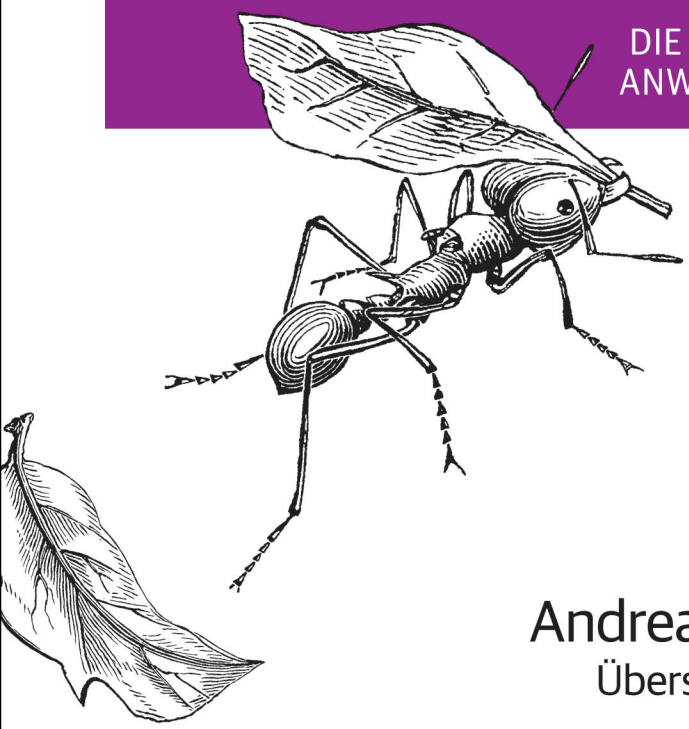
O'REILLY®

2. Auflage
US-Bestseller

# Bitcoin & Blockchain

## Grundlagen und Programmierung

DIE BLOCKCHAIN VERSTEHEN
ANWENDUNGEN ENTWICKELN



Andreas M. Antonopoulos
Übersetzung von Peter Klicman

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, und für die Kommentare in Listings, um eine bessere Lesbarkeit zu gewährleisten..

Mit diesem Symbol wird ein Tipp oder ein Vorschlag angezeigt.

Mit diesem Symbol wird ein allgemeiner Hinweis angezeigt.

Hiermit wird eine Warnung angezeigt.

# Codebeispiele

Die Beispiele sind in Python bzw. C++ geschrieben und verwenden die Kommandozeile Unix-artiger Betriebssysteme wie Linux oder macOS. Alle Code-Snippets finden Sie im Github-Repository (*https://github.com/bitcoinbook/bitcoinbook*) im *code*-Unterverzeichnis des Main-Repository. Laden Sie sich den Buchcode herunter, probieren Sie die Codebeispiele aus oder senden Sie Korrekturen über GitHub.

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. Die privaten Schlüssel und die zugehörigen öffentlichen Schlüssel etwa sind alle echt. Sämtliche Beispieltransaktionen,

Blöcke und Blockchain-Referenzen wurden in die Blockchain eingetragen und sind Teil des öffentlichen »Kassenbuchs«, d.h., man kann sie sich auf jedem Bitcoin-System ansehen.

## 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 von Beispielcode 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, *Mastering Bitcoin*, O'Reilly Media, Inc. 2017, ISBN 978-1-491-95438-6«.

Einige Auflagen dieses Buchs werden unter einer Open-Source-Lizenz wie CC-BY-NC (*https://creativecommons.org/licenses/by-nc/4.0/*) 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 uns auf.

## 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 und sie mit Ihren eigenen Skripten/Programmen abrufen.

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.

## Den Autor kontaktieren

Sie erreichen mich, Andreas M. Antonopoulos, über meine persönliche Website: *https://antonopoulos.com/*

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

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

Folgen Sie mir auf Twitter: *https://twitter.com/aantonop*

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

Mein herzlicher Dank an alle meine Förderer, die meine Arbeit durch monatliche Spenden unterstützen. Meine Patreon-Page finden Sie hier: *https://patreon.com/aantonop*

## Danksagungen

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 ich belegte 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 XXI. 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.