Debajani Mohanty

₿LOCK CHAIN

für Manager

So nutzen Sie die revolutionäre Technik für Ihr Business

FRANZIS

Blockchain für Manager

So nutzen Sie die revolutionäre Technik für Ihr Business

Debajani Mohanty

FRANZIS

Bibliografische Information der Deutschen Bibliothek

Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte Daten sind im Internet über http://dnb.ddb.de abrufbar.

Autorin: Debajani Mohanty
Übersetzung und Satz: G&U Language & Publishing Services GmbH
Coverdesign: Anna Gajowski
Korrektorat: Monika Paff
Programmleitung: Benjamin Hartlmaier
Druck: CPI-Books
Printed in Germany

ISBN 978-3-645-60611-0

Rezensionen

„ ‚Blockchain für Manager – So nutzen Sie die revolutionäre Technik für Ihr Business' richtet sich nicht nur an Programmierer, sondern an alle, die sich für die Blockchain-Technologie interessieren. Es erläutert anhand von Programmierbeispielen und Anwendungen, was eine Blockchain ist. Es handelt sich um ein kompaktes Werk, das seinen Lesern hilft, die Blockchain-Technologie in kürzester Zeit zu verinnerlichen." – Ratan Jyoti, Social Media Influencer für Cybersecurity, Ex-CISO der Vijaya-Bank und erster CISO der Ujjivan Small Finance Bank.

„Ein Werk für alle Frameworks." – Piyush Pratik Das, Senior Developer, Google USA

Über die Autorin

Debajani Mohanty ist Senior Architect bei NIIT Technologies Ltd., Delhi/NCR und verfügt über fast 17 Jahre Branchenerfahrung. Sie war an großen Projekten beteiligt und baute viele skalierbare B2B- und B2C-Produkte in den Bereichen Tourismus, eGovernance, eCommerce und BFSI auf – von der Idee bis zur Markteinführung.

Sie schreibt leicht verständliche Artikel zu komplexen technischen Sachverhalten und hat beinahe 10.000 Follower in den sozialen Medien.

Debajani ist außerdem Aktivistin und Roman-Autorin. Sie wurde vom Friedensnobelpreisträger Kailash Satyarthi mit dem renommierten Aarya-Preis für ihre herausragenden Beiträge zur Stärkung der Rolle der Frau im Bereich der Literatur ausgezeichnet.

Vorwort

Bei so vielen Büchern über Blockchain, die bereits erschienen sind, fragt man sich vielleicht: Warum noch eines? Nachdem ich mehr als 20 Bücher zu diesem Thema gelesen hatte, erkannte ich, dass der Markt nach einem Buch verlangte, das die Thematik umfassend und aus einem Guss erläutert, auf eine Weise, die sich gleichermaßen für Anfänger wie Experten eignet.

In diesem Buch lernen Sie:

- Blockchain-Grundlagen
- Blockchain-Frameworks: Bitcoin (1. Generation), Ethereum, Hyperledger, R3 Corda, Ripple, MultiChain (2. Generation) und IOTA (3. Generation)
- Proofs of Concept für die meisten dieser Frameworks
- Anwendungsbeispiele aus den Bereichen Bankwesen, Finanzen, Versicherungen, Touristik, Fertigung und Supply Chain im Hinblick auf das richtige Framework
- Blockchain as a Service von Anbietern wie Amazon AWS und Microsoft Azure für das Entwickeln und Testen von Blockchain-Frameworks

Zu den hier vorgestellten Anwendungsbeispielen zählen:

- Banken und Finanzen: Dreifachbuchführung, Zinsswaps, Kundenidentität (KYC)

- Versicherungswesen: Rückversicherungen
- Touristik: Auditing in Hotelreservierungssystemen, Kundenbindungsprogramme
- Supply Chain: Auftragsmanagement-System

Dieses Buch ist besonders geeignet für Führungskräfte und Systemarchitekten, die die Fähigkeiten und die unterschiedlichen Ansätze dieser Frameworks kennenlernen und das richtige für ihren Einsatzbereich auswählen möchten.

Danksagungen

Dieses Buch ist all den wunderbaren Frauen in meinem Leben gewidmet, die mir dabei geholfen haben, meinen Traum Wirklichkeit werden zu lassen: meiner Großmutter Renuka Pal Das, meiner Mutter Nirupama Mohanty, meiner Schwiegermutter Veena Rastogi, Cousine Sanjana Das, Schwägerin Anu Rastogi, meinen besten Freundinnen Sujata Madala und Bijayalaxmi Nanda und meinen beiden wunderbaren Töchtern. Ich danke auch dem Vorstand von NIIT Technologies Ltd. , einem sehr frauenfreundlichen Unternehmen, Herrn Rajendra S. Pawar, CEO Arvind Thakur, BFSI Suvrata Acharya, Projektleiter Vipin Chugh und meinen Managern Vikram Rathi und Avinash Sharma. Zu guter Letzt ein Dankeschön an meinen bibliophilen Ehemann Dr. Rajul Rastogi, der mir immer eine Stütze war und – bei Männern sehr selten – ein sehr weibliches Herz hat.

Inhaltsverzeichnis

Warum gerade Blockchain?

Man könnte sich fragen, ob Blockchain nicht einfach nur eine neue Art von Datenbank darstellt. Blockchain wurde als technologische Ergänzung zu Bitcoin entworfen, einer Kryptowährung, und bietet daher Ansätze für digitale Zahlungsmittel, die eine herkömmliche Datenbank nicht hat.

- Die Daten in einem Blockchain-Ledger können nicht geändert werden.

- Es handelt sich um eine hochsichere Datenbank, die öffentliche und private Schlüssel für Transaktionen verwendet.

- Die Datenbank ist für jedermann öffentlich zugänglich, um Transaktionen zu validieren und neue hinzuzufügen.

- Durch die dezentrale Natur gibt es keine Ausfallzeiten, und deshalb können jederzeit und von überall neue Transaktionen hinzugefügt werden.

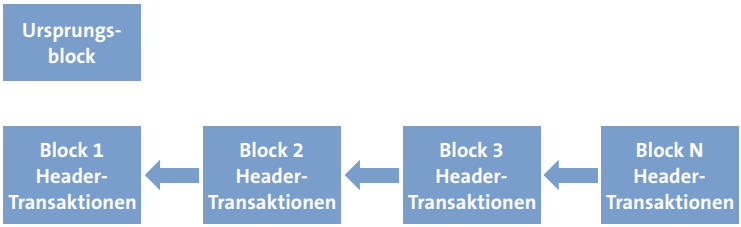
- Je nach individueller Anforderung kann sie öffentlich oder privat sein und ist damit flexibel.

- Der Ledger kann jederzeit überprüft werden.

Wie Blockchain funktioniert

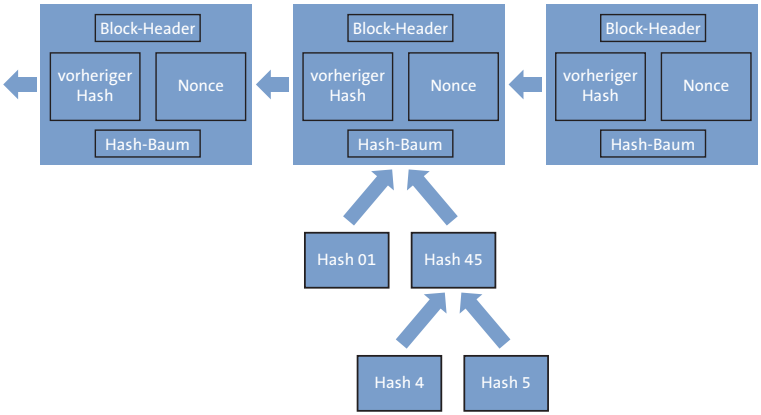
Nun wollen wir zeigen, wie einem Blockchain-Ledger Daten hinzugefügt werden. Wie der Name schon sagt, besteht die Blockchain aus einer Kette von Blöcken, bei der jeder Block auf den vorherigen Block zeigt. Jeder Block besteht aus:

1. einem Header
2. einer oder mehreren Transaktionen innerhalb des Blocks
3. einer Liste von Onkel-Blöcken (auch Ommers genannt), deren Eltern dieselben sind wie die des aktuellen Blocks



Der Block-Header

Die Blockchain besteht aus einer Reihe von Blöcken, die durch eine spezielle Logik miteinander verknüpft sind. Jeder Block hat einen Header, der folgende Informationen enthält:



1. Hash des vorherigen Blocks
2. Zeitstempel
3. Mining- oder Schwierigkeitsgrad
4. ein Nonce als Beweis
5. ein Root-Hash für den Hash-Baum, der die Transaktionen für diesen Block enthält

Der Hash-Baum

Tatsächlich sind die Blöcke viel komplexer, und jeder Block kann viele Transaktionen enthalten. Jeder Transaktion ist ein Hash zugeordnet. Dem Block wird also ein Hash zugewiesen, der der Hash aller darin enthaltenen Transaktionen ist. Dieser Hash wird im Header des Blocks gespeichert. Die gesamte Pyramide wird als Hash-Baum bezeichnet, der von den Minern verifiziert wird.

R3 Corda

R3 (R3CEV LLC) ist ein Unternehmen für verteilte Datenbanktechnologie, das ein Konsortium von mehr als 70 der weltweit größten Finanzinstitute in der Forschung und Entwicklung von Blockchain-Datenbanken im Finanzsystem leitet.

R3 Corda ist ein Joint Venture, das im September 2015 zwischen R3 und zahlreichen Banken und Finanzkonzernen gegründet wurde, um einen Rahmen zu schaffen, der mehr ist als eine traditionelle Blockchain. Corda ist speziell auf die Bedürfnisse von Finanzinstituten zugeschnitten hinsichtlich Geschwindigkeit, Privatsphäre, Skalierbarkeit, Sicherheit etc.

Das Blockchain-Problem in der Finanzindustrie

In der Finanzindustrie werden empfangsbedürftige Transaktionen auf Basis von Verträgen zwischen unterschiedlichen Parteien durchgeführt. Angenommen, Partei A und Partei B möchten eine Transaktion mit einem traditionellen Blockchain-Ledger durchführen. In diesem Fall würden Transaktionen im Netzwerk von Minern aufgezeichnet und validiert, die nichts mit der Transaktion selbst zu tun haben. Warum?

Was Ethereum fehlte

- Sie sind auf dieser Plattform an die Kryptowährung Ether gebunden.

- Transaktionen wurden durch Miner evaluiert und sind daher im ganzen Netzwerk sichtbar.

- Die Transaktionsdauer ist beträchtlich.
- Skalierbarkeit

Warum R3 Corda anders ist

Um diese Probleme anzugehen, haben einige Unternehmen begonnen, an ihrem eigenen Produkt zu arbeiten, und einer der Vorreiter ist R3 Corda. Das grundlegende Ziel ist die Synchronisation zwischen den Parteien A und B ohne die Möglichkeit zu betrügen. Die gemeinsame Nutzung der Daten in einem öffentlichen Ledger durch fremde Instanzen würde zu Datenschutz- und Skalierbarkeitsproblemen führen. Corda nutzt einen verteilten Ledger auf Basis einer Open-Source-Blockchain, in der nur die Parteien Daten einsehen können, die an der Transaktion beteiligt sind. Es wird mit gängigen Werkzeugen und Sprachen programmiert, sodass der Lernaufwand gering ist.

Funktionen von R3 Corda

Was macht R3 Corda einzigartig? Hier sind einige Punkte:

- Es ist unabhängig von einer bestimmten Kryptowährung.
- Smart Contracts werden in Java und Kotlin geschrieben, also Sprachen im Industriestandard.
- Es verwendet unterschiedliche Konsensverfahren.
- Es gibt keine gemeinsame Nutzung von Daten mit unabhängigen Validatoren.

- Transaktionen werden nur von den Parteien der Transaktion bearbeitet und bestätigt und gelangen nicht in die Hände anderer Validatoren.

- Es formt den Workflow zwischen Unternehmen ohne zentrale Steuerung.

- Es ist spezialisiert auf die Finanzindustrie.

Corda im Einzelnen

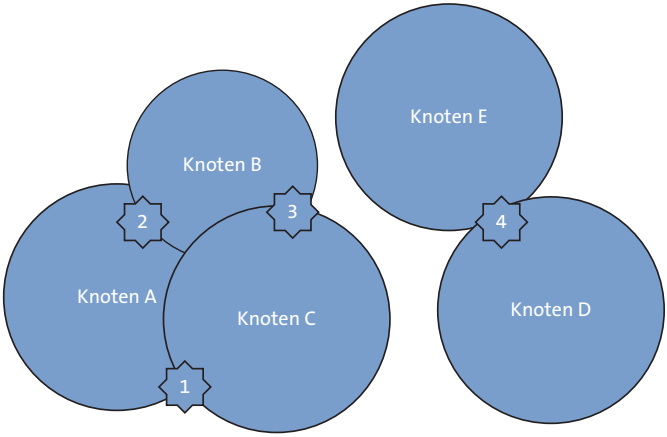
- Das Corda-Netzwerk besteht aus einer Anzahl von Knoten, die über Peer-to-Peer-Mechanismen miteinander kommunizieren. Es interagiert mit seinem Besitzer über RPC.

- Um Zugang zum Netzwerk zu erhalten, benötigt ein Knoten die Freigabe eines Doormans, der die Identitäten durch ein X.509-Zertifikat signiert.

- Das Netzwerk verfügt über spezielle Dienste, die das Signieren, Validieren und Aktualisieren im Ledger garantieren.

- Es gibt keine zentrale Datenbank, in der Informationen abgelegt werden können. Jeder Knoten hat seine eigene unabhängige Speicherstruktur für Daten, die als Vault bezeichnet werden und auf die nur er Zugriff hat. Wenn z. B. zwei Parteien in Knoten A und B eine Transaktion durchführen, werden diese Informationen nur zwischen ihnen ausgetauscht, und andere Knoten sehen diese Daten nicht. Der Vault ist ein Ort, an dem der Status von Verträgen und andere Informationen abgelegt werden. Im folgenden Bild sehen Sie, dass Knoten A und Knoten C Informa-

tion 1, Knoten A und Knoten B Information 2 usw. teilen, während andere Knoten keine Kenntnis davon haben.



- Smart Contracts in Corda können in Java, Kotlin oder einer anderen JVM-Sprache geschrieben werden. Verträge validieren Transaktionen in Abhängigkeit von Regeln und lokalen Daten, die ihnen zur Verfügung stehen. Der Konsensmechanismus in Corda prüft die Gültigkeit von Transaktionen und gleichzeitig die Einzigartigkeit, um Doppelbuchungen mittels spezieller Netzwerkdienste zu verhindern.

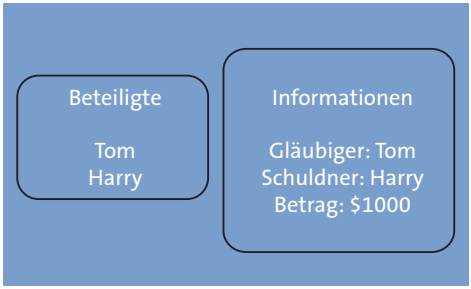
Das IOU-Modell

Die dezentrale Anwendung CorDapp oder Corda modelliert IOUs im Ledger. Ein IOU – kurz für „I O(we) (yo)U – Ich schulde dir" – dokumentiert, dass eine Person einer anderen Person einen bestimmten Geldbetrag schuldet. Diese Informationen werden als Zustand in der lokalen Datenbank des Knotens gespeichert, die als Vault bezeich-

net wird. Gewöhnlich sind die Informationen, die wir hier speichern, die folgenden (oder umfangreicher):

- Schuldner
- Gläubiger
- Betrag
- gezahlter Betrag
- Währung
- Strafe
- Zeitfenster

IOU-Modell



Datenflüsse

Die Kommunikation unter den Knoten könnte durch die Programmierung der Datenflüsse gelenkt werden und erfolgt auf Peer-to-Peer-Basis.

Schlussfolgerungen

Ich hoffe, Sie haben mit der Lektüre dieses Titels einen guten Überblick über die verschiedenen momentan auf dem Markt befindlichen Blockchain-Frameworks und ihre Funktionen erhalten, und darüber, wie sie in verschiedenen Projekten in der Praxis eingesetzt werden können. Ich habe versucht, die beliebtesten Frameworks in diesem Bereich abzudecken, wie z. B. Ethereum, Hyperledger, R3 Corda, Ripple und IOTA. Dabei überlasse ich es Ihnen zu entscheiden, welches Framework am besten zu Ihrem Geschäftsbereich und zu Ihren Anforderungen passt.

Ich denke, dass sich die Blockchain-Technologie in ihrem Frühstadium befindet, ähnlich wie damals das Internet. Viele Großunternehmen führen Experimente mit Prototypen durch und planen in einem Zeitrahmen von 2018 bis 2019 ihre eigenen Produkte. Die meisten von ihnen kämpfen jedoch mit Detailentscheidungen, ohne vorher die Vor- und Nachteile eines bestimmten Frameworks genau analysiert zu haben. Den Verfechtern der Blockchain-Technologie lege ich daher ans Herz, die aktuellen Entwicklungen in diesem Bereich genau zu beobachten, um gute Gelegenheiten zur rechten Zeit zu nutzen.

Bitte sehen Sie sich auch die Videos an, die ich für einige der Beispiele in diesem Buch erstellt habe:

1. https://youtu.be/OF0jS7Po6qg – Dreifachbuchführung: Mittels einer Blockchain unter R3 Corda werden Zwischenhändler ausgeschaltet.

2. https://youtu.be/cNwgRwlTcjU – Einführung in Ripple: Ein hochskalierbares Blockchain-Framework, vom Konzept zur Implementierung

3. https://youtu.be/A0z7z2gG8GA – Programmierung einer Ethereum-Blockchain mittels Solidity, Truffle und MetaMask

4. https://youtu.be/1zajIwUTZQA – Eine Einführung in die Blockchain-Programmierung in Java mit Mining und Proof of Work

Folgen Sie mir auf Twitter: https://twitter.com/debimr75

Folgen Sie mir auf LinkedIn: https://www.linkedin.com/in/debajanimohantypmp/

Die Blockchain ist mehr als Kryptowährungen: Sie ist die bedeutendste Technologie seit der Einführung des Internets und hat das Potenzial, bestehende digitale und analoge Geschäftsmodelle grundlegend zu transformieren. „Blockchain für Manager“ ist der ideale Begleiter für alle Entscheider und Führungskräfte, die sich schnell, kompetent und ohne technische Vorkenntnisse über die revolutionären Möglichkeiten, die die Blockchain bietet, informieren wollen.

Mit Beispielen aus dem Banken- und Versicherungswesen, der Tourismusbranche und dem Supply-Chain-Management zeigt „Blockchain für Manager“, wie Sie die Blockchain mit sofort verfügbaren Frameworks in der Praxis nutzen.

9 783645 606110

EUR 19,90 [D] ISBN: 978-3-645-60611-0