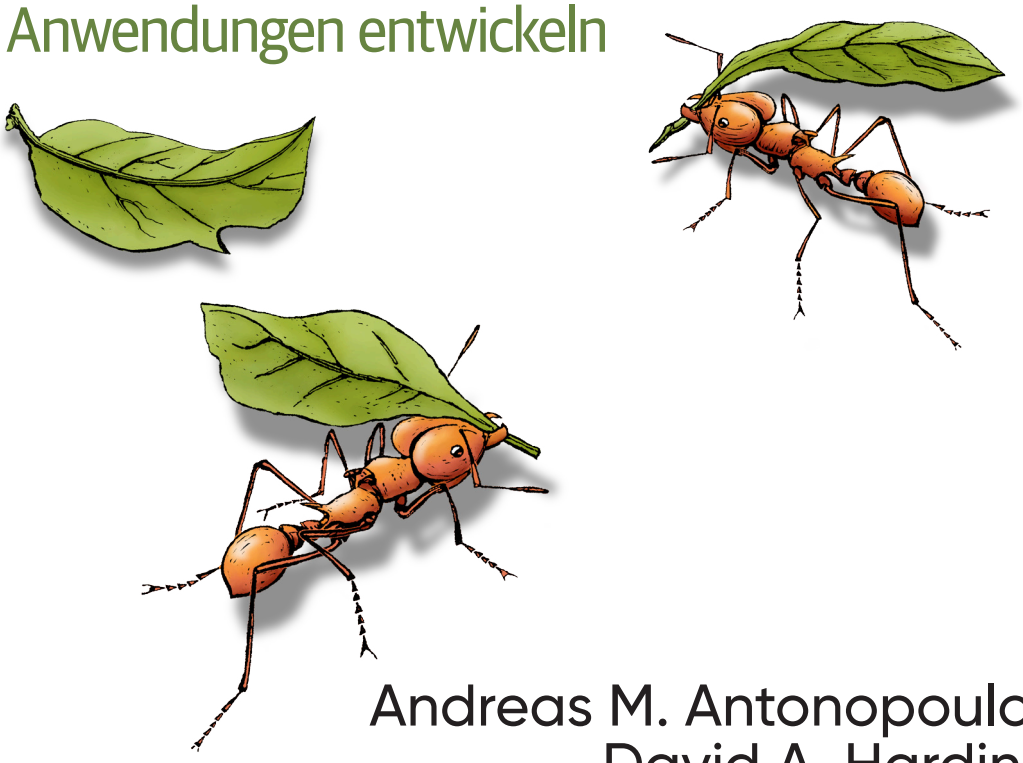
O'REILLY®

Übersetzung der 3. Auflage

Bitcoin

Grundlagen und Programmierung

Die Blockchain verstehen, Bitcoin-Anwendungen entwickeln



Andreas M. Antonopoulos
David A. Harding

Übersetzung von Peter Klicman

Stimmen zum Buch *Bitcoin – Grundlagen und Programmierung*

Bitcoin – Grundlagen und Programmierung ist sehr nützlich für jeden, der die Technologie von Bitcoin und die Konzepte des Protokolls verstehen will oder muss.

– René Pickhardt, Bitcoin Lightning Network Developer

Tauchen Sie in die faszinierende Welt von Bitcoin ein – mit *Bitcoin – Grundlagen und Programmierung*, dem definitiven Leitfaden, der Sie durch die Besonderheiten dieser digitalen Währung navigiert. Ganz gleich, ob Sie Entwickler, Investor oder einfach nur neugierig auf die Zukunft des Geldes sind, dieses umfassende Buch dient Ihnen als Wegweiser, der Ihnen wesentliches Wissen vermittelt und Sie in die Lage versetzt, sicher an der Ära des Internets des Geldes teilzunehmen.

– Jorge Lesmes, Senior Director bei NTT DATA

Fast ein Jahrzehnt nach der erstmaligen Veröffentlichung bestätigt die dritte Auflage von *Bitcoin – Grundlagen und Programmierung*, dass es die erste Anlaufstelle für technische Bitcoin-Lerninhalte ist. Kein anderes Buch ist so umfassend und aktuell.

– Olaoluwa Osuntokun, CTO bei Lightning Labs

Ein umfassender Überblick darüber, was unter der Haube von Bitcoin vor sich geht und wie die Dinge zusammenpassen.

– Mark »Murch« Erhardt, Bitcoin Engineer bei Chaincode Labs

3. Auflage

Bitcoin – Grundlagen und Programmierung

Die Blockchain verstehen,
Bitcoin-Anwendungen entwickeln

Andreas M. Antonopoulos,
David A. Harding

Deutsche Übersetzung von
Peter Klicman

O'REILLY®

Andreas M. Antonopoulos, David A. Harding

Lektorat: Ariane Hesse
Übersetzung: Peter Klicman
Korrektorat: Sibylle Feldmann, *www.richtiger-text.de*
Satz: III-satz, *www.drei-satz.de*
Herstellung: Stefanie Weidner
Umschlaggestaltung: Karen Montgomery, Michael Oréal, *www.oreal.de*

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.

ISBN:
Print 978-3-96009-247-6
PDF 978-3-96010-883-2
ePub 978-3-96010-884-9

3. Auflage 2025

Wieblinger Weg 17
69123 Heidelberg

Authorized German translation of the English edition of Mastering Bitcoin 3E ISBN 9781098150099

Dieses Buch erscheint in Kooperation mit O'Reilly Media, Inc. unter dem Imprint »O'REILLY«.
O'REILLY ist ein Markenzeichen und eine eingetragene Marke von O'Reilly Media, Inc. und wird mit Einwilligung des Eigentümers verwendet.

Schreiben Sie uns:
Falls Sie Anregungen, Wünsche und Kommentare haben, lassen Sie es uns wissen: *kommentar@oreilly.de*.

Inhalt

Vorwort

Ein Bitcoin-Buch schreiben

Ich (Andreas) stolperte Mitte 2011 das erste Mal über Bitcoin. Meine erste Reaktion war mehr oder weniger »Pfft! Nerd-Geld!«, und ich ignorierte es für weitere sechs Monate, ohne seine Bedeutung zu erkennen. Diese Reaktion habe ich bei vielen der klügsten Menschen, die ich kenne, beobachtet, was mich ein bisschen tröstet. Als ich in einer Mailinglistendiskussion das zweite Mal über Bitcoin stolperte, entschied ich mich, das Whitepaper von Satoshi Nakamoto zu lesen, um die maßgebliche Quelle zu studieren und herauszufinden, worum es denn da eigentlich ging. Ich erinnere mich immer noch an den Moment, als ich diese neun Seiten gelesen hatte und begriff, dass Bitcoin nicht einfach eine digitale Währung, sondern ein Vertrauensnetzwerk ist, das die Basis für weit mehr als nur Währungen sein konnte. Die Erkenntnis, dass das »kein Geld, sondern ein dezentralisiertes Vertrauensnetzwerk« ist, schickte mich auf eine viermonatige Reise, in der ich jedes Quäntchen an Informationen über Bitcoin, das ich finden konnte, aufsaugte. Es hatte mich gepackt, und wie besessen verbrachte ich täglich zwölf Stunden und mehr vor dem Bildschirm, in denen ich las, schrieb, programmierte und so viel lernte, wie ich konnte. Nachdem ich aus diesem Zustand wieder erwachte, war ich zehn Kilogramm leichter und hatte mich entschieden, zukünftig an Bitcoin zu arbeiten.

Zwei Jahre später, nachdem ich eine Reihe kleiner Start-ups gegründet hatte, um verschiedene Bitcoin-bezogene Dienste und Produkte zu erforschen, entschied ich, dass es an der Zeit wäre, mein erstes Buch zu schreiben. Bitcoin hatte mich in einen Kreativitätsrausch versetzt und meine Gedanken bestimmt. Das war die aufregendste Technologie, der ich seit Beginn des Internets begegnet war – Zeit also, meine Leidenschaft für diese faszinierende Technologie mit einem breiteren Publikum zu teilen.

Leserkreis

Dieses Buch richtet sich hauptsächlich an Entwicklerinnen und Entwickler. Wenn Sie eine Programmiersprache beherrschen, lehrt Sie dieses Buch, wie kryptografische

Währungen funktionieren, wie man sie nutzt und wie man Software entwickelt, die mit ihnen arbeitet. Die ersten Kapitel eignen sich ebenfalls als ausführliche Einführung in Bitcoin für Nichtprogrammierer, also für diejenigen, die die innere Funktionsweise von Bitcoin und Kryptowährungen verstehen wollen.

Warum sind Ameisen auf dem Cover?

Die Blattschneiderameise ist eine Spezies, die in einem Kolonie-Superorganismus ein hochkomplexes Verhalten zeigt. Doch jede einzelne Ameise agiert nach einem Satz einfacher Regeln, die durch soziale Interaktion und das Ausschütten chemischer Duftstoffe (Pheromone) gesteuert wird. Laut (englischer) Wikipedia bilden Blattschneiderameisen nach dem Menschen die größten und komplexesten Tiergesellschaften. Blattschneiderameisen essen keine Blätter, vielmehr nutzen sie sie, um einen Pilz anzubauen, der die zentrale Futterquelle der Kolonie bildet. Diese Ameisen betreiben also Landwirtschaft!!

Zwar bilden Ameisen eine kastenbasierte Gesellschaft und haben eine Königin, die für den Nachwuchs sorgt, doch es gibt weder eine zentrale Autorität noch einen Anführer. Das hochgradig intelligente und komplexe Verhalten, das eine aus mehreren Millionen Ameisen bestehende Kolonie zeigt, ist eine emergente Eigenschaft der Interaktion von Individuen in einem sozialen Netzwerk.

Die Natur demonstriert, dass ein dezentralisiertes System robust, komplex und unglaublich ausgereift sein kann, ohne eine zentrale Autorität, eine Hierarchie oder komplexe Teile zu benötigen.

Bitcoin ist ein kunstvolles dezentralisiertes Vertrauensnetzwerk, das eine Vielzahl finanzieller Prozesse unterstützen kann. Dennoch folgt jeder Knoten im Bitcoin-Netzwerk nur einigen wenigen einfachen mathematischen Regeln. Die Interaktion zwischen vielen Knoten führt zu diesem ausgeklügelten Verhalten, nicht die Komplexität eines einzelnen Knotens oder das in ihn gesetzte Vertrauen. Wie eine Ameisenkolonie ist das Bitcoin-Netzwerk ein robustes Netzwerk einfacher Knoten, die einfachen Regeln folgen, um erstaunliche Dinge ohne zentrale Koordinierung zu erreichen.

Verwendete Konventionen

Im Buch folgen wir diesen typografischen Konventionen:

Kursivschrift
: Wird für neue Begriffe, URLs, E-Mail-Adressen, Dateinamen und Dateierweiterungen verwendet.

`Nichtproportionalschrift`
: Wird für Programmlistings verwendet. Im normalen Fließtext werden damit Programmelemente wie Variablen- oder Funktionsnamen, Datenbanken, Datentypen, Umgebungsvariablen, Anweisungen und Schlüsselwörter hervorgehoben.

`Nichtproportionalschrift fett`
: Wird für Befehle oder andere Eingaben verwendet, die Sie wortwörtlich eingeben müssen.

`Nichtproportionalschrift kursiv`
: Wird für Text verwendet, der durch benutzereigene oder durch den Kontext bestimmte Werte ersetzt wird.

Tipp
Mit diesem Symbol wird ein Tipp oder ein Vorschlag angezeigt.

Hinweis
Dieses Symbol repräsentiert einen allgemeinen Hinweis.

Warnung
Hiermit wird eine Warnung angezeigt.

Codebeispiele

Alle Code-Snippets können für die meisten Betriebssysteme mit einer minimalen Installation der Compiler und Interpreter für die entsprechenden Sprachen repliziert werden. Wenn nötig, stellen wir grundlegende Installationsanweisungen und schrittweise Beispiele der Ausgaben bereit.

Einige der Code-Snippets wurden für den Druck aufbereitet. In diesen Fällen wurden die Zeilen mit einem Backslash-Zeichen (\) gefolgt von einem Newline-Zeichen getrennt. Wenn Sie mit den Beispielen arbeiten, sollten Sie diese beiden Zeichen entfernen und die Zeilen wieder zusammenfassen. Die Ergebnisse sollten dann denen der Beispiele entsprechen.

Alle Code-Snippets verwenden wann immer möglich reale Werte und Berechnungen. Sie können sich also von Beispiel zu Beispiel vorarbeiten und kommen immer zu den gleichen Ergebnissen wie das Buch.

Verwendung der Codebeispiele

Dieses Buch ist dazu gedacht, Ihnen bei der Erledigung Ihrer Arbeit zu helfen. Im Allgemeinen dürfen Sie den Code in diesem Buch in Ihren eigenen Programmen oder Dokumentationen verwenden. Solange Sie den Code nicht in großem Umfang reproduzieren, brauchen Sie uns nicht um Erlaubnis zu bitten. Zum Beispiel benötigen

Sie nicht unsere Erlaubnis, wenn Sie ein Programm unter Zuhilfenahme mehrerer Codestücke aus diesem Buch schreiben. Eine Frage mit einem Zitat oder einem Codebeispiel aus dem Buch zu beantworten, erfordert ebenfalls keine Genehmigung. Signifikante Teile des Beispielcodes aus dem Buch für die eigene Produktdokumentation zu verwerten, ist dagegen genehmigungspflichtig.

Wir freuen uns über eine Quellenangabe, verlangen sie aber nicht unbedingt. Zu einer Quellenangabe gehören normalerweise Autor, Titel, Verlagsangabe, Veröffentlichungsjahr und ISBN, hier also: »Andreas M. Antonopoulos und David A. Harding, *Mastering Bitcoin*, O'Reilly Media, Inc. 2024, ISBN 978-1098150099.

Einige Auflagen dieses Buchs werden unter einer Open-Source-Lizenz wie CC-BY-NC (*https://oreil.ly/RzUHE*) angeboten. In diesem Fall gelten die Bedingungen dieser Lizenz.

Sollten Sie befürchten, dass Ihre Verwendung der Codebeispiele gegen das Fairnessprinzip oder die Genehmigungspflicht verstoßen könnte, nehmen Sie bitte unter *permissions@oreilly.com* Kontakt mit O'Reilly Media, Inc. auf.

Neuerungen der dritten Auflage

Die dritte Auflage konzentriert sich auf die Aktualisierung des Texts der zweiten Auflage aus dem Jahr 2017 sowie der aus der ersten Auflage von 2014 verbliebenen Inhalte. Zusätzlich wurden viele Konzepte ergänzt, die für die Bitcoin-Entwicklung im Jahr 2023 von Bedeutung waren:

Kapitel 4
: Wir haben die Adressinfo neu organisiert, sodass alles in der historischen Reihenfolge durchgegangen werden kann. Wir haben einen neuen Abschnitt zu P2PK hinzugefügt (wo »Adresse« eine »IP-Adresse« war), die Abschnitte zu P2PKH und P2SH überarbeitet und Abschnitte zu Segwit/Bech32 und Taproot/Bech32m ergänzt.

Kapitel 6 und Kapitel 7
: Der Text der alten Kapitel 6, »Transaktionen«, und Kapitel 7, »Transaktionen und Skripting für Fortgeschrittene«, wurde in vier Kapiteln neu organisiert: Kapitel 6 (Transaktionen), Kapitel 7 (»Autorisierung und Authentifizierung«), Kapitel 8 (»Digitale Signaturen«) und Kapitel 9 (»Transaktionsgebühren«).

Kapitel 6
: Ein fast vollständig neuer Text beschreibt die Struktur einer Transaktion.

Kapitel 7
: Wir haben Text zu MAST, P2C, skriptlosen Multisignaturen, Taproot und Tapscript ergänzt.

Kapitel 8
: Der Text zu ECDSA wurde überarbeitet, und Text zu Schnorr-Signaturen wurde ergänzt.

Kapitel 9
: Der Text zu Gebühren, RBF- und CPFP-Fee-Bumping, Transaktions-Pinning, Paketweiterleitung (Package Relay) und CPFP-Carve-out wurde fast vollständig neu geschrieben.

Kapitel 10
: Wir haben Text zu Compact Block Relay hinzugefügt, Bloomfilter überarbeitet, um deren Probleme mit der Privatsphäre besser zu beschreiben, und Text zu kompakten Blockfiltern ergänzt.

Kapitel 11
: Text zu Signet ergänzt.

Kapitel 12
: Text zu BIP8 und Speedy Trial ergänzt.

Anhänge
: Bibliotheksspezifische Anhänge wurden entfernt. Auf den Anhang mit dem Original-Whitepaper folgt nun ein Anhang, der beschreibt, wie sich die Implementierung und die Eigenschaften von Bitcoin vom Whitepaper unterscheiden.

Bitcoin-Adressen und -Transaktionen in diesem Buch

Die Bitcoin-Adressen, Transaktionen, Schlüssel, QR-Codes und Blockchain-Daten in diesem Buch sind größtenteils real. Das bedeutet, dass Sie die Blockchain durchgehen und den größten Teil real nachverfolgen können. Sie können also die Blockchain durchsuchen, sich die in den Beispielen enthaltenen Transaktionen genau ansehen, sie mit Ihren eigenen Skripten/Programmen abrufen und so weiter.

Beachten Sie aber, dass die in diesem Buch zur Generierung von Adressen verwendeten privaten Schlüssel entweder in diesem Buch abgedruckt oder »verbrannt« wurden. Wenn Sie also Geld an diese Adressen senden, ist es für immer verloren, oder es kann von jedem abgeschöpft werden, der die hier abgedruckten privaten Schlüssel kennt.

Bitte senden Sie keinesfalls Geld an irgendeine der in diesem Buch verwendeten Adressen. Ihr Geld landet bei einem anderen Leser oder ist für immer verloren.

Die Autoren kontaktieren

Sie erreichen Andreas M. Antonopoulos über seine persönliche Website: *https://antonopoulos.com*.

Folgen Sie Andreas auf Facebook: *https://facebook.com/AndreasMAntonopoulos*.

Twitter-Account von Andreas (eingestellt): *https://twitter.com/aantonop*.

Folgen Sie Andreas auf LinkedIn: *https://linkedin.com/company/aantonop*.

Herzlichen Dank an die Förderer von Andreas, die seine Arbeit durch monatliche Spenden unterstützen. Seine Patreon-Seite finden Sie hier: *https://patreon.com/aantonop*.

Informationen zu *Mastering Bitcoin*, zur Open Edition und Übersetzungen finden Sie hier: *https://bitcoinbook.info*.

Sie erreichen David A. Harding über seine persönliche Website: *https://dtrt.org*.

Danksagungen der ersten und zweiten Auflage

Von Andreas M. Antonopoulos

Dieses Buch spiegelt die Bemühungen und Beiträge vieler Menschen wider. Ich bin sehr dankbar für die Hilfe, die ich von Freunden, Kollegen, aber auch völlig Fremden erhalten habe, die mich dabei unterstützt haben, diesen technischen Leitfaden zu Kryptowährungen und Bitcoin zu schreiben.

Es ist unmöglich, zwischen der Bitcoin-Technologie und der Bitcoin-Community zu unterscheiden, und dieses Buch ist ebenso ein Produkt dieser Community wie ein Buch über die Technologie. Meine Arbeit an diesem Buch wurde vom Anfang bis zum Ende von der Community befürwortet, angefeuert und unterstützt. Neben vielem anderen ermöglichte mir dieses Buch, über zwei Jahre Teil dieser wundervollen Community zu sein, und ich bin mehr als dankbar, in dieser Community akzeptiert worden zu sein. Eine große Menge an Menschen haben das Buch beeinflusst, und es sind viel zu viele, um sie beim Namen zu nennen. Es sind Menschen, die ich auf Konferenzen, Events, Seminaren, Meet-ups, beim Pizza-Plausch oder bei privaten Treffen kennengelernt habe, ebenso wie bei Twitter, auf reddit, bitcointalk.org und GitHub. Jede Idee, Analogie, Frage, Antwort und Erläuterung in diesem Buch wurde an irgendeinem Punkt durch die Community inspiriert, getestet und verbessert. Ich danke euch allen für die Unterstützung. Ohne euch hätte es dieses Buch nie gegeben, und ich bin euch für immer dankbar.

Der Weg zum Autor begann natürlich lange vor dem ersten Buch. Meine erste Sprache war Griechisch (und damit war auch mein erster Unterricht in Griechisch). Deshalb belegte ich im ersten Jahr an der Universität einen Schreibkurs. Ich danke meiner damaligen Lehrerin Diana Kordas, die mir in diesem Jahr dabei half, Selbstvertrauen und Fertigkeiten zu sammeln. Später schrieb ich für das *Network World Magazine* und entwickelte meine Fertigkeiten als technischer Autor im Bereich Data Center. Ich danke John Dix und John Gallant, die mir meinen ersten Job als Kolumnist bei *Network World* gaben, sowie meinem Lektor Michael Cooney und meinem Kollegen Johna Till Johnson, die meine Kolumnen lektorierten und für eine Veröffentlichung aufbereiteten. Vier Jahre lang 500 Wörter pro Woche zu schreiben, sorgten für ausreichend Erfahrung, um ernsthaft über ein Dasein als Autor nachzudenken.

Vielen Dank auch an diejenigen, die mich unterstützten, nachdem ich meinen Buchvorschlag bei O'Reilly eingereicht hatte, indem sie Empfehlungen aussprachen und

sich den Entwurf genauer ansahen. Mein Dank geht an John Gallant, Gregory Ness, Richard Stiennon, Joel Snyder, Adam B. Levine, Sandra Gittlen, John Dix, Johna Till Johnson, Roger Ver und Jon Matonis. Besonderer Dank geht an Richard Kagan und Tymon Mattoszko, die frühe Fassungen prüften, und an Matthew Taylor, der diese Fassung lektorierte.

Dank an Cricket Liu, Autor des O'Reilly-Titels *DNS and BIND*, der mich bei O'Reilly vorgestellt hat. Ein Dank auch an Michael Loukides und Allyson MacDonald von O'Reilly, die Monate daran arbeiteten, dass dieses Buch Wirklichkeit wurde. Allyson war besonders aufmerksam, wenn Abgabefristen verstrichen und Ergebnisse fehlten. Bei der zweiten Ausgabe gab Timothy McGovern die Richtung vor, Kim Cofer übernahm das Lektorat, und Rebecca Panzer sorgte für viele neue Diagramme.

Die ersten Entwürfe der ersten Kapitel waren die schwersten, schlicht weil Bitcoin ein kompliziertes Thema ist. Sobald ich einen Aspekt herauspickte, musste ich direkt schon wieder das große Ganze betrachten. Wiederholt blieb ich hängen und war frustriert, wenn ich versuchte, ein Thema leicht verständlich rüberzubringen, indem ich eine Geschichte um ein schwieriges technisches Thema herum erzählen wollte. Letztendlich entschied ich mich dafür, die Geschichte des Bitcoins über die Geschichten derjenigen zu erzählen, die Bitcoins nutzen. Das Buch zu schreiben, wurde dadurch erheblich einfacher. Ich schulde meinem Freund und Mentor Richard Kagan Dank, der mir dabei half, die Geschichte zu entwirren und meine Schreibblockaden zu überwinden. Ich danke Pamela Morgan, die frühe Fassungen jedes Kapitels der ersten und zweiten Auflage Korrektur las und die richtigen Fragen stellte. Mein Dank geht auch an die Entwickler der »San Francisco Bitcoin Developers Meetup«-Gruppe sowie an Taariq Lewis und Denise Terry, die dabei halfen, das frühe Material zu testen. Dank ebenfalls an Andrew Naugler für den Entwurf der Infografiken.

Während ich das Buch schrieb, machte ich frühe Fassungen auf GitHub verfügbar und lud dazu ein, diese zu kommentieren. Über 100 Kommentare, Vorschläge, Korrekturen und Beiträge sind daraufhin eingegangen. Für diese Beiträge bedanke ich mich explizit in »Early Release Draft (GitHub-Beiträge)« auf Seite 23. Zuallererst gilt mein Dank meinen freiwilligen GitHub-Lektoren Ming T. Nguyen (erste Auflage) und Will Binns (zweite Auflage), die auf GitHub unermüdlich Pull-Requests kuratiert, verwaltet und aufgelöst, Reports veröffentlicht und Bug-Fixes vorgenommen haben.

Sobald die erste Fassung stand, wurde sie mehrfach von technischen Korrektoren überarbeitet. Vielen Dank an Cricket Liu und Lorne Lantz für deren sorgfältiges Korrekturlesen sowie ihre Kommentare und die Unterstützung.

Verschiedene Bitcoin-Entwickler steuerten Codebeispiele, Korrekturen und Kommentare bei. Dank an Amir Taaki und Eric Voskuil für Beispielcode und viele gute Kommentare, Chris Kleeschulte für den Bitcore-Anhang, Vitalik Buterin und Richard Kiss für Codebeiträge und ihre Hilfe bei der Mathematik elliptischer Kurven, Gavin Andresen für Korrekturen und Kommentare, Michalis Kargakis für Kom-

mentare und Beiträge sowie Robin Inge für die Fehlerkorrektur der zweiten Auflage. Auch bei der zweiten Auflage erhielt ich wieder Hilfe von vielen Bitcoin-Core-Entwicklern, darunter Eric Lombrozo, der Segregated Witness entmystifizierte, Luke Dashjr, der mir beim Kapitel über Transaktionen half, Johnson Lau, der (unter anderem) das Kapitel zu Segregated Witness Korrektur las, und viele andere. Ich danke Joseph Poon, Tadge Dryja und Olaoluwa Osuntokun, die mir das Lightning Network erklärten, meinen Text Korrektur lasen und Fragen beantworteten, wenn ich nicht weiterkam.

Meine Liebe für Wörter und Bücher verdanke ich meiner Mutter Theresa, die mich in einem Haus aufzog, in dem Bücher jede Wand mit Beschlag belegten. Meine Mutter kaufte mir 1982 auch meinen ersten Computer, obwohl sie sich selbst als technophob beschrieb. Mein Vater Menelaos, ein Bauingenieur, der sein erstes Buch im Alter von 80 Jahren veröffentlichte, lehrte mich logisches und analytisches Denken und schürte meine Vorliebe für Wissenschaft und Technik.

Ich danke euch allen für eure Unterstützung während meiner Reise.

Danksagungen zur dritten Auflage

Von David A. Harding

Die Einführung in das nicht interaktive Schnorr-Signaturprotokoll in »Schnorr-Signaturen« auf Seite 209, die mit der Beschreibung des interaktiven Schnorr-Identitätsprotokolls beginnt, wurde stark von der Einführung in das Thema in »Borrommean Ring Signatures« (2015) von Gregory Maxwell und Andrew Poelstra beeinflusst. Ich stehe tief in beider Schuld für die Hilfe, die sie mir über die letzte Dekade hinweg gewährt haben.

Wertvolle technische Reviews früher Fassungen dieses Manuskripts kamen von Jorge Lesmes, Olaoluwa Osuntokun, René Pickhardt und Mark »Murch« Erhardt. Insbesondere Murchs ausführliches und aufschlussreiches Review und seine Bereitschaft, mehrere Versionen desselben Texts zu beurteilen, haben die Qualität dieses Buchs weit über meine Erwartungen hinaus verbessert.

Ich schulde auch Jimmy Song meinen Dank, der mich für dieses Projekt vorgeschlagen hat, meinem Mitautor Andreas, dass ich diesen Bestseller aktualisieren durfte, Angela Rufino, die mich durch den Prozess der Autorschaft bei O'Reilly geleitet hat, sowie allen anderen Mitarbeitenden bei O'Reilly, die das Schreiben der dritten Auflage zu einer angenehmen und produktiven Erfahrung gemacht haben.

Ich weiß nicht, wie ich all den Bitcoin-Beitragenden danken soll, die mir auf meinem Weg geholfen haben – sei es bei der Entwicklung der von mir genutzten Software oder dabei, mir beizubringen, wie sie funktioniert, und mir zu helfen, mein bisschen Wissen weiterzugeben. Es sind zu viele, um ihre Namen aufzuführen, doch ich denke oft an sie und weiß, dass mein Beitrag zu diesem Buch ohne all das, was sie für mich getan haben, nicht möglich gewesen wäre.

Early Release Draft (GitHub-Beiträge)

Viele Beitragende lieferten Kommentare, Korrekturen und Ergänzungen zum Early Release Draft auf GitHub. Ich danke euch allen für euren Beitrag zu diesem Buch.

Nachfolgend eine Liste wichtiger GitHub-Beitragender mit deren GitHub-IDs in Klammern:

- Abdussamad Abdurrazzaq (AbdussamadA)
- Adán SDPC (aesedepece)
- Akira Chiku (achiku)
- Alex Waters (alexwaters)
- Andrew Donald Kennedy (grkvlt)
- Andrey Esaulov (andremaha)
- andronoob
- AnejaBK
- Appaji (CITIZENDOT)
- ariesunny
- Arthur O'Dwyer (Quuxplusone)
- bargitta
- Basem Alasi (Bamskki)
- bisqfan
- bitcoinctf
- blip151
- Bryan Gmyrek (physicsdude)
- Carlos Sims (simsbluebox)
- Casey Flynn (cflynn07)
- cclauss
- Chapman Shoop (belovachap)
- chrisd95
- Christie D'Anna (avocadobreath)
- Cihat Imamoglu (cihati)
- Cody Scott (Siecje)
- coinradar
- Cragin Godley (cgodley)
- Craig Dodd (cdodd)
- dallyshalla
- Dan Nolan (Dan-Nolan)
- Dan Raviv (danra)
- Darius Kramer (dkrmr)
- Darko Janković (trulex)
- David Huie (DavidHuie)
- didongke
- Diego Viola (diegoviola)
- Dimitris Tsapakidis (dimitris-t)
- Dirk Jäckel (biafra23)
- Dmitry Marakasov (AMDmi3)
- drakos (Jolly-Pirate)
- drstrangeM
- Ed Eykholt (edeykholt)
- Ed Leafe (EdLeafe)
- Edward Posnak (edposnak)
- Elias Rodrigues (elias19r)
- Eric Voskuil (evoskuil)
- Eric Winchell (winchell)
- Erik Wahlström (erikwam)
- effectsToCause (vericoin)
- Esteban Ordano (eordano)
- ethers
- Evlix
- fabienhinault
- Fan (whiteath)
- Felix Filozov (ffilozov)
- Francis Ballares (fballares)
- François Wirion (wirion)
- Frank Höger (francyi)
- Gabriel Montes (gabmontes)
- Gaurav Rana (bitcoinsSG)
- genjix

- Geremia
- Gerry Smith (Hermetic)
- gmr81
- Greg (in3rsha)
- Gregory Trubetskoy (grisha)
- Gus (netpoe)
- halseth
- harelw
- Harry Moreno (morenoh149)
- Hennadii Stepanov (hebasto)
- Holger Schinzel (schinzelh)
- Ioannis Cherouvim (cherouvim)
- Ish Ot Jr. (ishotjr)
- ivangreene
- James Addison (jayaddison)
- Jameson Lopp (jlopp)
- Jason Bisterfeldt (jbisterfeldt)
- Javier Rojas (fjrojasgarcia)
- Jordan Baczuk (JBaczuk)
- Jeremy Bokobza (bokobza)
- JerJohn15
- jerzybrzoska
- Jimmy DeSilva (jimmydesilva)
- Jo Wo (jowo-io)
- Joe Bauers (joebauers)
- joflynn
- Johnson Lau (jl2012)
- Jonathan Cross (jonathancross)
- Jorgeminator
- jwbats
- Kai Bakker (kaibakker)
- kollokollo
- krupawan5618
- kynnjo
- Liangzx
- lightningnetworkstores
- lilianrambu
- Liu Yue (lyhistory)
- Lobbelt
- Lucas Betschart (lclc)
- Matt Wesley (MatthewWesley)
- Magomed Aliev (30mb1)
- Mai-Hsuan Chia (mhchia)
- Marco Falke (MarcoFalke)
- María Martín (mmartinbar)
- Marcus Kiisa (mkiisa)
- Mark Erhardt (Xekyo)
- Mark Pors (pors)
- Martin Harrigan (harrigan)
- Martin Vseticka (MartyIX)
- Marzig (marzig76)
- Matt McGivney (mattmcgiv)
- Matthijs Roelink (Matthiti)
- Maximilian Reichel (phramz)
- MG-ng (MG-ng)
- Michalis Kargakis (kargakis)
- Michael C. Ippolito (michaelcippolito)
- Michael Galero (mikong)
- Michael Newman (michaelbnewman)
- Mihail Russu (MihailRussu)
- mikew (mikew)
- milansismanovic
- Minh T. Nguyen (enderminh)
- montvid
- Morfies (morfies)
- Nagaraj Hubli (nagarajhubli)
- Nekomata (nekomata-3)
- nekonenene
- Nhan Vu (jobnomade)
- Nicholas Chen (nickycutesc)

- Ning Shang (syncom)
- Oge Nnadi (ogennadi)
- Oliver Maerz (OliverMaerz)
- Omar Boukli-Hacene (oboukli)
- Óscar Nájera (Titan-C)
- Parzival (Parz-val)
- Paul Desmond Parker (sunwu-konga)
- Philipp Gille (philippgille)
- ratijas
- rating89us
- Raul Siles (raulsiles)
- Reproducibility Matters (TheCharlatan)
- Reuben Thomas (rrthomas)
- Robert Furse (Rfurse)
- Roberto Mannai (robermann)
- Richard Kiss (richardkiss)
- rszheng
- Ruben Alexander (hizzvizz)
- Sam Ritchie (sritchie)
- Samir Sadek (netsamir)
- Sandro Conforto (sandroconforto)
- Sanjay Sanathanan (sanjays95)
- Sebastian Falbesoner (theStack)
- Sergei Tikhomirov (s-tikhomirov)
- Sergej Kotliar (ziggamon)
- Seiichi Uchida (topecongiro)
- shaysw
- Simon de la Rouviere (simondlr)
- simone-cominato
- sindhoor7
- Stacie (staciewaleyko)
- Stephan Oeste (Emzy)
- Stéphane Roche (Janaka-Steph)
- takaya-imai
- Thiago Arrais (thiagoarrais)
- Thomas Kerin (afk11)
- Tochi Obudulu (tochicool)
- Tosin (tkuye)
- Vasil Dimov (vasild)
- venzen
- Vlad Stan (motorina0)
- Vijay Chavda (VijayChavda)
- Vincent Déniel (vincentdnl)
- weinim
- wenxiaolong (QingShiLuoGu)
- wenzhenxiang
- Will Binns (wbnns)
- wintercooled
- wjx
- wll2007
- Wojciech Langiewicz (wlk)
- Yancy Ribbens (yancyribbens)
- yjjnls
- Yoshimasa Tanabe (emag)
- yuntai
- yurigeorgiev4
- Zheng Jia (zhengjia)
- Zhou Liang (zhouguoguo)

KAPITEL 1
Einführung

Bitcoin ist eine Sammlung von Konzepten und Technologien, die ein Ökosystem für digitales Geld bilden. Währungseinheiten namens Bitcoin werden genutzt, um Werte zu speichern und sie zwischen den Teilnehmenden des Bitcoin-Netzwerks zu übertragen. Bitcoin-Nutzerinnen und -Nutzer kommunizieren miteinander über das Bitcoin-Protokoll. Das geschieht hauptsächlich über das Internet, andere Transportprotokolle sind aber auch möglich. Der Bitcoin-Protokollstack steht als Open-Source-Software zur Verfügung und ist auf einer Vielzahl von Geräten (einschließlich Laptops und Smartphones) lauffähig, d.h., der Zugang zu dieser Technik gestaltet sich einfach.

Nutzer können Bitcoin über das Netzwerk transferieren und damit das tun, was man auch mit normalem Geld macht: Güter kaufen und verkaufen, Geld an Menschen oder Organisationen überweisen oder jemandem einen Kredit gewähren. Bitcoin kann an speziellen Börsen gekauft, verkauft und gegen andere Währungen getauscht werden. Bitcoin ist in gewissem Sinn das perfekte Geld für das Internet, da es schnell und sicher ist und keine Grenzen kennt.

Im Gegensatz zu traditionellen Währungen ist Bitcoin vollständig virtuell. Es gibt keine Münzen im herkömmlichen Sinn und auch keine digitalen Münzen. Die Münzen (also die Coins) sind in Transaktionen enthalten, die Werte vom Sender zum Empfänger transferieren. Bitcoin-Nutzer verfügen über Schlüssel, die den Besitz von Bitcoins im Bitcoin-Netzwerk nachweisen. Mit diesen Schlüsseln können sie Transaktionen signieren, um den Betrag freizugeben und an einen neuen Eigentümer zu transferieren. Die Schlüssel werden häufig in einer digitalen Geldbörse (der Wallet) auf dem Computer oder Smartphone des Nutzers gespeichert. Der Besitz des Schlüssels, mit dem eine Transaktion signiert werden kann, ist die einzige Voraussetzung, um Bitcoins auszugeben, d.h., die Kontrolle liegt vollständig in den Händen der Nutzenden.

Bitcoin ist ein verteiltes Peer-to-Peer-System. Daher gibt es keinen »zentralen« Server oder Kontrollpunkt. Bitcoins werden in einem als Mining bezeichneten Prozess erzeugt, bei dem darum gerungen wird, wer als Erster die Lösung eines mathematischen Problems findet, während die Bitcoin-Transaktionen verarbeitet werden. Jeder Teilnehmer am Bitcoin-Netzwerk (d.h. jeder, auf dessen Gerät der vollständige

Bitcoin-Protokollstack läuft) kann als Miner fungieren und die Rechenleistung seines Computers nutzen, um Transaktionen zu verifizieren und festzuhalten. Im Schnitt ist alle zehn Minuten jemand in der Lage, die Transaktionen der letzten zehn Minuten zu verifizieren, und wird dafür mit neuen Bitcoins belohnt. Im Grunde dezentralisiert das Mining die Geldausgabe und die Abrechnung (das Clearing), wodurch eine Zentralbank überflüssig wird.

Das Bitcoin-Protokoll enthält fest eingebaute Algorithmen, die die Mining-Funktion innerhalb des Netzwerks regeln. Der Schwierigkeitsgrad (die *Difficulty*) der Rechenaufgabe, die die Miner lösen müssen, wird dynamisch so angepasst, dass im Durchschnitt alle zehn Minuten jemand erfolgreich ist, und zwar unabhängig davon, wie viele Miner (und wie viel Rechenleistung) gerade an der Lösung arbeiten. Das Protokoll halbiert alle vier Jahre die Geschwindigkeit, mit der neue Bitcoins erzeugt werden, und beschränkt die Gesamtzahl der Bitcoins auf etwas unter 21 Millionen. Das führt dazu, dass die im Umlauf befindlichen Bitcoins einer einfach vorhersagbaren Kurve folgen, nach der die 21 Millionen im Jahr 2140 erreicht werden. Ungefähr bei Block 1.411.200, der um das Jahr 2035 erzeugt wird, werden 99% aller jemals existierenden Bitcoins erzeugt worden sein. Durch die sinkende Geschwindigkeit der Ausgabe ist die Währung Bitcoin auf lange Sicht deflationär. Darüber hinaus kann der Bitcoin nicht »aufgeblasen« werden, indem man neue Coins über oder unter der erwarteten Ausgaberate »druckt«.

Hinter den Kulissen ist Bitcoin auch der Name eines Protokolls, eines Peer-to-Peer-Netzwerks und einer Innovation in Sachen *Distributed Computing*. Tatsächlich ist die Währung Bitcoin nur die erste Anwendung dieser innovativen Technik. Bitcoin repräsentiert den Höhepunkt jahrzehntelanger Forschung zu den Themen Kryptografie und verteilte Systeme. Die Technik fasst vier Schlüsselinnovationen in einer einmaligen und leistungsfähigen Kombination zusammen. Bitcoin besteht aus:

- einem dezentralisierten Peer-to-Peer-Netzwerk (dem Bitcoin-Protokoll),
- einem öffentlichen Kassenbuch (der Blockchain),
- einer Reihe von Regeln für die unabhängige Validierung von Transaktionen und die Geldausgabe (Konsensregeln) sowie
- einem Mechanismus, mit dem ein globaler, dezentralisierter Konsens zur jeweils gültigen Blockchain erreicht wird (Proof-of-Work-Algorithmus).

Als Entwickler sehe ich Bitcoin als eine Art Internet des Geldes – als Netzwerk für die Verteilung von Werten und die Sicherung des Eigentums an digitalen Vermögenswerten mithilfe verteilter Berechnungen. Hinter Bitcoin steht viel mehr, als es auf den ersten Blick scheint.

In diesem Kapitel wollen wir einige der wesentlichen Konzepte und Begriffe erläutern, uns die notwendige Software beschaffen und Bitcoin für einfache Transaktionen nutzen. In den folgenden Kapiteln sehen wir uns dann schrittweise die tieferen Schichten der Technik an, die Bitcoin möglich machen, und untersuchen das Innenleben des Bitcoin-Netzwerks und -Protokolls.

Digitale Währungen vor Bitcoin

Das Aufkommen brauchbarer digitaler Währung ist eng mit den Entwicklungen in der Kryptografie verknüpft. Das ist nicht weiter überraschend, wenn man die Herausforderungen betrachtet, vor denen man steht, wenn man Bits nutzt, um Werte zu repräsentieren, die gegen Güter und Dienste getauscht werden können. Für jeden, der digitales Geld akzeptiert, stellen sich drei grundlegende Fragen:

- Kann ich sicher sein, dass das Geld echt und nicht gefälscht ist?
- Kann ich sicher sein, dass digitales Geld nur einmal ausgegeben werden kann (das sogenannte *Double-Spending-Problem*)?
- Kann ich sicher sein, dass niemand außer mir dieses Geld für sich beansprucht?

Die Herausgeber von Papiergeld bekämpfen das Fälschungsproblem mit immer ausgefeilteren Papieren und anspruchsvoller Drucktechnik. Physikalisches Geld verhindert das Problem des doppelten Ausgebens ganz einfach, weil eine Banknote nicht an zwei Orten gleichzeitig sein kann. Natürlich wird konventionelles Geld häufig digital gespeichert und überwiesen. In diesen Fällen werden Fälschungen und Double Spending verhindert, indem alle elektronischen Transaktionen durch zentrale Instanzen verarbeitet werden, die eine globale Übersicht über alle im Umlauf befindlichen Währungen haben. Bei digitalem Geld, das nicht auf esoterische Tinten oder Hologramme zurückgreifen kann, bildet Kryptografie die Basis für das Vertrauen in die Legitimität eines Besitzanspruchs. Insbesondere kryptografische digitale Signaturen ermöglichen einem Nutzer, ein digitales Gut oder eine Transaktion zu signieren und so das Eigentum an diesem Gut zu beweisen. Mit der richtigen Architektur können digitale Signaturen auch verwendet werden, um das Double-Spending-Problem in den Griff zu bekommen.

Als die Kryptografie in den späten 1980ern einer breiteren Masse zur Verfügung stand und besser verstanden wurde, versuchten viele Forschende, Kryptografie zum Aufbau digitaler Währungen zu nutzen. Diese frühen Projekte gaben digitales Geld heraus, das durch eine nationale Währung oder ein Edelmetall wie Gold gedeckt war.

Zwar funktionierten diese frühen digitalen Währungen, doch sie waren zentralisiert und dementsprechend von Regierungen und Hackern einfach anzugreifen. Frühe digitale Währungen nutzten (genau wie das traditionelle Bankensystem) eine zentrale Abrechnungsstelle, um alle Transaktionen in regelmäßigen Intervallen abzuwickeln. Leider gerieten die meisten dieser aufstrebenden digitalen Währungen ins Visier besorgter Regierungen und wurden letztendlich auf dem Rechtsweg aus dem Weg geschafft. Einige gingen spektakulär unter, als das Mutterunternehmen unvermittelt abgewickelt wurde. Um gegen Interventionen durch Antagonisten gewappnet zu sein, war eine *dezentralisierte* digitale Währung nötig, um einen zentralen Angriffspunkt zu vermeiden. Bitcoin ist ein solches System, es wurde bereits von Grund auf dezentralisiert entworfen. Es kommt vollständig ohne zentrale Autorität und ohne eine zentrale Kontrollstelle aus, die angegriffen oder geschädigt werden könnte.

Geschichte des Bitcoins

Bitcoin wurde 2008 erstmals beschrieben in einem Papier mit dem Titel »Bitcoin: A Peer-to-Peer Electronic Cash System«[1], das unter dem Pseudonym Satoshi Nakamoto veröffentlicht worden war. Nakamoto kombinierte verschiedene frühere Erfindungen wie digitale Signaturen und Hashcash, um ein vollständig dezentralisiertes Electronic-Cash-System zu entwickeln, das völlig unabhängig war von einer zentralen Instanz für Geldausgabe und Abrechnung sowie die Validierung von Transaktionen. Die Kerninnovation war die Nutzung eines verteilten Rechensystems (das als *Proof-of-Work-Algorithmus* bezeichnet wird), um alle zehn Minuten eine globale »Wahl« durchzuführen, die dem dezentralisierten Netzwerk zu einem *Konsens* über den Zustand der Transaktionen verhilft. Das löst auf elegante Weise das Double-Spending-Problem, bei dem eine einzelne Währungseinheit zweimal ausgegeben werden kann. Bis dahin war das Double-Spending-Problem eine Schwäche digitaler Währungen, die dadurch gelöst wurde, dass alle Transaktionen über eine zentrale Abrechnungsstelle verarbeitet wurden.

Das Bitcoin-Netzwerk startete 2009 basierend auf einer Referenzimplementierung von Nakamoto, die seitdem von vielen anderen Programmierern überarbeitet wurde. Anzahl und Leistung der den Proof-of-Work-Algorithmus ausführenden Maschinen (*Mining*), die für die Sicherheit und Belastbarkeit des Bitcoins sorgt, ist exponentiell angestiegen und übertrifft mittlerweile die kombinierte Rechenleistung der Top-Supercomputer auf der Welt. Satoshi Nakamoto zog sich im April 2011 zurück und übergab die Verantwortung für die Entwicklung des Codes und des Netzwerks an eine Gruppe von Freiwilligen. Die Identität der Person oder Personen hinter Bitcoin ist bisher nicht bekannt. Ungeachtet dessen kontrolliert weder Satoshi Nakamoto noch irgendwer sonst das Bitcoin-System. Es arbeitet auf vollständig transparenten mathematischen Prinzipien, Open-Source-Code und dem Konsens zwischen den Teilnehmenden. Diese Erfindung ist für sich genommen schon bahnbrechend und hat bereits zu neuen Forschungen in den Bereichen Distributed Computing, Wirtschaftswissenschaften und Ökonometrie geführt.

Eine Lösung für ein Distributed-Computing-Problem

Satoshi Nakamotos Erfindung liefert auch eine praktische und neue Lösung für ein Problem des Distributed Computing, das als »Problem der byzantinischen Generäle« bekannt ist. Kurz gefasst, besteht das Problem darin, sich über das Vorgehen oder den Zustand eines Systems zu einigen, in dem Informationen über ein unzuverlässiges und möglicherweise kompromittiertes Netzwerk ausgetauscht werden. Satoshi Nakamotos Lösung, die das Proof-of-Work-Konzept nutzt, um einen Konsens *ohne eine zentrale vertrauenswürdige Instanz* zu erzielen, stellt einen Bruch für das Distributed Computing dar.

1 »Bitcoin: A Peer-to-Peer Electronic Cash System« (*https://oreil.ly/KUaBM*)