

Bitcoin

Grundlagen und Programmierung

» Hier geht's
direkt
zum Buch

DAS 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 verwenden, 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 CFPF-Fee-Bumping, Transaktions-Pinning, Paketweiterleitung (Package Relay) und CFPF-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 »Borromean 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.