enthalten. Einige sind auch am »Mining«-Prozess beteiligt, bei dem neue Bitcoins erzeugt werden. Am häufigsten im Netzwerk vertreten sind es jedoch die Wallet-Softwareprogramme, die von Bitcoin-Investoren und -Nutzern verwendet werden.

- ✔ **Adresse:** Sämtliche Bitcoins sind in der Blockchain verschiedenen *Adressen* zugeordnet, bei denen es sich um lange, eindeutige Nummern handelt. Sie können eine Adresse besitzen, die im Blockchain-Ledger beispielsweise mit einem Zehntel eines Bitcoins (oder einem Tausendstel oder fünf Bitcoins und so weiter) verknüpft ist. Sie kontrollieren diese Adresse (und die damit verbundenen Bitcoins) mithilfe von Kryptografie.
- ✔ **Transaktion:** Eine Bitcoin-*Transaktion* findet statt, wenn jemand eine Nachricht an die Blockchain sendet, welche im Grunde besagt: »Nimm x Bitcoins von meiner Adresse und verschiebe sie auf diese andere Adresse.« Nehmen wir an, Sie haben einen halben Bitcoin und wollen ihn in Dollar umtauschen; Sie finden jemanden, der bereit ist, Ihren halben Bitcoin zu kaufen – zum Beispiel einen Bitcoin-Broker – und senden eine Transaktion an die Blockchain, um den Bitcoin von Ihrer Adresse zur Adresse des Käufers zu transferieren. Das Hauptbuch verzeichnet dann eine Transaktion, die besagt: »Ein halber Bitcoin wurde von Adresse x zu Adresse y transferiert.«
- ✔ **Wallet:** Nein, in der Wallet werden keine Bitcoins gespeichert. *Es gibt keine Bitcoins in einer Wallet!* Vielmehr speichert die Wallet Informationen, die Ihnen die Verfügungsgewalt über die Adresse in der Blockchain geben, mit der Ihre Bitcoins verknüpft sind. Mit Software-Wallets können Sie Nachrichten an das Bitcoin-Netzwerk senden und Transaktionen in das Bitcoin-Hauptbuch eintragen.

VERSTEHEN SIE, WAS GELD IST?

Wenn Sie an Geld denken, haben Sie wahrscheinlich Papierscheine und Münzen vor Augen. Die wichtigsten Währungen der Welt verfügen aber gar nicht über genug Münzen und Scheine für die gesamte im Umlauf befindliche Geldmenge. Ein Anteil von rund 90 Prozent der wichtigsten Währungen ist ohne physische Form! Es handelt sich lediglich (um den Historiker Yuval Noah Harari zu zitieren) um »Einträge auf einem Computerserver«.

Geld ist ein bloßes Konzept, eine Möglichkeit für Menschen, Werte zu speichern und sie in der Zukunft gegen reale Waren und Dienstleistungen einzutauschen. Geld kann durch aufpolierte Muscheln, Geldscheine, Gold, Salz, Gerste, Münzen oder große Steinscheiben verkörpert werden – viele verschiedene Dinge können die Rolle des Geldes übernehmen. Wenn Sie an

die Repräsentation *glauben*, dann kann alles, was zur Repräsentation verwendet wird, erfolgreich als Geld eingesetzt werden.

Na gut, eine weitere Anforderung gibt es da noch: Es darf nicht zu einfach sein, mehr von der Verkörperung herzustellen. »Muscheln?«, sagen Sie, »die kann ich doch am Strand auflesen.« Nicht so schnell! Frühere Kulturen, die auf Muschelgeld setzten, verwendeten eine ganz bestimmte Art von Muscheln, die zudem aufwendig bearbeitet werden mussten, und sie nahmen dafür sogar Muscheln aus einer weit entfernten Region. Es gab also keine einfache Möglichkeit, den Markt mit neuem Geld zu überschwemmen.

Also, ja, Bitcoin kann als eine Form von Geld oder zumindest als »Wertaufbewahrungsmittel« fungieren. Es gibt davon nur ein sehr begrenztes Angebot; jeden Tag wird eine feste, sich aber stetig verkleinernde Menge »geschürft«. Und Millionen von Menschen glauben daran.

VERWIRRENDE BLOCKCHAIN

Und wie funktioniert jetzt diese *Blockchain*-Geschichte? Nun, die Blockchain ist eine Art Datenbank (vergleichbar mit Datensätzen, die in einer Tabellenkalkulation oder in einem Buchhaltungsprogramm gespeichert sind). Und ihre Kopien werden über Tausende von Computern im Bitcoin-Netzwerk verteilt.

Aber das ist noch nicht alles. Erstens wäre da der Begriff *Block*. Der bezieht sich auf Datenblöcke. Blockchains können für viele verschiedene Zwecke genutzt werden, aber im Fall der Bitcoin-Blockchain enthält jeder Block Aufzeichnungen über Transaktionen. Etwa alle zehn Minuten wird ein neuer Datenblock an die Blockchain angefügt – und auf alle Kopien im Netzwerk repliziert.

Und dann ist da noch der Begriff *chain*, englisch für »Kette«. Eine Blockchain ist also eine Art Datenbank, deren Datenblöcke aneinandergereiht und miteinander *verkettet* sind. Wie funktioniert das? Nun, das ist etwas kompliziert, aber die Blöcke werden mithilfe von *Hash-Werten* miteinander verknüpft.

Ein *Hash-Wert* ist eine lange Zahl, die die Funktion eines digitalen Fingerabdrucks erfüllt. Er kennzeichnet einen Datenblock auf eindeutige Weise. Sie hashen also einen Datenblock (dies ist eine Rechenoperation), um diesen digitalen Fingerabdruck zu erstellen. Dieser Fingerabdruck – der Hash-Wert oder schlicht *Hash* – wird dann zusammen mit dem Datenblock gespeichert. Wenn der nächste Transaktionsblock bereitsteht, liest die Bitcoin-Software den Hash des *vorherigen* Blocks ein und hasht dann alle Daten – die neuen Transaktionen zusammen mit dem vorhergehenden Hash-Wert –, um den Hash-Wert des aktuellen Blocks zu erstellen; dieser wird dann wieder mit in den nächsten Block eingebunden und so weiter.

Auf diese Weise werden die Blöcke derart miteinander verkettet, dass es so gut wie unmöglich ist, auch nur ein einziges Textzeichen oder einen Zahlenwert zu ändern. Würde man dies tun, veränderte sich der Hash-Wert des editierten Blocks, was wiederum den Hash-Wert des nächsten Blocks veränderte, was wiederum jenen des übernächsten Blocks veränderte, und so weiter.

Und was ist das Ergebnis? Die Bitcoin-Blockchain ist praktisch unmöglich zu hacken.

KRYPTOGRAFIE — DAS »KRYPTO« IN KRYPTOWÄHRUNG

Kryptowährungen wie Bitcoin bedienen sich der Kryptografie – insbesondere der Verschlüsselung mit öffentlichen Schlüsseln –, um den Besitzern einen Weg zu bieten, ihre Besitzansprüche nachzuweisen. Hier ist ein kurzer Überblick über die Funktionsweise der *Public-Key-Verschlüsselung:*

- **Verschlüsselung:** Wenn Sie Daten »verschlüsseln«, chiffrieren Sie sie. Man nimmt zum Beispiel eine vertrauliche Nachricht, die nur der Empfänger lesen können soll, und verschlüsselt sie so, dass sie vollkommen unleserlich ist. Sie kann erst gelesen werden, nachdem sie wieder *entschlüsselt* (dechiffriert) wurde.
- **Der Schlüssel oder das Passwort:** Zur Verschlüsselung der Nachricht verwenden Sie einen Schlüssel oder ein Kennwort. Vielleicht benutzen Sie beispielsweise ein Buchhaltungsprogramm wie etwa Quicken. Um das Programm zu öffnen, müssen Sie ein Passwort eingeben. Sie nehmen also die zu entsperrenden Daten, geben den Schlüssel oder das Passwort hinzu und übergeben beides zusammen an das Programm. Dieses verwendet den Schlüssel, um die gewünschte Datei zu entsperren. Nur dieser spezielle Schlüssel kann die verschlüsselten Daten wieder freigeben.
- **Public-Key-Verschlüsselung:** Im vorherigen Beispiel, dem Öffnen einer Datei zum Beispiel aus einer Buchhaltungssoftware, würden Sie denselben Schlüssel verwenden, um die Daten zu verschlüsseln und sie wieder zu entschlüsseln. Das nennt sich symmetrische Verschlüsselung. Public-Key-Verschlüsselungssysteme funktionieren hier etwas anders. Sie verwenden zwei mathematisch (und eindeutig) einander zugeordnete Schlüssel, einen öffentlichen und einen privaten. Bei diesem System können Sie die Daten *nicht* mit demselben Schlüssel wieder entschlüsseln, den Sie zuvor zur Verschlüsselung der Daten verwendet haben. Es handelt sich um eine asymmetrische Verschlüsselung.

Daten, die Sie mit dem öffentlichen Schlüssel verschlüsselt haben, können Sie vielmehr nur mit dem privaten Schlüssel wieder entschlüsseln; und Daten, die mit dem privaten Schlüssel verschlüsselt wurden, lassen sich nur mit dem öffentlichen Schlüssel wieder in eine lesbare Form bringen. Wie das funktioniert? Nur wenige Menschen verstehen die entsetzlich komplexe *Mathemagie* hinter der Public-Key-Kryptografie. Das ist aber nicht schlimm, denn Sie wissen ja wahrscheinlich auch nicht, wie Ihr Smartphone funktioniert. Es funktioniert eben einfach.

- ✔ **Public Key:** Ein Public Key ist ein Schlüssel, der auf irgendeine Weise öffentlich gemacht wird. Sie brauchen ihn nicht geheim zu halten.
- ✔ **Private Key:** Den privaten Schlüssel müssen Sie unbedingt für sich behalten … der ist geheim.
- ✔ **Adresse:** Ihre Bitcoins sind einer Adresse in der Blockchain zugeordnet. Insbesondere sind der private Schlüssel, der öffentliche Schlüssel und die Adresse allesamt mathematisch – und eindeutig – miteinander verknüpft. Die Adresse ist mit Ihrem öffentlichen Schlüssel verknüpft, und zwar nur mit diesem öffentlichen Schlüssel. Und Ihr öffentlicher Schlüssel ist mit dem privaten Schlüssel verknüpft, und zwar nur mit diesem privaten Schlüssel.

  Eine Nachricht verschlüsseln: Wenn Sie geheime Nachrichten mit einem Public-Key-Verschlüsselungssystem kodieren, verschlüsseln Sie die Nachricht mit dem öffentlichen Schlüssel des Empfängers. Die einzige Person, die die Nachricht entschlüsseln kann, ist dann der Empfänger, da nur dieser im Besitz des privaten Schlüssels ist.

- ✔ **Eine Nachricht signieren:** Mit der Public-Key-Verschlüsselung können Sie eine Nachricht auch *signieren*. Denken Sie daran, dass der öffentliche Schlüssel tatsächlich allgemein bekannt ist. Wenn Sie eine Nachricht mit dem privaten Schlüssel verschlüsseln, ist sie also nicht besonders geheim – jeder, der den öffentlichen Schlüssel zur Hand hat, kann sie entschlüsseln, und der öffentliche Schlüssel ist ja öffentlich! Wenn sich die Nachricht mit dem öffentlichen Schlüssel entschlüsseln lässt, bedeutet dies aber, dass sie von der Person stammen muss, die im Besitz des privaten Schlüssels ist, der zu diesem öffentlichen Schlüssel passt. Die Nachricht wurde also von der Person signiert, die den privaten Schlüssel besitzt.
- ✔ **Nachrichten an die Bitcoin-Blockchain signieren:** Bitcoin setzt auf Public-Key-Verschlüsselung, aber *nicht*, um geheime Botschaften an die Blockchain zu übermitteln. Vielmehr dient sie zum *Signieren* von Nachrichten. Wenn Sie eine Nachricht an die Blockchain senden, mit der Bitcoins von Ihrer Adresse an eine andere übertragen werden soll, verschlüsselt Ihre Wallet-Software diese Transaktionsinformationen mit dem privaten Schlüssel, packt den öffentlichen Schlüssel im Klartext hinzu und versendet die Nachricht.

Klar, die Nachricht wurde verschlüsselt, aber sicher ist sie dennoch nicht, da sie von jedem entschlüsselt werden kann.

Der Knotenpunkt im Bitcoin-Netzwerk, der die Nachricht verarbeitet, nimmt den öffentlichen Schlüssel und entschlüsselt damit die Nachricht. Er überprüft auch, ob der öffentliche Schlüssel mit der in der Nachricht angegebenen Adresse verknüpft ist. Wenn dies der Fall ist – denken Sie daran, dass öffentlicher Schlüssel, privater Schlüssel und Adresse alle mathematisch und eindeutig miteinander zusammenhängen –, weiß der Knotenpunkt, dass die Person, die den zur Verschlüsselung der Nachricht verwendeten privaten Schlüssel besitzt, auch die Adresse »besitzen« muss, die mit dem zur erfolgreichen Entschlüsselung der Nachricht verwendeten öffentlichen Schlüssel verknüpft ist.

BITCOINS SICHER VERWAHREN

Wenn sich die Blockchain nicht hacken lässt, wieso verlieren dann immer wieder Leute ihre Bitcoins? Nun, da gibt es zwei Möglichkeiten:

- ✔ Sie verlieren Ihren Private Key: Wenn Sie Ihren privaten Schlüssel verlieren, können Sie nicht mehr nachweisen, dass Sie die Adresse in der Blockchain besitzen, mit der Ihre Bitcoins verknüpft sind. Sie können also keine Transaktionsnachrichten mehr an die Blockchain senden … Ihre Bitcoins stecken fest. Und zwar für immer, wenn Sie den Private Key nicht mehr wiederfinden können!
- ✔ Jemand anderes findet Ihren Private Key: Wenn jemand anderes Ihren privaten Schlüssel findet, hat er Zugang zu Ihren Bitcoins. Er kann Nachrichten an die Blockchain senden, um zu »beweisen«, dass er die Adresse und die damit verbundenen Bitcoins besitzt. Wer auch immer die Schlüssel hat, dem gehören die Bitcoins! Der Schutz Ihres privaten Schlüssels ist also unerlässlich. Sie müssen *absolut* sicherstellen, dass Sie Ihren Private Key niemals verlieren können – trotz Hochwasser, Feuer oder Hardwaredefekten – und gleichzeitig auch, dass niemand sonst an Ihren Private Key herankommt, es sei denn, Sie wollen es so.

MÖGLICHKEITEN ZUM BITCOIN-KAUF

Beim Kauf von Bitcoins haben Sie mehrere Möglichkeiten. Jede Variante hat ihre Vor- und Nachteile.

- ✔ Krypto-Exchanges: Sie haben die Wahl zwischen einer Vielzahl von Handelsplattformen und Brokern, die teilweise Hunderte verschiedener Kryptowährungen anbieten. Aber wählen Sie mit Bedacht! Die Preise variieren, und manche Anbieter sind seriöser als andere.
- ✔ Einen Sparplan bei einem Broker abschließen: Einige Anbieter bieten Ihnen die Möglichkeit, Bitcoins mit einer regelmäßigen Sparrate (DCA) zu kaufen. Auf diese Weise können Sie Preisschwankungen beim Einkauf ausgleichen und profitieren auf lange Sicht vom Anstieg des Bitcoin-Kurses.
- ✔ Direkter Handel von Mensch zu Mensch: Sehr riskant! Hier sollten Sie wirklich wissen, was Sie tun.

EINE (KURZE) BITCOIN-ZEITLEISTE

Bitcoin hat seit dem Jahr 2008 einen wilden Ritt hingelegt. Es hat ganz langsam angefangen. In den Anfangstagen war Bitcoin natürlich weitgehend wertlos. Tatsächlich hat erst Mitte 2010 ein Bitcoin-Nutzer erstmals ein greifbares Produkt damit bezahlt.

Doch Anfang 2011 war ein Bitcoin bereits einen Dollar wert, und obwohl der Wert mit der Zeit immer weiter anstieg, wurde die breite Öffentlichkeit erst Mitte 2017 darauf aufmerksam und der Bitcoin-Kurs schoss in die Höhe.

Hier sind ein paar Höhepunkte aus der verrückten Geschichte des Bitcoins, der ersten blockchainbasierten Kryptowährung:

18. August 2008: Der Domainname `bitcoin.org` wird registriert.

31. Oktober 2008: Satoshi Nakamoto veröffentlicht ein Dokument »Bitcoin: A Peer-to-Peer Electronic Cash System«, das die mögliche Funktionsweise von Bitcoin beschreibt.

3. Januar 2009: Die ersten Bitcoins entstehen, als Satoshi Nakamoto die Bitcoin-Blockchain einrichtet und die ersten 50 Bitcoins erzeugt (»schürft«).

9. Januar 2009: Die quelloffene Bitcoin-Client-Software wird veröffentlicht.

12. Januar 2009: In der weltweit ersten Bitcoin-Transaktion sendet Satoshi Nakamoto 10 (wertlose) Bitcoins an den Kryptografen Hal Finney.

22. Mai 2010: Laszlo Hanyecz zahlt 10.000 BTC für zwei Pizzen. Dies ist die erste geschäftliche Bitcoin-Transaktion und wird sich als der teuerste Pizzakauf der Geschichte herausstellen. Bei einem Bruchteil eines Cents pro Bitcoin scheint dieser Preis wohl angemessen zu sein. Bis April 2021 wird sich der Wert auf über 600 Millionen Dollar steigern.

Februar 2011: Bitcoin steigt auf einen Dollar.

Juni 2011: Wikileaks akzeptiert jetzt Bitcoin.

23. Juni 2013: Die U.S. Drug Enforcement Agency meldet die Sicherstellung von 11,02 BTC – die erste bekannte Beschlagnahmung durch eine Regierungsbehörde.

10. Oktober 2013: Bitcoin wird bei 130 Dollar gehandelt, ehe es zu einem großen Kursanstieg kommt.

Oktober 2013: Das FBI beschlagnahmt 26,000 BTC aus dem Darknet-Marktplatz *Silk Road*.

3. Dezember 2013: Bitcoin erreicht seinen Höchststand bei 1.151 Dollar. (Bis zum Jahresende wird er wieder auf etwa 800 Dollar fallen.)

4. Dezember 2013: Alan Greenspan, ehemaliger Vorsitzender der US-Notenbank FED, bezeichnet Bitcoin als Blase.

Februar 2014: Mt. Gox, eine der größten Handelsplattformen der Welt, stoppt die Bitcoin-Auszahlungen, nachdem der Diebstahl von 744.000 Bitcoins bekannt wurde.

13. Januar 2015: Nach etwas mehr als einem Jahr des Rückgangs wird Bitcoin bei 178 Dollar gehandelt.

Januar 2015: Die Bitcoin-Börse *Coinbase* sammelt in einer Finanzierungsrunde 75 Millionen Dollar ein.

31. März 2017: Bitcoin wird bei 1.080 Dollar gehandelt, aber der Preis wird schon bald weiter ansteigen.

April 2017: Japan akzeptiert Bitcoin als rechtmäßiges Zahlungsmittel und Russland plant die Regulierung von Bitcoin.

Sommer 2017: Die großen Medien schenken Bitcoin mehr und mehr Beachtung.

15. Dezember 2017: Bitcoin erreicht einen Höchststand von 19.497 Dollar – und fällt dann wieder ab.

2. Januar 2018: Der milliardenschwere Investor George Soros bezeichnet Bitcoin als Blase.

4. Februar 2018: Bitcoin ist wieder auf 6.955 Dollar zurückgefallen.

14. Dezember 2018: Ein schlimmes Jahr … Bitcoin wird bei 3.253 Dollar gehandelt.

25. Juni 2019: Es sieht gut aus. Der Bitcoin-Kurs liegt wieder bei über 13.000 Dollar.

13. März 2020: Okay, doch nicht so gut. Bitcoin fällt auf 5.200 Dollar zurück. Aber halten Sie durch, das wird sich noch ändern.

Oktober 2020: PayPal kündigt seinen Einstieg in das Bitcoin-Geschäft an.

14. März 2021: Nach einem Jahr des Anstiegs liegt Bitcoin bei 63.110 Dollar!

8. Juni 2021: El Salvador erklärt Bitcoin zum »offiziellen Zahlungsmittel«.

19. Juli 2021: Tja, das war nicht von Dauer. Bitcoin wird bei 29.807 Dollar gehandelt.

31. Dezember 2021: Zum Jahresende steht der Kurs bei 47.687 Dollar.

19. Juli 2022: Der Bitcoin-Kurs liegt bei 21.897 Dollar.

Peter Kent und Tyler Bain

Bitcoin

für dummies®

Übersetzung aus dem Amerikanischen
von Isolde Kommer

Fachkorrektur von Florian Dalwigk

WILEY
WILEY-VCH GmbH

Bitcoin für Dummies

Bibliografische Information der Deutschen Nationalbibliothek

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

1. Auflage 2023

Richtigkeit von Angaben, Hinweisen und Ratschlägen sowie eventuelle Druckfehler keine Haftung.

Coverfoto: Who is Danny – stock.adobe.com
Korrektur: Shangning Postel-Heutz

Print ISBN: 978-3-527-72006-4
ePub ISBN: 978-3-527-84015-1

Über die Autoren

Peter Kent und Tyler Bain haben zusammen *Krypto-Mining für Dummies* verfasst. Peter erklärt schon seit Jahrzehnten normalen Menschen komplizierte Fachthemen; er weiß, wie man Technik verständlich erklären kann. Er hat über 60 Fachbücher verfasst, darunter *SEO For Dummies*, *The Complete Idiot's Guide to the Internet*. Seit den 1980er-Jahren lehrt und informiert er Leser, Consulting-Klienten, Anwälte, Richterinnen und Geschworene (er ist Sachverständiger bei Rechtsstreitigkeiten im Zusammenhang mit Internettechnologie) und sogar den US-Kongress: Er hat mit einem Forschungsinstitut zusammengearbeitet, das Büros von Abgeordneten besucht, um ihnen beim Verständnis der neuen Welt der Kryptowährungen zu helfen.

Tyler dagegen ist bereits seit einigen Jahren im Kryptowährungsmining tätig und konnte dort viele Erfahrungen sammeln. Er ist zudem ein im Bundesstaat Colorado registrierter Ingenieur und hat Ingenieurwesen mit Spezialisierung auf Elektrotechnik an der Colorado School of Mines studiert – einer Universität, die zur Unterstützung der Bergbauindustrie gegründet wurde und noch immer zu den besten Bergbauschulen der Welt gehört (und nein, dort wird kein Kryptowährungsmining unterrichtet … noch nicht). Tyler ist ein aktives Mitglied des Institute of Electrical and Electronics Engineers (IEEE) und der Rocky Mountain Electrical League (RMEL) und hat das Electric Power Research Institute (EPRI) beraten. Zu seinen Leidenschaften gehören die Elektrifizierung des Finanz- und Transportwesens, Peer-to-Peer-Systeme und das Stromnetz.

Widmung

Tyler: Für Satoshi, wer auch immer das sein mag.

Peter: Für Monique, noch einmal. Jetzt ist es geschafft! Lass uns rausgehen und Ski fahren!

Danksagung

Vielen Dank an Steve Hayes und Chrissy Guthrie von Wiley für ihre Geduld und Flexibilität; beides war in diesem Fall vonnöten! Außerdem danken wir Margot Hutchison von Water-side für ihre Unterstützung und natürlich auch dem restlichen Wiley-Team, das die *Dummies*-Bücher bearbeitet, aufpoliert und produziert.

Inhaltsverzeichnis

Tabellenverzeichnis

Illustrationsverzeichnis

Kapitel 5

Kapitel 6

Kapitel 7

Kapitel 9

Kapitel 12

Einleitung

Willkommen zu *Bitcoin für Dummies,* einem Buch, in dem Sie alles Wissenswerte über die erste und ursprüngliche blockchainbasierte Kryptowährung erfahren (einschließlich der Frage, was eine Blockchain ist und was das »Krypto« in Kryptowährung bedeutet).

Dieses Thema ist sehr eigenwillig. Bitcoin ist ein sehr wertvolles Anlagegut, aber nicht jeder versteht die Technologie dahinter. Wie kann man in etwas investieren, *das man nicht einmal richtig verstanden hat?* Und lassen Sie sich nicht in die Irre leiten: Die allerwenigsten Menschen, selbst jene, die Bitcoins im Wert von Tausenden von Euros besitzen, wissen, was Bitcoin wirklich ist. Lesen Sie dieses Buch, um nicht mehr zu dieser Gruppe zu gehören!

Wir sind der festen Überzeugung, dass Sie Bitcoin verstehen sollten, wenn Sie sich in irgendeiner Form daran beteiligen wollen. Wenn Sie seine Natur *nicht* verstehen, ergeben sich daraus zwei große Probleme:

- **Tausenden von Bitcoin-Besitzern wurden ihre Bitcoins gestohlen.** Wir erklären, wie es dazu kommt und was Sie dagegen tun können.
- **Tausende von Bitcoin-Besitzern haben ihre Bitcoins »verloren«.** Wir erklären, wie es dazu kommen kann, wie Sie dies vermeiden und warum die Bitcoins nicht *wirklich* verloren sind (sondern Ihnen nur der Zugriff auf sie verwehrt bleibt).

Unsere Aufgabe ist es, das Ganze in gut verständliche, leicht verdauliche Häppchen zu zerlegen, die auch normale Menschen wie Sie nachvollziehen können.

Über dieses Buch

Dieses Buch erklärt, vereinfacht und entmystifiziert die Welt des Bitcoins. Sie erfahren darin alles, was Sie wissen und tun müssen, um für sich eine Entscheidung zu treffen, ob und wie Sie in die wunderbare Welt des Bitcoins einsteigen möchten.

In diesem Buch erklären wir Folgendes:

- ✔ welchen Ursprung Bitcoin hat (und wer ist diese*r ominöse Satoshi Nakamoto?)
- ✔ was Bitcoin eigentlich *ist* (und was *nicht*)
- ✔ die verschiedenen Bitcoin-Einheiten, bis hin zur kleinsten (einem hundertmillionstel Bitcoin)
- ✔ wie Geld funktioniert (Sie denken natürlich, Sie wüssten das, aber *tun Sie das wirklich?*)
- ✔ wie das Krypto in Kryptowährung funktioniert
- ✔ die besten Anlaufstellen, um Bitcoins zu kaufen, und *wie* Sie das anstellen
- ✔ den Umgang mit Ihrer eigenen Krypto-Wallet (nein, das ist nicht der Speicherort Ihrer Bitcoins, aber sie ist dennoch von entscheidender Bedeutung)
- ✔ wie Sie Ihre Bitcoins vor Diebstahl und Verlust schützen
- ✔ wie Sie in Bitcoin (und eventuell auch in andere Kryptowährungen) investieren

Und vieles mehr!

Törichte Annahmen über die Leser

Wir wollen keinerlei Vermutungen anstellen, aber wir müssen davon ausgehen, dass Sie, wenn Sie dieses Buch lesen, bereits ein paar Grundkenntnisse über das Internet haben. Bitcoin ist eine internetbasierte Technologie – kein Internet, kein Bitcoin. Sie müssen also technisch versiert genug sein, um ein Gerät mit Internetzugang zu verwenden, beispielsweise einen Desktop-PC, ein Notebook oder vielleicht auch nur ein Smartphone. Sie müssen in der Lage sein, Websites aufzurufen und Software herunterzuladen und auszuführen (das müssen nicht unbedingt allzu viele Programme sein, vielleicht auch nur eine einfache Krypto-Wallet, die auf Ihrem Smartphone läuft).

Wir erklären, wie Sie Ihr Bitcoin-Guthaben sicher aufbewahren können. Sie müssen also auch in der Lage sein, beispielsweise einen Passwortmanager zu laden, Antivirensoftware zu installieren oder Backups durchzuführen. Das ist weder Raketenwissenschaft noch Gehirnchirurgie, aber wenn Ihre Vorstellung von der Computernutzung darin besteht, Ihr Enkelkind mit einer Internetrecherche zu beauftragen, dann ist dieses Buch vielleicht doch nichts für Sie!

Symbole, die in diesem Buch verwendet werden

Wie alle *Für-Dummies*-Bücher enthält auch dieses Symbole, um bestimmte Absätze hervorzuheben und Sie auf besonders nützliche Informationen hinzuweisen. Hier finden Sie eine Übersicht über die Bedeutung dieser Symbole:


Ein Tipp-Symbol weist auf Zusatzinformationen hin, die Ihnen auf Ihrem Weg helfen oder einen zusätzlichen Einblick in die besprochenen Konzepte geben können.


Das Merke-Symbol weist auf Informationen hin, die Sie sich merken sollten.


Das Techniker-Symbol steht für Fachwissen, das Sie überspringen können, wenn Sie unbedingt möchten. Wenn Sie aber zu den Menschen gehören, die gerne Hintergrundinformationen haben, dann sollten Sie es lesen.


Das Warnsymbol hilft Ihnen, Probleme zu vermeiden. Es soll Ihre Aufmerksamkeit wecken und Sie vor potenziellen Fallstricken bewahren, die Ihrer Investition schaden könnten.

Wie es weitergeht

Wie alle guten Nachschlagewerke, ist auch dieses Buch so konzipiert, dass es bedarfsgerecht gelesen werden kann. Es gliedert sich in mehrere Teile: Hintergrundinformationen über das eigentliche Wesen von Bitcoin, wie Sie Bitcoins tatsächlich nutzen (kaufen, verkaufen und investieren), einige weitere Details über die Funktionsweise der Technologie und den Top-Ten-Teil.

Wir empfehlen Ihnen, das Buch von Anfang bis Ende durchzulesen, aber wenn Sie nur etwas über den Einsatz von Wallets wissen möchten, lesen Sie Kapitel 4. Wenn

Sie wissen wollen, wo Sie Bitcoins kaufen können, lesen Sie Kapitel 3. Wenn Sie einfach nur verstehen wollen, was das »Krypto« in »Kryptowährungen« bedeutet und wie diese funktionieren, sind Sie in Kapitel 2 richtig.

Bitcoin ist ein sehr komplexes Thema. Alle in diesem Buch behandelten Aspekte sind miteinander verknüpft. Wir empfehlen Ihnen daher unbedingt, das gesamte Buch zu lesen, bevor Sie in Bitcoin investieren. Es ist wesentlich, dass Sie alles verstanden haben, bevor Sie anfangen. Machen Sie es nicht wie die Tausenden, die ihre Bitcoins verloren haben. Ein bisschen Wissen kann schon viel bewirken!

Teil I

Bitcoin-Grundlagen

IN DIESEM TEIL ...

- ✔ Den Ursprung von Bitcoin entdecken
- ✔ Verstehen, wie Geld funktioniert
- ✔ Lernen, wie Bitcoin Kryptographie nutzt
- ✔ Nachrichten an die Bitcoin-Blockchain senden
- ✔ Bitcoin-Besitz mittels privater Schlüssel nachweisen

Kapitel 1

Bitcoin in aller Kürze

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

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.