

Kapitel 1

Vorwort

1.1 Vorwort der Autoren

Die Kryptowährung Bitcoin hat sich in den vergangenen Jahren langsam in die Schlagzeilen gekämpft. Zuerst diskutierten kleine Foren, dann berichtete die Fachpresse, und mittlerweile greifen auch Mainstream-Medien das Thema gerne in den Topmeldungen auf. Natürlich hängt das in erster Linie mit dem enormen Kursanstieg der digitalen Währung Bitcoin zusammen, deren Wert innerhalb der letzten Jahre von wenigen Cent auf mehrere Tausend Dollar gestiegen ist. Zusammen mit Bitcoin trat auch ein scheinbarer Nebendarsteller in das Rampenlicht: die Blockchain, also die Technologie, die die Realisierung von Bitcoin ermöglicht. Normalerweise ist den Endanwendern ziemlich egal, wie eine Anwendung im Hintergrund implementiert ist. Aber bei der Blockchain war das anders. Plötzlich interessierten sich auch Manager für Datenstrukturen, Busfahrer für Netzwerke und Großmütter für Mining-Algorithmen. Somit hat die Blockchain eine Anziehungskraft, die nur sehr wenigen Technologien vorbehalten ist. Am Anfang trieben eher Privatleute, die in Kryptowährungen investieren wollten, die Beliebtheit voran. Doch bald schon liebäugelten auch Firmen mit der Technologie, die eine manipulations sichere Datenbank verspricht, und suchten nach Anwendungsfällen im eigenen Umfeld.

Auf unseren zahlreichen Vorträgen und Seminaren zum Thema Blockchain haben wir das große Interesse und die Begeisterung der Zuhörer hautnah miterlebt. Dabei haben wir auch viel durch die Zuhörer vermittelt bekommen, etwa Fragestellungen, Missverständnisse oder schwer verständliche Aspekte der Technologie, die tiefer gehender Erklärung bedürfen. Und egal wie lange ein Vortrag oder ein Seminar dauerte: Die Zeit war immer zu kurz, um alle spannenden Blockchain-Themen aufzugreifen. In diesem Buch ist es uns nun möglich, Ihnen die ganze Welt der Blockchain näherzubringen. Dabei greifen wir die Fragestellungen auf, die uns am häufigsten in Gesprächen mit Privatleuten, Vertretern aus der Wirtschaft oder Entwicklern begegnen: Wie funktioniert die Blockchain? Wofür kann ich die Blockchain gebrauchen? Wie entwickle ich Blockchain-Anwendungen?

Wir möchten mit diesem Buch eine breite Gruppe an Lesern ansprechen. Der Theorieteil ist auch für Nicht-Techniker geeignet. Wir vermeiden mathematische Formeln, wo es nur geht, und erklären klar und verständlich, wie die Blockchain-Technologie funktioniert. Dabei kratzt das Buch nicht nur an der Oberfläche, sondern

zeigt ausführlich, wie die Blockchain funktioniert. Der Theorieteil richtet sich ausdrücklich auch an Entscheider, die über mögliche Geschäftsmodelle nachdenken. Der praktische Teil soll Ihnen dann die Herausforderungen bei der Entwicklung einer eigenen Blockchain näherbringen. Sie werden eine Blockchain in Java umsetzen und feststellen, wie viele Details in dieser Technologie schlummern. Nachdem Sie Ihre eigene Blockchain umgesetzt haben und dadurch ein tiefes Verständnis für die Technologie aufbauen konnten, erhalten Sie von uns eine detaillierte Einführung in die Entwicklung von Smart Contracts für die Ethereum-Plattform. Dabei zeigen wir Ihnen nicht nur, wie Sie Smart Contracts implementieren können, sondern auch, wie Sie diese testen, debuggen und deployen können. Darüber hinaus behandeln wir die Sicherheit und lassen Sie Sicherheitslücken selbst ausnutzen. Zum Schluss erklären wir Ihnen, wie Sie die Smart Contracts innerhalb von dezentralen Applikationen (DApps) einsetzen können. Dafür geben wir Ihnen eine Einführung in mehrere Frameworks, die die Entwicklung dieser DApps vereinfachen. Das Buch ist dabei so eingeteilt, dass es auch als Nachschlagewerk genutzt werden kann.

Dieses Buch behandelt alle Themen rund um die Blockchain-Technologie von Grund auf. Sie benötigen kein Vorwissen zur Blockchain und können dieses Buch verwenden, um die einzelnen Herausforderungen und Details zu meistern. In den Kapiteln 4 bis 9 zeigen wir Ihnen, wie Sie eine eigene Blockchain implementieren können. Da wir die beispielhafte Implementierung in Java umgesetzt haben, ist es hilfreich, wenn Sie Java bereits kennen. Allerdings genügt es auch, wenn Sie eine andere objektorientierte Programmiersprache kennen. Im Laufe des Buchs wird immer wieder JavaScript benötigt, weshalb es von Vorteil ist, wenn Sie zumindest Grundkenntnisse in JavaScript besitzen. Bei der Entwicklung von Smart Contracts werden wir Ihnen einige Frameworks zeigen, die für die Konfiguration JavaScript verwenden. Die letzten Kapitel des Buchs werden sich mit der Entwicklung von DApps beschäftigen, und in diesem Rahmen wird ein JavaScript-Framework namens Drizzle eingeführt. Dafür benötigen Sie keine Vorkenntnisse, wir werden Ihnen alles Schritt für Schritt erklären.

Dieses Buch trägt den Untertitel »für Entwickler«, daher werden in diesem Buch sehr viele Codebeispiele verwendet. Alle Codebeispiele können Sie unter der URL <https://www.rheinwerk-verlag.de/4677> herunterladen, verwenden und nach Belieben anpassen. Da Sie in diesem Buch unter anderem eine neue Programmiersprache kennenlernen, sollten Sie so viel wie möglich selbst experimentieren und die beschriebenen Beispiele selbst nachvollziehen. Vor allem die Grundlagenkapitel zu den Smart Contracts beinhalten sehr viele Informationen und Hinweise. Verwenden Sie auch hier gerne die beiliegenden Beispiele, um verschiedene Sonderfälle selbst auszuprobieren und zu verstehen. An einigen Stellen verweisen wir auf spätere Kapitel im Buch, um die Details dort erneut zu vertiefen. Das haben wir allerdings nur dann gemacht, wenn die Details sonst zu einer Überladung an Informationen führen würden. Fühlen Sie sich nicht verunsichert, wenn Sie ein Detail nicht sofort komplett verstehen.

Die Blockchain ist eine sehr neue Technologie, die einige Zeit benötigt, um vollständig verstanden zu werden. Hier hilft nur üben, üben, üben.

Viele Menschen haben uns tatkräftig bei diesem Buch unterstützt. Ein großer Dank geht an den Rheinwerk Verlag, insbesondere an Dr. Christoph Meister, für die umfassende Betreuung. Vielen Dank an Sibylle Feldmann für die Korrektur und an Christian Happ für die Begutachtung des Manuskripts. Ein Dankeschön geht zudem an Peter Fertig, Prof. Dr. Kristin Weber, Daniel Knogl, Vitaliy Schreibmann und Igor Eisenbraun für das Probelesen und die Tipps und Verbesserungsvorschläge. Weiterhin danken wir Miriam Schütz, Karolina Nold und Raoul Andersson für die Unterstützung.

Nun wünschen wir Ihnen viel Vergnügen beim Eintauchen in die Welt der Blockchain. Wir hoffen, Sie haben beim Lesen des Buchs ebenso viel Spaß wie wir beim Schreiben.

Würzburg, im Dezember 2018

Tobias Fertig und Andreas Schütz

1.2 Geleitwort

Liebe Leser,

ich kann mich noch sehr genau daran erinnern, wie ich 2010 zum ersten Mal etwas über *Bitcoin* gelesen hatte. Die *Kryptowährung* faszinierte mich von Anfang an so sehr, dass ich wochenlang Tag und Nacht an meinem Schreibtisch verbrachte und mich mit der zugrundeliegenden *Blockchain*-Technologie beschäftigte. Damals waren Informationen hierüber noch extrem rar gesät.

Weitere Monate sollten vergehen, in denen meine zukünftigen Partner und ich viel Erfahrung im *Mining*, also der Generierung von Coins, sammelten. Bis wir uns entschlossen, das Unternehmen *Genesis Mining* in diesem vielversprechenden Markt zu gründen.

Im Dezember 2013 wurde mir mitten in der Nacht bewusst, dass die Blockchain-Technologie in diesem Moment ihren endgültigen Durchbruch erreicht haben sollte – hatte ich doch meinen Computer vorab so programmiert, dass ein Alarm ausgelöst werden sollte, sobald der Bitcoin-Kurs die Marke von 1.000 Dollar durchbricht.

So rasant wie die Kursentwicklung von Bitcoin anstieg, so wuchs auch unser Unternehmen. Die immense Nachfrage ermöglichte es uns, rasant zu expandieren und weltweit einige *Mining-Farmen* aufzubauen. Unser Ziel dabei war und ist es weiterhin, jedem den Einstieg in die Blockchain-Technologie mittels Mining zu ermöglichen.

Dasselbe Anliegen verfolgen auch die Autoren und erfahrenen Kryptografie-Enthusiasten Tobias Fertig und Andreas Schütz mit dem vorliegenden Werk. Sie haben ein sehr verständliches Buch geschrieben, das sowohl Entwicklern als auch Entscheidern das notwendige Wissen anschaulich vermittelt. Technisch fundiert und tiefgehend, erläutern sie die Funktionsweise der Blockchain und geben eine Einführung in die Programmierung von *Smart Contracts* und *DApps*. So leistet das Buch einen wertvollen Beitrag dazu, die Nachfrage der Wirtschaft nach Blockchain-Entwicklern zu bedienen.

Vermutlich kann ich für uns alle drei sprechen, wenn ich sage, dass wir uns auf die Zukunft dieser spannenden Technologie freuen. Begleiten Sie uns doch dabei!

Ich wünsche viel Spaß mit diesem Buch und beim Eintauchen in die spannende Welt der Blockchain.

A handwritten signature in black ink, appearing to read 'Marco Streng', with a long, sweeping flourish extending upwards and to the right.

Ihr Marco Streng
CEO der Genesis Group Ltd.