Vorwort

Ein Bitcoin-Buch schreiben

Mitte 2011 stolperte ich das erste Mal über Bitcoin. Meine erste Reaktion war: »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 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, 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.