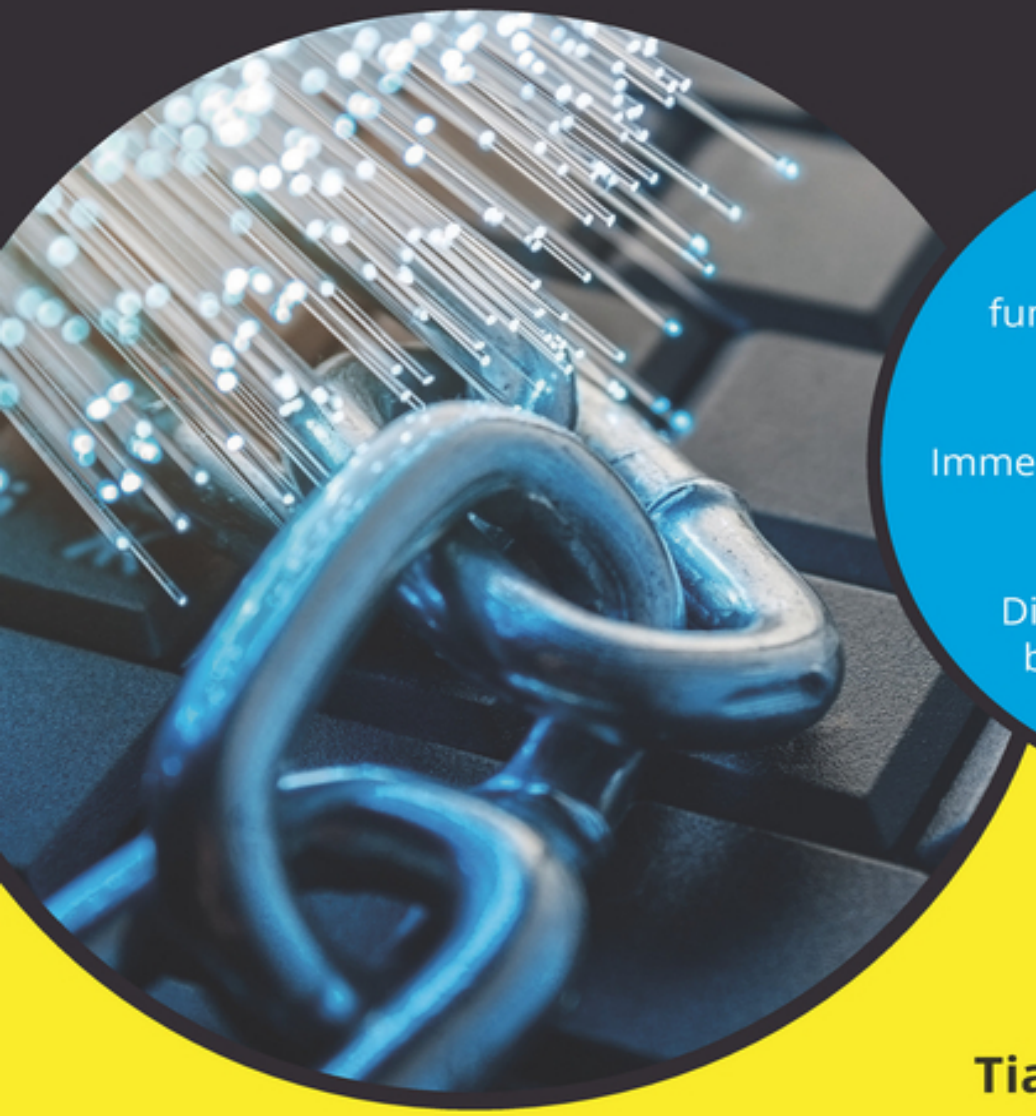
LERNEN EINFACH GEMACHT

2. Auflage

Blockchain

für dummies®



- Verstehen, wie Blockchains funktionieren und wie sie Daten sichern
- Immer die passende Blockchain finden
- Die Rolle der Blockchain bei Kryptowährungen nachvollziehen

Tiana Laurence

Blockchain für Dummies

Schummelseite

WIE BLOCKCHAINS FUNKTIONIEREN

Eine Blockchain ist eine dezentrale Datenbank, die von einem globalen Computernetzwerk verwaltet wird. Die darin aufbewahrten Daten sind verteilt und werden von den Netzwerkcomputern immer wieder untereinander abgeglichen. Diese Computer werden oft auch *Knoten*, *Miner* oder *Peers* genannt. Egal, wie sie heißen: Die Computer schreiben und bewahren die Blockchain ihres Netzwerks, indem sie Einträge überprüfen, genehmigen und weiterleiten. *Einträge* sind die Daten, die von den Nutzern des Netzwerks veröffentlicht werden.

Häufig stellen diese Daten die Übertragung von Kryptowährung von einem Netzwerkbenutzer zum anderen dar.

Wenn Sie etwa Bitcoin an Ihren Freund Tom senden, erstellen und veröffentlichen Sie einen Eintrag in der Bitcoin-Blockchain. Ihr Eintrag muss in diesem Beispiel einige Bedingungen erfüllen. Die Computer im Bitcoin-Netzwerk überprüfen, ob Sie Ihre Kryptowährung nicht vielleicht zuvor schon an eine andere Person gesendet haben. Wenn Sie Tom Bitcoin senden, erhält sein Konto eine Gutschrift und Ihres wird belastet.

Die Computer im Netzwerk verhindern, dass Sie Geld doppelt ausgeben. Im Bitcoin-Netzwerk wird das Problem gelöst, indem jedem Computer im Netzwerk eine vollständige Verlaufsaufzeichnung aller Einträge im Netzwerk – oder mit anderen Worten die gesamte Bitcoin-Blockchain – vorliegt. Dieser Gesamtverlauf zeigt den Saldo jeder Kontoadresse, einschließlich der Ihren.

Nicht alle Blockchain-Einträge stellen die Bewegung von Kryptowährung dar. Einige Blockchains ermöglichen die Veröffentlichung beliebiger Daten gegen eine Gebühr. Außerdem gestatten sie Ihnen, die Gültigkeit eines Eintrags zu bestätigen, ohne den gesamten Blockchain-Verlauf herunterladen zu müssen.

Die meisten Blockchains werden von zentraler Stelle aus kontrolliert und haben damit auch keinen *Single Point of Failure*, also keine zentrale Schwachstelle. Alle Einträge sind für das gesamte Netzwerk sichtbar. Daten, die einmal in eine Blockchain geschrieben wurden, können nicht mehr gelöscht werden. Sie bleiben für immer dort.

Die maßgebliche Innovation von Blockchains gegenüber normalen Datenbanken besteht darin, dass sie die Einigung auf eine gültige Datenhistorie auch ohne zentrale Autorität ermöglichen.

WIE SMART CONTRACTS FUNKTIONIEREN

Smart Contracts, auch *Smart Properties* oder *Chaincode*, sind Vereinbarungen, die in eine Blockchain hineinprogrammiert wurden. Smart Contracts sind Programmcode – einfache If-then- und If-then-else-Anweisungen. Dieser Code läuft innerhalb einer Blockchain ab. Ethereum und Hyperledger Fabric sind beliebte Blockchain-Plattformen für Smart Contracts.

Die Blockchains zeichnen die Verlaufsdaten ihrer Smart Contracts auf und führen Buch über die Kryptowährungssalden von Smart Contracts sowie über alle durchgeführten Transaktionen.

Smart Contracts haben einen internen Speicher, der ihren Code enthält. Dieser wird ausgeführt, wenn zuvor festgelegte Bedingungen erfüllt sind, die entweder intern im Smart Contract definiert oder durch äußere Parameter vorgegeben werden.

Wenn eine externe Quelle benötigt wird, um festzustellen, ob die Bedingung im Smart Contract erfüllt ist, erfordert dies ein *Orakel* (eine Wissensquelle). Es könnte sich dabei beispielsweise um einen Wetter-Datenfeed handeln. Das wäre etwa für eine per Smart Contract verankerte Ernteausfallversicherung sinnvoll. Für dieses Beispiel könnte der Smart Contract beispielsweise wie folgt lauten: »Wenn die Temperatur länger als eine Stunde unter 0 °C sinkt, zahle 5.000 Euro an Josef aus.«

Smart Contracts ermöglichen es, Vertragsbedingungen zu überprüfen und durchzusetzen. Es gibt keine externe Stelle und kein Rechtssystem, um den Vertrag auszulegen und die Absichten der Parteien zu prüfen. Der Code ist das Gesetz.

WAS SIND KRYPTOWÄHRUNGEN?

Kryptowährungen, manchmal auch als virtuelle Währungen, digitales Geld oder Token bezeichnet, lassen sich nicht direkt mit dem US-Dollar, Euro oder britischen Pfund vergleichen. Sie existieren ausschließlich online und werden nicht von Regierungen gestützt, sondern nur von ihren jeweiligen Netzwerken. Aus technischer Perspektive sind Kryptowährungen Einträge in einer Datenbank, für deren Änderung bestimmte Bedingungen erfüllt sein müssen.

Diese Einträge werden kryptografisch vorgenommen und über mathematische Formeln statt von Personen abgesichert.

Einträge, die allen Bedingungen entsprechen, werden in einer Datenbank veröffentlicht. Es handelt sich dabei um eine spezielle Datenbank, die über ein dezentrales Peer-to-Peer-Netzwerk verteilt wird. Wenn Sie beispielsweise Bitcoin an Ihre Freundin Caroline senden, erstellen und versenden Sie einen Eintrag im Bitcoin-Netzwerk, für den natürlich vorab bestimmte Bedingungen erfüllt sein müssen (Guthaben). Das Netzwerk stellt außerdem auch sicher, dass Sie denselben Eintrag nicht zweimal vornehmen. Für das Beispiel bedeutet das also, dass das Netzwerk sicherstellt, dass Sie nicht versucht haben, Ihrer Freundin Caroline und Ihrer anderen Freundin Anna dieselben Bitcoins zu senden.

Das Peer-to-Peer-Netzwerk löst das Problem doppelter Ausgaben (dass Sie zwei Personen dieselben Bitcoins senden) meist dadurch, dass jedem Knoten ein vollständiger Verlauf der Netzwerkeinträge vorliegt. Dieser Gesamtverlauf (Blockchain) zeigt den Saldo aller Konten, einschließlich des Ihren. Die Innovation der Kryptowährung ist, eine Einigung zum gültigen Verlauf zu erzielen, ohne dass ein zentraler Server oder eine zentrale Kontrollstelle beteiligt wären.

Blockchain-Einträge repräsentieren Kryptowährungsguthaben.

In den meisten Fällen erzeugt das Netzwerk Kryptowährung, um den Knoten (auch als Peers oder Miner bezeichnet) einen Anreiz zu bieten, das Netzwerk zu sichern und die Einträge zu überprüfen und zu bestätigen. Jedes Netzwerk hat eine eigene Methode zur Verteilung neu erzeugter Krypto-Token an die Knoten.

Bitcoin beispielsweise belohnt seine Knoten (im Bitcoin-Netzwerk als Miner bezeichnet) dafür, »den nächsten Block zu lösen«. Ein Block enthält eine Reihe von Einträgen. Die Miner konkurrieren darum, am schnellsten einen Hash-Wert zu finden, der den neuen Block mit dem alten verbindet. Daraus leitet sich auch der Begriff »Blockchain« ab. Der Block enthält Einträge, und der Hash sorgt für die Verkettung. Hash-Werte sind eine Art kryptologisches Rätsel. Sie können sie sich wie Sudoku-Rätsel vorstellen, die die Knoten ausfüllen, um die Blöcke miteinander zu verbinden.

Jede Kryptowährung ist ein wenig anders, aber die meisten von ihnen besitzen die folgenden grundlegenden Eigenschaften:

- ✔ **Sie sind irreversibel.** Wenn Sie eine Kryptowährung gesendet haben und das Netzwerk die Zahlung bestätigt hat, können Sie die Transaktion nicht mehr rückgängig machen. Bei Kryptotransfers gibt es keine Rückbuchungen.

- ✔ **Sie sind anonym.** Jeder kann eine Wallet anlegen. Dazu sind keine Ausweisdokumente erforderlich. Es gibt unterschiedliche Stufen der Anonymität, je nachdem, welches Token Sie verwenden.
- ✔ **Sie sind schnell und weltweit zugänglich.** Einträge werden unmittelbar an das gesamte Netzwerk übertragen und innerhalb von wenigen Minuten bestätigt.
- ✔ **Sie sind auf höchste Sicherheit ausgelegt.** Kryptowährungen verwenden die neuesten Verschlüsselungstechniken, stecken aber immer noch in den Kinderschuhen.
- ✔ **Die Geldmenge wird transparent durch das Netzwerk gesteuert und oftmals nach oben begrenzt.**

KRYPTOWÄHRUNGEN ABSICHERN

Das öffentliche Interesse an Kryptowährungen nimmt zu, aber in der Welt der Kryptowährungen geht es immer noch zu wie im sprichwörtlichen Wilden Westen. Hier treffen Sie auf hilfsbereite Pioniere, die Ihnen gerne weiterhelfen, aber auch auf durchgeknallte Banditen, die Ihnen Ihr ganzes Geld abnehmen wollen.

Am stärksten gefährdet sind Kryptowährungen in zentralen digitalen Systemen mit Zugang zum Internet. Dies sind etwa Online-Wallets, Exchanges, auf Ihrem Computer installierte Wallets, auf Cloud-Speichern abgelegte *private Schlüssel* (digitale Schlüssel zur Absicherung Ihrer Token) und Mobilgeräte-Apps.

Um Ihre Kryptowährungen vor Diebstahl zu schützen, setzen Sie am besten auf das *Cold-Storage-Prinzip*, bei dem Sie Ihre privaten Schlüssel offline archivieren. Geeignete Methoden sind etwa die Verwendung einer Offline-Hardware-Wallet, eines USB-Sticks oder einer Paper-Wallet.

Kryptowährungen laufen auf öffentlichen Blockchain-Netzwerken, deshalb gibt es unzählige Möglichkeiten, wie Dritte Ihres Geldes habhaft werden, Ihre Ausgaben nachverfolgen oder den Datenschutz verletzen können. Um das zu verhindern, sollten Sie die folgenden Tipps beherzigen:

- ✔ **Verwenden Sie mehrere Wallets**. Sie können beliebig viele Wallet-Adressen verwenden. Manche Nutzer generieren bei jedem Sende- oder Empfangsvorgang von Kryptowährungen eine neue Adresse.
- ✔ **Bewahren Sie in Web-Wallets nur kleinere Beträge auf**. Web-Wallets sind Angriffsziele für Hacker. Sie sollten deshalb nur kleine Beträge darin aufbewahren. Auch die Wallets auf Ihrem Computer sind

angreifbar. Bewahren Sie große Kryptowährungsbeträge daher stets offline in Ihrer Cold Storage auf.

- ✔ **Geben Sie nichts heraus**! Geben Sie niemals Ihre privaten Schlüssel für Ihr Kryptoguthaben weiter. Mit diesen Schlüsseln haben Dritte unbegrenzten Zugriff auf Ihr ganzes Geld.

Tiana Laurence

Blockchain für dummies®

2. Auflage

Übersetzung aus dem Amerikanischen von
Isolde Kommer und Judith Muhr

WILEY

WILEY-VCH Verlag GmbH & Co. KGaA

Blockchain für Dummies

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

2. Auflage 2019

Print ISBN: 978-3-527-71667-8
ePub ISBN: 978-3-527-82534-9

Coverfoto: © Alexander – stock.adobe.com
Korrektur: Birgit Volk, Bonn

Über die Autorin

Tiana Laurence ist Blockchain-Pionierin, Investorin und Start-up-Gründerin. Sie ist Mitbegründerin von Factom, Inc., einem Softwareunternehmen, das innovative Blockchain-Technologien entwickelt. Sie liebt es, über neue Technologien zu schreiben und dem Laien zu helfen, sie zu verstehen. Ihre Leidenschaft ist es, mit jungen, aufstrebenden Unternehmern Fragen zu Wirtschaft und Technologie zu diskutieren. Tiana hat einen B. A. in Business and Leadership von der Portland State University.

Inhaltsverzeichnis

- Cover
- Über die Autorin
- Einführung
  - Über dieses Buch
  - Törichte Annahmen über den Leser
  - Symbole in diesem Buch
  - Wie es von hier aus weitergeht
- Teil I: Erste Schritte mit Blockchains
  - Kapitel 1: Blockchain – eine Einführung
    - Von Anfang an: Was sind Blockchains?
    - Blockchain-Struktur
    - Blockchain-Anwendungen
    - Der Blockchain-Lebenszyklus
    - Konsens: Die treibende Kraft der Blockchains
    - Blockchains in der Praxis
  - Kapitel 2: Eine Blockchain auswählen
    - Wo Blockchains für Mehrwert sorgen
    - Eine Lösung auswählen
  - Kapitel 3: Einstieg in Blockchain
    - Die Blockchain-Technologie
    - Kryptowährungen absichern und handeln
    - Eine private Blockchain mit Docker und Ethereum erstellen
- Teil II: Ihr Wissen erweitern
  - Kapitel 4: Die Bitcoin-Blockchain kennenlernen
    - Eine kurze Geschichte der Bitcoin-Blockchain
    - Der neue Bitcoin: Bitcoin Cash
    - Häufige Missverständnisse über Bitcoin

Bitcoin: Der neue wilde Westen

Bitcoin-Mining

Ihre erste Paper-Wallet

Kapitel 5: Die Ethereum-Blockchain entdecken

Die kurze Geschichte von Ethereum

Ethereum: Der Open-Source-Weltcomputer

Eine Blockchain hacken

Ether-Mining

Die Zukunft der dezentralen autonomen Organisationen (DAOs)

Ihre eigenen ERC20-Token erstellen

Kapitel 6: Die Waves-Blockchain

Wie unterscheidet sich die Waves-Blockchain von anderen Blockchains?

Die volle Leistung von Waves ausschöpfen

Die Wallet-Funktionen entdecken

Ihre eigene Kryptowährung erstellen und verleihen

Kapitel 7: Die Factom-Blockchain

Eine Frage des Vertrauens

Anwendungen auf Factom aufbauen

Kapitel 8: Die EOS-Blockchain

EOS kennenlernen

EOS-Blockproduzenten wählen

Die EOS-DApp-Sammlung

Teil III: Leistungsstarke Blockchain-Plattformen

Kapitel 9: Hyperledger

Hyperledger kennenlernen

Wichtige Hyperledger-Projekte

Ein eigenes System in Fabric erstellen

Kapitel 10: Microsoft Azure

Bletchley: Die modulare Blockchain-Struktur

Entwicklung im Azure-Ökosystem
Die ersten Schritte mit Chain auf Azure
Bereitstellung von Blockchain-Tools auf Azure
Kapitel 11: IBM Bluemix
Unternehmens-Blockchains auf Bluemix
Die intelligente Watson-Blockchain
Ihr erstes Netzwerk auf Big Blue
Teil IV: Auswirkungen auf die Wirtschaft
Kapitel 12: Finanztechnologie
Holen wir die Kristallkugel heraus: Banking-Trends der Zukunft
Es wird international: Globale Finanzprodukte
Dem Betrug ein Ende setzen
Kapitel 13: Immobilien
Wegfall der Rechtstitelversicherung
Hypotheken in der Blockchain-Welt
Regionale Trends vorhersehen
Kapitel 14: Versicherungen
Präziser, maßgeschneiderter Versicherungsschutz
Das Internet der Dinge als vertrauenswürdige Datenquelle
Wegfall der Drittpartei bei Versicherungen
Kapitel 15: Regierung
Die intelligenten Städte Asiens
Der Kampf um das Finanzkapital der Welt
Sicherung der Grenzen auf der ganzen Welt
Kapitel 16: Weitere Branchen
Schlanke Regierungen
Die Vertrauensebene für das Internet
Blockchain-Orakel
Teil V: Der Top-Ten-Teil

Kapitel 17: (Ungefähr) zehn kostenlose Blockchain-Ressourcen

- Ethereum
- DigiKnow
- Blockchain University
- Bitcoin Core
- Blockchain Alliance
- Multichain Blog
- HiveMind
- Smith + Crown
- Die Podcast-Reihen Unchained und Unconfirmed

Kapitel 18: Zehn Blockchain-Regeln, die Sie niemals brechen dürfen

- Verwenden Sie Kryptowährungen oder Blockchains nicht, um das Gesetz zu umgehen
- Halten Sie Ihre Contracts so einfach wie möglich
- Veröffentlichungen nur mit größter Vorsicht
- Sichern Sie Ihre privaten Schlüssel! Unbedingt!
- Überprüfen Sie Adressen dreimal, bevor Sie Geld senden
- Seien Sie vorsichtig bei der Verwendung von Börsen
- Hüten Sie sich vor WLAN
- Wählen Sie Ihren Blockchain-Entwickler sorgfältig aus
- Lassen Sie sich nicht entmutigen
- Handeln Sie keine Token, wenn Sie nicht wissen, was Sie tun

Kapitel 19: Zehn herausragende Blockchain-Projekte

- Das R3-Konsortium
- T ZERO: Blockchains am Aktienmarkt
- Verteilte Systeme von Blockstream
- MadHive
- Blockdaemon

Gemini-Dollar und -Börse
Decentraland
TransferWise
Lightning Network
Bitcoin Cash
Stichwortverzeichnis
End User License Agreement

Tabellenverzeichnis

Kapitel 2

Tabelle 2.1: Häufige Anwendungsfälle und die dafür geeigneten Blockchains

Kapitel 10

Tabelle 10.1: Cryptlets im Vergleich zu Prognosen

Illustrationsverzeichnis

Kapitel 1

Abbildung 1.1: Der Aufbau des Blockchain-Netzwerks Bitcoin
Abbildung 1.2: Wie Blockchains arbeiten
Abbildung 1.3: Die Handelsplattform Altcoin

Kapitel 3

Abbildung 3.1: Gehen Sie in GitHub zu dieser Seite.
Abbildung 3.2: Auf dem Desktop öffnen

Kapitel 4

Abbildung 4.1: Ein Hash-Baum
Abbildung 4.2: Eine Paper-Wallet

Kapitel 5

Abbildung 5.1: Das weltweit erste unsterbliche Spiel: Etheria

Abbildung 5.2: Darstellung der Blockchain-Anwendung Ethereum.org

Kapitel 7

Abbildung 7.1: Der Aufbau der Factom-Blockchain

Abbildung 7.2: Die Kettenstruktur von Factom

Abbildung 7.3: Factom Harmony

Kapitel 10

Abbildung 10.1: Blockstack Core v14

Abbildung 10.2: Ein Cryptlet-Container

Kapitel 11

Abbildung 11.1: Wie IBM Bluemix und IoT mit IBM Watson kombiniert werden

Abbildung 11.2: Wie Bluemix Clients, Peers und IBM Watson integriert

Abbildung 11.3: Der Watson/API/Gerät-Ablauf

Kapitel 15

Abbildung 15.1: Das Smart-Nation-Projekt von Singapur

Einführung

Willkommen bei *Blockchain für Dummies*! Dies ist genau das richtige Buch für Sie, wenn Sie mehr darüber erfahren wollen, was Blockchains sind und wie man sie verwendet. Viele Menschen vermuten, Blockchains seien schwer zu verstehen. Vielleicht denken auch Sie, dass Blockchains einfach irgendwelche Kryptowährungen sind, wie beispielsweise Bitcoin, aber tatsächlich sind sie sehr viel mehr. Jeder kann die Grundlagen für das Blockchain-System verstehen.

In diesem Buch finden Sie viele praktische Hinweise, wie Sie sich in der Blockchain-Welt bewegen können, und ebenso zu den Kryptowährungen, die die Blockchains erhalten. Außerdem finden Sie nützliche Schritt-für-Schritt-Anleitungen, anhand derer Sie sehen, wie Blockchains funktionieren und wo sie nützlich sind. Um dieses Buch verstehen zu können, brauchen Sie keinerlei Hintergrundwissen hinsichtlich Programmierung, Wirtschaft oder Weltgeschehen. Es wird jedoch immer wieder um diese Themen gehen, weil die Blockchain-Technologie mit all diesen Themen Überschneidungen hat.

Über dieses Buch

Dieses Buch erklärt Ihnen die Grundlagen, die Sie brauchen, um Blockchains, Smart Contracts und Kryptowährungen zu verstehen. Wahrscheinlich haben Sie sich dieses Buch gekauft, weil Sie schon viel über Blockchains gehört haben und wissen, dass sie wichtig sind, aber keine Ahnung haben, worum es sich dabei handelt, wie sie funktionieren oder wie Sie damit umgehen sollten. Auf den folgenden Seiten finden Sie leicht verständliche Antworten auf all diese Fragen.

Dieses Buch unterscheidet sich von anderen Büchern über Blockchains: Es zeigt Ihnen die wichtigsten Blockchains auf dem öffentlichen Markt und erklärt, wie sie funktionieren, was sie leisten und was Sie heute Sinnvolles damit tun können.

Darüber hinaus beschäftigt sich dieses Buch auch mit der Welt der Blockchain-Technologie und erläutert Ihnen, was Sie bei Ihren eigenen Blockchain-Projekten beachten müssen. Hier erfahren Sie, wie Sie eine Wallet installieren, einen Smart Contract erstellen und ausführen, Einträge in Bitcoin und Factom vornehmen und Kryptowährungen verdienen.

Sie brauchen das Buch nicht von vorne bis hinten durchzulesen. Blättern Sie einfach zu dem Thema, das Sie gerade am meisten interessiert.

Manchmal finden Sie in diesem Buch Webadressen, die über zwei Textzeilen umbrochen sind. Wenn Sie dieses Buch auf Papier lesen und eine dieser Webseiten besuchen wollen, geben Sie sie einfach genauso ein, wie sie im Text dargestellt werden, so als ob der Zeilenumbruch gar nicht existieren würde. Und wenn Sie den Text als E-Book lesen, haben Sie es ohnehin ganz einfach: Sie klicken einfach auf die Webadresse und gelangen direkt auf die Webseite.

Törichte Annahmen über den Leser

Sie brauchen nichts über Kryptowährungen, Programmierung und rechtliche Angelegenheiten zu wissen, aber ich setze das Folgende voraus:

- ✔ Sie haben einen Computer, ein Smartphone und Zugriff auf das Internet.
- ✔ Sie wissen, wie der Computer und das Internet genutzt werden.
- ✔ Sie wissen, wie Sie sich mithilfe von Menüs in Programmen bewegen.
- ✔ Blockchains sind Ihnen relativ neu, und Sie sind kein erfahrener Programmierer. Aber auch als Programmierer

können Sie in diesem Buch viel lernen; vielleicht können Sie jedoch einige der Schritt-für-Schritt-Anleitungen überspringen.

Symbole in diesem Buch

In diesem Buch verwende ich Symbole, um Ihre Aufmerksamkeit auf bestimmte Arten von Informationen zu lenken. Und das bedeuten diese Symbole:


Das Tipp-Symbol kennzeichnet Tipps und Lösungen, die Ihnen das Leben mit Blockchains erleichtern.


Das Erinnerungssymbol kennzeichnet Informationen, die Sie unbedingt kennen sollten, also alles, was Sie sich merken sollten. Um sich schnell einen Überblick über die wichtigsten Informationen eines Kapitels zu verschaffen, suchen Sie einfach nach diesen Symbolen.


Das Techniker-Symbol kennzeichnet höchst technische Inhalte, die Sie überspringen können, ohne das Wesentliche des jeweiligen Themas zu verpassen.


Das Warnsymbol weist darauf hin, dass Sie aufpassen sollten! Es kennzeichnet wichtige Informationen, die Ihnen Kopfzerbrechen ersparen – oder Token.

Wie es von hier aus weitergeht

Sie können die Blockchain-Technologie in fast jeder Branche einsetzen. Derzeit ist ein explosionsartiges Wachstum in den Bereichen Finanzen, Gesundheitswesen, Regierung und Versicherungen zu beobachten, und das ist erst der Anfang. Die ganze Welt befindet sich im Wandel, und es gibt endlose Möglichkeiten.

Teil I

Erste Schritte mit Blockchains

IN DIESEM TEIL …

Erfahren Sie, was Blockchains sind und wie Ihr Unternehmen davon profitieren kann.

Identifizieren Sie die richtige Technologie für sich, und lernen Sie, in vier Schritten ein effektives Blockchain-Projekt zu entwickeln und umzusetzen.

Erstellen Sie Ihre eigenen Smart Contracts im Bitcoin-Netzwerk, und erkennen Sie, wo in Ihrem Unternehmen diese Technologie von Nutzen sein kann.

Kapitel 1

Blockchain – eine Einführung

IN DIESEM KAPITEL

- Die neue Welt der Blockchains kennenlernen
- Verstehen, warum Blockchains so wichtig sind
- Die drei Typen von Blockchains unterscheiden lernen
- Ihre Kenntnisse der Funktionsweise von Blockchains vertiefen

Ursprünglich war *Blockchain* in der Informatik der Begriff für eine bestimmte Art, Daten zu strukturieren und weiterzugeben. Heute werden Blockchains als »fünfte Evolution« der EDV bejubelt.

Blockchains sind ein neuer Ansatz für verteilte Datenbanken. Die eigentliche Innovation ergibt sich dadurch, dass alte Technologien auf neue Weise eingesetzt werden. Sie können sich Blockchains als verteilte Datenbanken vorstellen, die von einer bestimmten Personengruppe kontrolliert und in denen Informationen gespeichert und geteilt werden.

Es gibt viele verschiedene Arten von Blockchains und Blockchain-Anwendungen. Blockchain ist eine Technologie, die plattform- und hardwareübergreifend auf der ganzen Welt eingesetzt wird.

Von Anfang an: Was sind Blockchains?

Eine Blockchain ist eine Datenstruktur, die es ermöglicht, eine Art digitales Kontenbuch (das sogenannte *Ledger*) mit Daten zu erstellen und es über ein Netzwerk aus unabhängigen Parteien zu verbreiten. Es gibt verschiedene Typen von Blockchains:

- ✔ **Öffentliche Blockchains**: Öffentliche Blockchains, wie beispielsweise Bitcoin, sind große verteilte Netzwerke mit einer nativen Kryptowährung. Eine *Kryptowährung* ist ein eindeutiges Datenelement, das zwischen zwei Beteiligten ausgetauscht werden kann. Öffentliche Blockchains sind auf allen Ebenen für jedermann zugänglich und basieren auf quelloffenem Programmcode, der von der Community gepflegt wird.
- ✔ **Permissioned Blockchains**: Permissioned Blockchains, wie beispielsweise Ripple, legen die Rollen fest, die einzelne Teilnehmer innerhalb des Netzwerks übernehmen können. Es handelt sich ebenfalls um große und verteilte Systeme, die ein natives Token verwenden. Der zugrunde liegende Code kann quelloffen sein oder auch nicht.
- ✔ **Private Blockchains**: Private Blockchains – auch Distributed-Ledger-Technik (DLT) – sind meist kleiner und verwenden kein Token beziehungsweise keine Kryptowährung. Die Mitgliedschaft wird streng kontrolliert. Diese Art Blockchains werden von Gruppen mit vertrauenswürdigen Mitgliedern favorisiert, um vertrauliche Informationen weiterzugeben.

Alle drei Blockchain-Typen verwenden Kryptografie, um einem Teilnehmer in einem bestimmten Netzwerk zu gestatten, den Ledger (das Kontobuch) sicher zu verwalten, ohne dass eine zentrale Autorität die Regeln durchsetzt. Der Wegfall dieser zentralen Autorität aus der Datenbankstruktur ist eine der wichtigsten und leistungsstärksten Eigenschaften von Blockchains.

Blockchains legen permanente Aufzeichnungen und Transaktionsverläufe an, aber nichts währt wirklich ewig. Die Dauerhaftigkeit des Datensatzes ist auf die Weiterführung durch ein ordnungsgemäß funktionierendes Netzwerk angewiesen. Wenn sich hingegen ein großer Teil der Blockchain-Community darauf einigen würde, wäre es möglich, die in die Blockchain geschriebenen Informationen zu verändern. Kryptowährungen schaffen für die Beteiligten eine Motivation für die einwandfreie Funktion des Netzwerks. Datensätze in unlauterer Weise abzuändern, erfordert eine sogenannte 51-Prozent-Attacke. Kleine Netzwerke mit wenigen unabhängigen Minern sind eher angreifbar, und leistungsstarke Miner könnten auf diese Weise zusätzliche Kryptowährung generieren. Einen solchen Angriff erfuhr etwa Ethereum Classic.

In einer Blockchain aufgezeichnete Daten lassen sich nur sehr schwer ändern oder entfernen. Wenn jemand eine Transaktion oder einen Eintrag in einer Blockchain vornehmen will, überprüfen zur Validierung berechtigte Netzwerkteilnehmer die vorgeschlagene Transaktion. Und hier wird das Ganze unübersichtlich, weil jede Blockchain eine etwas andere Vorstellung davon hat, wie das geschieht und wer eine Transaktion validieren darf.

Was Blockchains können

Eine Blockchain ist ein Peer-to-Peer-System ohne zentrale Autorität zur Verwaltung des Datenstroms. Eine grundlegende Möglichkeit, die zentrale Kontrolle wegfallen zu lassen und gleichzeitig die Datenintegrität zu bewahren, ist ein großes, dezentrales Netzwerk unabhängiger Benutzer. Das heißt, dass sich die Netzwerkcomputer an unterschiedlichen Orten befinden. Solche Computer werden häufig auch als *vollständige Knoten* bezeichnet.

Abbildung 1.1 zeigt die Struktur des Blockchain-Netzwerks Bitcoin. In Aktion sehen Sie das Ganze unter

http://dailyblockchain.github.io.

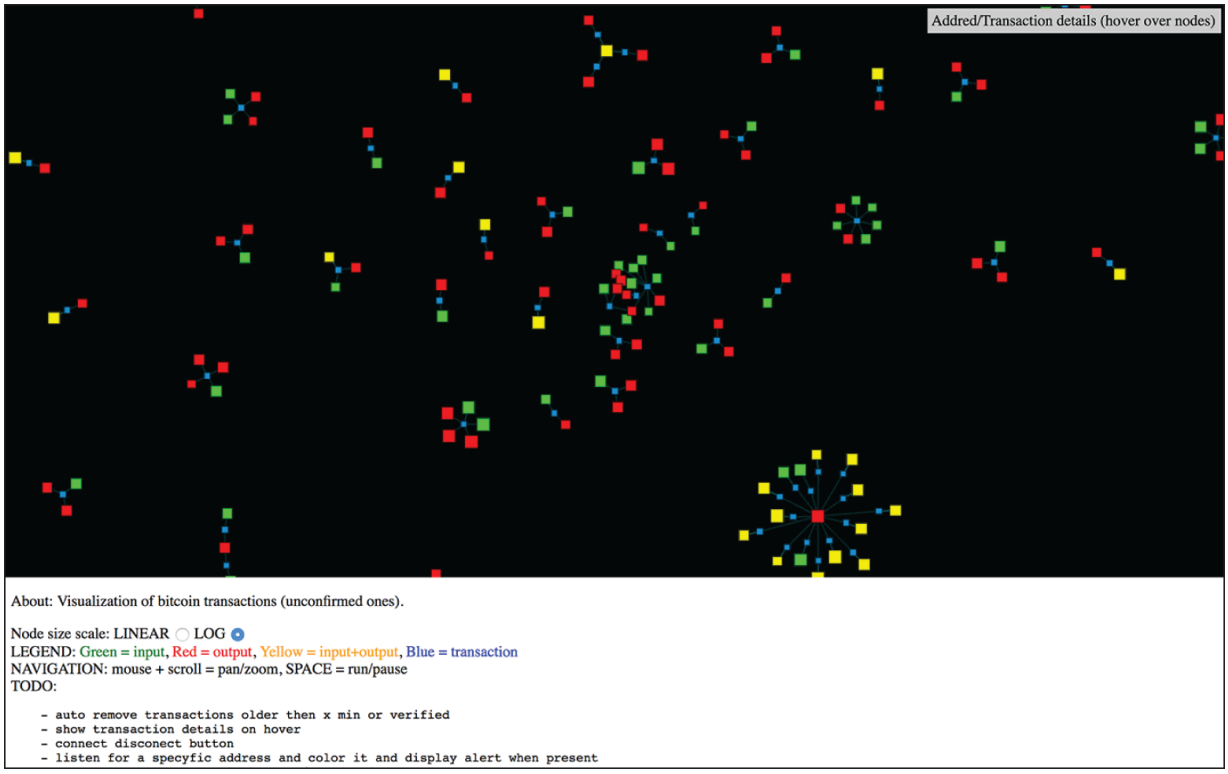


Abbildung 1.1: Der Aufbau des Blockchain-Netzwerks Bitcoin

Um eine Manipulation des Netzwerks zu verhindern, sind Blockchains nicht nur dezentral, sondern verwenden oft auch eine *Kryptowährung*. Blockchain-Netzwerke generieren Kryptowährungen als Anreiz zum Erhalt der Netzwerkintegrität. Viele Kryptowährungen werden wie Aktien an Börsen gehandelt.

Kryptowährungen funktionieren für jede Blockchain etwas anders. Im Prinzip belohnt das Softwareprotokoll die Teilnehmer für den Betrieb von Hardware. Bekannte Blockchain-Protokolle sind unter anderem Bitcoin, Ethereum, Ripple, Bitcoin Cash, Stellar oder EOS. Die Hardware ist ein Netzwerkknotenpunkt, auf dem die aktuelle Blockchain-Software läuft, um die Daten im Netzwerk zu sichern.

Warum Blockchains so wichtig sind

Blockchains werden als die »fünfte Evolution« der elektronischen Datenverarbeitung betrachtet, weil sie eine neue

Vertrauensebene im Internet darstellen.

Blockchains können Vertrauen in digitale Daten schaffen. Wenn Informationen in eine Blockchain-Datenbank geschrieben wurden, lassen sie sich hinterher praktisch nicht mehr entfernen oder verändern. Diese Möglichkeit hat nie zuvor existiert.

Bevor es Blockchains gab, wurde Vertrauenswürdigkeit über zentrale Stellen durch die Ausgabe von Zertifikaten gewährleistet. Ein bekanntes Beispiel sind etwa die SSL-Client-Zertifikate (Secure Sockets Layer) – die grünen Schlosssymbole neben einer Webdomain. Sie erkennen daran, dass Sie sich auf einer sicheren Website befinden. SSL-Zertifikate sind jedoch nicht hundertprozentig sicher. Sie wurden bereits von den Domains der CIA, des britischen Geheimdienstes (MI6), von Microsoft, Yahoo!, Skype, Facebook und Twitter gestohlen. Das Vertrauen in einen Dritten bedeutet immer auch eine zentrale Schwachstelle.

Die Vertrauenswürdigkeit von Blockchains wird indessen durch neue Methoden gewährleistet. Bei Proof-of-Work-Blockchains (POW) können die Miner nur mit einer vollständigen und exakten Transaktionshistorie am Netzwerk teilnehmen. Proof-of-Stake-Blockchains (POS) sind vertrauenswürdig, weil die zur Validierung berechtigten Knoten ihr Kryptoguthaben einsetzen oder »staken« müssen und weil sie dieses aufs Spiel setzen, wenn sie unzulässige Netzwerktransaktionen bestätigen. Private Blockchains wiederum verteilen die Daten über ein Netzwerk von verbundenen, aber unabhängigen Teilnehmern, die einander bekannt sind und sich gegenseitig zur Verantwortung ziehen können. Mit unterschiedlichen Anreizsystemen erreichen die einzelnen Blockchain-Typen, dass alle Netzwerkteilnehmer eine vollständige und unveränderte Historie aller einzelnen Transaktionen und Einträgen in der gemeinsam genutzten Datenbank erstellen.

Wenn Daten permanent und zuverlässig in einem digitalen Format vorliegen, können Sie Geschäfte online erledigen, die früher nur offline getätigt werden konnten. Alles, was bisher analog war, unter anderem Eigentumsrechte und Identitäten, kann

jetzt online erstellt und verwaltet werden. Langsame Unternehmens- und Bankprozesse wie Geldüberweisungen und Fondsabwicklungen lassen sich heute fast verzögerungsfrei durchführen. Die Möglichkeiten durch sichere digitale Aufzeichnungen sind von größter Bedeutung für die Weltwirtschaft.

Die ersten Anwendungen stützten sich auf die sichere digitale Übertragung von Vermögenswerten, die Blockchains durch den Austausch ihrer nativen Token ermöglichten. Dabei ging es unter anderem um die Überweisung von Geld und Kapital. Die Möglichkeiten von Blockchain-Netzwerken gehen aber weit über die Verschiebung von Vermögenswerten hinaus.

Blockchains sind insofern von Bedeutung, als sie eine neue Effizienz und Zuverlässigkeit beim Austausch wertvoller und privater Informationen ermöglichen. Dieser Austausch erforderte einst die Unterstützung durch Dritte, zum Beispiel beim Geldtransfer und bei der Überprüfung von Identitätsdaten. Dies ist eine wichtige Herausforderung, denn ein Großteil unserer Gesellschaft und Wirtschaft ist darauf ausgerichtet, Vertrauenswürdigkeit zu schaffen beziehungsweise durchzusetzen, entweder zwischen zwei Parteien oder über einen Vermittler. Sie können sich vorstellen, wie diese einfache Software Bereiche verbessern kann, die bisher nicht absolut sicher waren, zum Beispiel Wahlen, Lieferketten, Geldtransfers und Eigentumsübertragungen.

Blockchain-Struktur

Jede Blockchain ist etwas anders aufgebaut. Die Bitcoin-Blockchain eignet sich jedoch hervorragend für eine Strukturanalyse, da sie als Vorbild für die meisten späteren Blockchains diente. Bei Bitcoin sind die Daten so strukturiert, dass jeder vollständige Netzwerkknoten (jeder der Computer, auf denen das Netzwerk läuft) alle Daten des Netzwerks enthält. Dieses Modell ist unter dem Gesichtspunkt der Datenpersistenz überzeugend. Es stellt sicher, dass die Daten auch dann

unverändert bleiben, wenn einige Knoten ausfallen. Da jedoch jeder Knoten von Anfang an und auch in Zukunft eine vollständige Kopie der Transaktionshistorie enthält, sollten die Einträge hinsichtlich ihres Speicherbedarfs möglichst klein sein.

Im Gegensatz dazu sind andere dezentrale Netzwerke wie etwa Napster und Pirate Bay Online-Datenindizes. Einzelne Dateien werden von bestimmten Netzwerkknoten zur Verfügung gestellt. Das spart Speicherplatz. Da die Daten, an denen Sie interessiert sind, jedoch nicht für alle Teilnehmer im Netzwerk verfügbar sind, ist es unter Umständen problematisch, an diese Daten zu kommen. Es ist auch schwierig festzustellen, ob die abgerufenen Daten intakt und unbeschädigt sind oder ob sie vielleicht unerwünschte Informationen wie etwa ein Virus enthalten.

Bitcoin koordiniert die Verwaltung und Erfassung neuer Daten mithilfe von drei Kernelementen:

- **Block**: eine Liste mit Transaktionen, die über einen bestimmten Zeitraum in einem Ledger (»Kontobuch«) aufgezeichnet werden. Die Größe, der zeitliche Abstand und das auslösende Ereignis für einen Block unterscheiden sich zwischen allen Blockchains.

  Nicht alle Blockchains haben das primäre Ziel, einen Datensatz über eine Bewegung ihrer Kryptowährung aufzuzeichnen und zu sichern, aber alle Blockchains zeichnen die Ströme ihrer Kryptowährung oder ihres Tokens auf. Sie können sich eine *Transaktion* einfach als die Aufzeichnung von Daten vorstellen. Durch die Zuweisung eines Werts (wie es beispielsweise in einer Finanztransaktion geschieht) wird interpretiert, was diese Daten bedeuten.
- **Kette (»Chain«)**: Ein kryptografischer Hash-Schlüssel, der die Blöcke verknüpft, sie mathematisch »verkettet«. Dies ist eines der komplexesten Blockchain-Konzepte und nicht gerade einfach zu verstehen. Aber genau dieser scheinbar magische Mechanismus erzeugt das feste Blockchain-Gefüge und ermöglicht mathematisch gestütztes Vertrauen.

Der Hash-Schlüssel in Blockchains wird aus den Daten des jeweils vorhergehenden Blocks erzeugt. Es handelt sich um einen Fingerabdruck dieser Daten, der die Blockreihenfolge und -zeiten unveränderbar festschreibt.

Blockchains sind relativ neu – das Hashing nicht: Es wurde bereits vor über 30 Jahren erfunden. Diese betagte Technik wird deshalb verwendet, weil sie eine nicht entschlüsselbare Einwegfunktion schafft. Eine Hash-Funktion erzeugt einen mathematischen Algorithmus, der Daten beliebiger Größe auf einen Bit-String fester Größe abbildet. Ein Bit-String ist normalerweise 32 Zeichen lang und repräsentiert die Daten, für die das Hashing durchgeführt wurde. Der Secure Hash Algorithm (SHA) ist eine von mehreren verschlüsselnden Hash-Funktionen, die in Blockchains verwendet werden. Ein gebräuchlicher Algorithmus ist SHA-256, der einen nahezu eindeutigen Hash-Schlüssel fester Größe (256 Bit, 32 Byte) erzeugt. Praktisch können Sie sich einen Hash-Schlüssel als digitalen Fingerabdruck von Daten vorstellen, mit dem diese innerhalb der Blockchain an einer festen Position gehalten werden.

- **Netzwerk**: Das Netzwerk setzt sich aus »vollständigen Knoten« zusammen. Sie können sich das so vorstellen, dass diese Computer einen Algorithmus ausführen, der das Netzwerk sichert. Jeder Knoten enthält eine vollständige Aufzeichnung aller Transaktionen, die je in dieser Blockchain aufgezeichnet wurden.

  Die Netzwerkknotenpunkte befinden sich auf der ganzen Welt und können von jedermann betrieben werden. Es ist schwierig, teuer und zeitaufwendig, einen vollständigen Knoten zu betreiben. Darum tun die Betreiber es nicht kostenlos. Der Anreiz für den Betrieb besteht im Verdienst von Kryptowährung. Der zugrunde liegende Blockchain-Algorithmus belohnt die Netzwerkteilnehmer für ihre Dienste.

Die Begriffe *Bitcoin* und *Blockchain* werden häufig synonym verwendet, bedeuten aber nicht dasselbe. Bitcoin verfügt über eine Blockchain. Die Bitcoin-Blockchain ist das Protokoll, das die sichere Übertragung von Bitcoins ermöglicht. Bitcoin ist der Name der Kryptowährung, auf der das Bitcoin-Netzwerk basiert. Blockchain ist eine bestimmte Softwaregattung, Bitcoin ist eine spezifische Kryptowährung.

Blockchain-Anwendungen

Blockchain-Anwendungen basieren auf dem Gedanken, das Netzwerk als Vermittler einzusetzen. Ein solches System ist absolut blind und unerbittlich. Computercode wird zum Gesetz, und die Regeln werden vom Netzwerk unveränderbar interpretiert und ausgeführt. Computer haben keine sozialen Tendenzen und Verhaltensweisen wie Menschen. Das Netzwerk kann keine Absicht interpretieren (zumindest noch nicht).

Eine weitere interessante Eigenschaft von Blockchains ist die absolut unfehlbare Datenaufzeichnung. Blockchains können als unmissverständliche Zeitleiste dienen, die aufzeichnet, wer was wann gemacht hat. Auf genau dieses Problem sind in vielen Branchen und Aufsichtsbehörden bereits unzählige Stunden verwendet worden. Durch blockchaingestützte Aufzeichnungen fallen viele Schwierigkeiten bei der Interpretation vergangener Geschehnisse weg.

Der Blockchain-Lebenszyklus

Blockchains wurden mit Bitcoin aus der Taufe gehoben. Dabei zeigte sich, dass einander völlig unbekannte Einzelpersonen online in einem Systems zusammenarbeiten konnten, in dem es unmöglich war, andere Netzwerkteilnehmer zu betrügen.

Das ursprüngliche Bitcoin-Netzwerk sollte die Kryptowährung Bitcoin sichern. Es besteht aus ca. 5.000 vollständigen Knoten, ist dezentral über die gesamte Welt verteilt und wird hauptsächlich

für den Handel von Bitcoin und den Austausch von Vermögenswerten verwendet. Die Community erkannte jedoch das viel weiter reichende Potenzial des Netzwerks. Wegen seiner Größe und lange erprobten Sicherheit wird es auch zur Absicherung anderer, kleinerer Blockchains und von Blockchain-Anwendungen verwendet.

Das Ethereum-Netzwerk ist eine Weiterentwicklung des Blockchain-Konzepts, das die bekannte Blockchain-Struktur um mehrere neue, integrierte Programmiersprachen ergänzt. Wie Bitcoin hat auch das Ethereum-Netzwerk über 10.000 auf dem ganzen Erdball verteilte Full Nodes. Ethereum wird in erster Linie verwendet, um Ether zu handeln und Smart Contracts abzuschließen. Der bekannteste Ethereum-Smart-Contract ist ERC 20. Er ermöglicht die Erstellung handelbarer Token. Diese Token können für Fundraising-Zwecke verwendet werden. Weitere Informationen zu Smart Contracts finden Sie in Kapitel 5.

Ein dritter Evolutionsschritt der Blockchain-Technologie befasst sich aktuell mit den Beschränkungen hinsichtlich Geschwindigkeit und Datenmenge. Wenn diese Probleme einmal gelöst sind, wird der Einsatz der Blockchain-Technologie für Mainstream-Anwendungen realistischer. Es wird aber noch einige Jahre dauern, bis sich hier eine bestimmte Struktur durchgesetzt hat.

Bekannte Neuentwicklungen sind *Sharding*, eine Art Datenbankpartitionierung, bei der große Datenbanken in kleinere Teile, sogenannte *Data Shards*, aufgeteilt werden. Das Ethereum-Entwicklungsprojekt *Fork Choice Rule* teilt dabei die Ethereum-Blockchain in mehrere parallele Netzwerke auf. Möglicherweise kann Ethereum dadurch effizienter skalieren und die Netzwerklast deutlich verringern, die Transaktionsgeschwindigkeit erhöhen und Transaktionskosten senken.

Eine weitere bekannte Skalierungsmethode ist POS. In Kapitel 8 beschäftige ich mich ausführlicher damit. Im Wesentlichen geht es bei POS darum, Token oder Kryptowährungen als Sicherheit für die Abwicklung von Transaktionen zu hinterlegen. Wenn der Knoten korrumpiert ist und die Transaktionen nicht korrekt im

Sinne des Netzwerks verarbeitet, kann der Teilnehmer seine Token oder Kryptowährung verlieren.

Ein dritter Ansatz zur Skalierung der Blockchain-Technologie nutzt vertrauenswürdige Knoten. Das Factom-Netzwerk beispielsweise arbeitet mit mehreren zu einem Bund vereinigten Knoten und einer unbegrenzten Anzahl an Prüfknoten. Diesen Knoten wird die Sicherheit des Systems übertragen. Das Factom-Netzwerk ist klein, etwas mehr als 60 Knoten. Um Sicherheitsrisiken vorzubeugen, verankert sich Factom in anderen dezentralen Netzwerken und nutzt so die Sicherheit größerer Systeme. Das Factom-Netzwerk ist zudem in kleinere, schnellere und einfacher zu verwaltende Teile unterteilt. Diese werden als *Chains* bezeichnet. Factom verfügt über höhere Transaktionsgeschwindigkeiten und niedrigere Transaktionskosten als POW-Blockchains.

Konsens: Die treibende Kraft der Blockchains

Blockchains sind leistungsstarke Tools, weil sie ehrliche Systeme schaffen, die selbstkorrigierend sind, ohne dass eine dritte Partei diese Regeln durchsetzen muss. Die Regeln werden durch ihren Konsensalgorithmus erzwungen.

In der Blockchain-Welt ist *Konsens* der Prozess, mit dem eine Einigung innerhalb einer Gruppe grundsätzlich misstrauischer Teilnehmer erzielt wird. Diese Teilnehmer sind die vollständigen Knoten des Netzwerks. Die vollständigen Knoten werten die in das Netzwerk eingegebenen Transaktionen daraufhin aus, ob sie als Teil des Ledgers aufgezeichnet werden sollen.

Abbildung 1.2 zeigt, wie Blockchains eine Einigung erzielen.

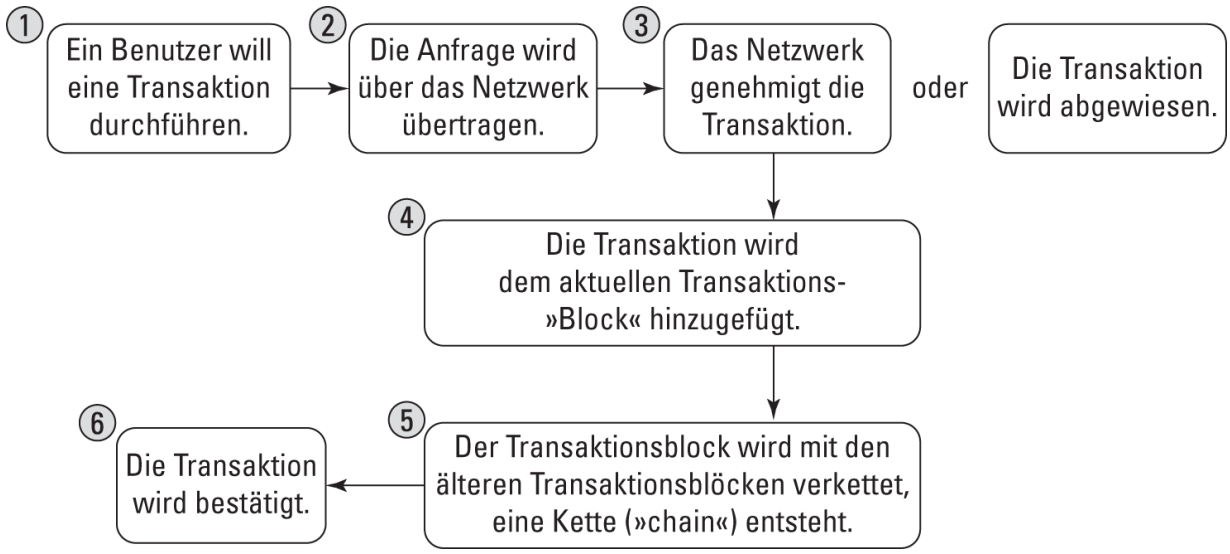


Abbildung 1.2: Wie Blockchains arbeiten

Jede Blockchain hat ihre eigenen Algorithmen, um sich über die hinzugefügten Netzwerkeinträge zu einigen. Es gibt viele verschiedene Modelle, Konsens zu erzielen, weil jede Blockchain andere Einträge erzeugt. Einige Blockchains handeln Vermögenswerte, andere speichern Daten, wieder andere sichern Systeme und Verträge.

Bitcoin beispielsweise handelt den Wert seines Tokens zwischen den Mitgliedern in seinem Netzwerk. Die Token haben einen Marktwert, die Anforderungen im Hinblick auf Leistung, Skalierbarkeit, Konsistenz, Angriffsmodell und Ausfallmodell sind deshalb höher. Bitcoin arbeitet unter der Annahme, dass ein böswilliger Angreifer den Verlauf der Handelstransaktionen verändern könnte, um Token zu stehlen. Bitcoin verhindert dies durch ein Konsensmodell, das auch als *Proof of Work* (POW) bezeichnet wird. Es löst das aus der Informatik und Mathematik bekannte Problem der byzantinischen Generäle: »Wie können Sie wissen, ob die Informationen, die Sie gerade sehen, nicht intern oder extern verändert wurden?« Datenintegrität ist ein großes Problem in der Informatik, weil es fast immer möglich ist, Daten zu verändern oder zu manipulieren.

Die meisten Blockchains arbeiten unter der Annahme, dass sie von außen oder durch Benutzer des Systems angegriffen werden.

Die erwartete Bedrohung und der Vertrauensgrad des Netzwerks in die Knoten, die die Blockchain betreiben, bestimmt die Art des Konsensalgorithmus, mit dem sie ihren Ledger (»Kontobuch«) führen. Bitcoin und Ethereum beispielsweise gehen von einer sehr hohen Bedrohung aus und verwenden mit Proof of Work einen starken Konsensalgorithmus. In diesen Netzwerken gibt es kein gegenseitiges Vertrauen.

Auf der anderen Seite des Spektrums können Blockchains, die Finanztransaktionen zwischen einander bekannten Parteien aufzeichnen sollen, einen leichteren und schnelleren Konsens verwenden. Hier ist es wichtiger, dass die Transaktionen schnell vonstattengehen. Proof of Work ist in diesem Zusammenhang zu langsam und zu teuer, weil es vergleichsweise wenige Teilnehmer im Netzwerk gibt und jede Transaktion unmittelbar abgeschlossen werden muss. Sie benötigen auch kein Token und keine Kryptowährung als Anreiz für die Transaktionsverarbeitung. Ohne diese Dinge laufen sie schneller und kostengünstiger als POW-Systeme.

Blockchains in der Praxis

Heute gibt es Tausende von Blockchains und Blockchain-Anwendungen. Die ganze Welt ist besessen von der Idee, Geld noch schneller zu bewegen, Verwaltungsaufgaben mithilfe eines verteilten Netzwerks zu lösen und sichere Anwendungen sowie sichere Hardware zu entwickeln.

An Kryptowährungsbörsen finden Sie viele Token dieser öffentlichen Blockchains wieder. Abbildung 1.3 zeigt beispielsweise die Altcoin-Börse für Poloniex (`https://poloniex.com`), eine Handelsplattform für Kryptowährungen.

Abbildung 1.3: Die Handelsplattform Altcoin

Blockchains dienen längst nicht mehr nur dem Handel von Marktwerten, sondern werden in den unterschiedlichsten Branchen eingesetzt. Sie schaffen eine neue Vertrauensebene, die Online-Transaktionen so sicher macht wie nie zuvor.

Derzeitige Anwendungen für Blockchains

Die meisten Blockchain-Anwendungen werden heute eingesetzt, um Geld oder andere Vermögenswerte schnell und kostengünstig zu bewegen. Dazu zählen der Aktienhandel, die Bezahlung von Mitarbeitern im Ausland oder auch der Währungsumtausch.

Blockchains werden auch als Teil eines Software-Sicherheitspakets eingesetzt. Das US-Ministerium für innere Sicherheit hat sich in jüngster Zeit mit Blockchain-Software beschäftigt, die IoT-Geräte (IoT = Internet of Things, Internet der Dinge) absichert. Der IoT-Bereich zieht den größten Nutzen aus dieser Innovation, weil er sehr empfindlich gegenüber

Manipulationen und Hacking ist. IoT-Geräte sind inzwischen allgegenwärtig, weshalb Sicherheit ein immer dringenderes Thema wird. Zu den wichtigsten Beispielen gehören Krankenhaussysteme, selbstfahrende Autos und Sicherheitssysteme.

Eine weitere interessante Blockchain-Innovation sind Initial Coin Offerings (ICOs). Es handelt sich um eine Art Smart Contract, der es dem Anbieter ermöglicht, ein Token im Austausch gegen Investmentkapital anzubieten. Initial Coin Offerings stellen oft eine eigenständige Fundraising-Option dar und haben Unternehmen weltweit viele Milliarden Dollar eingebracht. Regierungen sowie Regulierungsbehörden sind schnell gegen ICOs vorgegangen. Möglicherweise handelt es sich bei einigen Token um nicht lizenzierte Wertpapiere, und bei manchen Angebot werden die Investoren schlichtweg getäuscht. Die Technologie ist beeindruckend, auch wenn noch nicht alle rechtlichen Fragen geklärt sind.

Eine der herausragenden Eigenschaften der ICO-Token ist, dass sie ohne externes Clearing und Settlement auskommen. In unserem derzeitigen System für den Wertpapierhandel gibt es zwei Arten von Clearing-Stellen: Clearing-Gesellschaften und Verwahrstellen. Clearing-Gesellschaften prüfen Transaktionen und fungieren als Vermittler bei der Abwicklung. Die Verwahrstellen verfügen über Wertpapierzertifikate und führen Aufzeichnungen über die Eigentumsrechte an den Wertpapieren. Blockchains erfüllen beide Funktionen für Token, ohne dass Dritte die Vermögenswerte überprüfen und verwahren müssen. Mehr über ICO-Token erfahren Sie in Kapitel 5.

Blockchain-Anwendungen der Zukunft

Mittlerweile werden größere und langfristigere Blockchain-Projekte erforscht, unter anderem Anwendungen für behördliche Grundbuchsysteme, die digitale Identitätsvergabe sowie die Sicherheit im internationalen Reiseverkehr.

Die Möglichkeiten einer Zukunft mit allgegenwärtigen Blockchains haben die Fantasie von Geschäftsleuten, Regierungen, politischen Gruppen und humanitären Einrichtungen auf der ganzen Welt angeregt. Länder wie England, Singapur und die Vereinigten Arabischen Emirate betrachten Blockchains als Mittel zur Kostenreduktion, für neue Finanzinstrumente und saubere Datenaufzeichnungen. Dort wird aktiv im Bereich Blockchain investiert und geforscht.

Blockchains haben die Grundlage geschaffen, um Vertrauen aus der Gleichung herauszustreichen. Bislang war es sehr wichtig, Vertrauen zu schaffen. Mit Blockchains ist das kein Problem mehr. Außerdem kann die Infrastruktur, die bei Vertrauensbrüchen einspringt, um die Vereinbarungen durchzusetzen, viel schlanker ausfallen. Unsere Gesellschaft basiert zu einem großen Teil auf Vertrauen und der Umsetzung von Regeln. Die sozialen und wirtschaftlichen Auswirkungen von Blockchain-Anwendungen können aber auch emotional und politisch polarisieren, weil sich dadurch die Strukturen wertbasierter und sozialer Transaktionen ändern.

Kapitel 2

Eine Blockchain auswählen

IN DIESEM KAPITEL

- Die richtige Blockchain für Ihre Anforderungen finden
- Ihr Projekt planen
- Projekthindernisse erkennen
- Eine Roadmap für ein Projekt erstellen

Die Blockchain-Branche ist komplex und wächst beständig weiter; täglich kommen neue Möglichkeiten hinzu. Wenn Sie die drei Haupttypen von Blockchains mit ihren Einschränkungen kennen, wissen Sie, was mit dieser neuen Technologie möglich ist.

In diesem Kapitel wollen wir vor allem die Blockchain-Technologie einschätzen und einen Projektplan entwickeln. Es schafft die Grundlage für die folgenden Kapitel, die dann einzelne Blockchain-Plattformen und -Anwendungen behandeln.

Hier erfahren Sie, wie Sie die drei verschiedenen Blockchain-Plattformtypen einordnen und nutzen können – und warum. Ich gebe Ihnen einige Werkzeuge an die Hand, mit denen Sie Ihr Projekt besser umreißen, Hürden im Voraus erkennen und Herausforderungen bewältigen können.

Wo Blockchains für Mehrwert sorgen

Es ranken sich zahlreiche Gerüchte um Blockchains und die dazugehörigen Kryptowährungen. Einige davon sind in den Wertschwankungen der Kryptowährungen begründet. Sie

spiegeln aber auch die Angst wider, dass die Blockchain-Technologie viele Funktionen in Wirtschaft und Verwaltung überflüssig machen könnte.

Es wurde viel Geld in die Forschung und Entwicklung gesteckt, weil die Beteiligten auf der Höhe der Zeit bleiben und die Unternehmer neue Geschäftsmodelle erkunden wollen. Häufig stellt sich also die Frage: »Wo liegt der Mehrwert von Blockchains, und wie unterscheiden sie sich von vorhandenen Technologien?«

Blockchains sind eine besondere Art von Datenbank. Sie können überall eingesetzt werden, wo man eine normale Datenbank verwenden würde. Jedoch ist es eigentlich wenig sinnvoll, Arbeit und Geld in eine Blockchain zu investieren, wenn eine normale Datenbank auch ausreichen würde.

Die Blockchain lohnt sich dann, wenn man Informationen mit Parteien austauschen will, denen man nicht vollständig vertraut, wenn Daten von Dritten überprüft werden müssen oder wenn das Risiko besteht, dass Daten intern oder extern manipuliert werden. Es ist nicht einfach, diesen Anforderungen zu genügen, und es kann sehr schwierig sein, die richtigen Lösungen zu finden.

Dieser Abschnitt hilft Ihnen, Ihre Optionen einzugrenzen.

Anforderungen bestimmen

Blockchains gibt es in den unterschiedlichsten Varianten. Sie werden die passende Blockchain für Ihre Anforderungen finden, aber die Suche ist nicht ganz einfach! Es kann sehr aufwendig sein, Ihre Anforderungen an die optimale Blockchain zu formulieren. Wenn ich mit vielen Möglichkeiten und teils widersprüchlichen Anforderungen konfrontiert bin, nutze ich gerne eine gewichtete Entscheidungsmatrix.

Die gewichtete Entscheidungsmatrix ist ein tolles Werkzeug, um Projektanforderungen zu bewerten und sie dann möglichen Lösungen zuzuordnen. Der wichtigste Vorteil der Matrix ist, dass sie damit einzelne Anforderungen an Ihr Projekt besser quantifizieren und ihnen Prioritäten zuordnen können. So

vereinfachen Sie Ihren Entscheidungsprozess. Außerdem laufen Sie mit diesem Hilfsmittel nicht mehr Gefahr, sich in der Fülle der Kriterien verlieren. Wenn Sie das Tool richtig einsetzen, finden Sie am Ende eine optimale Lösung, die mit allen Ihren Zielen kompatibel ist.

Gehen Sie folgendermaßen vor, um eine gewichtete Entscheidungsmatrix zu erstellen:

1. **Ermitteln Sie in einem Brainstorming die wichtigsten Kriterien oder Ziele für Ihr Team.**

   
   Wenn Sie nicht sicher sind, welche Kriterien Sie bei der Bewertung Ihres Blockchain-Projekts berücksichtigen sollen, könnten Sie beispielsweise die folgenden Aspekte in Betracht ziehen:

   - ✔ Skalierbarkeit und Durchsatz
   - ✔ Geschwindigkeit und Latenz
   - ✔ Sicherheit und Unveränderbarkeit
   - ✔ Speicherkapazität und strukturelle Anforderungen

   Ihr Team hat wahrscheinlich eine eigene Liste mit Zielen und Prioritäten. Hier sind nur ein paar wenige aufgeführt, an die Sie bei der Suche nach der richtigen Plattform für Ihre Anforderungen denken sollten.

2. **Reduzieren Sie die Kriterienliste, bis sie höchstens noch zehn Einträge enthält.**

   
   Wenn Sie Schwierigkeiten beim Kürzen Ihrer Kriterienliste haben, nutzen Sie eine Vergleichsmatrix.

3. **Erstellen Sie in Microsoft Excel oder mit einem vergleichbaren Programm eine Tabelle.**
4. **Geben Sie in die erste Spalte die Entwicklungskriterien ein.**
5. **Weisen Sie jedem Kriterium ein relatives Gewicht zu, abhängig davon, wie wichtig dieses Ziel für den**

Projekterfolg ist.

Begrenzen Sie die Anzahl der Punkte auf zehn, und verteilen Sie sie gleichmäßig auf alle Ihre Kriterien, zum Beispiel 1 = geringe, 2 = mittlere und 3 = hohe Priorität.


Wenn Sie in einem Team arbeiten, lassen Sie jedes Teammitglied die Kriterien separat gewichten.

6. **Addieren Sie die Punkte für jedes Ziel, und dividieren Sie die Summe durch die Anzahl der Teammitglieder, um eine zusammengesetzte Teamgewichtung zu erhalten.**
7. **Nehmen Sie alle notwendigen Anpassungen an den Gewichtungen vor, um sicherzustellen, dass alle Kriterien korrekt gewichtet sind.**

Herzlichen Glückwunsch! Jetzt haben Sie eine Rangfolge Ihrer Kriterien, die erfüllt sein müssen, um Ihr Blockchain-Projekt zum Erfolg zu führen.

Ihr Ziel definieren

In einem Blockchain-Projekt, dessen Ziel oder Zweck nicht präzise definiert ist, können Sie sich leicht verlieren. Nehmen Sie sich genug Zeit, um herauszufinden, was Sie mit Ihrem Team erreichen möchten. Ein Ziel könnte beispielsweise sein, mit einem Partnerunternehmen Vermögenswerte ohne Vermittler zu handeln. Dies ist ein häufig formuliertes und wichtiges Ziel.

Planen Sie zunächst ein kleines Projekt, das einen passenden Anwendungsfall für die Technologie darstellt und anhand dessen Sie leicht erkennen können, ob sich ein Mehrwert oder Einsparungen für Ihr Unternehmen ergeben. Ein Etappenziel könnte auch ein privates Netzwerk sein, über das Vermögenswerte zwischen vertrauenswürdigen Parteien ausgetauscht werden können.

Auf diesem Ergebnis bauen Sie auf. Die nächste Stufe könnte die Entwicklung eines Instruments sein, das auf Ihrer neuen Plattform

handelbar ist. Jeder Schritt sollte ein kleiner Schritt nach vorne sein und einen Mehrwert generieren.

Eine Lösung auswählen

Es gibt drei wichtige Arten von Blockchains: öffentliche Netzwerke wie Bitcoin, Permissioned Blockchains wie Ripple und private Netzwerke wie Hijro.

Blockchains erfüllen einige Grundfunktionen:

- ✔ Sie transferieren und handeln Vermögenswerte schnell und zu sehr geringen Kosten.
- ✔ Sie erstellen nahezu dauerhafte Datenverläufe.

Die Blockchain-Technologie unterstützt auch etwas komplexere Anwendungsfälle: Sie können beispielsweise beweisen, dass Sie eine bestimmte »Sache« besitzen, ohne diese der anderen Partei offenlegen zu müssen. Und es ist auch möglich, einen »Negativbeweis« zu führen beziehungsweise zu überprüfen, was innerhalb einer Datenmenge oder eines Systems fehlt. Diese Funktion ist besonders für Betriebsprüfungen etc. nützlich.

Tabelle 2.1 listet allgemeine Anwendungsfälle auf, für die sich die verschiedenen Blockchain-Typen eignen.

Primärer Zweck	*Blockchain-Typ*
Vermögenswerte zwischen nicht vertrauenswürdigen Parteien übertragen	öffentlich
Vermögenswerte zwischen vertrauenswürdigen Parteien übertragen	privat
Nicht gleichartige Gegenstände übertragen	permissioned
Gleichartige Gegenstände übertragen	öffentlich
Eine dezentrale Organisation aufbauen	öffentlich oder permissioned

Primärer Zweck	*Blockchain-Typ*
Einen dezentralen Vertrag erzeugen	öffentlich oder permissioned
Verbriefte Vermögenswerte handeln	öffentlich oder permissioned
Digitale Identität für Menschen oder Dinge entwickeln	öffentlich
Öffentliche Aufzeichnungen veröffentlichen	öffentlich
Private Aufzeichnungen veröffentlichen	öffentlich oder permissioned
Aufzeichnungen oder Systeme prüfen	öffentlich oder permissioned
Grundbuchdaten veröffentlichen	öffentlich
Digitales Geld oder Vermögenswerte handeln	öffentlich oder permissioned
Systeme für die IoT-Sicherheit (Internet of Things) entwickeln	öffentlich
Systemsicherheit aufbauen	öffentlich

Tabelle 2.1: Häufige Anwendungsfälle und die dafür geeigneten Blockchains

Je nach Projekt kann es Ausnahmen geben, und es kann sein, dass Sie Ihr Ziel mit einem anderen Blockchain-Typ besser erreichen. Im Allgemeinen können die verschiedenen Netzwerke mit ihren Stärken und Schwächen jedoch folgendermaßen eingeteilt werden:

- **Öffentliche Netzwerke** sind groß und dezentral, und jeder kann sich an ihnen auf beliebiger Ebene beteiligen: etwa einen voll funktionsfähigen Netzwerkknoten betreiben, Kryptowährungen schürfen, Token handeln oder Einträge veröffentlichen. Öffentliche Blockchains sind sicherer und unveränderlicher als private oder Permissioned Blockchains. Häufig sind sie langsamer und teurer in der Verwendung. Sie werden mit einer Kryptowährung abgesichert und haben eine begrenzte Speicherkapazität.

- ✔ **Permissioned Blockchains** können von der Öffentlichkeit eingesehen werden, aber die Teilnahme erfolgt kontrolliert. Viele von ihnen nutzen eine Kryptowährung, aber die darauf aufgebauten Anwendungen sind im Betrieb häufig kostengünstiger. Projekte lassen sich dadurch besser skalieren und Transaktionsvolumina erhöhen. Permissioned Blockchains sind teilweise sehr schnell und weisen mitunter eine sehr viel geringere Latenz und eine höhere Speicherkapazität gegenüber öffentlichen Netzwerken auf.
- ✔ **Private Netzwerke** werden von vertrauenswürdigen Parteien geteilt und sind nicht unbedingt für die Öffentlichkeit einsehbar. Sie sind sehr schnell, eventuell sogar latenzfrei. Außerdem ist ihr Betrieb günstiger, und sie lassen sich innerhalb eines arbeitsintensiven Wochenendes einrichten. Die meisten privaten Netzwerke verzichten auf eine eigene Kryptowährung und sind nicht so unveränderbar und sicher wie dezentrale Netzwerke. Die Speicherkapazität ist teilweise unbegrenzt.

Es gibt auch Hybridformen dieser drei Blockchain-Haupttypen, die das richtige Maß an Sicherheit, Überprüfbarkeit, Skalierbarkeit und Speicherkapazität für die darauf aufbauenden Anwendungen erreichen sollen.

Einen Entscheidungsbaum für eine Blockchain zeichnen

Manche Entscheidung im Zusammenhang mit einem Blockchain-Projekt in Ihrem Unternehmen kann schwierig und komplex sein. Nehmen Sie sich unbedingt genug Zeit für die Entscheidungsfindung hinsichtlich folgender Punkte:

- ✔ **Unsicherheit**: Viele Faktoren rund um die Blockchain-Technologie sind möglicherweise neu und ungetestet.
- ✔ **Komplexität**: Es gibt viele zusammenhängende Faktoren, die im Hinblick auf Blockchains berücksichtigt werden müssen.

- ✔ **Hoch riskante Folgen**: Die Entscheidungen können sich später signifikant auf Ihr Unternehmen auswirken.
- ✔ **Alternativen**: Es gibt möglicherweise alternative Technologien und Blockchain-Typen mit jeweils eigenen Unsicherheiten und Konsequenzen.
- ✔ **Personelle Aspekte**: Sie müssen herausfinden, wie sich die Blockchain-Technologie auf die verschiedenen Mitarbeiter Ihres Unternehmens auswirken könnte.

Ein Entscheidungsbaum ist ein praktisches Werkzeug, mit dem Sie Konsequenzen, Ergebnisse, Ressourcenkosten und den Nutzen eines Blockchain-Projekts besser erkennen können.

Sie können Entscheidungsbäume auf Papier zeichnen oder ein Programm dafür verwenden. So zeichnen Sie einen Entscheidungsbaum, der weitere Herausforderungen im Zusammenhang mit Ihrem Projekt aufdeckt:

1. **Nehmen Sie ein großes Blatt Papier.**


Je mehr Auswahlmöglichkeiten es gibt und je komplizierter die Entscheidung ist, desto größer sollte der Bogen sein.

2. **Zeichnen Sie auf der linken Seite des Bogens ein Quadrat.**
3. **Notieren Sie in diesem Quadrat eine Beschreibung des Hauptziels sowie der Kriterien für Ihr Projekt.**
4. **Ziehen Sie rechts vom Quadrat für jedes Problem eine Linie.**
5. **Notieren Sie auf jeder Linie eine Beschreibung des Problems.**


Weisen Sie jedem Aspekt einen Wahrscheinlichkeitswert zu.

6. **Suchen Sie per Brainstorming Lösungen für jedes Problem.**

7. **Notieren Sie an jeder Linie eine Beschreibung der einzelnen Lösungen.**
8. **Fahren Sie so fort, bis Sie jedes Problem untersucht und mögliche Lösungen gefunden haben.**

Bitten Sie Ihre Teammitglieder, die Probleme und Lösungen zu überprüfen, bevor Sie die Auswertung abschließen.

Einen Plan machen

Jetzt sollten Sie eine genaue Vorstellung von Ihren Zielen und den auftretenden Hürden haben und wissen, welche Blockchain-Optionen für Sie infrage kommen.

Hier ist ein einfacher Entwicklungsplan für Ihr Projekt:

1. **Erläutern Sie das Projekt den wichtigsten Beteiligten, und diskutieren Sie mit ihnen die Kernkomponenten und die erwarteten Ergebnisse.**
2. **Erstellen Sie einen Projektplan.**

   Diese Dokumente verändern sich im Laufe Ihres Projekts immer wieder.
3. **Entwickeln Sie Erfolgskennzahlen, Rahmenbeschreibung, Zeitplan und Kostenvoranschlag.**
4. **Denken Sie über einen Risikomanagementplan und einen Personalplan nach.**
5. **Holen Sie Zustimmungen ein, definieren Sie Rollen und Verantwortlichkeiten.**
6. **Organisieren Sie ein Kick-off-Meeting, um das Projekt zu starten.**

   Bei dem Meeting sollten die folgenden Dinge angesprochen werden:

   - Vision
   - Strategie
   - Zeitleiste

- Rollen und Verantwortlichkeiten
- Aufbau des Teams
- Pflichten des Teams
- Wie soll das Team Entscheidungen treffen?
- Schlüsselkennzahlen zur Projektbewertung

Nach Projektabschluss sind Sie längst nicht fertig! Analysieren Sie Ihre Erfolge und Misserfolge. Hier sind einige Fragen, die Sie sich stellen sollten:

- ✔ Sind die wichtigsten Beteiligten zufrieden?
- ✔ Liegt das Projekt im Zeitplan?
- ✔ Wenn nicht: Wodurch ist die Verzögerung entstanden?
- ✔ Was habe ich aus diesem Projekt gelernt?
- ✔ Was hätte ich anders machen können?
- ✔ Habe ich für mein Unternehmen einen Mehrwert geschaffen oder Geld eingespart?

Lesen Sie dieses Kapitel noch einmal, wenn Sie mehr über die Blockchain-Technologie erfahren haben und einen Projektplan entwickeln möchten.

Kapitel 3

Einstieg in Blockchain

IN DIESEM KAPITEL

- Eine Bitcoin- und eine Ethereum-Wallet erstellen und nutzen
- Bitcoin in Ether umtauschen
- Ein Blockchain-Asset erstellen
- Ein Blockchain-Asset vermieten
- Eine private Blockchain bereitstellen

Blockchains sind sehr mächtige Werkzeuge. Sie werden weltweit tief greifende Änderungen bei Finanztransaktionen, Systemsicherheit und digitalen Identitäten bewirken. Wenn Sie nicht gerade ein Core-Entwickler sind, werden Sie in naher Zukunft wahrscheinlich kaum tiefer in die Blockchain-Entwicklung einsteigen. Sie sollten aber verstehen, wie Blockchains funktionieren und welche Grenzen sie grundsätzlich haben, da sie schon bald Bestandteil vieler alltäglicher Online-Interaktionen sein werden: von Unternehmen, die darüber ihre Mitarbeiter bezahlen, bis hin zu Regierungen, die mit ihrer Hilfe die Integrität ihrer Systeme und Daten sicherstellen.

In diesem Kapitel steigen Sie direkt in die Blockchain-Technologie ein. Sie kaufen Ihre erste Kryptowährung und lernen, sie in andere Währungen umzutauschen. Sie richten besondere Anwendungen ein, die Ihnen Zugang zu einem ganzen Ökosystem von dezentralen Anwendungen (Dapps) ermöglichen. Sie richten auch eine sichere Umgebung zur Verwendung Ihrer Kryptowährung ein. In diesem Kapitel erstellen und vermieten Sie außerdem digitale Blockchain-Assets in einem Blockchain-Spiel.

Nachdem Sie dieses Kapitel durchgearbeitet haben, werden Sie viele Grundfunktionen der Blockchain-Technologie verstehen. Sie bekommen auch ein grundlegendes Verständnis für einige zusätzliche Sicherheitsvorkehrungen, die Sie beim Umgang mit Kryptowährungen treffen sollten. Außerdem erfahren Sie in diesem Kapitel, wie Sie die Kryptokonten anlegen, die Sie in späteren Kapiteln brauchen.

Die Blockchain-Technologie

Die Ethereum-Blockchain ist eine der größten und leistungsstärksten Blockchains der Welt. Ihr Hauptziel ist es, eine Plattform zur Entwicklung von Dapps bereitzustellen. Das sind Anwendungen, die auf einem dezentralisierten Netzwerk aufbauen, dessen Teilnehmer sich nicht gegenseitig vertrauen müssen. Im Ethereum-Netzwerk realisieren Entwickler diese Anwendungen mithilfe sogenannter Smart Contracts. Auch für Ethereum gibt es eine Kryptowährung namens Ether. Dies wird verwendet, um Netzwerkteilnehmer für die Bereitstellung von Rechenleistung und die Schaffung des Trustless-Systems zu belohnen, auf dem die Smart Contracts überhaupt erst ausgeführt werden können.

Smart Contracts sind keine normalen Verträge. Es handelt sich dabei um Programmcode, der auf einem dezentralen Netzwerk ausgeführt wird. Wie ein Geschäftsvertrag enthalten sie vordefinierte Bedingungen. Ein wesentlicher Unterschied ist, dass die Einhaltung von Smart Contracts durch das jeweilige Blockchain-Netzwerk durchgesetzt wird. Smart Contracts stellen eine wichtige IT-Innovation dar. Personen, die sich nicht kennen oder gegenseitig vertrauen, können plötzlich zusammenarbeiten, ohne dass jemand Angst haben müsste, dass sich die andere Partei nicht an die zuvor vereinbarten Bedingungen hält.

Blockchains mit Kryptowährungen werden manchmal als Trustless-Systeme bezeichnet, weil der Code vom Netzwerk durchgesetzt wird (anders als ein Geschäftsvertrag, der durch die Gesetzgebung abgesichert ist).

In den folgenden Abschnitten richten Sie Konten für Ihren ersten Bitcoin-Kauf ein. Außerdem tauschen Sie Bitcoin in Ether, damit Sie in den nachfolgenden Abschnitten Ethereum-Dapps nutzen können.

Eine sichere Umgebung einrichten

Zuerst müssen Sie sich eine sichere Online-Umgebung schaffen. Immer mehr Gründe sprechen für einen sicheren Browser und ein Virtual Private Network (VPN). Diese verhindern, dass Ihre Daten ohne Ihre Zustimmung gesammelt werden, und helfen, Hacker abzuwehren. Wenn Sie Kryptowährungen mit einer ungesicherten Internetverbindung verwenden, können Sie leicht zum Ziel von Hackerangriffen werden

In diesem Abschnitt laden Sie den Brave-Webbrowser, ProtonVPN und die Browser-Erweiterung MetaMask herunter. Alle drei Dienste können Sie kostenfrei nutzen. Gegen Gebühr bieten sie aber erweiterte Funktionen.

Legen Sie ein Blatt Papier und einen Stift bereit, um wichtige Informationen aufzuschreiben. Machen Sie niemals Screenshots oder Fotos von sensiblen Informationen wie Passwörtern oder Seed-Phrasen.

Den Brave-Browser herunterladen und installieren

Brave ist ein neuer, sicherer Webbrowser auf der Basis von Google Chromium. Er ist schnell, quelloffen und legt den Fokus auf Datenschutz. Werbung und Tracker werden blockiert, und über eine besondere Funktion können Sie die Herausgeber Ihrer Lieblingswebsites mit Token belohnen. Brave ist ein Projekt des

Internetpioniers Brendan Eich, der bereits JavaScript erfand und auch Mozilla mitbegründete.

Um den Brave-Webbrowser herunterzuladen, gehen Sie wie folgt vor:

1. **Gehen Sie auf** https://brave.com**.**
2. **Klicken Sie auf DOWNLOAD BRAVE.**
3. **Öffnen Sie Ihren Downloads-Ordner.**
4. **Doppelklicken Sie die Brave-Browser-Datei.**
5. **Ziehen Sie das neue Brave-Browser-Symbol in Ihren Anwendungsordner.**

Jetzt haben Sie einen sichereren Web-Browser und können die Blockchain-Erweiterung hinzufügen, mit der Sie dezentrale Anwendungen ausprobieren können.

ProtonVPN herunterladen und installieren

ProtonVPN ist ein VPN eines Schweizer Unternehmens. Wenn Sie mit ProtonVPN im Internet surfen, ist Ihre Internetverbindung verschlüsselt, sodass potenzielle Angreifer Ihre Aktivitäten nicht belauschen können. Sie bekommen damit teilweise auch auch Zugriff auf geoblockierte Websites.

Befolgen Sie diese Schritte, um ProtonVPN herunterzuladen:

1. **Gehen Sie auf** https://protonvpn.com .
2. **Klicken Sie auf GET PROTONVPN NOW.**
3. **Klicken Sie auf GET FREE.**
4. **Geben Sie Ihre E-Mail-Adresse ein.**

Befolgen Sie diese Schritte, um ProtonVPN zu installieren:

1. **Öffnen Sie Ihren Downloads-Ordner am Mac oder PC.**
2. **Doppelklicken Sie auf die ProtonVPN-Datei.**

3. **Ziehen Sie das neue ProtonVPN-Symbol in Ihren Anwendungsordner.**

Ein VPN ist eine gute zusätzliche Sicherheitsebene für Ihre Internetverbindung.

MetaMask herunterladen, installieren und absichern

MetaMask ist eine Browser-Erweiterung, mit der Sie Ethereum-Dapps direkt in Ihrem Browser ausführen können, ohne einen Ethereum-Fullnode zu betreiben. (Ethereum ist eine der größten Blockchains der Welt; siehe Kapitel 5 für weitere Informationen.) MetaMask verfügt über einen sicheren Identitätsspeicher. Sie können sich damit auf Websites anmelden, Ihre Identitäten im Web verwalten und Blockchain-Transaktionen signieren. Sie können auch etwas Ether in Ihrer MetaMask-Wallet aufbewahren, um Online-Zahlungen durchzuführen.

Befolgen Sie diese Schritte, um MetaMask herunterzuladen und zu installieren:

1. **Öffnen Sie den Brave-Webbrowser.**

   Lesen Sie den Abschnitt »Den Brave-Browser herunterladen und installieren« weiter vorne in diesem Kapitel, falls Sie das Programm noch nicht installiert haben.
2. **Gehen Sie auf** `https://metamask.io`**.**
3. **Klicken Sie auf GET CHROME EXTENSION.**
4. **Klicken Sie auf ADD TO CHROME.**
5. **Klicken Sie im Pop-up-Fenster auf ADD EXTENSION.**

   In der oberen rechten Ecke Ihres Brave-Browsers sollte jetzt ein kleines Fuchssymbol erscheinen.

Da MetaMask eine Wallet ist, müssen Sie diese auch mit einem starken Passwort schützen und Ihre Backup-Phrase sicher aufbewahren. Damit können Sie die Wallet wiederherstellen, wenn Sie Ihr Passwort verlieren.

Schnappen Sie sich einen Stift und einen Notizblock oder ein Blatt Papier, das Sie gut verstecken können. Befolgen Sie dann diese Schritte:

1. **Schreiben Sie oben auf den Zettel »MetaMask«, »Brave-Browser«, das Datum und das Gerät, auf dem Sie es installiert haben.**
2. **Öffnen Sie den Brave-Webbrowser.**
3. **Klicken Sie oben rechts auf das Fuchssymbol.**
4. **Klicken Sie auf GET STARTED.**
5. **Klicken Sie auf CREATE A WALLET.**
6. **Geben Sie ein starkes und einzigartiges Passwort ein.**
7. **Schreiben Sie Ihr Passwort auf.**
8. **Klicken Sie auf CREATE.**

Holen Sie sich für die nächsten Schritte ein weiteres Notizbuch oder einen anderen Zettel. Verwenden Sie nicht dasselbe Notizbuch oder denselben Zettel, auf dem Sie gerade Ihr Passwort notiert haben.

1. **Schreiben Sie oben auf den Zettel »MetaMask«, »Brave-Browser«, das Datum und das Gerät, auf dem Sie es installiert haben, und »Seed-Phrase«.**
2. **Klicken Sie auf das Schlosssymbol.**
3. **Schreiben Sie die Passphrase aus zwölf Wörtern auf.**
4. **Klicken Sie auf NEXT.**
5. **Klicken Sie die Wörter der notierte Passphrase in der richtigen Reihenfolge an.**
6. **Klicken Sie auf ALL DONE.**

Laminieren Sie die Zettel mit Ihrem Passwort und der Back-up-Phrase gegebenenfalls. Und denken Sie daran, die beiden Dokumente nicht am selben Ort aufzubewahren.

Zum ersten Mal Bitcoin kaufen

Es gibt mehrere Orte, an denen Sie Bitcoin kaufen können. Wenn Sie in Europa sind, müssen Sie beim Einrichten Ihres Benutzerkontos erst einen Verifizierungsprozess durchlaufen und es mit Ihrer Kreditkarte oder Ihrem Bankkonto verknüpfen. Es kann ein oder zwei Tage dauern, bis Sie authentifiziert sind und Ihre ersten Coins kaufen können. In Europa empfiehlt sich eine der folgenden Websites:

- ✔ Bitcoin.de: www.bitcoin.de
- ✔ Bl3P: https://bl3p.eu
- ✔ LiteBit: www.litebit.eu
- ✔ AnycoinDirect: https://anycoindirect.eu

Gehen Sie auf eine dieser Seiten – oder auf eine andere –, und legen Sie ein Benutzerkonto an. Zunächst sollten Sie Kryptowährungen im Wert von zehn bis 20 Euro erwerben. Ich empfehle den Kauf von Bitcoin, weil diese Währung überall akzeptiert wird und gegen sämtliche anderen Kryptowährungen gehandelt werden kann. Vielleicht haben Sie auch die Möglichkeit, direkt Ether zu erwerben, die Kryptowährung von Ethereum, die zur Ausführung von Dapps verwendet wird. Falls ja, kaufen Sie auch gleich Ether im Wert von fünf bis zehn Euro, denn Sie werden sie im nächsten Abschnitt benötigen. Wenn Sie nur Bitcoin für Euro bekommen, ist das aber auch kein Problem. Sie können sie später in Ihrer Wallet mit dem Umtauschdienst Shapeshift in Ether wechseln.

Denken Sie bitte stets daran, dass Kryptowährungen eine regulatorische Grauzone darstellen. Während ich dies schreibe, ist es möglich, Geld über diese Websites zu kaufen und abzuheben. In der Zukunft sind der Kauf oder die Abhebung von Kryptowährungen eventuell nicht mehr möglich, oder vielleicht ist das in Ihrem Land sogar bereits jetzt der Fall. Falls Sie davon betroffen sind, sollten Sie zu Kapitel 5 übergehen. Dort können

Sie durch Mining im Ethereum-Testnetz Ihre eigenen Test-Ether erhalten.

Kryptowährungen absichern und handeln

Wenn Sie in Ihrem Benutzerkonto Ether direkt erwerben konnten, überspringen Sie diesen Abschnitt ruhig. Sie richten hier eine Jaxx-Wallet ein, über deren integrierte Handelsbörse ShapeShift Sie Ihre Bitcoin in Ether umtauschen können. Die Jaxx-Wallet wurde von Anthony Di Iorio entwickelt. Er ist ein Blockchain-Pionier und Mitbegründer von Ethereum.

Sie können die Wallet auf einen Computer oder ein Smartphone herunterladen. Für diese Übung nutzen Sie die Chrome-Erweiterung. Wenn Sie sich für die anderen Wallet-Arten entscheiden, bedenken Sie, dass Ihre Geräte gefährdet sein können. Kryptodiebstahl erfolgt über Social Engineering, wie etwa einen SIM-Karten-Hack. Auch eine unsichere Internetverbindung kann Sie um Ihr Erspartes bringen. Jaxx ist mit dem Internet verbunden und gilt als sogenannte Hot Wallet, die daher auch entsprechende Angriffsflächen aufweist.

Ein paar Dinge können Sie tun, um das Risiko zu minimieren:

- ✔ Nutzen Sie Ihr VPN.
- ✔ Nutzen Sie Google Authenticator.
- ✔ Nutzen Sie eine Google-Voice-Telefonnummer.
- ✔ Verwenden Sie eine separate E-Mail-Adresse exklusiv für Ihre Kryptowährungskonten.
- ✔ Verwenden Sie für Ihre Kryptoaktivitäten einen Rechner, der stets eine gesicherte Internetverbindung nutzt.

- ✔ Speichern Sie niemals Passwörter oder Recovery-Seeds in elektronischer Form.

Jaxx herunterladen

In diesem Abschnitt laden Sie eine Kryptowährungs-Wallet herunter und richten sie ein. Von diesen Programmen zur sicheren Verwahrung von Bitcoin und andere Kryptowährungen gibt es etliche. Jaxx Liberty ist eine benutzerfreundliche Wallet, die über 85 verschiedene Kryptowährungen unterstützt. Sie funktioniert gut unter iOS, Android, am Desktop-PC und auch als Google-Chrome-Version. Natürlich können Sie sich auch Alternativen ansehen. Exodus.io (www.exodus.io) ist beispielsweise eine weitere sehr gute und benutzerfreundliche Wallet.

1. **Gehen Sie in Ihrem Brave-Browser auf https://jaxx.io.**
2. **Klicken Sie auf DOWNLOAD.**
3. **Klicken Sie auf AVAILABLE IN THE CHROME WEB STORE.**
4. **Klicken Sie auf ADD TO CHROME.**
5. **Klicken Sie im Pop-up-Fenster auf ADD EXTENSION.**

Die Jaxx-Wallet absichern

Jetzt sind Sie bereit, Ihre Jaxx-Wallet abzusichern. Sie brauchen mindestens zwei leere Zettel, um Ihr Passwort und Ihre Seed-Phrase aufzuschreiben.


Bewahren Sie Passwort und Seed-Phrase immer getrennt voneinander auf.

Befolgen Sie diese Schritte:

1. **Schreiben Sie oben auf den Zettel »Jaxx«, »Brave-Browser«, das Datum und das Gerät, auf dem Sie Jaxx installiert haben.**

2. **Öffen Sie den Brave-Webbrowser.**
3. **Klicken Sie auf das Herz in der oberen rechten Ecke.**
4. **Klicken Sie auf CREATE NEW WALLET.**
5. **Klicken Sie auf I AGREE.**
6. **Klicken Sie auf CONTINUE.**
7. **Klicken Sie auf BACK UP NOW.**
8. **Haken Sie das Kontrollfeld im Warnfenster ab.**
9. **Klicken Sie auf START BACKUP.**
10. **Schreiben Sie Ihre Seed-Phrase durchnummeriert auf.**
11. **Tippen Sie die Worte in der richtigen Reihenfolge ein.**
12. **Klicken Sie auf CONFIRM.**
13. **Klicken Sie auf JAXX LIBERTY HOME.**

Im nächsten Abschnitt erstellen Sie ein sicheres Passwort für Ihre Jaxx-Wallet im Brave-Browser. Überspringen Sie diesen Schritt nicht! Sie brauchen das Passwort später, um auf Ihr Guthaben zuzugreifen.

Befolgen Sie diese Schritte:

1. **Schreiben Sie oben auf den Zettel »Jaxx«, »Brave-Browser«, das Datum und das Gerät, auf dem Sie Jaxx installiert haben.**
2. **Öffen Sie den Brave-Webbrowser.**
3. **Klicken Sie auf das Herz in der oberen rechten Ecke.**
4. **Klicken Sie auf das Menüsymbol in Ihrer Jaxx-Wallet.**
5. **Klicken Sie auf SECURITY PASSWORD.**
6. **Haken Sie die Kontrollfelder im Warnfenster ab.**
7. **Klicken Sie auf SET PASSWORD.**
8. **Schreiben Sie ein starkes, einzigartiges Passwort auf Ihren Zettel.**

9. **Geben Sie Ihr Passwort zweimal ein, und klicken Sie auf CONTINUE.**


Bewahren Sie die beiden Zettel an zwei verschiedenen Orten auf. Zur Sicherheit können Sie sie auch laminieren.

Bitcoin in die Jaxx-Wallet transferieren

In diesem Abschnitt überweisen Sie einen geringen Bitcoin-Betrag an Ihre Jaxx-Wallet im Brave-Browser. Überspringen Sie diesen Schritt nicht! Sie brauchen die Bitcoins später, um Ether für die CryptoKitties-Übung zu kaufen.

Befolgen Sie diese Schritte:

1. **Öffen Sie den Brave-Webbrowser.**
2. **Klicken Sie auf das Herz in der oberen rechten Ecke.**
3. **Klicken Sie auf WALLETS.**
4. **Klicken Sie auf BITCOIN.**
5. **Klicken Sie auf RECEIVE.**
6. **Klicken Sie auf COPY ADDRESS.**

Bitcoin in Ether umtauschen

Jetzt müssen Sie das Benutzerkonto öffnen, in dem Sie Ihr Bitcoin-Guthaben aufbewahren. Sie suchen nach einem Transfer- oder Senden-Button und fügen die Adresse in das Empfängerfeld ein. Sobald Ihre Bitcoins in der Jaxx-Wallet sichtbar werden, können Sie die Exchange-Funktion nutzen. Befolgen Sie diese Schritte:

1. **Öffen Sie den Brave-Webbrowser.**
2. **Klicken Sie auf das Herz in der oberen rechten Ecke.**
3. **Klicken Sie auf WALLETS.**

4. **Klicken Sie auf BITCOIN.**
5. **Klicken Sie auf EXCHANGE.**
6. **Wählen Sie unter RECEIVE FROM SHAPESHIFT den Eintrag ETHEREUM (ETH).**
7. **Geben Sie den gewünschten Wechselbetrag ein.**

   Für die nächste Übung brauchen Sie fünf bis zehn Euro in Ether.
8. **Klicken Sie auf CONTINUE.**
9. **Klicken Sie auf CONNECT SHAPESHIFT.**

   Eventuell werden Sie aufgefordert, ein ShapeShift-Konto einzurichten. Wenn ja, richten Sie eines ein und treffen dabei die gleichen Vorsichtsmaßnahmen wie bei Ihren Jaxx- und MetaMask-Konten.
10. **Klicken Sie auf EXCHANGE.**

Guthaben in die MetaMask-Wallet transferieren

Nachdem der Umtausch abgeschlossen ist, können Sie die gleichen Anweisungen wie zuvor befolgen, um Ether an Ihr MetaMask-Konto zu senden:

1. **Öffnen Sie das Benutzerkonto mit Ihrem Ether-Guthaben.**
2. **Klicken Sie auf SEND.**
3. **Klicken Sie auf das Fuchssymbol oben rechts im Browser-Fenster.**
4. **Klicken Sie auf das Menüsysmbol.**
5. **Klicken Sie auf die Ether-Adresse, um sie in die Zwischenablage zu kopieren.**
6. **Fügen Sie Ihre MetaMask-Ether-Adresse in das Empfängerfeld ein.**
7. **Geben Sie den zu sendenden Betrag ein.**

8. **Klicken Sie auf SEND.**
9. **Klicken Sie auf CONFIRM.**

Ein CryptoKitties-Benutzerkonto anlegen

In diesem Abschnitt werden Sie etwas Spaß mit der Ethereum-Blockchain haben. Sie lernen dabei, wie Sie ein einzigartiges Blockchain-Asset kaufen, Ihr ganz persönliches, einzigartiges Blockchain-Asset erstellen und dieses dann auf einem globalen Markt verkaufen.

Diese unglaublich komplexe Aufgabe versteckt sich hinter niedlichen Katzenbildern. Unter der Bezeichnung »CryptoKitties« können Sie digitale Katzen sammeln und neu erstellen. Jedes Bild hat seine individuellen Eigenschaften, die es von seinen Ausgangsbildern geerbt hat. Wenn Sie ein neues CryptoKitty »gezüchtet« haben, können Sie Ihre Katze dann an andere Züchter verpachten, um neue Assets zu erstellen oder sie für Ether zu verkaufen.

Befolgen Sie diese Schritte:

1. **Gehen Sie in Ihrem Brave-Browser auf** www.cryptokitties.co**.**
2. **Klicken Sie auf START.**
3. **Klicken Sie auf CONNECT.**
4. **Klicken Sie auf SIGN IN.**
5. **Klicken Sie im Pop-up-Fenster auf SIGN IN.**

CryptoKitties kaufen

In diesem Abschnitt suchen Sie sich zwei Kätzchen aus und kaufen sie. Auf dieser Grundlage können Sie eine neue Katze »züchten« und Ihre Katzen zu Zuchtzwecken an andere Teilnehmer verpachten.

Befolgen Sie diese Schritte:

1. **Gehen Sie in Ihrem Brave-Browser auf** www.cryptokitties.co**.**
2. **Klicken Sie auf SIGN IN.**
3. **Klicken Sie im Pop-up-Fenster auf SIGN IN.**
4. **Klicken Sie unter GREAT-VALUE KITTIES auf BROWSE ALL.**
5. **Suchen Sie sich ein niedliches Kätzchen aus.**


Die Auswahl ist groß, aber weil wir diese Übung vor allem zum Spaß durchführen, geben Sie nicht zu viel Geld aus. Halten Sie außerdem Ausschau nach Kätzchen mit dem Merkmal »Swift« und einem niedrigen Gen-Wert. Diese lassen sich schneller züchten, und auch die Regenerationszeit nach der Fortpflanzung ist kürzer.

6. **Klicken Sie auf BUY NOW.**
7. **Klicken Sie auf OK, BUY THIS KITTY.**
8. **Klicken Sie auf CONFIRM.**
9. **Wählen Sie Ihre zweite Katze aus, und befolgen Sie die Kaufanleitung.**

CryptoKitties züchten

In diesem Abschnitt züchten Sie mit den beiden zuvor gekauften Katzen eine neue Katze. Dies ist eine sehr interessante Sache, da Sie hier ein neues und einzigartiges digitales Asset mit Herkunftsnachweis erstellen, das auf einem offenen globalen Markt gehandelt werden kann, ohne dass für die Authentifizierung oder Übertragung ein Vermittler erforderlich wäre.

Abhängig von der Geschwindigkeit des Ethereum-Netzwerks zum Zeitpunkt des Kaufs Ihrer Katzen kann es einige Minuten dauern, bis sie unter KITTIES angezeigt werden. Haben Sie Geduld, sie werden dort auftauchen. Sie können jederzeit Ihr Transaktionsprotokoll einsehen, um den Status abzufragen.

Befolgen Sie diese Schritte:

1. **Gehen Sie in Ihrem Brave-Browser auf** www.cryptokitties.co**.**
2. **Klicken Sie auf SIGN IN.**
3. **Klicken Sie auf MY PROFILE.**
4. **Wählen Sie eine Ihrer Katzen aus.**
5. **Klicken Sie auf BREED.**

   Der Zuchtvorgang wird durch ein Auberginensymbol dargestellt.
6. **Klicken Sie auf SIRE WITH MY KITTIES.**
7. **Klicken Sie auf OK, LET'S GET STARTED.**
8. **Klicken Sie in das Feld mit der Aufschrift SELECT YOUR KITTY.**
9. **Wählen Sie die andere Katze.**
10. **Klicken Sie auf OK, GIVE THEM SOME PRIVACY.**
11. **Klicken Sie im Pop-up-Fenster auf CONFIRM.**

CryptoKitties verpachten

In diesem Abschnitt werden wir eine unserer Katzen zur Zucht anbieten. Hiermit vermieten Sie Ihr Objekt auf einem offenen Markt ohne Vermittler. Falls eine Ihrer Katzen noch trächtig ist, wählen Sie die andere Katze aus.

Befolgen Sie diese Schritte:

1. **Gehen Sie in Ihrem Brave-Browser auf** www.cryptokitties.co**.**
2. **Klicken Sie auf SIGN IN.**
3. **Klicken Sie auf MY PROFILE.**
4. **Wählen Sie eine Ihrer Katzen aus.**
5. **Klicken Sie auf BREED.**
6. **Klicken Sie auf SIRE TO THE PUBLIC.**

7. **Passen Sie die Preise und die Zeit nach Ihren Vorstellungen an, oder behalten Sie die Standardwerte bei.**
8. **Klicken Sie auf DONE.**
9. **Klicken Sie im Pop-up-Fenster auf CONFIRM.**

Herzlichen Glückwunsch! Sie haben zum ersten Mal Bitcoin gekauft und gegen Ether getauscht. Dann haben Sie Blockchain-Anlagegüter erworben und selbst welche hergestellt. Schließlich haben Sie Ihre Assets auf einem offenen globalen Marktplatz verpachtet, um mehr Ether zu verdienen. Abgesehen von Ihrem ersten Kauf wurden alle diese Aktionen in einer öffentlichen Blockchain ausgeführt, und es brauchte dafür keine Bank oder keinen Vermittler. Wenn Ihnen CryptoKitties gefallen hat und Sie Ihr eigenes blockchainbasiertes Spiel erstellen möchten, sehen Sie sich das Online-Tutorial unter https://cryptozombies.io an.

Eine private Blockchain mit Docker und Ethereum erstellen

Private Blockchains bieten sowohl die Vorteile einer privaten Datenbank als auch die Sicherheit von Blockchains.

- ✔ **Private Blockchains sind hervorragend für Entwickler geeignet, weil sie damit Ideen ohne Verwendung von Kryptowährung testen können**. Zudem bleiben die Ideen der Entwickler geheim, weil die Daten nicht öffentlich erscheinen.
- ✔ **Große Institutionen können von der Sicherheit und Permanenz der Blockchain-Technologie profitieren, ohne dass ihre Transaktionen öffentlich werden, wie es bei herkömmlichen Blockchains der Fall ist**.

In diesem Buch wird größtenteils angenommen, dass Sie sich zum ersten Mal mit Blockchains beschäftigen und wenig Programmiererfahrung besitzen. Für diesen Abschnitt sollten Sie sich mit GitHub, Docker und Ihrem Computer auskennen. Wenn Sie nicht selbst mit der Blockchain-Technologie arbeiten möchten, können Sie den Rest dieses Kapitels auch überspringen.

Dieser Abschnitt behandelt die Details zur Erstellung Ihrer ersten Blockchain. Sie benötigen dazu zwei Schritte. Im ersten Schritt bereiten Sie Ihren Computer vor, um die Blockchain erstellen zu können. Keine Sorge, mit den Docker-Tools und den Hilfestellungen der talentierten Entwickler bei GitHub ist das ganz einfach. Im zweiten Schritt erstellen Sie Ihre Blockchain in Ihrem Docker-Terminal.

Ihren Computer vorbereiten

Für dieses Blockchain-Projekt müssen Sie Software auf Ihren Computer herunterladen. Laden Sie zuerst die Docker-Toolbox herunter. Öffnen Sie `www.docker.com/toolbox`, um die richtige Version für Ihr Betriebssystem zu bekommen.

Anschließend laden Sie den GitHub-Desktop herunter. Öffnen Sie `http://desktop.github.com`. Nachdem Sie den GitHub-Desktop installiert haben, legen Sie unter `www.github.com` ein GitHub-Konto an, indem Sie auf SIGN UP (anmelden) klicken, einen Benutzernamen, eine E-Mail-Adresse und ein Passwort eingeben und dann auf die Schaltfläche SIGN UP FOR GITHUB (für GitHub anmelden) klicken.

Jetzt brauchen Sie einen Ort, an dem Sie Ihre Blockchain-Daten ablegen können. Legen Sie auf dem Desktop Ihres Computers einen Ordner namens `ethereum` an. In diesem Ordner legen Sie Ihr zukünftiges Repository und andere Dateien ab. Gehen Sie wie folgt vor:

1. **Öffnen Sie den GitHub-Desktop.**

2. **Melden Sie sich auf Ihrem Computer bei der GitHub-Desktop-Anwendung unter Ihrem neuen GitHub-Konto an.**
3. **Gehen Sie zurück in Ihren Webbrowser und öffnen Sie** `www.github.com/Capgemini-AIE/ethereum-docker`**.**

   Die in Abbildung 3.1 gezeigte Seite wird geöffnet.

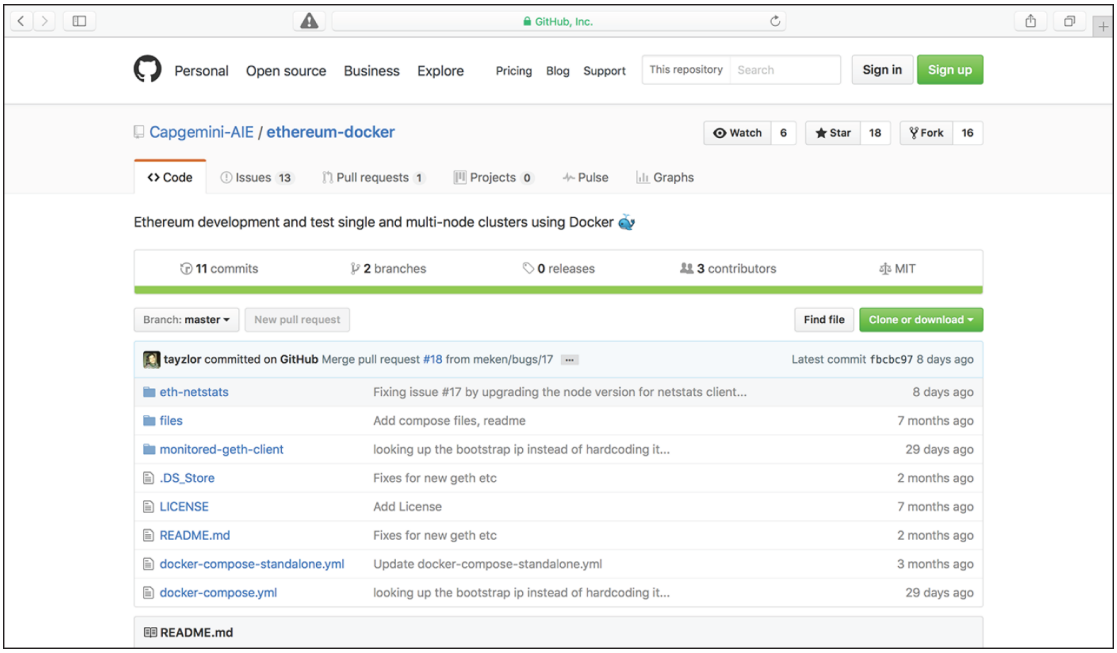


Abbildung 3.1: Gehen Sie in GitHub zu dieser Seite.

4. **Klicken Sie auf die Schaltfläche CLONE OR DOWNLOAD (klonen oder herunterladen).**

   Sie haben zwei Möglichkeiten: OPEN IN DESKTOP (auf dem Desktop öffnen) oder DOWNLOAD ZIP (Zip herunterladen; siehe Abbildung 3.2).

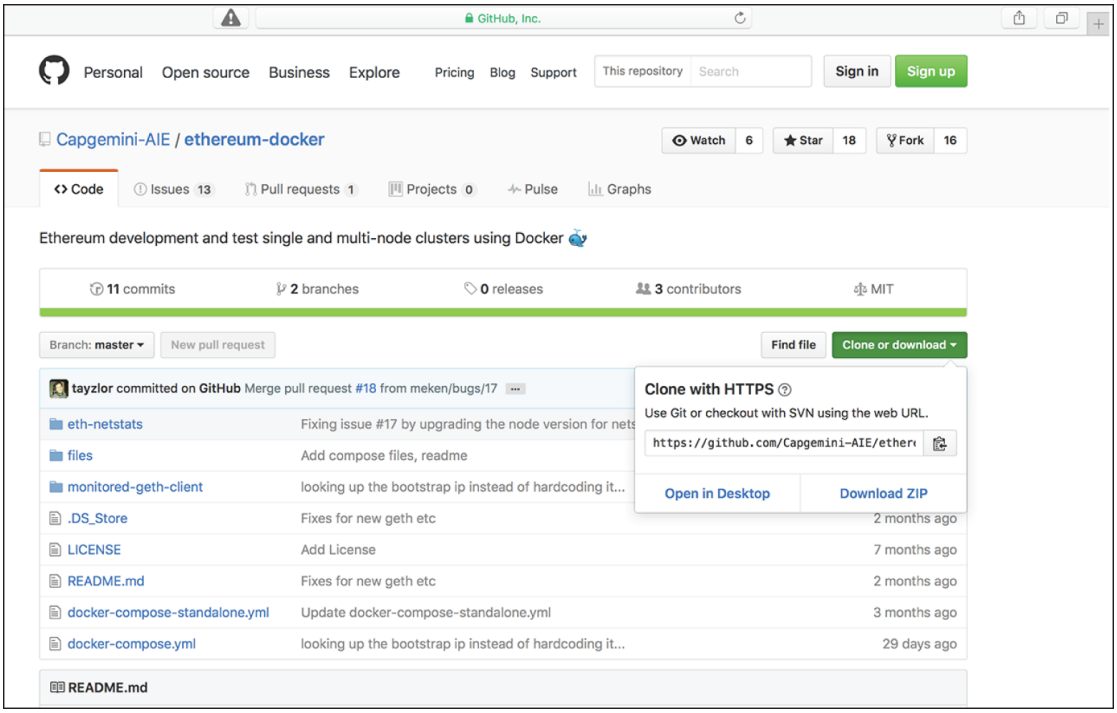


Abbildung 3.2: Auf dem Desktop öffnen

5. **Wählen Sie die Option OPEN IN DESKTOP (auf dem Desktop öffnen).**

   Die GitHub-Desktop-Anwendung wird wieder geöffnet.

   Gehen Sie in der GitHub-Desktop-Anwendung zum Projektordner `ethereum`, und klicken Sie auf CLONE (klonen).

Durch das Klonen aus GitHub werden die Informationen kopiert, die Sie brauchen, um Ihre neue Blockchain zu erstellen. Gehen Sie wie im folgenden Abschnitt beschrieben vor, um Ihre private Blockchain zu erstellen.

Ihre Blockchain erstellen

Jetzt werden Sie mit dem kostenlosen Tool Docker Quick Start Terminal Ihre Blockchain erstellen. Sie erhalten damit Zugriff auf eine virtuelle Maschine, wodurch die Zeit für die Einrichtung und das Debugging Ihres Systems verkürzt wird. Auf diese Weise können Sie schneller eine stabile Umgebung für Ihre Blockchain erstellen und müssen sich nicht um die Einstellungen auf Ihrem Computer kümmern.

Gehen Sie wie folgt vor:

1. **Starten Sie Docker auf Ihrem Computer unter Verwendung des Docker Quick Start Terminals.**

    Das Quick Start Terminal sollte sich bei Ihren Anwendungen auf dem Desktop befinden.

   Die Docker-Anwendung startet ein Terminal, mit dessen Hilfe Sie Ihre Blockchain erstellen.

2. **Wechseln Sie im Terminal zum Verzeichnis `ethereum`.**

   Die Dateien, die Sie erstellen, um die neue Blockchain anzulegen, werden in der im vorigen Abschnitt erzeugten Desktop-Datei abgelegt. Sie müssen im Terminal einen Befehl ausführen, um in ein anderes Verzeichnis zu wechseln. Wenn Sie auf einem Mac oder unter Linux arbeiten, geben Sie den folgenden Befehl ein:

   ```
   cd ~ /Desktop/ethereum/ethereum-docker/
   ```

   Auf dem Windows-PC geben Sie den folgenden Befehl ein:

   ```
   cd ~ \Desktop\ethereum\ethereum-docker\
   ```

    Wenn diese Befehle aus irgendeinem Grund nicht funktionieren, suchen Sie im Internet nach Informationen, wie Sie auf Ihrem System andere Verzeichnisse öffnen.

   Jetzt können Sie die Ethereum-Docker-Dateien verwenden.

3. **Legen Sie einen eigenständigen Ethereum-Knoten an, indem Sie den folgenden Befehl in Ihr Terminal eingeben:**

   ```
   docker-compose -f docker-compose-standalone.yml up -d
   ```

   Diese Codezeile erzeugt Folgendes:

   - einen Ethereum-Bootstrapped-Container,
   - einen Ethereum-Container, der mit dem Bootstrapped-Container verbunden ist,

    - einen Netstats-Container mit einer Web-UI, um Aktivitäten im Cluster anzuzeigen.
4. **Sehen Sie sich Ihre neue Blockchain an, indem Sie in einem Webbrowser `http://$(docker-machine ip default):3000` öffnen.**

Herzlichen Glückwunsch! Damit haben Sie Ihre eigene private Blockchain angelegt. Wenn Sie so freundlich wären, ein Wort des Dankes an Graham Taylor und Andrew Dong auszusprechen, die so viel Arbeit in die Ethereum/Docker-Integration gesteckt haben!

Teil II

Ihr Wissen erweitern

IN DIESEM TEIL …

Lernen Sie mit der Bitcoin-Blockchain die Anfänge der Blockchain-Technologie kennen.

Vertiefen Sie Ihr Wissen über das Ethereum-Netzwerk, und erweitern Sie Ihr Verständnis von dezentralen autonomen Organisationen und Smart Contracts.

Lernen Sie mit dem EOS-Netzwerk und seinen Kernkonzepten eine neue Plattform für skalierbare Blockchain-Anwendungen kennen.

Sehen Sie sich die Factom-Blockchain mit ihrer Fähigkeit, Daten und Systeme zu sichern, an.

Erforschen Sie die Waves-Plattform, und lernen Sie, auf dieser Blockchain Ihre eigenen Token zu erstellen und zu handeln.

Kapitel 4

Die Bitcoin-Blockchain kennenlernen

IN DIESEM KAPITEL

- Verstehen, woher die Bitcoin-Blockchain stammt
- Bitcoin Cash entdecken
- Einige Mythen über Bitcoin berichtigen
- Fehler bei der Verwendung von Bitcoins vermeiden
- Bitcoin-Mining
- Eine Paper-Wallet für Ihre Bitcoins anlegen

Achtung: Nachdem Sie dieses Kapitel gelesen haben, werden Sie von dieser neuen Technologie fasziniert sein. Lesen Sie auf eigene Gefahr weiter!

Die Bitcoin-Blockchain demonstriert die ursprünglichsten Aspekte der Blockchain-Technologie. Sie ist Vergleichsmaßstab für alle anderen Blockchains und diente auch häufig als Blaupause bei der Entwicklung. Wenn Sie wissen, wie die Bitcoin-Blockchain funktioniert, können Sie alle anderen Technologien in diesem Ökosystem viel besser verstehen.

In diesem Kapitel erkläre ich Ihnen die grundsätzliche Arbeitsweise der Bitcoin-Blockchain. Sie erhalten Sicherheitstipps, damit Ihre ersten Gehversuche mit Bitcoin reibungslos und erfolgreich verlaufen. Ich zeige Ihnen Anwendungsmöglichkeiten, die Sie sofort mit Bitcoin ausprobieren können. Sie erfahren, wie Sie ein Bitcoin-Token erhalten und wie Sie an Bitcoins kommen, ohne sie zu kaufen. Außerdem lernen

Sie, wie Sie Ihre Token in eigene Wallets übertragen und welche anderen praktischen Methoden es gibt, Ihre Token online sicher aufzubewahren.

Eine kurze Geschichte der Bitcoin-Blockchain

Bitcoin und das Konzept der dazugehörigen Blockchain wurden im Herbst 2008 vorgestellt, zunächst als Whitepaper und 2009 als Open-Source-Software. (Das Bitcoin-Whitepaper finden Sie unter www.bitcoin.org/bitcoin.pdf.)

Der Autor, der Bitcoin 2008 in seinem Whitepaper vorstellte, ist ein anonymer Programmierer oder eine Gruppe mit dem Pseudonym Satoshi Nakamoto. Nakamoto arbeitete bis 2010 mit vielen anderen Open-Source-Entwicklern an Bitcoin. Heute ist er beziehungsweise die Gruppe nicht mehr an dem Projekt beteiligt, und die Kontrolle wurde an bekannte Bitcoin-Core-Entwickler übertragen. Es gab viele Behauptungen und Gerüchte über die Identität von Nakamoto, aber bisher konnte nichts davon endgültig bewiesen werden.

In jedem Fall hat Nakamoto ein außergewöhnliches Peer-to-Peer-Zahlungssystem entwickelt, mit dem die Benutzer Bitcoin, das Token für die Wertübertragung, direkt und ohne Vermittler zwischen zwei Parteien transferieren können. Das Netzwerk selbst dient als Vermittler. Es verifiziert die Transaktion und stellt zugleich sicher, dass niemand versucht, zu betrügen und dieselben Bitcoins zweimal auszugeben.

Ziel von Nakamoto war es, die riesige Vertrauenslücke bei digital abgewickelten Geschäftsvorgängen zu schließen, und sein Ansatz war das Konzept der Blockchain. Sie löst das Problem der byzantinischen Generäle, also das ultimative Problem der Menschheit, insbesondere im Online-Bereich: Wie können Sie den Informationen vertrauen, die Sie erhalten, und denjenigen, die Ihnen diese Informationen übermitteln, böswillige Dritte Sie

aus Eigennutz hintergehen können usw.? Viele Bitcoin-Fans sind davon überzeugt, dass die Blockchain-Technologie das fehlende Puzzleteil ist, das allen Unternehmen die vollständige Digitalisierung ermöglicht: Das digitale Vertrauen wird neu definiert, indem relevante Informationen in einem öffentlichen Raum aufgezeichnet werden. Diese Aufzeichnungen können nicht gelöscht werden und stehen jederzeit zur Verfügung, sodass ein Betrug sehr viel schwieriger wird.

Blockchains kombinieren viele jahrtausendealte Techniken auf völlig neue Art. Beispielsweise werden Kryptografie und Zahlungsvorgänge zur Kryptowährung zusammengefasst. *Kryptografie* ist die Kunst der sicheren Kommunikation unter den Augen Dritter. Zahlungen über ein Token, das einen Wert darstellt, werden ebenfalls schon seit sehr langer Zeit verwendet. In der Kombination entstehen daraus jedoch Kryptowährungen – etwas völlig Neues. Sie wandeln das Konzept des Geldes in eine Online-Lösung um: Werte können sicher über ein Token verschoben werden.

Blockchains verwenden zudem das Konzept des *Hashings* (die Umwandlung von Daten beliebiger Größe in kurze Werte fester Länge). Das Hashing nutzt eine weitere alte Technologie, die sogenannten Hash-Bäume, die viele Hash-Werte zu einem einzigen Hash-Wert komprimieren, während es weiterhin möglich ist, jeden Datenabschnitt zu belegen, der dem Hash-Wert hinzugefügt wurde (siehe Abbildung 4.1).

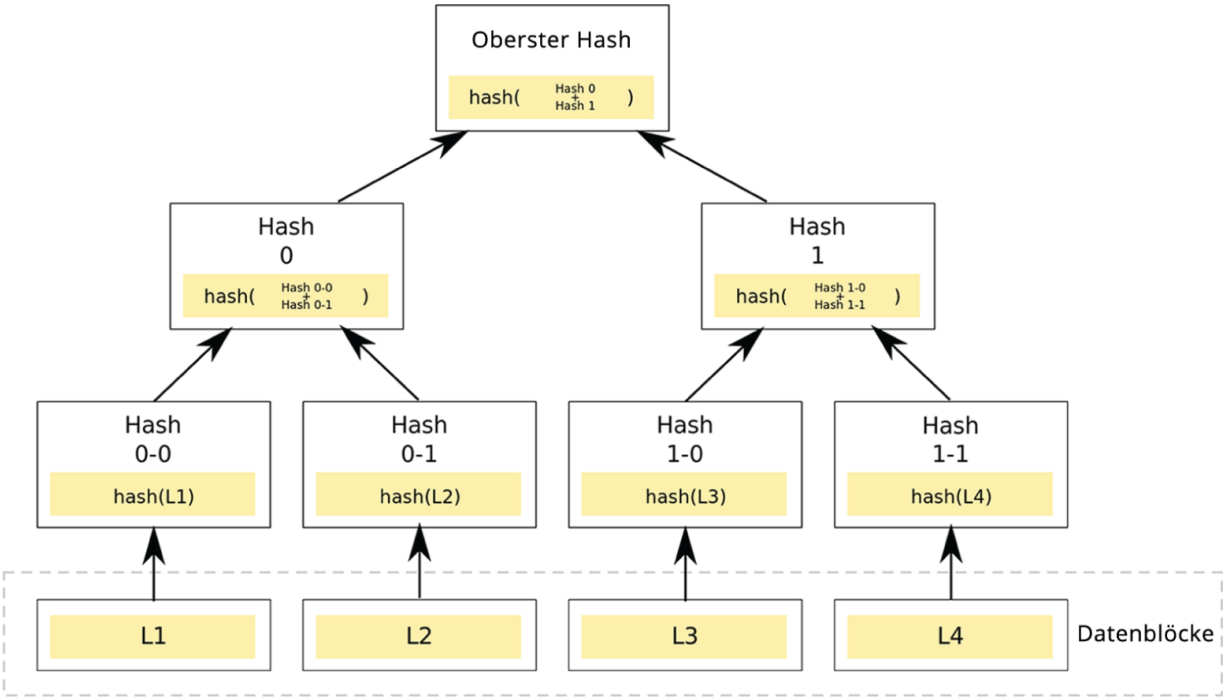


Abbildung 4.1: Ein Hash-Baum

Letztlich sind Blockchains nichts anderes als Kontobücher (*Ledger*), wie sie schon seit Jahrtausenden zur Kontenverwaltung dienen. Werden all diese Modelle online in einer verteilten Datenbank zusammengeführt und vereinfacht, ergibt sich daraus eine revolutionäre Innovation.

Das Bitcoin-Protokoll wurde hauptsächlich für den Austausch der Kryptowährung Bitcoin entwickelt. Die Erfinder erkannten jedoch schnell, dass das Ganze noch viel mehr Potenzial hatte. Deshalb bauten sie die Bitcoin-Blockchain so auf, dass mehr als nur die Daten über die Transaktionshistorie des Tokens aufgezeichnet werden kann. Die Bitcoin-Blockchain ist die älteste und eine der größten Blockchains der Welt. Sie wird von Tausenden von Knoten fortgeschrieben, die das Bitcoin-Protokoll ausführen. Das Protokoll erzeugt und sichert die Blockchain.

Einfach ausgedrückt ist die *Blockchain* ein öffentliches Kontobuch (Ledger) aller Transaktionen im Bitcoin-Netzwerk, und die *Knoten* sind Computer, die Einträge in diesem

Kontobuch aufzeichnen. Das *Bitcoin-Protokoll* gibt die Regeln vor, die dafür sorgen, dass dieses System funktioniert.

Das Netzwerk wird durch Knoten überwacht. Diese führen dazu ein Mining der Kryptowährung Bitcoin durch (siehe unten). Als Belohnung für die Verarbeitung von Transaktionen und die Aufzeichnung in der Blockchain entstehen neue Bitcoins. Außerdem erhalten die Knoten eine kleine Gebühr für die Bestätigung der Transaktionen.

Jeder kann das Bitcoin-Protokoll ausführen und nach Token schürfen (»Mining«). Es handelt sich um ein Open-Source-Projekt, das wächst und gedeiht, weil sich immer mehr Teilnehmer dem Netzwerk anschließen. Je weniger Teilnehmer es gibt, desto zentralisierter wird es – und Zentralisierung schwächt das System. Gerade die große Anzahl unabhängiger, weltweit verteilter Knoten macht Bitcoin so sicher.

Die erfolgreichsten Miner haben leistungsfähige Rechensysteme, die langsamere Miner ausbooten können. Ganz zu Anfang genügte noch ein Desktop-Rechner, um das Bitcoin-Protokoll auszuführen und damit Bitcoins zu verdienen. Inzwischen brauchen Sie dafür sehr teure, spezialisierte Hardware oder müssen auf einen Cloud-Service zurückgreifen, um überhaupt noch auf selbst geschürfte Bitcoins hoffen zu dürfen.

Um in der Bitcoin-Blockchain eine Nachricht zu erstellen, müssen Sie einen Bitcoin-Betrag von einer Adresse zu einer anderen senden. Sobald Sie die Transaktion absenden, wird die Nachricht an das gesamte Netzwerk übertragen. Wenn die Nachricht in der Bitcoin-Blockchain aufgezeichnet wurde, lässt sie sich nachträglich nicht mehr verändern. Deshalb ist es sehr wichtig, dass Sie Ihre Nachrichten sorgfältig auswählen und niemals sensible Informationen übertragen.

Wenn dieselbe Nachricht an Tausende von Knoten übertragen und dann für immer in der Blockchain gespeichert wird, kommt schnell einiges an Daten zusammen. Bitcoin verwendet daher eine rigide Längenbegrenzung auf derzeit 40 Zeichen.

Der neue Bitcoin: Bitcoin Cash

Die Weiterentwicklung des Bitcoin-Codes sorgt immer wieder für Zündstoff. Der »Bitcoin-Bürgerkrieg« oder die Debatte um die Blockgrößenbegrenzung steht stellvertretend für die Frage, ob der Code im Kern unverändert bleibt oder ob die Funktionalität der Software erweitert werden soll. Dieser Streit wirkt einfach, aber die Auswirkungen sind enorm. Durch die Permanenz des Bitcoin-Netzwerks und die damit abgesicherten Vermögenswerte im Wert von Milliarden von Dollar wird jede Code-Revision gründlichst überprüft und diskutiert.

Im Jahr 2017 gab es eine Hard Fork von Bitcoin, bei der sich die Blockchain in zwei separate Stränge aufteilte. (Dieser Vorgang wird auch als *harte Abspaltung* bezeichnet, das heißt, es erfolgt eine nicht abwärtskompatible Änderung des Protokolls.) Die Entwicklergemeinschaft und die Bitcoin-Miner konnten sich nicht einigen, wie mit dem Wachstum umgegangen werden sollte. Bitcoin war immer unzuverlässiger (langsamer) und teurer in der Anwendung geworden. Waren die Transaktionen zu Beginn noch fast verzögerungsfrei und kostenlos, so kosteten sie nun bis über 50 US-Dollar, und die Abwicklung konnte Stunden bis Tage dauern. Durch die hohen Kosten und die geringe Geschwindigkeit wandten sich immer mehr Nutzer ab.

Ein Hauptproblem war der geringe Datendurchsatz von Bitcoin mit nur sieben Transaktionen pro Sekunde. Damit ließ sich die gestiegene Nachfrage im Netzwerk nicht mehr decken. Die Transaktionsgebühren stiegen deshalb an, weil sich die Nutzer für eine schnellere Abwicklung ihrer Zahlungen gegenseitig überboten. Einer der limitierenden Faktoren im Jahr 2017 war die Blockgrößenbegrenzung von Bitcoin auf 1 MB.

Bitcoin Cash setzte auf die gleiche Codebasis wie Bitcoin, hob aber die maximale Blockgröße auf 32 MB an. Im Zuge der Hard Fork wurde jeder Bitcoin-Adresse die gleiche Anzahl an Bitcoin Cash gutgeschrieben. Die Anhebung der Blockgröße war

umstritten, weil sich für kleinere Miner mit weniger Rechenleistung Nachteile ergaben.

Viele Miner fürchteten, beim Schürfen größerer Blöcke nicht mehr wettbewerbsfähig zu sein. In diesem Zusammenhang gab es auch die Befürchtung, dass größere Blöcke die Zentralisierung des Netzwerks befördern könnten.

Die Einschränkungen von Bitcoin

Die Blöcke der Bitcoin-Blockchain sind auf eine Größe von 1 MB beschränkt. Es dauert im Mittel zehn Minuten, bis ein neuer Block erzeugt ist. Damit ist die Anzahl der Transaktionen, die die Bitcoin-Blockchain verarbeiten kann, auf sieben Stück pro Sekunde begrenzt.

Diese Einschränkungen sind im Bitcoin-Protokoll festgeschrieben und tragen dazu bei, dass das Netzwerk dezentral bleibt. Die Dezentralisierung ist der Schlüssel zur Robustheit von Bitcoin. Größere Blöcke würden das Mining deutlich erschweren und kleinere Wettbewerber aus dem Rennen werfen.

Bitcoin enthält eingebaute Beschränkungen, die verhindern, dass alle globalen Geldströme über das System laufen können. Mit Bitcoin werden außerdem auch andere Arten von Daten und Systemen gesichert. Die Nachfrage nach der Nutzung des sicheren Bitcoin-Ledgers ist hoch. Man spricht auch vom *Bitcoin Bloat*, also der Aufblähung von Bitcoin. Dadurch wurde das Netzwerk verlangsamt, die Kosten für die Transaktionen haben sich erhöht.

Derzeit beschränken sich die meisten Blockchain-Entwickler auf Experimente zur Erweiterung des Nutzens der Bitcoin-Blockchain. Die meisten sind noch nicht bereit, ihre Prototypen und Konzepte zu skalieren, sodass die Bitcoin-Blockchain den zusätzlichen Anforderungen im Moment noch standhält. Andere, neue Blockchain-Technologien haben auch dazu beigetragen, den Druck von Bitcoin zu nehmen und Entwicklern kostengünstigere Optionen zur Sicherung von Daten an die Hand zu geben.

Die Welt dreht sich weiter: Das Bitcoin-Drama

Bitcoin steht unter intensiver Beobachtung von außen. Die dezentrale Natur von Bitcoin, die zentrale Autoritäten überflüssig machen könnte, rückt die Technik ins Blickfeld von Regulierungsbehörden. Bitcoin wird außerdem auch gerne für den anonymen Verkauf illegaler Waren oder zur Geldwäsche verwendet. All diese Faktoren haben dafür gesorgt, dass Bitcoin ein negativer Ruf anhaftet und dass die Öffentlichkeit das Phänomen argwöhnisch

betrachtet. Unternehmer, die von der Bitcoin-Technologie profitieren wollen, haben daher vor allem den Begriff *Blockchain* besetzt. Die Änderung der Terminologie sollte insbesondere die Softwarestruktur von Bitcoin und anderen Kryptowährungen hervorheben. Man begann also, Software, die die Struktur von Kryptowährungen verwendete, als Blockchain zu bezeichnen. Dies verschob den Schwerpunkt von den umstrittenen Token auf die Struktur der Kryptowährungen. In der Folge begannen sich sowohl Regierungen als auch die Wirtschaft stärker für Bitcoin zu interessieren, statt ihn zu fürchten.

Bitcoin ist ein lebendiges und in stetigem Wandel befindliches System. Die Community der Bitcoin-Kernentwickler sucht aktiv nach Methoden, um das System zu verbessern und es stärker und schneller zu machen. Jeder kann zum Bitcoin-Protokoll beitragen, indem er sich auf der entsprechenden GitHub-Seite (`www.github.com/bitcoin`) engagiert. Es gibt jedoch eine kleine Community dominanter Kernentwickler für Bitcoin. Die produktivsten Entwickler sind Wladimir van der Laan, Pieter Wuille und Gavin Andresen.

Häufige Missverständnisse über Bitcoin

Wir stehen Neuerungen oft argwöhnisch gegenüber, besonders wenn sie nicht leicht zu verstehen sind. Es ist also nur natürlich, dass Bitcoin – eine völlig neue Währung und etwas, das die Welt zuvor nie erlebt hat – viele Menschen verwirrt und zu Missverständnissen geführt hat.

Hier einige Missverständnisse, von denen Sie vielleicht schon gehört haben:

- **Bitcoin wurde gehackt**. 2011 gab es einen bekannten Fall, dass jemand seine Bitcoins doppelt ausgegeben hatte. Dieses Problem wurde innerhalb einer Stunde behoben. Seither wurden keine erfolgreichen Angriffe mehr auf die Bitcoin-Blockchain bekannt, die zum Diebstahl oder Verlust von Bitcoins geführt hätten. Viele zentrale Stellen, die mit Bitcoin

arbeiten, wurden jedoch gehackt. Auch Wallets und Bitcoin-Börsen werden häufig wegen ihrer unzureichenden Sicherheit gehackt. Die Bitcoin-Community hat mit der Entwicklung eleganter Lösungen zur Sicherung der Coins reagiert, beispielsweise mit verschlüsselten Wallets, Mehrfachsignaturen, Offline-Wallets, Paper-Wallets und Hardware-Wallets, um nur ein paar wenige zu nennen.

- ✔ **Mit Bitcoin werden Menschen erpresst**. Wegen seiner halb anonymen Natur wird Bitcoin gerne in Ransomware-Angriffen verwendet. Hacker dringen in Netzwerke ein und sperren sie, bis eine Lösegeldzahlung erfolgt. Zu den Opfern dieser Angriffe gehören Krankenhäuser und Schulen. Allerdings hinterlässt Bitcoin in der Blockchain stets eine Spur, der die Ermittler folgen können.
- ✔ **Bitcoin ist ein Schneeballsystem**. Bitcoin ist aus der Perspektive der Bitcoin-Miner das genaue Gegenteil eines Schneeballsystems. Das Bitcoin-Protokoll ist wie ein kannibalisches Wettrüsten ausgelegt. Jeder zusätzliche Miner erschwert das Mining für alle anderen. Aus sozialer Perspektive ist Bitcoin ein reiner Markt. Der Preis von Bitcoins fluktuiert aufgrund von Angebot und Nachfrage auf dem Markt ebenso wie aufgrund des wahrgenommenen Werts. Bitcoin ist kein Schneeballsystem, aber es gibt viele Betrügereien rund um Bitcoin. Also seien Sie auf der Hut!
- ✔ **Bitcoin kollabiert nach 21 Millionen Coins**. Das Bitcoin-Protokoll begrenzt die Anzahl der herauszugegebenden Token im Code auf 21 Millionen. Der letzte Bitcoin wird voraussichtlich im Jahr 2140 geschürft werden. Niemand kann vorhersehen, was zu diesem Zeitpunkt passieren wird, aber die Miner werden stets auch noch einen Gewinn aus den Transaktionsgebühren schöpfen. Darüber hinaus liegt es im Interesse der Benutzer der Blockchain und des Bitcoins, das Netzwerk zu schützen, denn falls das Mining gestoppt wird, stehen sowohl die Bitcoins als auch die in der Blockchain festgeschriebenen Daten auf dem Spiel.

- **Mit genug Rechenleistung könnte man das gesamte Bitcoin-Netzwerk übernehmen**. Das stimmt, aber es wäre extrem schwierig und wenig attraktiv. Je mehr Knoten sich am Bitcoin-Netzwerk beteiligen, desto schwieriger wird ein solcher Angriff. Beispielsweise würde der Angreifer dazu die gesamte Energieerzeugung Irlands benötigen. Und die Amortisation eines solchen Angriffs wäre ebenfalls sehr fraglich. Der Angreifer könnte höchstens seine eigene Transaktion rückgängig machen. Er könnte niemand anderem Bitcoins wegnehmen oder Transaktionen oder Coins fälschen.
- **Bitcoin ist eine gute Investition**. Bitcoin ist eine neue und interessante Entwicklung im Handel mit Vermögenswerten. Die Kryptowährung wird nicht durch einzelne Regierungen oder Unternehmen gestützt und ist nur deshalb etwas wert, weil es eine Nachfrage dafür gibt und sie gegen Waren oder Dienstleistungen gehandelt wird. Die Bereitschaft und die Fähigkeit der Menschen, Bitcoin zu verwenden, schwanken erheblich. Es ist ein sehr volatiles Investment, das gut überlegt werden sollte.

Bitcoin: Der neue wilde Westen

Die Bitcoin-Welt lässt sich mit den frühen Tagen des Wilden Westens vergleichen. Sie müssen sich ihr vorsichtig nähern, bis Sie herausgefunden haben, wer die Guten und wer die Bösen sind und welcher Saloon das beste Bier serviert. Wenn Sie Opfer eines Betrugs werden, gibt es so gut wie keinen Schutz für Sie.

Bitcoins und andere dezentrale Kryptowährungen werden in vielen Ländern als Währung betrachtet, aber es gibt keine Aufsicht und kaum Regulierungen oder Schutz für Investoren.

In diesem Abschnitt beschreibe ich drei der häufigsten Betrugsmöglichkeiten, die in der Welt der Kryptowährung auftreten. Alle haben es auf ihre Coins abgesehen, und sie sind den herkömmlichen Betrügereien ganz ähnlich, die Sie vielleicht bereits kennen. Die Liste ist nicht vollständig, und die Gauner sind

äußerst kreativ. Seien Sie also beim Umgang mit Bitcoins äußerst vorsichtig. Sie wissen nie, was hinter der nächsten Ecke lauert.

Fake-Websites

Websites, die wie Börsen oder Web-Wallets aussehen, in Wirklichkeit aber Fakes sind, haben einige der größten Bitcoin-Websites plagiiert. Diese Betrugsform ist in der Krypto-Welt üblich, wie auch im Internet ganz allgemein. Die Betrüger hoffen, die Anmeldeinformationen von Benutzern zu ergattern und zu Geld zu machen oder Benutzer in die Irre zu führen, damit sie ihnen Bitcoins senden.

Überprüfen Sie jede URL sehr sorgfältig und verwenden Sie nur sichere Websites, die mit `https://` beginnen. Wenn eine Website oder eine Aufforderung zweifelhaft aussehen, überprüfen Sie, ob sie in Badbitcoin.org (www.badbitcoin.org) aufgelistet sind. Diese Liste ist nicht vollständig, aber viele der Gauner sind aufgeführt.

Nein, Sie zuerst!

»Senden Sie mir Ihre Bitcoins, dann sende ich Ihnen die Waren.« Hört sich verdächtig an, oder? Betrugsmaschen wie diese sind vergleichbar mit dem Überweisungsbetrug. Dabei behauptet jemand, Ihnen etwas zu verkaufen, die Ware wird aber niemals geliefert.

Aufgrund der halb anonymen Natur von Bitcoins – in Verbindung mit der Unmöglichkeit einer Rückbuchung – haben Sie schlechte Karten, Ihr Geld wiederzusehen. Darüber hinaus bieten die Regierungen derzeit keinen Schutz für Bitcoin-Transaktionen, deshalb müssen Sie sich selbst so gut wie möglich absichern.

Betrüger versuchen, Ihr Vertrauen zu gewinnen, indem sie Ihnen Fake-IDs senden oder sogar so tun, als wären sie Personen, die Ihnen bekannt sind. Prüfen Sie die Ihnen gesendeten Informationen immer nach.

Am besten schützen Sie sich gegen diese Form des Betrugs, indem Sie auf Ihre innere Stimme hören und niemals höhere Bitcoin-Beträge riskieren, als Sie bereit sind zu verlieren. Wenn es eine Möglichkeit gibt, die Identität der Person offline zu überprüfen, machen Sie das!

Schnell-reich-werden-Geschichten

In der Kryptowelt kursieren die seltsamsten Geschichten über schnellen Reichtum. Das Gute daran: Sie erkennen sie leicht, wenn Sie wissen, worauf Sie achten müssen.

Häufig verspricht man Ihnen riesige Gewinne, und es gibt eine Art Anwerbe- oder Unterweisungsprozess. Dieser könnte beispielsweise Marketing-Schulungen beinhalten, wobei Sie aufgefordert werden, Ihre Freunde und Ihre Familie anzuwerben. Außerdem wird stets versichert, dass die Investition risikofrei ist und Sie kein Geld verlieren können. Denken Sie daran, niemals Ihre privaten Schlüssel an Dritte herauszugeben!

Fazit: Wenn eine Geschichte zu gut aussieht, um wahr zu sein, ist sie es wahrscheinlich auch nicht. Sehen Sie sich genau an, welchen Mehrwert die Investition generiert (außer, dass Sie eine Einzahlung vornehmen). Wenn es keinen klaren und nachvollziehbaren Grund gibt, dass ein riesiger Gewinn generiert wird, handelt es sich sehr wahrscheinlich um Betrug.

Lassen Sie alle Investitionen nachprüfen. Fachleute können Ihnen helfen, Risiken und steuerliche Auswirkungen besser zu verstehen.

Bitcoin-Mining

Es gibt verschiedene Möglichkeiten, Bitcoins zu verdienen. Beim Mining verdienen Sie Bitcoins, indem Sie Teil des Netzwerks werden. Normalerweise erfolgt dies über eine besondere Mining-Hardware, die hoch spezialisiert und teuer ist. Außerdem

benötigen Sie die passende Software, um eine Verbindung zur Blockchain und gegebenenfalls zu Ihrem *Mining-Pool* aufzubauen. (Ein Mining-Pool ist ein Zusammenschluss mehrerer Miner, die zusammenarbeiten und sich dann die Belohnung für ihren Aufwand teilen.)

Hier die Standardmethoden, um am Bitcoin-Mining teilzunehmen:

- **Bitcoin-QT**: Der Bitcoin-QT-Client ist die Originalsoftware von Satoshi Nakamoto. Sie können sie unter https://bitcoin.org/en/download herunterladen.
- **CGminer**: CGminer ist eine sehr verbreitete Mining-Software. Sie ist quelloffen und für Windows, Linux und OS unter www.github.com/ckolivas/cgminer erhältlich.
- **Multiminerapp**: Die Multiminerapp ist ein einfacher Bitcoin-Client. Sie können ihn unter www.multiminerapp.com herunterladen.

Bitcoin ist eine Umgebung mit hohem Wettbewerbsdruck, und ohne spezielle Mining-Ausrüstung, werden Sie wahrscheinlich nie irgendwelche Bitcoins verdienen. Ich gebe in diesem Buch keine Hardwareempfehlungen, weil die Branche stetig in Bewegung ist und die Geräte schnell veralten. Durchschnittlich sollten Sie mit 500 bis 5.000 Euro pro Maschine rechnen. Geeignete Hardware finden Sie beispielsweise bei Amazon. Dort gibt es ein großes Angebot, und viele Kundenrezensionen helfen Ihnen bei der Auswahl.

Einen Cloud-Mining-Account können Sie sich an einem Nachmittag einrichten und damit die ersten Bitcoins verdienen, ohne dass Sie sich dafür Software herunterladen oder Ausrüstung kaufen müssen. Gehen Sie einfach wie folgt vor:

1. **Öffnen Sie** https://hashflare.io/panel**.**


Die Rendite beim Cloud-Mining kann negativ sein. Überprüfen Sie die Angebote sorgfältig, um sicherzustellen, dass es sich um eine geeignete Investition handelt.

2. **Blättern Sie auf der Seite nach unten, und klicken Sie unter SHA-256 CLOUD MINING auf BUY NOW (jetzt kaufen).**


Als ich dieses Buch geschrieben habe, erbrachte diese Option die höchste Rendite bei den niedrigsten Einstandskosten. Nehmen Sie sich die Zeit, dies genau zu überprüfen, weil es sich in der Zwischenzeit geändert haben kann.

3. **Durchlaufen Sie den Anmeldeprozess.**
4. **Richten Sie einen Link zu Ihrer Bitcoin-Adresse ein.**

   Wenn Sie keine Bitcoin-Adresse haben, blättern Sie zurück zu Kapitel 3. Dort erfahren Sie, wie Sie eine Bitcoin-Wallet anlegen. Sie brauchen eine Bitcoin-Wallet, um mit dem Mining etwas verdienen zu können.
5. **Kaufen Sie eine kleine Menge Mining-Leistung.**

   Damit können Sie dem Bitcoin-Netzwerk beitreten.
6. **Treten Sie einem Mining-Pool bei.**

   Mit diesem Schritt gelangen Sie schneller zu einer Mining-Rendite, als wenn Sie alleine arbeiten. Damit werden die Ressourcen mehrerer Miner in einem Pool zusammengefasst, und die spätere Vergütung wird zwischen den Pool-Mitgliedern aufgeteilt.

Herzlichen Glückwunsch! Sie können sich zurücklehnen und darauf warten, dass Ihre Mining-Gewinne anrauschen (oder vielleicht doch eher eintröpfeln).

Ihre erste Paper-Wallet

Eine Paper-Wallet ist ein Ausdruck Ihres öffentlichen und privaten Schlüssels für Ihre Bitcoins auf Papier. Paper-Wallets sind vollständig offline und stellen daher eine der sichersten Methoden zur Aufbewahrung von Bitcoins dar (wenn Sie es richtig anstellen). Der Vorteil dabei ist, dass Ihr privater Schlüssel nicht digital gespeichert wird und damit auch nicht durch Hacking offengelegt werden kann. Es ist relativ einfach, eine Paper-Wallet anzulegen:

1. **Öffnen Sie** www.bitaddress.org**.**
2. **Bewegen Sie Ihre Maus über den Bildschirm, bis der Zufälligkeitsgrad 100 % anzeigt.**
3. **Klicken Sie auf die Schaltfläche PAPER-WALLET.**

   Damit erhalten Sie die Möglichkeit, eine Paper-Wallet zu erstellen, die Sie ausdrucken können.
4. **Geben Sie in das Feld ADDRESSES TO GENERATE (zu generierende Adressen) 1 ein.**

   Sie können bei Bedarf auch mehrere Wallets gleichzeitig erstellen, für den Anfang genügt aber vielleicht auch eine, um sich damit vertraut zu machen.
5. **Klicken Sie auf die Schaltfläche GENERATE (generieren).**

   Abbildung 4.2 zeigt eine Paper-Wallet, die ich für mich erstellt habe.

Abbildung 4.2: Eine Paper-Wallet

6. **Klicken Sie auf die Schaltfläche PRINT (drucken).**

Lassen Sie niemanden zusehen, wenn Sie die Paper-Wallet erstellen. Sie sollten dabei also nicht auf einem öffentlichen Computer arbeiten. Stellen Sie sicher, dass Sie einen privaten Drucker benutzen und nicht mit dem Internet verbunden sind, sodass Sie nicht Gefahr laufen, dass Ihre privaten Schlüssel gehackt werden.

Laminieren Sie Ihre Paper-Wallet, damit sie ein wenig robuster wird.

Kapitel 5

Die Ethereum-Blockchain entdecken

IN DIESEM KAPITEL

- Erfahren, wie und warum Ethereum ins Leben gerufen wurde
- Die Ethereum-Blockchain kennenlernen
- Blockchain-Hacks entdecken
- Die ersten Schritte mit Ethereum unternehmen
- Eigene Token erstellen
- Smart Contracts und dezentrale Unternehmen erstellen

Das Ethereum-Projekt ist eine der am weitesten entwickelten und besten zugänglichen Blockchains im Ökosystem. Außerdem steht es an vorderster Stelle, was Innovation und vielfältige Anwendungsmöglichkeiten für Blockchains betrifft. Sie sollten diese Technologie unbedingt verstehen, weil sie im Hinblick auf Smart Contracts, dezentrale Organisationen und Token-Ausgaben führend ist.

Dieses Kapitel beleuchtet die Struktur von Ethereum und die neuen Möglichkeiten, Organisationen und Unternehmen auf der Ethereum-Blockchain aufzubauen. Außerdem gehe ich auf die Sicherheit und praktische Geschäftsanwendungen der Ethereum-Blockchain ein. Sie erfahren, wie und mit welchem Ziel das Projekt ins Leben gerufen wurde.

Nachdem Sie dieses Kapitel gelesen haben, können Sie das Ethereum-Token handeln. Außerdem können Sie eigene Token erstellen, die weltweit handelbar sind.

Die kurze Geschichte von Ethereum

Ethereum wurde zuerst 2013 in einem Whitepaper von Vitalik Buterin beschrieben, der in der Bitcoin-Community als Autor und Programmierer sehr aktiv war. Buterin hatte erkannt, dass in Bitcoin sehr viel mehr Potenzial steckte als die Möglichkeit, Vermögenswerte ohne zentrale Autorität zu transferieren. Für ihn war Bitcoin mehr als nur ein Vehikel, um das dort verwendete (»native«) Token zu handeln. Daher begründete er die Colored-Coin-Plattform innerhalb von Bitcoin. Buterin war der Überzeugung, dass andere Anwendungen in Wirtschaft und Verwaltung, die eine zentrale Kontrollinstanz benötigen, ebenfalls mit Blockchain-Strukturen abgebildet werden könnten.

Damals entbrannte eine hitzige Debatte darüber, dass das Bitcoin-Netzwerk durch die unzähligen Mikrotransaktionen von Anwendungen, die Bitcoin zur Absicherung nutzten, »aufgebläht« würde. Die größte Sorge war, dass zusätzliche auf dem Bitcoin-Protokoll aufsetzende Anwendungen Probleme durch ein steigendes Transaktionsvolumen verursachen würden. Damals gab es auch noch keine Scripting-Funktionen zur Ausführung von Smart Contracts und Ähnlichem. Bitcoin war nicht darauf ausgelegt, so viele Transaktionen zu verarbeiten, wie die Anwendungen benötigten. Vitalik und viele andere erkannten, dass der Code der Bitcoin-Blockchain stark überarbeitet werden musste, um dezentrale Anwendungen nutzen zu können, oder dass man eine völlig neue Blockchain benötigte.

Bitcoin war zu diesem Zeitpunkt bereits fest etabliert, und die benötigten Upgrades am Kerncode erschienen völlig unrealistisch. Das Konzept von Bitcoin würde Änderungen am Netzwerk nur sehr schleppend oder überhaupt nicht zulassen. Vitalik und sein Team gründeten Anfang 2014 die Ethereum Foundation, mit der sie Kapital sammelten, um ein Blockchain-Netzwerk mit eingebauter Programmiersprache aufzubauen.

Vitalik wollte ein Netzwerk erstellen, das Anwendungen durch die Blockchain absichern konnte.

Die anfängliche Entwicklung wurde durch einen online durchgeführten öffentlichen Crowdsale im Juli und August 2014 finanziert. Mit dem Verkauf des Kryptowährungs-Token Ether erzielte man rekordverdächtige 18 Millionen US-Dollar. Es wurde leidenschaftlich diskutiert, ob diese Art Crowdsale illegal sei, weil dabei möglicherweise ein nicht lizenziertes Wertpapier in Umlauf gebracht wird.

Diese regulatorische Grauzone konnte das Projekt nicht stoppen. Ganz im Gegenteil, die Innovationskraft des Projekts erregte weitere Aufmerksamkeit, und viele Talente schlossen sich ihm an. Unzufriedene und benachteiligte Entwickler und Unternehmer aus der ganzen Welt kamen in Scharen. Die Dezentralisierung wird als perfekte Lösung betrachtet, um korrupte und repressive Behörden zu umgehen.

Dank der 18 Millionen US-Dollar aus dem Token-Verkauf konnte ein großes Entwicklerteam zur Programmierung von Ethereum aufgestellt werden. Mit Ethereum Frontier ging im Juli 2015 die erste Version des Ethereum-Netzwerks live. Die Software war sehr rudimentär, und nur technisch bewanderte Nutzer konnten damit Anwendungen erstellen.

2016 wurde die Ethereum-Version Homestead veröffentlicht. Sie ist sehr viel benutzerfreundlicher. Die Anwendungsvorlage kann von fast jedem verwendet werden, und es gibt intuitive und unkomplizierte Benutzeroberflächen und eine große, eifrige Entwickler-Community.

2017 folgte der Ethereum-Release Metropolis. Der größte Unterschied ist, dass die Anwendungen vollständig entwickelt und gut getestet sind. Die Anwendungen wurden noch benutzerfreundlicher und können selbst von nicht technisch begabten Anwendern einfach benutzt werden.

Die letzte Planungsphase der Ethereum-Entwicklung ist Serenity. Damit wird Ethereum von einem *Proof-of-Work*-Konsens (bei dem

Miner in einem Leistungswettbewerb darum stehen, wer den nächsten Block erstellen darf) zu einem *Proof-of-Stake*-Modell wechseln. Beim Proof-of-Stake-Modell werden die Knoten zur Blockproduktion pseudozufällig ausgewählt, wobei die Wahrscheinlichkeit hierfür proportional mit dem Kryptowährungsguthaben steigt. Der größte Vorteil der Neuerung ist die Reduzierung der enormen Energiekosten, die beim Proof-of-Work-Modell entstehen. Auf diese Weise wird es für Einzelpersonen attraktiver, Netzwerkknoten zu betreiben, was wiederum der Dezentralisierung und der Sicherheit zugutekommt.

Ethereum: Der Open-Source-Weltcomputer

Ethereum ist vielleicht eine der komplexesten Blockchains, die je erstellt wurden. Es hat mehrere eigene *Turing-vollständige Programmiersprachen* (vollfunktionale Programmiersprachen, die es Entwicklern gestatten, beliebige Anwendungen zu erstellen). Diese neuen Programmiersprachen sind populären Programmiersprachen wie JavaScript und Python sehr ähnlich. Das Ethereum-Protokoll kann so gut wie alles, was andere durchschnittliche Programmiersprachen können. Der Unterschied ist, dass der Code in die Ethereum-Blockchain integriert ist, was zusätzliche Vorteile und Sicherheit bietet. Egal, welches Softwareprojekt Sie planen, es kann auf Ethereum aufgebaut werden.

Das Ethereum-Ökosystem ist derzeit der beste Ort, um dezentrale Anwendungen zu erstellen. Es ist sehr gut dokumentiert und hat benutzerfreundliche Schnittstellen, sodass Sie Ihre Anwendungen schnell fertigstellen können. Eine kurze Entwicklungszeit, Sicherheit für kleine Anwendungen und eine einfache Möglichkeit zur Interaktion dieser Anwendungen untereinander sind maßgebliche Eigenschaften dieses Systems.

Die Turing-vollständigen Programmiersprachen sind der Schlüssel, um Ethereum bei der Erstellung neuer Programme

sehr viel leistungsstärker zu machen als Bitcoin. Die Skripting-Sprache von Ethereum ermöglicht etwa die sichere Integration von Twitter mit wenigen Codezeilen.

Smart Contracts wie der in Kapitel 3 erstellte können ebenfalls auf Ethereum aufbauen. Das Ethereum-Protokoll hat ein völlig neues Anwendungsgenre geschaffen. Sie können Abläufe aus jedem Bereich – von Regierungsstellen oder aus Unternehmen – digital in Ethereum darstellen. Derzeit wird die Ethereum-Plattform zur Verwaltung *digitaler Assets* eingesetzt. Es handelt sich dabei um eine neue Klasse von Vermögenswerten, die online existieren und einen vollständig digitalen Vermögenswert (beispielsweise ein Bitcoin-Token) oder auch die digitale Repräsentation eines realen Vermögenswerts (beispielsweise landwirtschaftliche Erzeugnisse wie Mais) darstellen. Dasselbe wird für Finanzinstrumente untersucht (beispielsweise hypothekarisch gesicherte Wertpapiere), für die Dokumentation des Eigentums an Vermögenswerten (beispielsweise für Grundstücke) und für DAOs (dezentrale autonome Organisationen). Ethereum hat es auch weltweit sehr vielen Start-ups ermöglicht, mithilfe von ERC20-Token Kapital zur Umsetzung ihrer Innovationen einzusammeln. Ethereum bietet neue Wege der Organisation für Unternehmen, NGOs oder Regierungsstellen. Vermögenswerte können dadurch gehalten, weitergereicht und gehandelt werden, ohne die andere Partei jemals zu treffen oder Dritte mit einzubeziehen. Der Code erledigt die ganze Arbeit.

Dezentralisierte Anwendungen: Willkommen in der Zukunft

Die revolutionärste und kontroverseste Manifestation von Ethereum ist die dezentralisierte Applikation (DApp). DApps können beispielsweise digitale Vermögenswerte und DAOs verwalten.

DApps wurden ins Leben gerufen, um die zentrale Verwaltung von Vermögenswerten und Organisationen zu ersetzen. Dieses Konzept ist sehr attraktiv, weil viele Menschen davon überzeugt

sind, dass absolute Macht zu absoluter Korruption führt. Für diejenigen, die Angst haben, ihren Status quo zu verlieren, hat diese Struktur erhebliche Auswirkungen.

Fast täglich erscheinen neue DApps. Neuigkeiten für Ethereum finden Sie auf der Seite https://dappradar.com. DappRadar pflegt eine Liste der aktuellsten Ethereum-DApps und bietet ihnen eine Vorschau ihrer Funktionen. Zu den ersten DApps überhaupt zählt Etheria (siehe Abbildung 5.1).

Abbildung 5.1: Das weltweit erste unsterbliche Spiel: Etheria

Die Macht der DAOs

DAOs sind Ethereum-Anwendungen, die eine virtuelle Entität innerhalb von Ethereum darstellen. Wenn Sie eine DAO erstellen, können Sie andere einladen, an der Führung der Organisation mitzuwirken. Die Teilnehmer können anonym sein und müssen sich nie treffen. Dadurch könnten KYC-Vorschriften (Know Your Customer) und Anti-Geldwäsche-Gesetze ins Spiel kommen.

DAOs sollten ursprünglich Fundraising-Zwecken dienen, können aber auch für bürgerschaftliche oder gemeinnützige Anwendungen genutzt werden. Ethereum bietet ein

grundlegendes Verwaltungsgerüst. Jeder kann selbst bestimmen, was damit verwaltet werden soll. Ethereum stellt Vorlagen bereit, die Ihnen bei der Erstellung von DAOs helfen.

Abbildung 5.2 zeigt die Organisation einer Ethereum-Anwendung.

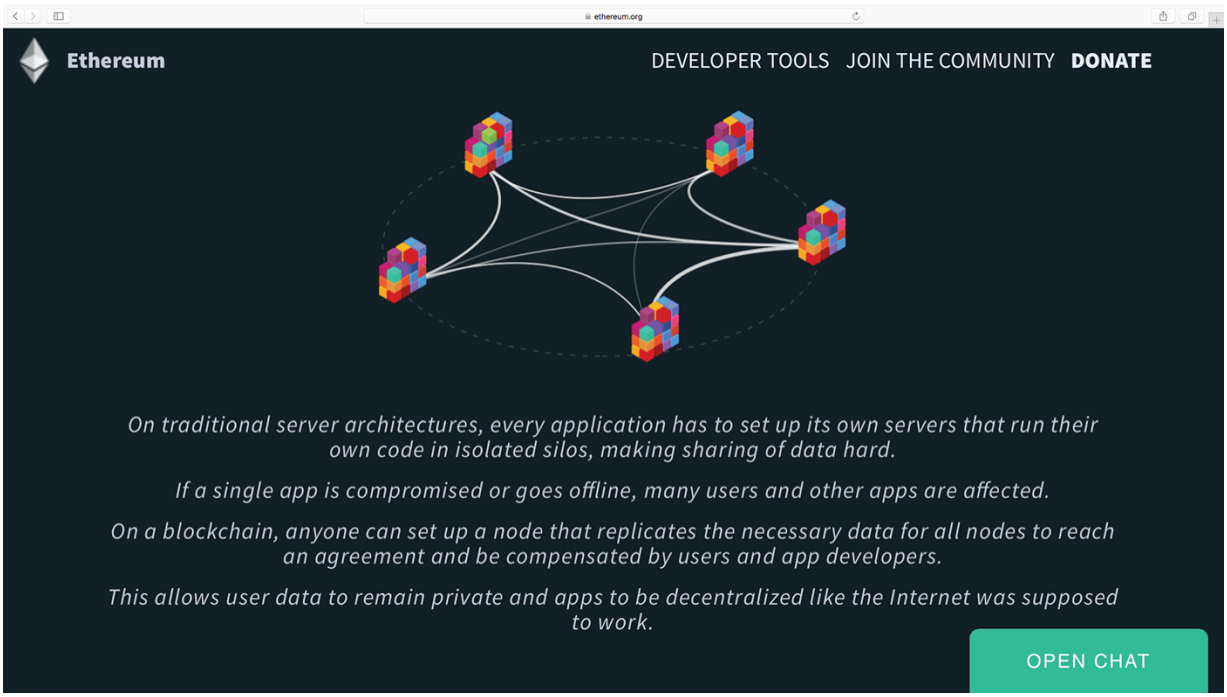


Abbildung 5.2: Darstellung der Blockchain-Anwendung Ethereum.org

Große Macht bewirkt … große Macht

Die erste je erstellte Ethereum-DAO heißt *The DAO*, was die Verwirrung nur noch steigert. Sie ist ein Beispiel für die Gefahren, die dezentrale und autonome Entitäten mit sich bringen können. Es handelt sich um das größte Crowdfunding-Projekt der Welt: Man hat innerhalb von 26 Tagen mit mehr als 11.000 Mitgliedern ca. 163 Millionen Dollar gesammelt. Was eigentlich als die größte Stärke von The DAO vermutet wurde, ist zu ihrer größten Schwäche geworden. Der unabänderliche Code in The DAO schrieb präzise vor, wie die Organisation zu verwalten und wie das Kapital zu verteilen war. Damit konnten die Mitglieder sich ihrer Investitionen sicher fühlen. Der Code war zwar gut überprüft worden, aber es waren eben doch noch nicht alle Fehler beseitigt worden.

Die erste ernsthafte Krise erlebte Ethereum nach dem Hacking von The DAO. Ein unerwarteter Codepfad im Smart Contract von The DAO gestattete es jedem fortgeschrittenen Benutzer, Kapital herauszuziehen. Ein unbekannter

Benutzer schaffte es so, etwa 50 Millionen Dollar herauszuholen, bevor er aufgehalten werden konnte.

Die Ethereum-Community debattierte heftig darüber, ob sie den Ether zurückfordern konnte oder sollte. Der DAO-Hacker hatte technisch nichts Falsches getan, geschweige denn die Blockchain gehackt. Die Fundamentalisten in der Ethereum-Community waren der Meinung, dass der Code das Gesetz sei und dass deshalb nichts unternommen werden sollte, um das Geld zurückzuholen.

Was Ethereum so stark machte, war gleichzeitig seine größte Schwäche: Dezentralisierung, Unveränderbarkeit und Autonomie bedeuteten, dass keine zentrale Autorität entscheiden konnte, was auf die Schnelle zu tun sei. Es gab auch niemanden, der den Missbrauch des Systems ahnden würde. Es gab tatsächlich keinerlei Schutzmaßnahmen für die Anwender. Es war eine ganz neue Sphäre, wie der Name der Software schon aussagt.

Nachdem das Problem mehrere Wochen lang diskutiert worden war, entschied die Ethereum-Community, The DAO zu schließen und ein neues Ethereum zu erstellen. Dieser Vorgang wird auch als *harte Abspaltung* oder *Hard Fork* bezeichnet, das heißt, es erfolgte eine nicht abwärtskompatible Änderung des Protokolls. Bei der Hard Fork des Netzwerks machte die Ethereum-Community die Transaktion des Hackers rückgängig, und es entstanden zwei Ethereum-Blockchains: Ethereum und Ethereum Classic.

Nicht jeder war mit dieser Entscheidung einverstanden. Die Community verwendet weiterhin auch Ethereum Classic. Die Token für Ethereum Classic werden noch gehandelt, haben aber maßgeblich an Marktwert verloren.

Die Entscheidung für die Hard Fork erschütterte die Blockchain-Welt. Zum ersten Mal kam es in einem großen Blockchain-Projekt zu einer Hard Fork, um eine Ausgleichszahlung an einen Investor vorzunehmen. Das stellte viele der Prinzipien infrage, die die Blockchain-Technologie so attraktiv gemacht hatten.

Und so funktionieren DAOs grundsätzlich:

1. **Eine Personengruppe schreibt einen Smart Contract, der die Organisation steuert.**
2. **Benutzer zahlen in die DAO ein und erhalten Token, die ihr Eigentum repräsentieren.**

   Diese Struktur funktioniert wie die Aktienausgabe eines Unternehmens, die Mitglieder haben jedoch vom ersten an Tag die Kontrolle über das Guthaben.

3. **Wenn die benötigten Mittel zusammengekommen sind, beginnt die DAO zu arbeiten. Die Mitglieder schlagen vor, wie das Geld verwendet werden soll. Das Gewicht ihrer Stimme hängt dabei oft vom Kryptoguthaben ab, das ein Mitglied in die DAO einbringt und dort riskiert.**
4. **Die Mitglieder stimmen über diese Vorschläge ab.**
5. **Wenn die vorab festgelegte Zeit abgelaufen ist und die vorgegebene Anzahl an Stimmen gesammelt wurde, wird der Vorschlag angenommen oder abgelehnt.**
6. **Einzelpersonen agieren als Stimmberechtigte in der DAO.**

Anders als die meisten herkömmlichen Anlageinstrumente, bei denen eine zentrale Partei Entscheidungen über die Investitionen trifft, kontrollieren bei einer DAO uneingeschränkt die Mitglieder die Vermögenswerte. Sie stimmen über neue Investitionen und andere Entscheidungen ab. Durch eine solche Struktur könnten herkömmliche Finanzmanager überflüssig werden.

DAOs werden mit Code generiert, der nicht dynamisch verändert werden kann. Attraktiv daran ist, dass sich böswillige Hacker die Vermögenswerte nicht im herkömmlichen Sinne verschaffen können. Sie finden jedoch immer wieder Wege, den Code auf unvorhergesehene Weise auszuführen und Kapital zu entnehmen. Die unveränderbare Natur des DAO-Codes macht es so gut wie unmöglich, Fehler zu korrigieren, wenn eine DAO erst einmal in Ethereum gestartet wurde.

Eine Blockchain hacken

Ethereum wurde nie gehackt. Die Hard Fork, zu der es 2016 aufgrund des Hacks von The DAO kam (siehe Kasten *Große Macht bewirkt … große Macht*), war im eigentlichen Sinne kein Hack des Systems, wird aber verwirrenderweise häufig als solcher bezeichnet. Ethereum funktionierte perfekt – zu perfekt. Es wurde notwendig, das System neu zu starten, als sehr viel Geld und ein Großteil seiner Benutzer gefährdet waren.

Die einzige Möglichkeit, eine Aktion in einer Blockchain wie Ethereum zu korrigieren, ist eine Hard Fork, die eine grundlegende Änderung des Protokolls bedeutet. Eine solche harte Abspaltung macht zuvor gültige Blöcke und Transaktionen ungültig. Ethereum hat diesen Schritt vollzogen, um das Kapital zu schützen, das ein Benutzer der ersten DAO entnahm.

In der Kryptowelt gibt es ständig Betrugs- und Hacking-Versuche. Die meisten dieser Angriffe richten sich gegen zentrale Börsen und Anwendungen. Viele Hacker wollen sich Kryptoguthaben aneignen. Es hat einen realen Wert und ist nicht auf dieselbe Weise von den Regierungen geschützt wie normales Geld. Die anonyme Natur der Kryptowährungen macht sie für Gauner attraktiv. Es ist schwierig, diese zu erwischen und zu verurteilen. Die Kryptocommunity schlägt jedoch zurück, indem sie Maßnahmen einführt, um sich selbst zu schützen.

Es ist wesentlich einfacher und billiger, eine zentrale Stelle zu hacken, als zu versuchen, ein dezentrales Netzwerk zu überwinden. Wenn Sie etwas über Hacking in der Blockchain-Welt lesen, dann wurde wahrscheinlich eine einzelne Website oder eine Kryptowährungs-Wallet gehackt und nicht das gesamte Netzwerk.

Smart Contracts verstehen

Smart Contracts mit Ethereum entsprechen herkömmlichen vertraglichen Vereinbarungen, außer dass es keine zentrale Partei gibt, die den Vertrag durchsetzt. Das Ethereum-Protokoll »erzwingt« die Umsetzung von Smart Contracts, indem es wirtschaftlichen Druck erzeugt. Sie können auch die Umsetzung einer Anforderung durchsetzen, die in Ethereum vorliegt, weil das Netzwerk belegen kann, ob bestimmte Bedingungen erfüllt sind oder nicht.

Smart Contracts in Ethereum lassen sich noch nicht gesetzlich einfordern. Möglicherweise wird das auch niemals der Fall sein, weil es zum Ethereum-Konzept gehört, dass keine externen Autoritäten benötigt werden, um die Vereinbarungen durchzusetzen. Rechtssysteme werden von Staaten kontrolliert, also von zentralen Autoritäten – manche mit mehr oder weniger Unterstützung und demokratischen Prinzipien. In einem Smart Contract in Ethereum hat jeder Teilnehmer eine Stimme, die ihm nicht entzogen werden kann.

Smart Contracts in Ethereum beinhalten keine künstliche Intelligenz. Dies ist jedoch eine spannende Option für die nahe Zukunft. Momentan ist Ethereum jedoch nichts weiter als Softwarecode, der auf einer Blockchain ausgeführt wird.

Smart Contracts in Ethereum sind nicht sicher. Der Hack von The DAO ist ein hervorragendes Beispiel für mögliche Gefahren. Wir befinden uns noch in der Frühphase, und es wäre unklug, viel Geld in ein unerprobtes System zu investieren. Stattdessen sollten Sie mit kleinen Beträgen experimentieren, bis alle Bugs beseitigt und neue Contracts ausgearbeitet wurden.

Die Kryptowährung Ether

Die Kryptowährung für die Ethereum-Blockchain heißt Ether. Sie wurden nach der Substanz benannt, von der angenommen wurde, dass sie den gesamten Raum ausfüllt und damit das Universum möglich macht. In diesem Sinne ist Ether die Substanz, die Ethereum ermöglicht. Ether setzt den Anreiz zur Sicherung des Netzwerks durch Proof-of-Work-Mining, genau wie es der Bitcoin im Bitcoin-Netzwerk tut. Die Ausführung von Code im Ethereum-Netzwerk muss mit Ether bezahlt werden. Wird es für die Ausführung eines Contracts in Ethereum verwendet, wird Ether als *Gas* bezeichnet.

Die Ausführung von Code innerhalb eines Smart Contracts kostet auch Ether. Damit erhält das Token eine zusätzliche Funktion. Solange Einzelpersonen Ethereum für Anwendungen und

Contracts verwenden wollen, besitzt Ether mehr als nur spekulativen Wert.

Der steile Wertanstieg hat Ether zu einem beliebten Token für Spekulanten gemacht. Es wird auf Börsen auf der ganzen Welt gehandelt. Einige neue Hedgefonds überprüfen es bereits als Anlageinstrument. Die hohe Volatilität und die geringe Markttiefe machen Ether allerdings zu einer riskanten Investition.

Ether-Mining

Ethereum läuft als Netzwerk aus Computern auf der ganzen Welt, die den Code der Smart Contracts verarbeiten und das Netzwerk sichern. Diese Computer werden manchmal auch als *Knoten* bezeichnet, die dazugehörige Kryptowährung ist Ether.

Als Entschädigung für die Zeit und den Aufwand beim Mining gibt es eine Belohnung von etwa fünf Ether alle zwölf Sekunden. Dieser Betrag wird an den Knoten ausgeschüttet, der den letzten Block in der Ethereum-Blockchain erstellen konnte.

Alle neuen Blöcke enthalten eine Liste der neuesten Transaktionen. Der Proof-of-Work-Konsensalgorithmus garantiert, dass die Vergütungen am häufigsten an die Knoten mit der höchsten Rechenleistung fließen. Weniger leistungsstarke Computer können ebenfalls gewinnen, es dauert nur länger. Wenn Sie sich am Ether-Mining versuchen möchten, können Sie dies mit Ihrem privaten Computer tun, aber es wird sehr lange dauern, bis Sie einen Block finden und die Mining-Rewards erhalten.

Ether-Mining ist nichts für technisch Unerfahrene. Sie müssen mit der Kommandozeile vertraut sein. Wenn Sie nicht wissen, was eine Kommandozeile ist, sollten Sie deshalb besser darauf verzichten. Außerdem müssen Sie den aktuellsten Anweisungen von Ethereum GitHub folgen (http://github.com/ethereum).

Die Zukunft der dezentralen autonomen Organisationen (DAOs)

DAOs (dezentrale autonome Organisationen) werden die Geschäfte der Zukunft verändern. Sie gestatten jedem Menschen auf der Welt, online eine neue Art Unternehmen zu gründen, das nach vorab festgelegten Regeln verwaltet wird, die durch das Blockchain-Netzwerk durchgesetzt werden.

Smart Contracts und dezentrale Organisationen sind äußerst vielversprechend. Ihre rein demokratische und hyperrationale Natur ist sehr attraktiv. Momentan gibt es aber mehr Möglichkeiten als erwiesene Erfolge, und jeder neue Contract kann entweder bahnbrechend oder ein riesiger Flop sein.

Wenn Sie Ethereum als neue Sphäre betrachten, werden Sie mehr Erfolg haben. Das Ethereum-Netzwerk hat bei vorsichtiger Verwendung mehr Vorteile als Nachteile. Wenn Sie aber erwarten, dass immer alles reibungslos läuft und alle Teilnehmer integer handeln, werden Sie größere Verluste erleiden. Auch in Ethereum gibt es Gauner, aber auch viele freundliche Unterstützer, die Ihnen den Erfolg gönnen.

Die Smart-Contract-Hacks im Jahr 2016 haben die Bedeutung der Sicherheit und der genauen Überprüfung von Contracts hervorgehoben. Außerdem wurde deutlich, dass es viele integre Persönlichkeiten gibt, die dafür kämpfen, dass Probleme behoben werden.

Dieses Buch zu lesen kann nur ein Anfang sein. Es erklärt die Grundlagen von Ethereum, aber genau wie andere neue Technologien entwickelt sich Ethereum schnell weiter. Informieren Sie sich regelmäßig über die besten Verfahrensweisen und Sicherheitsmaßnahmen.

In den folgenden Abschnitten weise ich auf einige Dinge hin, die Sie bei der Einrichtung Ihrer ersten DAOs und Smart Contracts und beim Debugging Ihrer neuen Blockchain-Systeme unbedingt berücksichtigen sollten.

Geld in eine DAO stecken

Vertrauen Sie ungetesteten und nicht genau überprüften Contracts keine hohen Geldsummen an. Große Contracts sind häufig das Ziel von Hackern. Der zuvor in diesem Kapitel beschriebene Hack von The DAO (siehe Kasten *Große Macht bewirkt … große Macht*) hat demonstriert, dass selbst gut durchdachte Contracts unerwartete Schwächen aufweisen können.

Mit Smart Contracts und Blockchains können Sie auf der ganzen Welt Geschäfte machen, aber die Technologie steckt noch in den Kinderschuhen. Sie können das Risiko abmildern, indem Sie nur mit bekannten und vertrauenswürdigen Parteien zusammenarbeiten.

Es tauchen ständig neue Sicherheitslücken auf. Informieren Sie sich stets aktuell über die besten Vorgehensweisen. Seien Sie vorsichtig mit dem Geld, das Sie einsetzen, und setzen Sie die Contracts langsam und phasenweise ein. Ethereum ist eine neue Technologie, und es gibt noch keine ausgereiften Lösungen.

Intelligentere Smart Contracts erstellen

Für die Programmierung von Smart Contracts brauchen Sie eine andere Denkweise als bei herkömmlichen Verträgen. Es gibt keine Schlichter, die alles in Ordnung bringen, wenn der Contract anders ausgeführt wird als vorgesehen oder erwartet. Die unveränderbare und verteilte Natur von Blockchains macht es schwierig, ein unerwünschtes Ergebnis zu korrigieren.

Ihr Contract kann Lücken haben und möglicherweise scheitern. Bauen Sie Sicherheitsschranken in Ihre Contracts ein, sodass Sie auf Bugs und Sicherheitslücken reagieren können, wenn diese offensichtlich werden. Für Smart Contracts benötigen Sie auch einen Not-Aus-Schalter, damit Sie den Stecker ziehen und Ihren Contract unterbrechen können, wenn irgendetwas schiefläuft.

Wenn Ihr Contract groß genug ist, bitten Sie die Community, Sicherheitslücken oder Bugs zu finden, indem Sie eine Belohnung aussetzen.

Mit der Komplexität Ihres Contracts nehmen auch die Fehlerwahrscheinlichkeit und die Zahl der Angriffsvektoren zu. Verwenden Sie eine einfache Logik für Ihren Contract. Erstellen Sie kleine Module, die einzelne Abschnitte des Contracts aufnehmen. Auf diese Weise können Sie Probleme auf kleine Bereiche begrenzen.

Bugs im System erkennen

Versuchen Sie nicht, das Rad neu zu erfinden, indem Sie eigene Tools wie etwa Zufallsgeneratoren entwickeln. Nutzen Sie lieber die Arbeit, die die Community bereits geleistet hat und die umfangreich getestet wurde.

Sie können nur Ihren eigenen Contract kontrollieren. Seien Sie vorsichtig mit externen Contracts. Diese können böswilligen Code enthalten und sich Ihrer Kontrolle entziehen.

Die Ethereum-Community besitzt eine hervorragende Liste bekannter Bugs und noch mehr hilfreiche Tipps, wie sichere Smart Contracts erstellt werden. Besuchen Sie dazu die GitHub-Seite unter https://github.com/ethereum/wiki/wiki/safety.

Ihre eigenen ERC20-Token erstellen

In diesem Abschnitt zeige ich Ihnen, wie Sie mit Polymath einen eigenen Token erstellen können. Polymath ist ein Dienst zur Erstellung von Security-Token, der auf der Ethereum-Blockchain aufsetzt. Damit erzeugen Sie auf Ethereum mit wenigen Mausklicks und ganz ohne harte Programmierarbeit eigene Token.

Bevor Sie diesen Abschnitt durchlesen sollten Sie unbedingt MetaMask eingerichtet haben. In Kapitel 3 finden Sie detaillierte Anweisungen zum Einrichten Ihres Computers und zur Installation von MetaMask.

Sie benötigen auch einige Kovan-Test-Ether (KETH), um die Smart Contracts für Ihren neuen Token einzurichten. KETH sind die Test-Ether aus dem Kovan-Testnetzwerk, einem Testnetzwerk für Entwickler von Ethereum-Anwendungen. KETH besitzen keinen Marktwert. Sie können sie kostenlos beziehen, wenn Sie ein GitHub-Konto haben.

In diesem Abschnitt zeige ich Ihnen, wie Sie Ihr GitHub-Konto einrichten, KETH beziehen und Ihre Token erstellen.

Ihr GitHub-Konto einrichten

GitHub ist eine Entwicklungsplattform, auf der Sie Ihren in der Entwicklung befindlichen Code speichern können. Für Open-Source-Projekte bietet GitHub kostenlose Konten an. Wenn Sie Ihren Code also weitergeben möchten, eignet sich GitHub hervorragend zur Verwaltung Ihrer Projekte und zur Erstellung von Software. Es gibt auch eine kostenpflichtige Version von GitHub, wenn Sie den Code unter Verschluss halten wollen. Für unsere Zwecke hier eignet sich ein kostenloses Konto hervorragend.

Um ein GitHub-Konto zu eröffnen, befolgen Sie diese Schritte:

1. **Öffnen Sie den Brave-Webbrowser.**

   Wenn Sie den Brave-Browser nicht installiert haben, lesen Sie in Kapitel 3 nach, wie das geht.
2. **Gehen Sie auf** https://github.com**.**
3. **Geben Sie die gewünschten Benutzerdaten ein.**
4. **Klicken Sie auf SIGN UP FOR FREE.**

Jetzt kann‘s losgehen.

KETH über das Gitter Faucet anfordern

Um KETH anzufordern, befolgen Sie diese Schritte:

1. **Öffnen Sie den Brave-Webbrowser.**
2. **Gehen Sie auf** https://gitter.im/kovan-testnet/faucet**.**
3. **Klicken Sie auf SIGN IN TO START TALKING.**
4. **Klicken Sie auf SIGN IN WITH GITHUB.**

Als Nächstes kopieren Sie Ihre MetaMask-Wallet-Adresse, um sie in das Chatfenster einzufügen. Eines der Community-Mitglieder wird Ihnen dann einige KETH zusenden. Befolgen Sie diese Schritte:

1. **Öffnen Sie Ihre MetaMask-Wallet.**


Um die MetaMask-Wallet zu öffnen, klicken Sie auf das Fuchssymbol rechts oben im Brave-Browser.

2. **Klicken Sie oben in der MetaMask-Wallet auf das Dropdown-Menü.**
3. **Wählen Sie KOVAN TEST NETWORK.**
4. **Kopieren Sie Ihre MetaMask-Adresse, indem Sie auf ACCOUNT 1 klicken.**

Jetzt können Sie Test-Ether (KETH) aus der Kovan-Community anfordern. Veröffentlichen Sie dazu Ihre Kovan-Ethereum-Adresse aus MetaMask im Chatfenster. Achten Sie darauf, nur Ihre Adresse zu posten. Befolgen Sie diese Schritte:

1. **Gehen Sie zurück auf** https://gitter.im/kovan-testnet/faucet**.**
2. **Fügen Sie Ihre kopierte Adresse in das Chatfenster ein.**

Jetzt müssen Sie warten, bis eines der Community-Mitglieder Ihr GitHub-Konto überprüft und sich vergewissert hat, dass Sie kein Spam im Netzwerk versenden. Dies kann einige Zeit in Anspruch nehmen, auch weil Ihnen die KETH manuell zugesendet werden. Nach der erfolgreichen Transaktion sehen Sie die KETH in Ihrer MetaMask-Wallet. Bei mir hat es drei Tage gedauert, aber das war auch über ein langes Wochenende hinweg.

Um Ihr Polymath-Konto einzurichten, befolgen Sie diese Schritte:

1. **Öffnen Sie den Brave-Webbrowser.**
2. **Gehen Sie auf** https://tokenstudio.polymath.network**.**
3. **Klicken Sie auf CREATE YOUR SECURITY TOKEN.**
4. **Klicken Sie im MetaMask-Fenster auf CONNECT.**
5. **Klicken Sie im MetaMask-Fenster auf SIGN.**

Ihr Token erstellen

Sie haben nun die erforderlichen KETH, um Ihr eigenes Token zu erstellen, und können endlich loslegen. In diesem Abschnitt bauen Sie sich mithilfe des Polymath-Smart-Contracts ein benutzerdefiniertes ERC20-Token.

Ihr Token-Symbol reservieren

Mit Polymath können Sie Ihr Token-Symbol für 60 Tage reservieren. Dieser Reservierungsprozess ist unabdingbar für die Einrichtung Ihres Tokens. Auf https://etherscan.io/token

können Sie mithilfe der Suchfunktion überprüfen, welche Namen bereits vergeben sind.


Eine Namensresrevierung in Polymath schützt den Namen nur innerhalb des Polymath-Systems. Sie verhindert nicht, dass jemand anderes ein gleichnamiges Token im Ethereum-Netzwerk herausgibt.

Gehen Sie in Ihre Jaxx-Wallet, und nutzen Sie Shapeshift, um etwas von Ihren Bitcoins oder Ether gegen POLY einzutauschen. Senden Sie anschließend Ihre neuen POLY-Token aus der Jaxx-Wallet an Ihre MetaMask-Wallet. (In Kapitel 3 ist beschrieben, wie Sie Token von einer Adresse zur anderen verschieben können.)

Mit diesen Schritten vergeben Sie einen Namen für Ihr Token:

1. **Geben Sie den gewünschten Ticker-Namen für Ihr Token ein.**

   Hier dürfen Sie maximal zehn Zeichen verwenden.
2. **Geben Sie den Token-Namen ein.**
3. **Klicken Sie auf RESERVE TOKEN SYMBOL.**

   Diese Buchstabenfolge repräsentiert Ihr Token im Netzwerk.
4. **Klicken Sie auf CONFIRM.**
5. **Klicken Sie auf das Fuchssymbol, um Ihre MetaMask-Wallet zu öffnen.**
6. **Klicken Sie auf APPROVE ON CONTRACT.**
7. **Klicken Sie auf APPROVE ON FEE.**

Falls Ihre Transaktion nicht durchgeht, überprüfen Sie, ob Sie genügend Ether zum Entrichten der Mining-Gebühr in der Wallet haben. Es wird einige Zeit dauern, bis Ihr Smart Contract akzeptiert wird. Dies liegt an der Latenzzeit der Blockchain.

Ihr Token erstellen

Nachdem Sie einen Namen reserviert haben, können Sie jetzt Ihr neues Token erstellen. Polymath hat Ihnen eine E-Mail mit einem

Link zu Ihrem Token Creation Dashboard geschickt.

In Ihrem Dashboard sind mehrere Dienstleister integriert, die (Rechts)Beratungs-, KYC/AML-, Marketing- und Vermögenssicherungs-Dienstleistungen anbieten. Wenn Sie Ihre Token der Allgemeinheit zugänglich machen möchten, benötigen Sie diese möglicherweise. KYC (Know Your Customer) ist ein Verfahren zur Bekämpfung der Geldwäsche, mit dem Kunden identifiziert werden, die Gelder verschieben möchten. Es ist Teil einer globalen Initiative zur Bekämpfung von Geldwäsche und Terrorismus namens *Anti-Money Laundering* (AML) und *Combating Financing Terrorism* (CFT). Kommen Sie stets Ihrer Sorgfaltspflicht nach und suchen Sie sich einen Rechtsbeistand. Wenn Sie mit diesen integrierten Anbietern zusammenarbeiten, werden all Ihre Formulareingaben automatisch an die von Ihnen ausgewählten Unternehmen gesendet. Die Unternehmen werden sich an Sie wenden, um Sie bei den nächsten Schritten zu unterstützen.

In den nachfolgenden Schritten gehe ich davon aus, dass Sie Ihre Token *nicht* öffentlich zum Verkauf anbieten.

1. **Öffnen Sie die E-Mail, die Sie von Polymath erhalten haben.**
2. **Klicken Sie auf den Link CLICK HERE TO CONTINUE WITH YOUR TOKEN CREATION.**
3. **Öffnen Sie Ihre MetaMask-Wallet.**
4. **Klicken Sie auf SIGN.**
5. **Klicken Sie bei allen Dienstleistern auf I HAVE MY OWN.**

Nachdem Sie bestätigt haben, dass Sie eigene Dienstleister einsetzen, können Sie mit der Definition Ihres Tokens beginnen. Links auf der Seite finden Sie mehrere Symbole, die Sie über Ihren aktuellen Fortschritt informieren.

1. **Klicken Sie links auf der Seite auf TOKEN.**
2. **Klicken Sie unter MY SECURITY TOKEN MUST BE auf DIVISIBLE.**
3. **Klicken Sie auf CREATE MY SECURITY TOKEN.**
4. **Öffnen Sie Ihre MetaMask-Wallet, und klicken Sie auf CONFIRM.**
5. **Klicken Sie auf CONFIRM.**
6. **Warten Sie eine Minute, öffnen Sie Ihre MetaMask-Wallet erneut, und klicken auf CONFIRM FOR THE MINING FEE.**

Wenn die Seite beim Überprüfen Ihres Contracts länger als fünf Minuten hängen bleibt, aktualisieren Sie die Seite, und melden Sie sich ernuet mit MetaMask an. In Ihrer MetaMask-Wallet können Sie außerdem auch den Status Ihres Contracts einsehen. Für eine schnellere Bearbeitung können Sie die Mining-Gebühr erhöhen. Dadurch können die Kosten für die Transaktion allerdings in die Höhe schnellen, also nutzen Sie diese Funktion mit Bedacht.

Polymath hat für diejenigen, die sie als Mittel zur Kapitalbeschaffung verwenden, eine eingebaute Funktion zur Ausgabe von Token. In Ihrem Polymath-Dashboard wird das als STO bezeichnet. Das ist die Abkürzung für *Security Token Offering*. Ich gehe hier davon aus, dass Ihre Token nicht zur Kapitalbeschaffung genutzt werden. Klicken Sie daher auf SKIP MINTING und dann auf CONFIRM.

Polymath bietet Vorlagen zur Erstellung von Security-Token. In dieser Anleitung nutzen Sie den Smart Contract, der die Anzahl der erzeugten Token auf einen festen Wert begrenzt. Sie legen eine Zeit und die Anzahl der zu erstellenden Token fest. Da diese Token an Ihre eigene Adresse gehen, erzeugen Sie nur geringe Mengen, um Ihren Ether nicht zu verschwenden.

Jetzt erstellen Sie einen gedeckelten, benutzerdefinierten Security-Token. Die Deckelung bezieht sich auf die Tatsache, dass die Gesamtzahl der Token von Ihnen zum

Erstellungszeitpunkt festgelegt wird. Befolgen Sie diese Schritte, um zu beginnen:

1. **Wählen Sie den Erstellungszeitpunkt.**

   Geben Sie sich ein paar Stunden zur Eingabe der Transaktion, falls Sie zwischendurch etwas aufhält.
2. **Wählen Sie unter RAISE IN den Eintrag ETH.**
3. **Geben Sie unter HARD CAP die gewünschte Token-Anzahl ein.**
4. **Unter RATE geben Sie 1000 ein.**

Betrachten Sie dies als Gebühr zur Erstellung Ihrer neuen Token. Sie werden Sie dem Smart Contract »abkaufen«. Wenn Sie 1.000 unter RATE eingeben, dann belaufen sich die Kosten für die Erstellung Ihrer neuen Token auf einen ETH je 1.000 neue Token.

5. **Geben Sie unter ETH ADDRESS TO RECEIVE THE FUNDS RAISED DURING THE STO Ihre MetaMask-Adresse ein.**
6. **Klicken Sie auf DEPLOY AND SCHEDULE STO.**
7. **Klicken Sie auf CONFIRM.**
8. **Gehen Sie in Ihre MetaMask-Wallet.**
9. **Klicken Sie auf CONFIRM.**

Die Token in Empfang nehmen

Sie erhalten eine E-Mail von Polymath, die Sie über die erfolgreiche Einrichtung Ihrer Token informiert. Wenn Sie diese E-Mail erhalten, führen Sie diese Schritte aus:

1. **Gehen Sie auf** https://tokenstudio.polymath.network**.**
2. **Melden Sie sich mithilfe von MetaMask an.**
3. **Klicken Sie rechts auf TOKEN.**
4. **Laden Sie unter MINT YOUR TOKEN die CSV-Beispieldatei herunter.**

5. **Öffnen Sie die CSV-Datei.**
6. **Entfernen Sie die Platzhaltereinträge.**
7. **Geben Sie stattdessen Ihre Adresse im Kovan-Testnetz ein.**
8. **Speichern Sie die neue CSV-Datei.**

Nachdem Sie nun Ihre Adresse eingegeben haben, um Ihr Token zu erhalten, können Sie die Datei auf die gleiche Seite hochladen, von der Sie die Beispieldatei heruntergeladen haben:

1. **Gehen Sie wieder auf** https://tokenstudio.polymath.network**.**
2. **Melden Sie sich mithilfe von MetaMask an.**
3. **Klicken Sie rechts auf TOKEN.**
4. **Klicken Sie auf UPLOAD FILE.**
5. **Klicken Sie auf CONFIRM.**
6. **Öffnen Sie MetaMask.**
7. **Klicken Sie auf CONFIRM.**

Herzlichen Glückwunsch! Sie haben Ihr eigenes Test-Security-Token erstellt. Ethereum ist ein mächtiges Werkzeug, und mit Tools wie Polymath können Sie Ihre gewünschten Blockchain-Anwendungen besonders einfach und schnell erstellen.

Kapitel 6

Die Waves-Blockchain

IN DIESEM KAPITEL

- Die Waves-Blockchain kennenlernen
- Die Waves-Wallet einrichten und absichern
- Die verschiedenen Wallet-Funktionen kennenlernen
- Eine ganz eigene Kryptowährung erstellen

In diesem Kapitel stelle ich Ihnen die Waves-Blockchain vor. Diese ist eine relativ neue Blockchain mit außergewöhnlichen Funktionen. Das Waves-Team hat mehrere Technologien – wie etwa eine Wallet mit Unterstützung für mehrere Währungen, eine dezentrale Handelsplattform und Tools zur Erstellung von Kryptowährungen – in einer einfach zu bedienenden Benutzeroberfläche zusammengefasst.

Die Waves-Blockchain ist auch für Entwickler sehr spannend, weil sie Smart Contracts unterstützt und einen weiterentwickelten Konsensalgorithmus verwendet, der sie zu einer der schnellsten öffentlichen Blockchains macht. Aber Sie müssen nicht unbedingt programmieren können, um mehr aus Waves herauszuholen.

Wenn Sie eigene digitale Assets erstellen oder an dezentralen Börsen handeln möchten, sollten Sie dieses Kapitel unbedingt lesen. Hier erfahren Sie, wie Sie Ihre Web-Wallet absichern, Bitcoins transferieren, Coins durch den Verleih Ihrer Vermögenswerte verdienen und außerdem auch Ihre ganz eigene Kryptowährung erstellen.

Wenn Sie nach der Lektüre dieses Kapitels noch mehr über die Waves-Plattform erfahren möchten, besuchen Sie die

Website https://docs.wavesplatform.com/en/overview/how-to-use-this-guide.html.

Wie unterscheidet sich die Waves-Blockchain von anderen Blockchains?

Waves ist eine öffentliche Blockchain-Plattform, die auf dem Proof-of-Stake-Protokoll (PoS) Nxt basiert. Es ist komplett dezentral, transparent und überprüfbar. Jeder kann die Plattform nutzen, um sogenannte *Colored Coins* herauszugeben, zu verbreiten und zu handeln. Diese ähneln den Token, die über Ethereum-Smart-Contracts ausgegeben werden. Colored Coins können alles repräsentieren, was Sie vielleicht auf einer Blockchain handeln möchten (zum Beispiel Aktien, Anleihen, Wertpapiere, Güter oder Immobilien). Mit einem einfachen Download und wenigen Klicks können Sie anfangen, allerlei neue und coole Dinge zu erstellen.

Nur weil Sie Token und Colored Coins so leicht erstellen können, ist es nicht unbedingt legal, diese herauszugeben. Sprechen Sie immer zuerst mit Ihrem Anwalt, bevor Sie ein mögliches Finanzinstrument erstellen.

Das Waves-Netzwerk wird dadurch gesichert, dass bestehende Konten anhand ihres Guthabens zum *Forging* (»Schmieden«) von Blöcken berechtigt sind. Statt spezielles Equipment zum »Mining« neuer Coins vorauszusetzen, belohnt Waves die Inhaber der Kryptowährungs für die Validierung von Blöcken. Diese sogenannten »Forger« erhalten Transaktionsgebühren anstelle von Blockprämien. Der PoS-Algorithmus ist populär geworden, weil er sehr energieeffizient arbeitet und sogar auf kleinen Geräten wie dem Raspberry Pi ausgeführt werden kann. Außerdem gibt es bei PoS nicht dieselben Skalierungs- und Sicherheitsprobleme wie bei PoW-Systemen.

Konkret sind viele PoW-Blockchains anfällig für eine 51-Prozent-Attacke, bei der die überwiegende Mining-Leistung von einigen wenigen Personen erzeugt wird, die dann die Datensätze in der Blockchain-Historie manipulieren können. PoS-Systeme haben aber ihre eigenen Probleme: Auch hier könnten einige wenige Parteien gemeinsam über mehr als die Hälfte des Netzwerkwerts verfügen und dieses dann ebenfalls böswillig übernehmen. Wenn Sie sich verschiedene Plattformen für Ihr Unternehmen ansehen, müssen Sie immer die Kostensenkung, Geschwindigkeit und Sicherheit gegeneinander abwägen.

Waves bietet auch eine dezentrale Peer-to-Peer-Handelsbörse, eine Abstimmungsfunktion, ein Messaging-/Chat-System und ein dezentrales Domain-Namensystem (»DNS«). Viele Blockchains verfügen über ein bis zwei dieser Funktionen. Waves hat sie *alle* und basiert zudem auf einem neueren Netzwerkmodell.

Eine kurze Geschichte der Waves-Blockchain

Die Waves-Plattform wurde 2016 von Sasha Ivanov geschaffen. Er wollte eine Blockchain-Software entwickeln, die einfach und intuitiv von normalen Menschen genutzt werden kann. Das war damals ein umstrittener Ansatz in der Szene, da die meisten Blockchain-Clients bisher eher für Leute entwickelt worden waren, die mit der Kommandozeile und dem Terminal ihres Computers vertraut waren. In den Entwicklerteams herrschte oft die Meinung: »Wer nicht schlau genug ist, sollte lieber außen vor bleiben«.

Aber viele glaubten an Sashas Traum, und er sammelte rund 30.000 Bitcoin zum damaligen Wert von etwa 18 Millionen Dollar für die Entwicklung der Waves-Plattform ein. Seitdem hat er eine der größten Communitys aufgebaut und spricht von 300.000 aktiven Nutzern in 25 Ländern. Er beschäftigt auch ein Team von 100 Entwicklern, die an der Verbesserung der Plattform arbeiten.

Die volle Leistung von Waves ausschöpfen

Die Waves-Wallet ist mehr als nur ein Aufbewahrungsort für Ihre Waves-Coins. Sie unterstützt auch mehrere andere Kryptowährungen, wie etwa Bitcoin und Ethereum. Die Waves-Wallet bietet Ihnen auch Zugriff auf eine dezentrale Börse (siehe »Nutzung einer dezentralen Börse« weiter unten in diesem Kapitel).

In der Waves-Wallet können Sie auch ganz ohne Programmierkenntnisse eigene Colored Coins erzeugen. Colored Coins funktionieren ähnlich wie die in Kapitel 5 beschriebenen ERC20-Token, obwohl sie etwas anders aufgebaut sind. Colored Coins können Sie für den einmaligen Gebrauch einrichten, wie einen digitalen Coupon, oder wie eine Währung zirkulieren lassen.

Die Waves-Wallet ist sehr benutzerfreundlich, und ihre Bedienung ist einfach zu erlernen. Sie werden feststellen, dass es sich um eine der einfachsten, aber leistungsfähigsten Blockchain-Anwendungen für Normalsterbliche handelt.

Es gibt eine Download-Version der Waves-Wallet, die Ihre privaten Schlüssel auf Ihrem Gerät speichert. Das ist die sicherere Variante, mit der Sie auch offline arbeiten können. Waves hat zudem eine fantastische Web-Wallet, die nur online verfügbar ist. In diesem Kapitel zeige ich Ihnen den Umgang mit der Web-Version, weil dies die einfachste und unkomplizierteste Waves-Wallet ist, die außerdem auch Zugang zur dezentralen Handelsplattform bietet.

In diesem Abschnitt erkläre ich Ihnen Schritt für Schritt, wie Sie Ihre Waves-Wallet einrichten und absichern. Eine kleine Randbemerkung: Zum Öffnen eines Bitcoin-Kontos innerhalb der Waves-Wallet benötigen Sie eine Mindesteinlage von 0,001 Bitcoin. Während ich dies schreibe entspricht das knapp zehn Euro.

Die Waves-Wallet einrichten

Der Waves-Client ist die Wallet, in der Sie Ihr Waves-Guthaben aufbewahren, Kryptowährungen handeln und neue Assets erstellen können. Durch das spezielle PoS-System, mit dem Wave sein Netzwerk sichert, können Sie Ihre Waves auch verleihen und dafür mit Transaktionsgebühren aus dem Netzwerk belohnt werden, und das alles aus Ihrer Waves-Wallet heraus.

So richten Sie eine sogenannte *Seed-Phrase* zur bedarfsweisen Wiederherstellung Ihrer Wallet ein:

1. **Rufen Sie die Website des Waves-Clients auf:** https://client.wavesplatform.com/create.
2. **Klicken Sie auf MIT WEBCLIENT FORTFAHREN.**
3. **Klicken Sie auf WAS SIE ÜBER IHREN SEED WISSEN MÜSSEN.**
4. **Klicken Sie auf SCHÜTZEN SIE SICH SELBST.**
5. **Klicken Sie auf ICH VERSTEHE.**
6. **Klicken Sie auf WEITER.**

Ihre Wallet sichern

In diesem Abschnitt unternehmen Sie wichtige Schritte, um Ihre digitalen Vermögenswerte zu schützen und sicherzustellen, dass Sie stets Zugang dazu haben.

Blockchain-Software funktioniert anders als andere Internetseiten, bei denen Sie ein Benutzerkonto anlegen können. Die meisten Online-Konten haben Funktionen, mit denen Sie Ihren Zugang bei Passwortverlust wiederherstellen können. Dies ist bei Kryptowährungen nicht der Fall. Sie haben die vollständige Kontrolle über Ihr Konto und die Vermögenswerte in Ihrer Wallet, und wenn Sie den Zugang dazu verlieren, sind die Inhalte für immer verloren.

Nehmen Sie sich zunächst einen Stift und ein Blatt Papier. Um Ihre Brieftasche zu sichern, befolgen Sie dann diese Schritte:

1. **Schreiben Sie sich Ihre Kontobezeichnung auf.**
2. **Schreiben Sie Ihr Passwort auf.**
3. **Geben Sie Ihr Passwort und Ihre Kontobezeichnung in die entsprechenden Felder ein.**
4. **Klicken Sie auf WEITER.**

Schützen Sie Ihren Zettel durch Laminieren vor Beschädigungen. Erstellen Sie keine digitale Kopie, und machen Sie kein Foto von Ihrem Passwort oder Ihrer Seed-Phrase. Krypto-Enthusiasten haben aus Nachlässigkeit bei der Absicherung ihrer Wallets schon Millionen von Dollars verloren, mich eingeschlossen.

Nachdem Sie Ihr Konto angelegt haben, sollten Sie unbedingt die Seed-Phrase als Back-up aufschreiben. Folgen Sie diesen Schritten, um ein Back-up Ihres Kontos anzulegen:

1. **Holen Sie sich ein zweites Blatt Papier.**
2. **Klicken Sie auf ICH VERSTEHE.**
3. **Schreiben Sie die 15 Worte, die die Seed-Phrase für Ihr Konto bilden, auf das Papier.**
4. **Klicken Sie auf ICH HABE ES AUFGESCHRIEBEN.**
5. **Klicken Sie die 15 Worte in der richtigen Reihenfolge an.**
6. **Klicken Sie auf BESTÄTIGEN.**
7. **Markieren Sie die Kontrollfelder, und klicken Sie auf BESTÄTIGEN UND BEGINNEN.**

Herzlichen Glückwunsch! Sie haben nun Ihr Waves-Konto eingerichtet und gesichert. Bewahren Sie Ihren Benutzernamen, Ihr Passwort und Ihre Back-up-Phrase (die 15 Wörter, die Sie aufgeschrieben haben) unbedingt an einem sicheren Ort auf.


Die Back-up-Phrase wird auch als Seed-Phrase bezeichnet. Damit können Sie Ihr Konto wiederherstellen, wenn Sie Ihr Passwort vergessen haben. Da niemand das Kontopasswort für Sie zurücksetzen kann, achten Sie darauf, dass Sie Ihre Zettel nicht verlieren, und bewahren Sie die Seed-Phrase aus 15 Worten an einem anderen Ort auf als Ihren Benutzernamen und Ihr Passwort.

Die Wallet-Funktionen entdecken

Nachdem Sie Ihr Konto eingerichtet und abgesichert haben, können Sie einige der tollen Funktionen der Waves-Wallet entdecken. Wenn Sie außerhalb der USA leben, können Sie mit der Waves-Wallet Kryptowährungen per Kreditkarte kaufen. Es ist aber jedem erlaubt, mehrere Kryptowährungen zu halten und sie auf der dezentralen Börse zu handeln, Vermögenswerte auf andere Nutzer zu übertragen und einzigartige Colored Coins zu erstellen (entweder zum einmaligen Gebrauch wie einen digitalen Coupon, oder mit unbegrenzter Lebensdauer wie eine Währung).


Im folgenden Abschnitt zeige ich Ihnen, wie Sie Bitcoin an Ihre neue Waves-Wallet senden. Ich empfehle Ihnen hierfür ein Startkapital von mindestens zehn Euro, da Waves eine Mindesteinlage vorsieht, um die integrierte Bitcoin-Wallet zu aktivieren. Lesen Sie noch einmal das Kleingedruckte, bevor Sie ein Bitcoin-Guthaben dorthin senden; das Limit kann sich seit dem Verfassen dieses Buches geändert haben.

Ich zeige Ihnen auch, wie Sie Ihre Bitcoins an einer dezentralen Börse in Waves umtauschen können.

Krypto-Assets transferieren

Falls Sie noch keine Kryptowährung besitzen, müssen Sie welche erwerben, um die Waves-Plattform weiter zu erkunden. In Kapitel

3 finden Sie detaillierte Anweisungen, wie Sie Ihr erstes Bitcoin-Guthaben erhalten.

Nachdem Sie sich etwas Bitcoin oder Ether besorgt haben, können Sie damit die Kryptowährung Waves kaufen. Und mit Ihren Waves können Sie später Ihren ganz eigenen Colored Coin erstellen. Praktischerweise können Sie Bitcoin oder Ether direkt innerhalb der Waves-Wallet handeln, ohne dafür eine externe Kryptobörse zu bemühen.

Ehe Sie mit diesem Abschnitt fortfahren, beachten Sie Folgendes:

- ✔ Der Kauf und die Verwendung von Kryptowährungen haben viele unbekannte regulatorische und steuerliche Auswirkungen, die noch immer heftig diskutiert werden. Der Kauf und Handel von Kryptowährungen kann steuerpflichtig sein.
- ✔ Web-Wallets sind keine besonders sichere Aufbewahrungsmöglichkeit für Ihre Vermögenswerte. Zahlen Sie zu keinem Zeitpunkt mehr auf Ihr Konto ein, als Sie für diese Übungen benötigen. Zehn Dollar in Bitcoin oder Ether reichen aus.

Wenn Sie Ihre Wallet auf der Waves-Plattform noch nicht eingerichtet haben, tun Sie dies jetzt. Wenn Sie noch keine Bitcoins gekauft haben, lesen Sie außerdem Kapitel 3, und richten Sie ein Konto bei Bitcoin.de ein. Befolgen Sie dann diese Schritte:

1. **Öffnen Sie zwei Browser-Fenster.**
2. **Gehen Sie in einem Fenster auf** `www.bitcoin.de`**, und loggen Sie sich in Ihr Benutzerkonto ein.**
3. **Gehen Sie im anderen Fenster auf** `https://client.wavesplatform.com`**, und loggen Sie sich in Ihren Waves-Account ein.**
4. **Kopieren Sie die Bitcoin-Adresse für Ihren Waves-Account.**

5. **Fügen Sie die Bitcoin-Adresse in das Bitcoin.de-Fenster ein.**
6. **Senden Sie Bitcoin im Wert von zehn Euro an Ihre Waves-Wallet.**

Die Bitcoin-Überweisung an Ihre Waves-Wallet kann etwas Zeit in Anspruch nehmen. Beachten Sie auch, dass Waves eine Mindesteinlage von 0,001 Bitcoin vorsieht, um die Bitcoin-Wallet erstmals freizuschalten. Während ich dies schreibe sind das knapp zehn Euro.

Eine dezentrale Börse verwenden

Bei dezentralen Exchanges – oder kurz DEXs –brauchen Sie Ihr Geld oder Ihre Kryptowährung keiner zentralen Institution anzuvertrauen. Ihre Vermögenswerte verbleiben in Ihrer eigenen Wallet, bis Sie sich zum Verkauf entscheiden und einen passenden Käufer finden.

Wenn Sie Kryptowährung über eine DEX verkaufen wollen, müssen Sie zunächst eine Order in das dezentrale Orderbuch dieser Börse eintragen. Daraufhin kann ein anderer Benutzer eine digital signierte Gegenorder hinzufügen und Ihre Kryptowährung kaufen. Die abgeschlossene Transaktion wird in die Blockchain der DEX geschrieben, und die Vermögenswerte werden zwischen Ihnen und dem Käufer ausgetauscht.

In diesem Abschnitt stelle ich Ihnen die Innovationen des DEX-Systems von Waves vor. Ich zeige Ihnen auch, wie Sie auf der Waves-DEX Bitcoin gegen Waves handeln können. Wenn Sie später in diesem Kapitel Ihren ganz persönlichen Colored Coin erstellen möchten, sollten Sie diesem Abschnitt unbedingt gründlich lesen, da Sie hierfür Waves-Token benötigen.

Vergleich zwischen zentralisierten und dezentralen Handelsplätzen

Zentralisierte Exchanges sind Angriffsziele für Hacker, weil sie große Werte an einer zentralen Stelle konzentrieren. Seien Sie stets vorsichtig beim Umgang

mit zentralisierten Börsen, und überlegen Sie sich zweimal, ob Sie dort größere Werte hinterlegen möchten. Diese Vorsicht ist angebracht, weil Sie sich niemals sicher sein können, ob Sie Ihr Guthaben beim nächsten Log-in noch vorfinden.

Einer der bekanntesten Fälle von Diebstahl an einer zentralen Börse war die Attacke auf Mt. Gox. Die Bitcoin-Börse brach 2014 zusammen, nachdem Hacker in das zentrale System eingedrungen waren. Die Angreifer erbeuteten rund 650.000 , die bis heute nicht sichergestellt werden konnten. Der Zusammenbruch der Handelsplattform war ein Schock für die Kyptocommunity. Seither wurden Dutzende neuer zentraler Börsen eröffnet und von Angreifern ins Visier genommen.

Blockchain-Pioniere haben durch Hartnäckigkeit, Entschlossenheit und Kreativität viele neue Lösungen entwickelt, wie etwa die dezentrale Waves-Exchange. Aber auch DEXs haben ihre Schwächen. Viele DEXs leiden unter einer zu geringen Liquidität. Händler müssen jedoch schnell am Markt kaufen und verkaufen, ohne den Preis des Assets zu stark zu beeinflussen. Viele DEXs sind nicht nach außen vernetzt und können alleine keinen signifikanten Marktanteil gewinnen. Häufig sind dezentrale Börsen vollständig in eine Blockchain integriert. Das erhöht zwar die Sicherheit, macht sie aber abhängig von der Blockgeschwindigkeit dieser speziellen Blockchain. Die geringe Geschwindigkeit und die hohen Transaktionskosten, die mit der vollständigen Integration einhergehen, machen sie für Händler eher unattraktiv. Dezentrale Börsen sind außerdem anfällig für Arbitrage durch Händler, die von den leichten Preisunterschieden zwischen den Börsen profitieren wollen. Ein solcher Handel kann das Geld der Benutzer an DEXs vernichten.

Neue, hybride Ansätze wie die Waves-DEX versuchen, die Vorteile zentraler Börsen, wie etwa den schnellen Handel, automatisches Order-Matching und niedrige Kosten, mit den Vorteilen von DEXs zu kombinieren, bei denen die Eigentümer bis zum Trade die volle Kontrolle über ihre Vermögenswerte behalten.

Handeln auf der dezentralen Waves-Exchange

Auf der Waves-DEX können Sie Vermögenswerte aus der Sicherheit Ihrer Wallet heraus handeln. Da die Waves-Wallet mehrere Kryptowährungen unterstützt, können Sie sie alle auf der Waves-DEX handeln – nicht nur Waves-Token oder mit Waves erstellte Colored Coins. Der Handel mit Kryptowährungen birgt viele eigene Herausforderungen und muss mit Bedacht durchgeführt werden.

Die Waves-DEX hat eines der vielen Probleme behoben, die die weitere Verbreitung dieser Technologie gehemmt haben. Durch eine Zentralisierung des Orderbuch-Matchings ermöglicht sie den Handel in Echtzeit. Die Waves-DEX ist ein Hybrid aus zentraler und dezentraler Handelstechnologie. Der zentralisierte Matcher bündelt eingehende Orders und führt die Trades typischerweise innerhalb von Millisekunden aus. Das ist ein Vorteil gegenüber anderen DEXs, die vollständig in eine Blockchain integriert sind. Vollständig dezentrale Börsen sind von der Blockgeschwindigkeit ihrer Netzwerke abhängig und haben viel höhere Handelsgebühren.

Indem Sie eine Limit-Order erstellen, unterschreiben und an den Waves-Matcher senden, signalisieren Sie Ihre Bereitschaft zum Kauf oder Verkauf von Krypto-Assets. Die Orders auf Waves entsprechen denen auf anderen Börsen. Eine Kauforder schreibt einen Preis für eine bestimmte Anzahl eines Tokens fest, der gleich oder besser sein muss als von Ihnen angegeben. Wenn Sie eine neue Order erstellen, wird sie an die DEX übermittelt. Ihre Order wird auf Richtigkeit überprüft und Ihre Signatur durch den öffentlichen Schlüssel Ihrer Wallet bestätigt.

Die Orders auf der Waves-DEX werden paarweise verknüpft und von den Knoten des Waves-Netzwerks geprüft. Dann erstellt der Matcher eine Handelstransaktion, signiert sie und schreibt sie in den Handelsverlauf der Waves-Blockchain. Eine Order muss dabei nicht komplett ausgeführt werden. Der Waves-Matcher kann auch Teilaufträge zuordnen. Die validierenden Nodes berechnen für diese teilweise ausgeführten Orders auch nicht die volle Ordergebühr. Ihre Assets werden erst dann übertragen, wenn der Handel in der Waves-Blockchain veröffentlicht wurde. Wenn das Matching aus irgendeinem Grund fehlschlägt, wird Ihr Handel nicht ausgeführt. Alle unerfüllten Orders werden automatisch nach 30 Tagen storniert.

Bitcoin in Waves umtauschen

Um Bitcoins aus Ihrer Waves-Bitcoin-Wallet über die Waves-DEX in Waves-Token umzutauschen, befolgen Sie diese Schritte:

1. **Loggen Sie sich auf https://client.wavesplatform.com in Ihren Account ein.**
2. **Klicken Sie auf das Exchange-Symbol.**
3. **Klicken Sie auf WAVES/BTC.**
4. **Geben Sie Ihre minimale Waves/BTC-Order ein.**
5. **Klicken Sie auf WAVES KAUFEN.**
6. **Klicken Sie auf das Wallet-Symbol.**
7. **Warten Sie, bis Ihr Trade ausgeführt wird.**

Es kann etwas dauern, bis Sie Ihre Waves empfangen. Ihre Order muss zuerst zum von Ihnen angegebenen Preis mit einem Verkäufer abgeglichen werden. Sie erkennen, dass Ihr Handel ausgeführt wurde, wenn sich auf der Wallet-Seite das Bitcoin-Guthaben geändert hat und Ihr Waves-Guthaben gestiegen ist.

Herzlichen Glückwunsch! Sie haben gerade auf einem dezentralen Handelsplatz Bitcoin gegen Waves gehandelt.


Belassen Sie keine großen Werte in einer Online-Wallet. Und denken Sie daran, dass Ihre Trades möglicherweise steuerpflichtig sein könnten.

Ihre eigene Kryptowährung erstellen und verleihen

Colored Coins sind die Token der Waves-Plattform. Colored Coins haben viele Anwendungsgebiete. Alles, was sich quantifizieren und digital für den Handel repräsentieren lässt, könnte einen Colored Coin als Online-Mechanismus zur Eigentumsübertragung verwenden.

In diesem Abschnitt erstellen Sie mit dem einfachen, in der Web-Wallet integrierten Colored-Coin-Generator Ihren eigenen Colored Coin. Mit wenigen Klicks haben Sie ein einzigartiges Asset geschaffen, das unabhängig von Ihnen für die restliche Bestandsdauer der Waves-Plattform fortbesteht. Sie müssen dazu noch nicht einmal programmieren können, benötigen aber ein wenig Kryptogeld.

Möglicherweise können Sie die Waves-Währung in Ihrer Web-Wallet kaufen. Diese Funktionalität ist nicht in allen Ländern freigeschaltet. Wenn Sie Teile dieses Kapitels übersprungen haben, gehen Sie jetzt zurück, um Ihre ersten Waves zu bekommen. Sie brauchen mindestens einen, um Token zu generieren. Sobald Sie einige Waves besitzen, befolgen Sie diese Schritte:

1. **Klicken Sie auf das Würfelsymbol.**

   Wenn oben TOKEN GENERATION steht, befinden Sie sich auf der richtigen Seite.
2. **Geben Sie ins Feld NAME OF YOUR ASSET einen Namen Ihres neuen Colored Coins ein.**
3. **Fügen Sie eine Beschreibung hinzu.**
4. **Geben Sie die Gesamtanzahl der zu erstellenden Token ein.**
5. **Belassen Sie die Einstellung im Dropdown-Menü auf ERWEITERBAR.**

   Dies bedeutet, dass Ihre Colored Coins nach der Erstellung und Übertragung an eine andere Person weiter im Umlauf bleiben.
6. **Geben Sie ins Feld DECIMALS die Zahl 8 ein.**

   Das ist die kleinste Stückelung, die für Ihre neuen Colored Coins möglich ist. Die meisten Kryptowährungen verwenden acht Dezimalstellen.

7. **Klicken Sie auf GENERIEREN.**
8. **Klicken Sie auf BESTÄTIGEN.**
9. **Klicken Sie auf DETAILS.**

Herzlichen Glückwunsch! Sie haben Ihre ganz individuellen Colored Coins erstellt. Sie können sie ansehen, indem Sie auf die Wallet-Seite zurückkehren, wo Ihre Bitcoins und Waves angezeigt werden, und dort am Ende der Seite auf das Plussymbol klicken. Daraufhin erscheint eine Option, um Ihre neuen Coins auf der Asset-Homepage anzuheften.

Nachdem Sie jetzt Ihre Colored Coins erstellt haben, können Sie einen Teil Ihrer Waves-Token verleihen und sich so zur Sicherung und zum Erhalt des Netzwerks in die Gemeinschaft einbringen. Das Beste daran ist, dass Sie durch das *Staking* Ihres Guthabens auch neue Waves verdienen können. Folgen Sie einfach diesen Schritten:

1. **Klicken Sie auf LEASING.**
2. **Klicken Sie auf START LEASE.**
3. **Klicken Sie auf LISTE DER KNOTEN.**
4. **Wählen Sie einen Leasing-Pool.**
   Hier stehen mehrere zur Auswahl. Wählen Sie einen mit aktiven Nutzern und regelmäßigen Auszahlungen.
5. **Klicken Sie auf den Namen des Pools.**
6. **Kopieren Sie die Leasing-Adresse oben auf der Seite.**
7. **Fügen Sie die Leasing-Adresse in das Empfängerfeld ein.**
8. **Geben Sie die Anzahl der Waves ein, die Sie verleihen möchten.**
   Wenn Sie alle Waves verleihen wollen, klicken Sie auf MAX.
9. **Klicken Sie auf START LEASE.**
10. **Klicken Sie auf CONFIRM.**

Wenn Sie Ihre Waves zurückhaben möchten, klicken Sie auf das Detailsymbol und dann auf CANCEL LEASING.

Kapitel 7

Die Factom-Blockchain

IN DIESEM KAPITEL

- Einträge in Factom erstellen
- Die Kettenstruktur kennenlernen
- Eine Identität in der Blockchain offenlegen
- Factom in der Praxis

Die Factom-Blockchain ist ein leistungsstarkes Tool, das bei der Skalierung der Blockchain-Technologie helfen wird. Sie unterscheidet sich von anderen öffentlichen Blockchains und besitzt einzigartige Eigenschaften, die sie ideal für die Veröffentlichung von Datenströmen und die Absicherung von Systemen machen. Hinter der Factom-Blockchain steht das Unternehmen Factom, Inc., das ihre Entwicklung vorantreibt und Tools und Produkte auf dem Protokoll aufbaut.

Factom-Software wird in Systeme integriert, die die Identität und Sicherheit von Menschen und Dingen verwalten. Sie integriert wiederum andere Blockchains und Blockchain-Technologien und verbindet sie miteinander. Die Verknüpfung mehrerer Blockchains verbessert einerseits die Sicherheit durch erhöhte Redundanz und andererseits die Möglichkeiten des Datenaustauschs.

Dieses Kapitel erklärt, wie Factom funktioniert. Sie werden seine einzigartigen Eigenschaften kennenlernen und erhalten einfache Anleitungen, die Ihnen bei den ersten Schritten mit Factom helfen. Nachdem Sie dieses Kapitel gelesen haben, werden Sie viele Kernaspekte der Factom-Blockchain-Technologie verstehen und wissen, wo Sie sie in Ihren Blockchain-Projekten am gewinnbringendsten einsetzen.

Ich sollte vielleicht erwähnen, dass ich Mitgründerin von Factom, Inc. bin. Selbstverständlich will ich Objektivität bewahren, aber meine Begeisterung für Factom ist schwerlich zu verbergen.

Eine Frage des Vertrauens

Bei Blockchains geht es vor allem darum, verschiedenen Parteien eine Zusammenarbeit zu ermöglichen, ohne dass sie der Datensicherheit oder den Geschäftsprozessen der jeweils anderen Partei vertrauen müssen. In der Vergangenheit mussten vertrauenswürdige Vermittler oder Branchenkonsortien diese Aufgabe erfüllen. Das führte jedoch zu hohen Kosten, und die Vertrauensfrage wurde im Grunde einfach an eine andere Partei abgeschoben. Blockchains hingegen übertragen die Vertrauensfrage an ein Netzwerk leidenschaftsloser Dritter und letztlich an die Mathematik.

Factom, Inc. ist ein Unternehmen, das Blockchain-Software auf Grundlage der offen zugänglichen Factom-Blockchain entwickelt. Die Software für die Datensatzverwaltung von Factom arbeitet auf einem sehr hohen Niveau, indem sie verschlüsselte Daten oder einen kryptografisch eindeutigen Fingerabdruck dieser Daten in der Factom-Blockchain veröffentlicht (siehe Abbildung 7.1). Als zusätzliche Absicherung des Netzwerks wird alle zehn Minuten in mehreren anderen öffentlichen Blockchains ein Hash der gesamten Factom-Blockchain veröffentlicht. Diese zusätzlichen Blockchain-Einträge unterscheiden Factom von den meisten öffentlichen Blockchains.

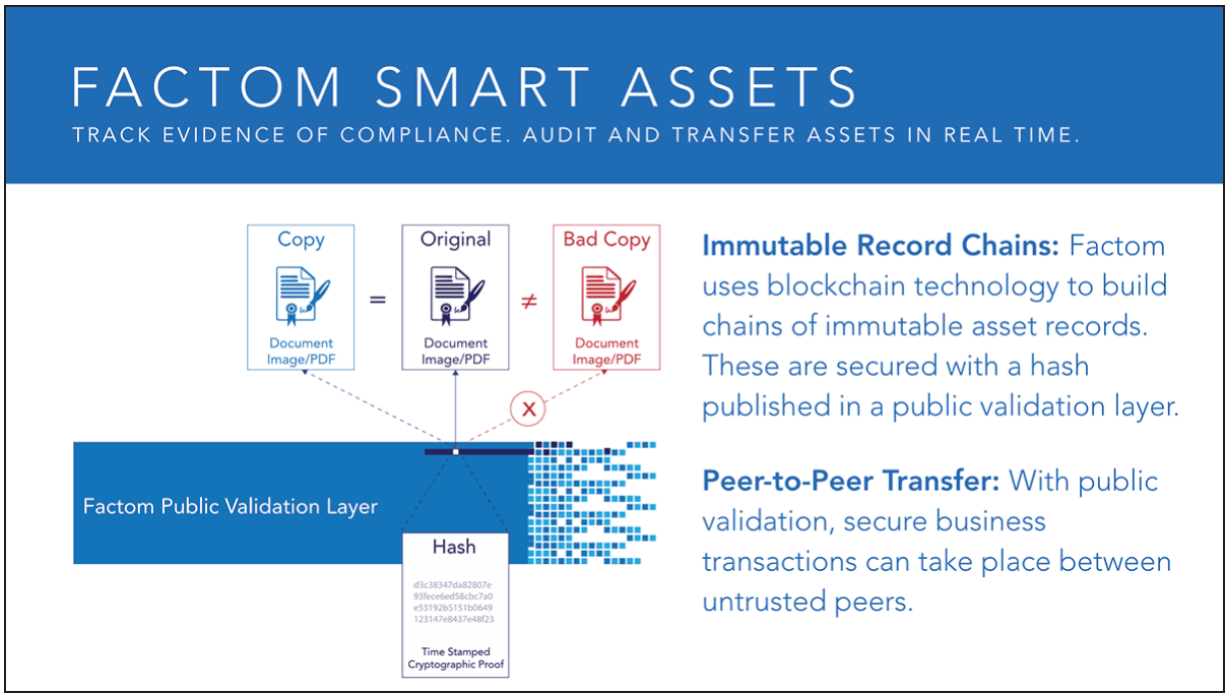


Abbildung 7.1: Der Aufbau der Factom-Blockchain

Das Protokollkonzept wurde 2014 als Whitepaper vorgestellt. Es sollte die Skalierbarkeitsprobleme von Bitcoin lösen. Als dezentrale Anwendungen begannen, sich selbst im Bitcoin-Netzwerk abzusichern, wurde schnell klar, dass Dateneinträge in die Bitcoin-Blockchain bei umfangreicher Nutzung viel zu teuer waren und dass Bitcoin keine hohen Transaktionsvolumina verarbeiten konnte. Metaphorisch könnte man sagen: Zehn Kilo Daten passen nicht in eine Fünf-Kilo-Bitcoin-Tasche.

Das Factom-Protokoll wurde darauf ausgelegt, die Kosten- und Volumenbeschränkungen anderer Blockchains aufzuheben. Das eigentliche Ziel war, Daten und Systeme abzusichern. Aufgrund dieser Zielsetzung wird Factom häufig auch als *Publishing-Engine* bezeichnet. Die Benutzer können gegen eine kleine Gebühr Daten in ihr Ledger schreiben. Diese Einträge sind auf zehn Kibibyte begrenzt und haben einen festen Preis, der sehr günstig ist. Und auch die Kapazität für das Transaktionsvolumen ist um eine Größenordnung höher als bei Proof-of-Work-Blockchains. Die festen Kosten für die Dateneingabe sind auch ein Alleinstellungsmerkmal von Factom. Andere Blockchain-Netzwerke mit einem öffentlich gehandelten Token oder einer

Kryptowährung weisen im Gegensatz zum von Factom verwendeten Zwei-Token-System Kostenschwankungen auf, die vom Marktpreis der entsprechenden Kryptowährung und der Netzwerkauslastung abhängen.

Ein wichtiges Konzept ist, dass die Factom-Blockchain in Schichten und Ketten (*Chains*) aufgebaut ist. Die Schichten haben mit der Datenstruktur zu tun. Sie nutzen Hash-Bäume, um kryptografisch zu belegen, dass bestimmte Daten in Factom veröffentlicht wurden. Der kryptografische Beleg, ein sogenannter *Root Hash* (32 scheinbar zufällige Zeichen, die einen ganzen Baum individueller Daten darstellen können), wird dann in anderen öffentlichen Blockchains veröffentlicht, wie beispielsweise Ethereum. Diese Art der Redundanz bieten andere Blockchains nicht.

Ein Hash-Baum ist ein mathematischer Baum, der konstruiert wird, indem ein Hashing für paarweise Daten und dann immer weitere Hashings für die Ergebnisse durchgeführt werden, bis nur noch ein einziger Hash übrig bleibt, der sogenannte *Root-Hash* oder *Merkle-Root*. Dieser kryptografische Beleg wurde 1979 nach Ralph Merkle benannt.

Die Anordnung von Daten in Ketten unterstützt die Skalierbarkeit. Ketten ermöglichen Anwendungen, nur die Daten aus der Factom-Blockchain zu extrahieren, an denen sie interessiert sind, ohne die komplette Datenmenge herunterladen zu müssen. Ihre Arbeitsweise ist ganz einfach: Sie können Ihre Daten in einer vorhandenen Kette (Chain) in Factom veröffentlichen oder eine neue Kette einrichten. Die ID der Kette wird dann in den nachfolgend veröffentlichten Einträgen verwendet, um die für Sie relevanten Daten zurückverfolgen zu können.

Der Zweck der Factom-Blockchain: Beliebige Daten veröffentlichen

Factom ist eine Publishing-Plattform. Im Grunde wurde sie entwickelt, um beliebige Daten zu veröffentlichen und zu überprüfen. Alle anderen Tools darin sind um diese einfachen Funktionalitäten herum aufgebaut. Factom kann Transaktionen von bis zu zehn Kibibyte verarbeiten. Größere Transaktionen erfordern eine spezielle Struktur und mehrere Einträge. Alternativ kann auch ein Hash veröffentlicht werden, der die Daten darstellt.

Das Factom-Protokoll ist quelloffen, deshalb kann das System auch öffentlich verwendet werden. Jeder kann alles veröffentlichen und es durch die Factom-Blockchain absichern. Es überrascht kaum, dass bestimmte Individuen bereits auch obszöne Inhalte veröffentlicht haben, aber aufgrund der Begrenzung der Eintragsgröße können sie nicht viel veröffentlichen. Spam kommt im System ohnehin kaum vor, weil jeder Eintrag eine kleine Gebühr kostet. Wenn Sie also in der Blockchain herumpöbeln möchten, müssen Sie dafür bezahlen.

Die Kryptowährung des Factom-Netzwerks sind *Factoids*. Dezentrale Systeme brauchen einen Belohnungsmechanismus als Anreiz für die Teilnehmer. Dieses geschlossene System bedingt eine Zusammenarbeit und baut die langfristige Wertschöpfung des Netzwerks auf. Factoids können genau wie Tausende anderer Kryptowährungen und Token frei gehandelt werden. Letztlich werden Factoids verwendet, um *Entry Credits*, die zu Einträgen im Factom-Netzwerk berechtigen, zu kaufen.

Die Kosten für einen Eintrag sind festgelegt, während die Kosten für einen *Factoid* schwanken. Wenn ein Factoid im Wert steigt, kann der Benutzer damit mehr Entry Credits kaufen. Dadurch wird das System von den handelbaren Token abgekoppelt, und es behält feste Kosten für die Anwender bei, während auf dem freien Markt mit Factoids spekuliert werden kann. Diese Funktionalität wurde bereits in die erste Version von Factom eingebaut, damit stark regulierte Branchen und Regierungen die Blockchain-Technologie nutzen können, ohne sich mit handelbaren Token herumzuschlagen.

Anfang 2017 verarbeitete das Factom-Netzwerk etwa 40.000 Einträge pro Tag. Unter anderem sind darunter Dinge wie der Russell-3000-Index oder eine Aufzeichnung der Altcoin-Preise. Diese Datensätze dienen als historische Referenzen und können als Eingabeparameter für Smart Contracts oder als Beleg für einen historischen Verlauf dienen. Diese Methoden werden an vielen Orten weltweit eingesetzt. China hat angefangen, auf Factom-Einträge zu verweisen. Und auch das US-Ministerium für innere Sicherheit nutzt Factom-Einträge zur Absicherung von Hardware.

Die Speicherung von Daten und der Zugriff darauf sind heute größtenteils gelöste Probleme. Computersicherungskopien lassen sich in riesigen Größenordnungen replizieren und archivieren. Ein großes, weiterhin aktuelles Problem ist die Frage, welches Dokument die aktuellste Version darstellt, insbesondere über verschiedene Unternehmen hinweg. Mit einem Dokumentenmanagementsystem auf Blockchain-Basis können Unternehmen sicherstellen, dass sie dieselben Dokumente verwenden wie ihre Partner.

Anreize für den Zusammenschluss

Viele Blockchains, beispielsweise Bitcoin und Ethereum, verwenden einen Proof-of-Work-Konsensmechanismus, um festzulegen, wie die Blockchain den Eintrag neuer Daten in das System gestattet. Das Konsenssystem überprüft, ob neue Daten gültig sind. Öffentliche Blockchains benötigen ein robustes System, weil jeder Daten in die Blockchain schreiben kann. Die Konsensmechanismen von Blockchains sind die Spielregeln, die bestimmen, wann ein Block gültig ist und welcher Chain vertraut werden soll.

Proof of Work (POW) ist in mehrfacher Hinsicht sehr attraktiv. Oft muss dafür aber in spezielle Computer-Hardware investiert werden, und der Energiebedarf an (möglichst billigem) Strom ist sehr hoch. Die einzige Anforderung, um als Knoten im System tätig zu werden, besteht also (abgesehen von der Netzwerkverbindung) darin, Strom mit spezieller Hardware zu

verbrauchen. Gleichzeitig bedeutet es, dass für eine Veränderung des Verlaufs mindestens dieselbe Menge an Strom verbraten werden muss. Dieser Aufwand macht eine Verlaufsänderung unrentabel und somit unwahrscheinlich.

Proof-of-Work ist hervorragend zur Absicherung von Blockchains geeignet. Andererseits werden dabei gigantische Mengen an Strom verbraucht, und der Betrieb ist dementsprechend teuer. Es ergibt sich ein kannibalisches Wettrüsten, bei dem die schnellsten Computer gewinnen. Jeder zusätzliche Gigahash im Netzwerk steigert die Anforderungen an alle Teilnehmer.

Je mehr Daten in einem Block enthalten sind, desto schwieriger ist er zu überprüfen. Bei Proof-of-Work-Systemen wie Bitcoin braucht man die komplette Blockchain, um einen bestimmten Datenpunkt im System zu überprüfen. Damit andere überprüfen können, ob die in Bitcoin vorgenommene Transaktion gültig ist, müssen sie die gesamte Blockchain von Bitcoin herunterladen. Dies dauert momentan mehrere Tage.

Factom hat einen einzigartigen Konsensmechanismus und fragt nicht: »Ist ein Eintrag gültig?« Stattdessen validieren hier eigens gewählte Konsensknotenpunkte Transaktionen anhand der Frage: »Wurde für den Eintrag bezahlt?« Die Benutzer des Systems validieren zugleich auch die Einträge. Factom ordnet Daten zudem auch in Unterketten an, die sich einzeln durchsuchen lassen, um die Gültigkeit eines Eintrags zu belegen, ohne dafür die gesamte Blockchain herunterladen zu müssen.

Abbildung 7.2 zeigt ein Diagramm der Kettenstruktur von Factom.

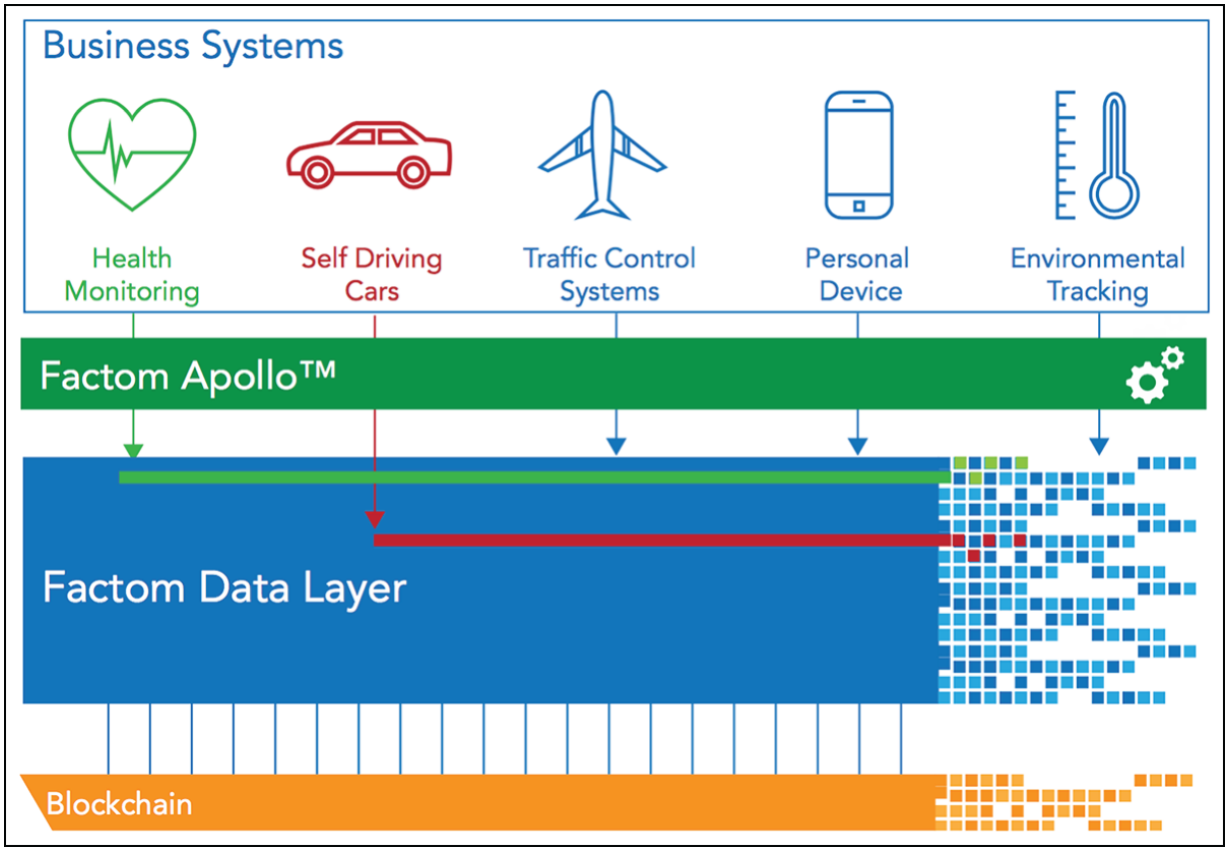


Abbildung 7.2: Die Kettenstruktur von Factom

Factom wurde für kommerzielle Anwendungen auf diese Weise strukturiert, damit die Angehörigen einer Branche nicht alle irrelevanten Daten über einen anderen, irrelevanten Industriezweig herunterladen müssen. Um beispielsweise zu überprüfen, ob alle Dokumente für eine Hypothek berücksichtigt wurden, muss kein jahrelanger Verlauf von Aktienkursen heruntergeladen werden.

Die Factom-Blockchain hinterlässt außerdem zusätzliche Signaturen auf anderen Blockchains, um ihr Netzwerk gegen Datenverfälschung zu sichern. Alle paar Minuten erzeugt sie einen kleinen Ankerpunkt in Bitcoin und Ethereum. Das garantiert zwei wichtige Dinge:

- ✔ **Erstens – und ganz wichtig – werden die Server der Factom-Blockchain daran gehindert, die Blockchain-Historie unbemerkt zu verfälschen.** Das ist der wichtigste

Aspekt. Die Server haben keinen Einfluss auf Bitcoin oder Ethereum; deshalb ist jeder Verlauf, der dort aufgezeichnet wird, permanent.

- ✔ **Es wird verhindert, dass die Factom-Server unterschiedlichen Personen zwei unterschiedliche Versionen der Blockchain anzeigen.** Die Personalisierung von Websites ist etwa bei Amazon oder Facebook bereits Standard. Bekommen unterschiedliche Unternehmen nicht übereinstimmende Verläufe von Geschäftstransaktionen angezeigt, führt dies unweigerlich zu Missverständnissen. Es gibt nur eine Bitcoin-Blockchain, und diese verhindert, dass abgeänderte Versionsverläufe erstellt werden können.

Die verrückten Acht

Factom, Inc. wurde als Projekt zur Skalierung von Bitcoin ins Leben gerufen. Daraus entstand schließlich ein Software-Unternehmen, das Anwendungen und Produkte für Regierungen und große Organisationen entwickelt. Das Unternehmen wurde von acht Mitgliedern des Factom-Teams gegründet, die jeweils einen unterschiedlichen Hintergrund hatten. Sie stammen aus den Bereichen Vertrieb, Entwicklung und Engineering.

Dies ist ein ungewöhnlich großes Gründungsteam, und man brauchte eine andere Möglichkeit, das Unternehmen zu führen, Verantwortung zu teilen und Eigenkapital zu verteilen. Man entschied sich für Holokratie, eine Managementstruktur, die stark an die von Factom, Inc. entwickelten dezentralen Netzwerke erinnert. Die Handlungsvollmachten und die Entscheidungsbefugnisse sind über mehrere Manager verteilt. Die Abstimmung erfolgt wöchentlich innerhalb eines 45-minütigen Management-Meetings.

Das Unternehmen hat seinen Hauptsitz in Austin, Texas, mit weltweiten Projekten, in denen es um Identität, Dokumentenmanagement, Immobilien und das Internet der Dinge (Internet of Things; IoT) geht. In jedem Fall befasst sich Factom mit der Verwaltung und Bereitstellung von Aufzeichnungen. Es arbeitet mit Smartrac zusammen, einem Hersteller und Anbieter von RFID-Produkten (*Radio-Frequency Identification*) und IoT-Lösungen, um wichtige Dokumente wie etwa Geburtsurkunden, die Grundlage für andere Dokumente wie Krankenkassenkarten oder Führerscheine sind, abzusichern und Identitätsdiebstahl zu verhindern. Factom arbeitet mit dem US-Ministerium für innere Sicherheit im Hinblick auf IoT-Sicherheit und Identitäten ebenso

zusammen wie mit der Gates-Stiftung zur Verwaltung medizinischer Aufzeichnungen.

Anwendungen auf Factom aufbauen

Factom wurde entwickelt, um Anwendungen darauf aufzubauen. In der Anfangszeit bestand der Hauptzweck vieler Blockchains darin, ihre eigenen Daten zu sichern, also die Eigentumsverläufe der nativen Kryptowährungen. Factom hingegen wurde als skalierbares System ausgelegt. Die Hauptprobleme, die Factom angeht, sind Geschwindigkeit und Kosten. Factom wurde auch geschaffen, um andere Blockchains miteinander zu verbinden.

Mit APIs Dokumente authentifizieren und Identitäten erstellen

Factom bietet mehrere APIs (Application Programming Interfaces, Programmierschnittstellen) an, mit denen Entwickler Dokumente verwalten und authentifizieren sowie Identitäten für Menschen und Dinge erstellen können. Um sie nutzen zu können, benötigen Sie also einen Entwickler. Außerdem sind die APIs vor allem für den Einsatz in großen Unternehmen vorgesehen und derzeit nicht für kleinere Projekte geeignet.

Um die APIs zu verwenden, müssen Sie keine Blockchain einrichten und kein Kryptowährungs-Wallet besitzen. Das vereinfacht den ganzen Prozess, und die APIs sind damit ideal für alle geeignet, die sich Sorgen um die regulatorische Grauzone machen, in der Kryptowährungen immer noch angesiedelt sind.

Factoid: Keine normale Kryptowährung

Factom besitzt ein einzigartiges Zwei-Token-System, das sogenannte Factoids und Entry Credits verwendet. Factoid ist

eine Kryptowährung, die genau wie Bitcoin an verschiedenen Börsen gehandelt wird. Gleichzeitig handelt es sich dabei aber nicht um eine Währung im Sinne von Bitcoin. Der Hauptzweck von Factoids besteht darin, in Entry Credits umgetauscht zu werden. Diese nicht übertragbaren Token, dienen zum Erwerb von Veröffentlichungsrechten innerhalb des Factom-Netzwerks. Das Netzwerk gibt eine feste Umtauschrate von Factoids in Entry Credits vor, um die Kosten für die Nutzer gering zu halten. Auch die Factom-Blockchain generiert mit jedem neuen Block neue Factoids, aber jeder neue Eintrag entzieht dem Kreislauf auch Factoids. Das System zerstört oder »verbrennt« dabei also diese Factoids.

Der Preis für Factoids schwankt abhängig von Preisspekulation und Nutzung. Entry Credits haben dagegen einen stabilen Preis, der immer bei 0,001 US-Dollar liegt. So bleiben die für die Veröffentlichung anfallenden Kosten vorhersagbar.

Das Team von Factom hat beim Crowd-Sale eine bestimmte Anzahl von Token herausgegeben, um die Finanzierung der Kernentwicklung des Protokolls abzudecken. Das Kapital aus dem Crowd-Sale wurde in einem Treuhandkonto eingefroren, das von einem Konsortium von Drittparteien überwacht wurde, um sicherzustellen, dass das Factom-Team seine Entwicklungsziele erreichen würde, bevor es auf die Gelder zugreifen kann.

Anwendungen und Factom im Zusammenspiel

Die Blockchain-Technologie hat die Tore für neue Produkte und Dienstleistungen geöffnet. Die Blockchains selbst dienen als Grundebene, über die sich eine alte Technologie selbst neu erfinden kann oder auf der Innovationen aufsetzen können. Jede Blockchain hat spezifische Eigenschaften, die sie für ganz bestimmte Anwendungen prädestiniert.

Factom ist vor allem gut im Sichern von Informationen, hat aber auch seine Grenzen: die Größe eines einzelnen Eintrags. Und je mehr Sie veröffentlichen, desto teurer wird es. Factom eignet sich

ideal, um große Dateien in einer Cloud-Lösung zu speichern und in Factom dann nur noch entsprechende Zeiger zu hinterlegen, die Ihre Anwendung auf diese Daten verweisen.

Factom dient hauptsächlich als System zur Verwaltung von Dokumenten, Daten und Identitäten. Jede einzelne Chain innerhalb von Factom ist eine permanente Historie der Daten (was immer sie auch widerspiegeln mögen), die in diese spezielle Chain eingegeben wurden. Diese »Geschichtsschreibungen« sind in einer festen und nicht manipulierbaren Reihenfolge angeordnet. Wenn ein Eintrag erstellt und veröffentlicht wurde, lässt er sich nicht mehr entfernen oder bearbeiten. Das ist ein mächtiges Tool, um zeitliche Verläufe abzubilden. Da Factom eine öffentliche Blockchain ist, kann jeder einen neuen Eintrag in eine beliebige Chain vornehmen. Eine speziell entwickelte Software überprüft alle neuen Einträge und ignoriert solche, die nicht kryptografisch signiert wurden. Spam-Einträge bleiben damit außen vor. Factom lässt sich auch gut mit anderen Blockchains verknüpfen, und Sie können damit ein sogenanntes Orakel für Ihren Smart Contract erstellen. Mit diesem können Sie preisgünstiger als über Proof-of-Stake-Systeme auf externe Daten zugreifen.

Auf Factom veröffentlichen

Factom wurde von Entwicklern für Entwickler erzeugt. Sie müssen über das Terminal spezielle Software herunterladen, um Ihre Wallets nutzen und Einträge in dem Netzwerk vornehmen zu können.

Das Factom-Team hat insbesondere alles dafür getan, ein robustes System zu entwickeln. Es stellt eine Dokumentation bereit, die Ihnen die Vorgehensweise erklärt, sowie ein GitHub-Repository, in dem Sie die gesamte Open-Source-Software finden. Sie können sich diese ansehen und sogar dazu beitragen. Factom soll in Zukunft auch noch benutzerfreundlicher werden, aber dies wird noch eine Weile dauern.

Transparenz in der Hypothekenbranche schaffen

Das erste kommerzielle Produkt des Unternehmens ist der Blockchain-Dokumentenmanagementservice Factom Harmony. Er ist für Hypothekenanbieter vorgesehen, also Einrichtungen, die Verbrauchern Hypotheken für den Hauskauf bereitstellen.

Factom Harmony (siehe Abbildung 7.3) funktioniert, indem verschiedene von Banken verwendete Bilderfassungssysteme in einen Blockchain-Tresor für Dokumente umgewandelt werden. Während die Hypothek verarbeitet wird, werden Einträge in Echtzeit erstellt und verwaltet. Anschließend wird die Aufzeichnung der Daten in Factom gesichert, sodass Metadaten transparent geteilt werden können und auf vertrauliche Daten zwischen vertrauenswürdigen Parteien verweisen.

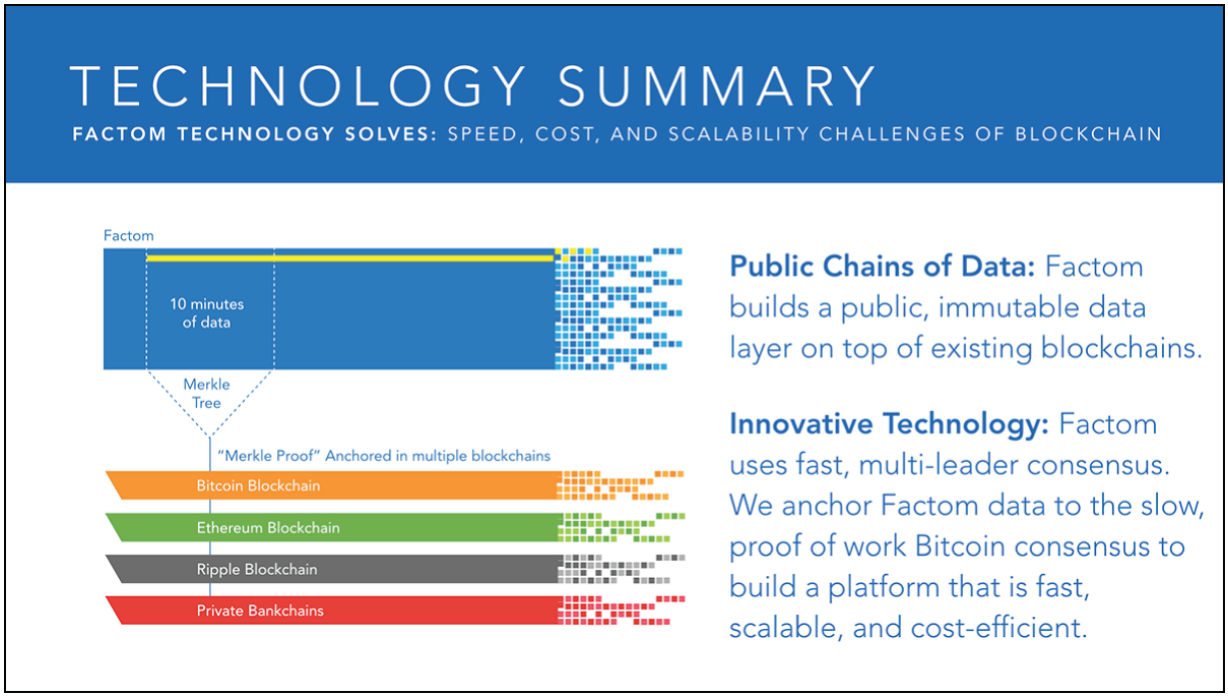


Abbildung 7.3: Factom Harmony

Einfach ausgedrückt ist Factom Harmony ein Dokumentenkatalog, der auf einem Bildgebungssystem aufbaut. Es handelt sich dabei um eine enorme Verbesserung gegenüber

vorhandenen Systemen, weil Personen, die Jahre später damit zu tun bekommen, sicher sein können, dass die ihnen übergebenen Aufzeichnungen identisch mit denjenigen sind, die für die Hypothek ausgestellt wurden. Und der Hypothekenkäufer muss nicht mehr der korrekten Arbeitsweise der vielen Zwischenstationen von der Ausstellung bis zu ihm selbst vertrauen.

Factom hofft, einen Teil des Mehrwerts zu monetarisieren, der durch den Wegfall der Kosten für die Zusammenstellung der Dokumente entsteht. Banken und andere Anbieter wenden derzeit sehr viel Zeit auf, um sicherzustellen, dass die Überprüfung der Aufzeichnungen ausschließlich anhand der korrekten Dokumente und Daten erfolgt. Das ist bei mehreren Beteiligten und Hypothekenunterlagen aus unterschiedlichen Quellen häufig sehr schwierig.

Sicherung von Daten in der Blockchain: Der digitale Tresor

Factom Harmony (siehe obiger Abschnitt) bietet die Möglichkeit, spezifische Daten und Dokumente, die für eine Entscheidung und die Einhaltung von Vertragsbedingungen notwendig sind, in einer permanenten Blockchain zu speichern, während diese Daten gleichzeitig allen berechtigten Parteien bereitgestellt werden. In diesem System gespeicherte Daten haben einen eindeutigen Versionsverlauf. Und auch das Fehlen von Daten ist offensichtlich. Factom Harmony wurde für Szenarien wie Audits, Gerichtsverfahren, Zwangsvollstreckungen, den Hypothekenhandel, Verbriefungen und behördliche Überprüfungen entwickelt.

Die wichtigsten technischen Einschränkungen waren im Jahrzehnt vor dem Marktcrash 2008 in erster Linie Geschwindigkeit, Datendurchsatz, Dokumentenverwaltung und -zusammenstellung. Die Systeme waren nicht darauf ausgelegt, Datensätze und dazugehörige Daten so zu erfassen, dass daraus ein dauerhafter Beleg für Entscheidungen und Handlungen entstand.

Heute ist die Gesetzgebung sehr viel strenger und fordert von den Unternehmen viel größere Sorgfalt bei der Dokumentation und Pflege ihrer Aufzeichnungen und der Daten, die den einzelnen Entscheidungen zuzuordnen sind. Dokumentationsdefizite werden häufig als Vorsatz interpretiert.

Wie Harmony mit der Factom-Technologie arbeitet

Die Factom-Technologie ist eine Kombination aus Blockchain-Technologie, digitalen Signaturen und verschiedenen Verschlüsselungsfunktionen, die vom U.S. National Institute of Standards and Technology (NIST) entwickelt wurden. Verschiedene Datenpunkte werden zusammen mit einem kryptografischen Beleg in anderen Blockchains aufbewahrt, sodass Benutzer Daten und Dokumente für eine spätere Nutzung speichern können. Dieser Vorgang erzeugt einen elektronischen Dateikatalog, auf den berechtigte Benutzer jederzeit zugreifen können.

Factom erzeugt mit dem Verschlüsselungsalgorithmus SHA-256 einen Hash für alle Dokumente und alle Dateien, die innerhalb der Factom-Blockchain gespeichert werden. Der Hash ist der kryptografische Beleg, dass eine Datei nicht geändert oder modifiziert wurde.

Ein *Hash* ist eine Art »Fingerabdruck« für eine Datenmenge, die den Inhalt einer Datei darstellt, aber ohne das Risiko, dass die Daten offengelegt werden.

Darüber hinaus erzeugt und speichert Harmony für jedes Dokument und die der Aufzeichnung zugeordnete Datei zusammen mit dem Hash mehrere Schlüssel-Metadatenpunkte. Innerhalb der Metadaten werden die Dokumente und Dateien einander unter Verwendung derselben Verschlüsselungsmethoden zugeordnet und miteinander verknüpft. Diese Metadaten werden zusammen mit den Datei-Hashes in die Factom-Blockchain geschrieben.

Blockchains als öffentliche Zeugen

Factom nutzt mehrere öffentliche Zeugen für seine gesicherten Daten. Die Factom-Blockchain ist im Vergleich zu den Giganten wie Bitcoin und Ethereum winzig. Das System verwendet kein Mining für den Konsensmechanismus. Derzeit erzeugt das System nicht einmal neue Token. Je größer und dezentraler eine Blockchain ist, desto sicherer ist sie gegenüber einem erfolgreichen Angriff.

Die meisten öffentlichen Blockchains setzen zur Absicherung auf das Mining von Kryptowährungen. Es bildet einen Anreiz für die Knoten, dem Netzwerk beizutreten und es zu schützen.

Factom überwindet diese Hürde durch eine clevere Methode, die ihm mehr Sicherheit verschafft: Die Daten der Factom-Blockchain werden in den Netzwerken von Bitcoin und Ethereum verankert. Das erfolgt alle zehn Minuten durch ein Hashing. Dabei wird die komplette Datenmenge gehashed, bis nur noch ein einziger Hash übrig bleibt, der die gesamte Factom-Blockchain darstellt. Auf diese Weise ist das Protokoll besser gegen Angriffe wie etwa eine 51-Prozent-Attacke geschützt.

Überprüfung physischer Dokumente: dLoc mit Factom

Smartrac, der weltweit führende Entwickler, Hersteller und Anbieter von RFID-Chips, arbeitet mit Factom zusammen. Aus dieser Partnerschaft ist eine neue Möglichkeit entstanden, physische Gegenstände mit Blockchains zu sichern. Dieses Produkt und dieser Service heißen dLoc. DLoc ist ein Aufkleber, der an fast jedem Gegenstand angebracht werden kann. Er ist vor allem für Papierdokumente wie etwa Geburtsurkunden oder andere Ausgangsdokumente sehr praktisch.

DLoc ist ein durchgängig sicheres Dokumentenmanagementsystem mit Hard- und Software-Komponenten. Der von Smartrac codierte NFC-Transponder-Aufkleber (Near Field Communication, Nahfeldkopplung) mit eingebettetem Chip wird auf Dokumenten oder anderen

Gegenständen angebracht und sichert diese unter Verwendung der Factom-Blockchain.

Durch NFC-Kommunikationsprotokolle können zwei elektronische Geräte eine Verbindung aufbauen, wenn sie in die Nähe voneinander gelangen.

Durch Kombination der cloudbasierten Software mit der Technologie von Factom entsteht mit der Zeit eine unveränderbare digitale Identität für so gut wie alles. Menschen mit einer bestimmten Berechtigung können unter Verwendung der Handy-App dLoc auf das physische Dokument zugreifen und es überprüfen.

DLoc ermöglicht es ausstellenden Behörden oder Einrichtungen außerdem, ihre Offline-Dokumente in digitale Instanzen umzuwandeln, die sich ganz einfach mit den vorhandenen digitalen Systemen verbinden lassen und damit die Lücke zwischen Offline- und Online-Welt schließen. Diese Lösung kann auf die unterschiedlichsten Dokumente angewendet werden, wie etwa Geburtsurkunden, Grundbesitzurkunden, Gerichtsurkunden oder medizinische Unterlagen.

DLoc stellt das erste praktische Dokumentenauthentifizierungssystem dar, mit dem die Factom-Blockchain die Lücke im Hinblick auf die Datenintegrität zwischen der physischen und der digitalen Welt schließt. Es ist die erste zuverlässige Methode, Informationen auf Papierdokumenten mithilfe der Blockchain-Technologie digital zu sichern. Die Daten- und Identitätsauthentifizierungslösung von dLoc ist vielversprechend für den öffentlichen wie für den privaten Sektor, in dem hauptsächlich Papierdokumente verwendet werden.

DLoc kann keinen Betrug ausschließen. Menschen bleiben Menschen und finden immer eine Möglichkeit, etwas zu umgehen oder zu stehlen. Die Technik macht es nur schwieriger und kostspieliger. Heute kann man fast überall eine neue Identität oder gefälschte Waren kaufen. In einigen Fällen sind diese Identitäten nicht von authentischen Dokumenten oder Waren zu unterscheiden.

DLoc wurde als Möglichkeit geschaffen, die Fälschungssicherheit der Blockchain-Technologie auf physische Objekte und Dokumente auszuweiten. Das Unternehmen hat außerdem ein System entwickelt, das Sie benachrichtigt, wenn ein Angriff auf Ihre Identität stattfindet, und Sie haben die Möglichkeit, etwas dagegen zu unternehmen.

Kapitel 8

Die EOS-Blockchain

IN DIESEM KAPITEL

- EOS kennenlernen
- EOS-Blockproduzenten wählen
- Spiele und EOS-DApps nutzen

EOS ist eine neuere Blockchain, deren Entwickler auf dem Erfolg von Ethereum aufbauen und zugleich die Skalierbarkeit verbessern möchten. EOS gehört zu den beliebtesten Kryptowährungen am Markt. Die Entwicklerfirma Block.one sammelte 2017 bei einem einjährigen Initial Coin Offering (ICO) vier Milliarden Dollar für das Projekt ein. Wie Ethereum ermöglicht EOS seinen Nutzern die Programmierung von Smart Contracts, die eine Vielzahl von Funktionen erfüllen können.

Der entscheidende Unterschied zwischen EOS und Ethereum liegt im Konsensmechanismus von EOS. Hier lohnt es sich, mehr zu erfahren. EOS setzt auf ein neues System namens *Delegated Proof-of-Stake* (DPOS). Besitzer von EOS-Token können durch Abstimmung Blockproduzenten wählen. Theoretisch kann jeder zum Blockproduzent werden, solange er genug Token-Besitzer von sich überzeugen kann. Wenn Sie Kapitel 7 über den Konsensalgorithmus von Factom gelesen haben, klingt das vielleicht vertraut.

Dieses Kapitel behandelt praktische Anwendungen und die Zukunft der EOS-Blockchain und erläutert Einsatzmöglichkeiten der Technologie. Da EOS eine relativ neue Blockchain ist, muss Block.one noch einen benutzerfreundlichen Client entwickeln. Dank der enormen Entwicklungsressourcen ist es wohl nur eine

Frage der Zeit, bis bessere Angebote für den täglichen Gebrauch bereitstehen. Wegen seiner enormen finanziellen Mittel sollten Sie das Projekt im Auge behalten; es wird irgendwann wahrscheinlich jedes andere Projekt im Blockchain-Bereich überragen.

EOS kennenlernen

Die auf den Kaimaninseln ansässige Kryptofirma Block.one sammelte per ICO rund 7,12 Millionen Ether im Wert von damals vier Milliarden Dollar ein. Die Investoren tauschten dabei ihren Ether gegen EOS-Token ein. Wie die meisten ICOs verwendete auch EOS einen ERC20-Token zur Kapitalbeschaffung. Finden Sie es nicht auch bemerkenswert, dass EOS als sogenannter »Ethereum-Killer« durch Ethereum überhaupt erst auf den Weg gebracht werden konnte?

Das EOS-Projekt versprach einen ähnlichen Zugang, wie wir ihn derzeit von zentralisierten Diensten her kennen: die Sicherheit und Redundanz der Blockchain-Technologie zum Preis und mit der Geschwindigkeit einer Amazon-Cloud. Die meisten Blockchain-Entwickler wollen die Preise trotz steigender Nutzerzahlen auf ihrer Plattform niedrig halten und gleichzeitig die Transaktionsgeschwindigkeit und den Durchsatz erhöhen. Proof-of-Work-Blockchains werden bei steigender Teilnehmerzahl tendenziell immer teurer und langsamer.

Die ersten Blockchain-Implementierungen verfolgten einen eindeutigen Zweck: Bitcoin ermöglichte es, Kryptogeld von einem Benutzer zum anderen zu senden und die Eigentumsverhältnisse in der Blockchain festzuhalten. Ethereum war die erste Blockchain 2.0; sie verband die digitale Unauslöschbarkeit und vertrauenslose Architektur von Bitcoin mit der Möglichkeit, Code und damit Smart Contracts in eine Blockchain zu schreiben. Die EOS-Entwickler haben eine neue Blockchain-3.0-Architektur entwickelt, in der die Anzahl der Transaktionen pro Sekunde vertikal und die Anzahl der verarbeiteten dezentralen Anwendungen horizontal skaliert werden.

Auch EOS ist eine transparente Blockchain-Technologie mit der Möglichkeit, Smart Contracts auszuführen. Dazu kommen noch Benutzerkonten, Authentifizierung, Datenbanken, asynchrone Kommunikation und die terminierte Abarbeitung von Anwendungen über mehrere CPU-Kerne hinweg. Dank seiner Architektur kann EOS theoretisch Millionen von Transaktionen pro Sekunde verarbeiten, was die Gebühren senkt und dezentrale Anwendungen (DApps) leichter verfügbar macht.

EOS begegnet einigen wichtigen Problemen, die Entwickler früherer Blockchain-Systemen hatten:

- ✔ Die Blockchain-Technologie muss täglich viele Millionen aktiver Nutzer bewältigen, genau wie Google, Facebook, Twitter und Amazon, und zwar ohne erhöhte Kosten oder Systemabstürze.
- ✔ Die Blockchain-Technologie muss deutlich kostengünstiger werden, um alle Arten von Anwendungen zu hosten, die von vertrauenslosen Systemen profitieren könnten. Eine kostenfreie Blockchain-Plattform findet wahrscheinlich eine größere Verbreitung.
- ✔ Blockchain-Software muss unpolitische Upgrades und Bugfixes ermöglichen. Bitcoin und Ethereum stehen sich hierbei durch Streitigkeiten unter den Core-Entwicklern und finanziellen Druck vonseiten der Miner immer wieder selbst im Weg.
- ✔ Blockchain-Entwickler brauchen Spielraum zur Verbesserung ihrer Anwendungen mit neuen Funktionen. Dabei muss aber immer auch die Sicherheit der Blockchain-Software gewährleistet bleiben.
- ✔ Blockchain-Software muss auch schnell und benutzerfreundlich sein. Lange Wartezeiten erschweren die Benutzerbindung und machen blockchainbasierte Anwendungen weniger wettbewerbsfähig.

Das Team von Block.one hofft, all diese Probleme durch den dezentralen DPOS-Konsensalgorithmus zu lösen und Blockchain-

Software damit endlich attraktiver für die kommerzielle Nutzung zu machen. Mit dem DPOS-Algorithmus können Token-Inhaber über ein Abstimmungssystem Blockproduzenten wählen.

Alle 0,5 Sekunden entstehen durch DPOS Transaktionsblöcke auf der EOS-Blockchain. Die Blöcke werden in 126er-Runden produziert, wobei 21 gewählte Produzenten jeweils sechs Blöcke erstellen. Alle Block-Producer können alle Blöcke signieren, aber immer nur einen mit dem gleichen Zeitstempel oder der gleichen Blockhöhe. Sobald 15 Block-Producer unterzeichnet haben, gilt der Block als unveränderlich. Dank dieser Struktur kann eine Transaktion in durchschnittlich 0,25 Sekunden bestätigt werden. Für eine Blockchain ist das extrem schnell.

Wenn sich ein Blockproduzent verpflichtet hat, einen Block zu produzieren, dies aber nicht tut, wird er übersprungen, und es entsteht eine Lücke von mindestens 0,5 Sekunden in der EOS-Blockchain. Wenn ein Blockproduzent seinen Block auslässt und innerhalb von 24 Stunden keinerlei Blöcke produziert hat, wird er ausgeschlossen.

Auf den DPOS-Knoten entstehen kaum Verzweigungen (Forks) der Blockchain-Datensätze, weil sie nicht im gleichen Sinne konkurrieren wie die Mining-Knoten auf Proof-of-Work-Blockchains wie etwa Bitcoin. Die EOS-Blockproduzenten kooperieren miteinander. Wenn eine Fork entsteht, wechselt der DPOS-Konsens automatisch auf die längste Chain. Block-Producer könnten auch Schindluder treiben, wie etwa Blöcke auf zwei Versionen (Forks) der EOS-Blockchain gleichzeitig herzustellen. Der Gedanke hinter EOS ist aber, dass ein unredlicher Blockproduzent sofort abgewählt wird, sobald er auffliegt. In der EOS-Blockchain werden kryptografische Nachweise solcher Doppelproduktionen abgespeichert, um Betrüger leichter zu entlarven.

Die Skalierbarkeit von EOS hat auch Nachteile. Die Blockchain wird nur von wenigen Knoten (21) aufrechterhalten und ist damit sehr zentralisiert. Das birgt Sicherheitsrisiken.

Die Evolution des Minings

In den Anfangstagen von Bitcoin eignete sich jeder Desktop-Computer für das Mining. Die zunehmende Hash-Rate des Bitcoin-Netzwerks sorgte jedoch schnell dafür, dass die Rechenleistung normaler Computer nicht mehr mithalten konnte.

Blockchains mit einer Hashing-Difficulty im Gigahash-Bereich überschreiten die Kapazität durchschnittlicher Computer. Diese Rate kann selbst für viele professionelle Miner zu hoch sein. Sie müssen viel Strom, Zeit und Ressourcen aufwenden, um profitabel zu arbeiten. Da die Konsensbildung bei EOS über das DPOS-System erfolgt, genügt hier immer noch ein normaler Computer, um Token zu verdienen.

Bitcoin-Miner haben entdeckt, dass sie die GPU (den Grafikprozessor) von Grafikkarten für das Mining umkonfigurieren können. Die GPU brachte den Minern einen bis zu 50-fachen Geschwindigkeitsvorteil. Außerdem verbrauchte die GPU weniger Strom, der Betrieb war also wirtschaftlicher.

Im Jahr 2011 eröffneten die ersten Mining-Farmen mit speziellen FPGA-Prozessoren (*Field-Programmable Gate Array*). Diese Geräte wurden per USB an die Computer der Miner angeschlossen und verbrauchten weniger Strom als das Mining per CPU oder GPU.

Die beste Mining-Hardware nutzt heute anwendungsspezifische integrierte Schaltkreise (*ASICs*). ASIC-Miner erreichen extrem hohe Hash-Raten. Nach meiner persönlichen Erfahrung können sie aber auch sehr laut sein. Wenn Sie die Anschaffung einer solchen Maschine in Betracht ziehen, nehmen Sie sich die Zeit, die Rezensionen dazu zu lesen. Rechnen Sie auch nach, ob sie

eine angemessene Amortisationszeit haben und ob sie kompatibel zu dem Coin sind, den Sie minen möchten.

Für Blockchain-Software gibt es inzwischen immer mehr ernsthafte Anwendungen. Darum muss sich auch das Mining weiterentwickeln. Die EOS-Blockchain wird im Unterschied zu Proof-of-Work-Blockchains nicht mehr durch Mining fortgeschrieben. Die Blöcke werden von ausgewählten Knoten produziert, die dafür eine Belohnung erhalten.

Im Prinzip kann sich jeder dafür bewerben, aber am Ende werden nur 21 Block-Producer gewählt. Deshalb ist es schwierig, dort hineinzukommen. Sie können Ihre EOS-Token aber vielleicht auch einem beliebten Block-Producer ausleihen und dafür ebenfalls entlohnt werden. Das funktioniert ähnlich wie das Staking von Token auf der Waves-Plattform (siehe Kapitel 6).

Die 21 Block-Producer

Im Gegensatz zu Bitcoin, wo jeder Transaktionen verifizieren und Blöcke erstellen kann, pflegten bei EOS nur einige ausgewählte Knotenpunkte die EOS-DPOS-Blockchain. Als Teilnehmer und Besitzer von EOS-Token können Sie wie bei einer politischen Wahl über diese Nodes abstimmen.

Die gewählten Nodes, sogenannte *EOS-Delegates*, sind als Einzige dazu berechtigt, die Transaktionen auf EOS abwickeln. Es gibt immer nur 21 aktive Delegates. Viele weitere warten im Hintergrund darauf, nachzurücken, falls einer der gewählten Nodes ausfällt. Die Knoten mit den meisten Stimmen dürfen Blöcke produzieren. Viele Delegates teilen ihre Block-Rewards mit den Benutzern, die für sie gestimmt haben.

Als Token-Besitzer können Sie Ihre Stimme jederzeit anders vergeben. Theoretisch soll das verhindern, dass Blockproduzenten gegen die Interessen der Gemeinschaft handeln. Momentan ist die Stimmvergabe nicht gerade intuitiv gelöst. Außerdem ist es für Normalsterbliche auch ziemlich schwer herauszufinden, ob die Stimme bei einem bestimmten Delegante sinnvoll aufgehoben ist oder nicht.

Der EOS-Blockproduzent Greymass hat ein Voting-Tool herausgebracht. Das Programm wurde von einem Dritthersteller geschrieben. Damit ist es nicht ganz so sicher, wie wenn Sie Ihre Stimme über die Kommandozeile vergeben. Es handelt sich aber um quelloffene Software, die auch von einigen konkurrierenden Block-Produzenten unterstützt wird.

Das EOS-System belohnt Blockproduzenten mit neuen Token. Die Menge der im Umlauf befindlichen EOS-Token steigt jedes Jahr um fünf Prozent. Dabei gehen 0,25 Prozent an die aktiven Blockproduzenten und 0,75 Prozent an Blockproduzenten auf der Warteliste; das sind rund 100 EOS pro Tag für qualifizierte Blockproduzenten auf der Warteliste. Vier Prozent der neuen Token gehen in einen Pool, der zur Weiterentwicklung von EOS und für Forschungszwecke genutzt wird. Verbesserungsvorschläge werden der Gemeinschaft vorgelegt, und die Token-Besitzer stimmen darüber ab, ob sie umgesetzt werden sollen.

EOS-Blockproduzenten wählen

EOS-Token werden an den meisten Börsen gehandelt. Aktuell können Sie beispieslweise bei Poloniex EOS für Bitcoin oder Ethereum kaufen. Sobald Sie etwas Bitcoin oder Ethereum gegen EOS-Token eingetauscht haben, sind Sie stimmberechtigt. Außerdem müssen Sie sich eine neue EOS-Wallet einrichten. Befolgen Sie diese Schritte:

1. **Öffnen Sie den App-Store auf Ihrem Smartphone.**
2. **Suchen Sie nach `EOS Lynx`.**

   Die Website des Unternehmens finden Sie unter https://eoslynx.com.
3. **Laden Sie die Wallet herunter.**
4. **Geben Sie einen Account-Namen an.**

Ihr Account-Name ist zugleich Ihre Wallet-Adresse. Er muss exakt zwölf Zeichen lang sein (nur Ziffern und Buchstaben).


Wählen Sie einen einfachen und leicht zu merkenden Namen, denn Sie werden den Account-Namen in Zukunft vielleicht ähnlich wie eine E-Mail-Adresse verwenden.

5. **Schreiben Sie Ihren privaten Schlüssel auf.**

   Notieren Sie sich unbedingt Ihren privaten Schlüssel, und bewahren Sie ihn an einem sicheren Ort auf.

6. **Senden Sie EOS-Token an Ihre Wallet.**

   Hier verwenden Sie den Wallet-Namen und keine Adresse wie bei anderen Blockchains.

   EOS-Token können Sie auf Exchanges wie Poloniex (www.poloniex.com) oder Binance (www.binance.com) erwerben.

Nun haben Sie einen EOS-Account und einige EOS-Token und sind damit bereit für das Voting.

Das Greymass-Voting-Tool einrichten

Die Greymass-App hat einige sehr praktische Funktionen. Sie können damit nach Blockproduzenten suchen, EOS-Token auf andere Accounts transferieren und EOS-Token im Austausch gegen CPU-Leistung verleihen. Damit erhalten Sie das Recht, als Entwickler Netzwerkressourcen zu nutzen, und Sie geben Ihrer Stimme mehr Gewicht.

Folgen Sie diesen Schritten, um für einen EOS-Block-Producer zu stimmen:

1. **Besuchen Sie Greymass' GitHub unter** https://github.com/greymass/eos-voter**.**
2. **Laden Sie sich das Greymass-Voting-Tool für Ihr Betriebssystem herunter, und installieren Sie es.**

3. **Klicken Sie auf CONNECT TO AN API NODE.**
4. **Geben Sie den Namen Ihrer EOS-Wallet ein.**

   Dies ist der Wallet-Name, den Sie im letzten Abschnitt festgelegt haben.
5. **Geben Sie Ihren privaten EOS-Schlüssel ein.**

   Den privaten Schlüssel für Ihre EOS-Wallet finden Sie auf dem Zettel, auf dem Sie ihn notiert haben. Oder Sie suchen in der Lynx-Wallet danach. Sie finden ihn unter EXPORT PRIVATE KEY und unter dem Symbol links von Ihrem Account-Namen in der Wallet.
6. **Geben Sie ein sicheres Passwort ein.**

   Vergessen Sie nicht, sich das Passwort zu notieren und es getrennt von Ihrem Private Key an einem sicheren Ort aufzubewahren.

Einen Blockproduzenten auswählen

Sie haben Greymass jetzt installiert und können an der Abstimmung teilnehmen. Zuvor ist es jedoch sinnvoll, sich genauer mit den möglichen Kandidaten zu befassen, die Ihre Blockchain-Einträge und -Anwendungen absichern sollen. Das ist bei EOS sehr wichtig, weil hier kein Proof-of-Work-Modell zum Einsatz kommt. Die Teilnehmer werden nur durch Abstimmung zur Ehrlichkeit gezwungen. Die Blockproduzenten bilden das Rückgrat der EOS-Infrastruktur, und wenn sie versagen, wird das System angreifbar.

Im Greymass-Programm sehen Sie unter VOTING eine Liste aller Kandidaten. Von hier aus können Sie deren Websites und Social-Media-Auftritte aufrufen. Achten Sie auf einige Schlüsselmerkmale, um Ihre Auswahl einzuengen:

- ✔ Haben sie eine Website?
- ✔ Werden sie von der Gemeinschft überwiegend positiv bewertet?
- ✔ Teilen sie die Block-Rewards?

- ✔ Nutzen sie soziale Medien?
- ✔ Wie bringen sie sich in die Community ein?
- ✔ Haben sie eine Roadmap für zukünftige Entwicklungen?
- ✔ Gibt es eine E-Mail-Adresse, einen Telegram-Kanal oder andere Kommunikationsmöglichkeiten über soziale Medien?
- ✔ Wie steht es um die technische Expertise?

Wenn Sie bereit zur Abstimmung sind, befolgen Sie diese Schritte:

1. **Öffnen Sie die Greymass-Anwendung auf Ihrem Computer.**

   Dieses Programm haben Sie im letzten Abschnitt installiert.
2. **Klicken Sie auf PRODUCER VOTING.**

   Auf der linken (Mac) oder rechten (PC) Bildschirmseite sehen Sie die Kandidatenliste potenzieller Blockproduzenten.
3. **Stöbern Sie in der Kandidatenliste, und lesen Sie sich ein wenig ein.**
4. **Wenn Sie wissen, wem Sie Ihre Stimme geben möchten, klicken Sie auf das Symbol rechts vom Namen des Blockproduzenten.**

   Das Symbol sieht wie ein kleines Kästchen mit einem Minuszeichen darin aus. Sie können bis zu 30 Plock-Producer markieren, müssen das aber nicht tun.
5. **Klicken Sie auf SUBMIT VOTES FOR SELECTED PRODUCERS.**

   Glückwunsch! Sie haben abgestimmt und sich in die EOS-Blockchain eingebracht!

Die EOS-DApp-Sammlung

EOS verfügt inzwischen über eine der größten DApp-Sammlungen im Internet. DApps sind blockchainbasierte

Anwendungen, die sich digitale Permanenz, Dezentralität, Zensurresistenz und native Kryptowährungen zunutze machen. Viele Start-ups entwickeln ihre Apps auf EOS, weil hier sowohl die Latenzzeiten als auch die Kosten im Vergleich zu anderen Blockchains niedrig sind.

Ethereum ist immer noch die beliebteste Plattform für DApps, aber EOS könnte schon bald aufholen, da es immer mehr Smart-Contract-Entwickler von anderen Plattformen anzieht. Ein weiterer Grund hierfür ist auch, dass bei EOS gängige Programmiersprachen wie WebAssembly (WASM, ein Webstandard mit Unterstützung von Google, Microsoft und Apple) und C++ zum Einsatz kommen. Dank des beträchtlichen Kapitals konnte Block.one für EOS hervorragende Entwicklertools und Bibliotheken bereitstellen.

Auf DappRadar können Sie einen Blick auf die neuesten EOS-basierten Anwendungen werfen:
https://dappradar.com/rankings/protocol/eos.

Everipedia: Die Enzyklopädie der nächsten Generation

Everipedia ist eine EOS-Blockchain-Version der beliebten Website Wikipedia. Als zensurresistente, wikibasierte Online-Enzyklopädie führt sie eine Historie aller Änderungen an ihren Seiten. Sie nutzt ihr eigenes natives IQ-Token, um die Erstellung von Inhalten zu unterstützen. Everipedia ist etwas älter als EOS, das Projekt wurde bereits 2014 gegründet und ist im Jahr 2018 auf die EOS-Blockchain migriert.

Everipedia möchte die am besten zugängliche Online-Enzyklopädie sein. Daher lassen sich Inhalte viel einfacher erstellen als bei Wikipedia. Der Everipedia-Gründer übernahm auch Elemente von traditionellen Social-Media-Seiten und ermöglichte es Prominenten, mit ihren Fans zu kommunizieren.

Sie können Seiten zu jedem Thema erstellen. Die Seiten müssen mit Belegen versehen und neutral sein, da die Erstellung neuer

Seiten hier so einfach ist und nicht der gleichen Kontrolle unterliegt wie bei Wikipedia. Sie können sich vorstellen, dass Everipedia und die Zensurresistenz der Blockchain zum Missbrauch einladen und Inhalte falsch sein können. Everipedia bietet einen Service an, um Seiten individuell anzupassen und auf Änderungen zu überwachen sowie Vandalismus zu verhindern. Denken Sie daran, wenn Sie die Website durchsuchen.

Befolgen Sie diese Schritte, um Ihre ganz persönliche, über die EOS Blockchain gesicherte Seite zu erstellen:

1. **Gehen Sie auf** https://everipedia.org**.**
2. **Klicken Sie auf MENÜ.**
3. **Klicken Sie ANMELDEN/REGISTRIEREN.**
4. **Wählen Sie auf der Anmeldeseite Ihren bevorzugten Social-Media-Zugang. Momentan werden Facebook, Twitter und Kakao unterstützt.**
5. **Erstellen Sie Ihre vierstellige PIN.**

   Schreiben Sie die PIN auf, und verwahren Sie sie an einem sicheren Ort.
6. **Klicken Sie auf das Pluszeichen (+) in der linken (Mac) oder rechten (PC) oberen Ecke.**
7. **Geben Sie den Namen der Seite an, die Sie erstellen möchten**

   Ich habe beispielsweise eine Autorenseite für meinen Fachlektor Scott Robinson angelegt: https://everipedia.org/wiki/lang_en/the-scott-rob/.
8. **Geben Sie Ihren Inhalt ein.**

   Denken Sie dabei auch an ein Bild und die erforderlichen Quellenangaben.
9. **Klicken Sie auf SUBMIT.**

Dezentrale EOS-Spiele

Spiele reizen die Blockchain-Technologie voll aus. Sie schaffen etwa souveräne Identitäten (eine Identität, die der Inhaber des Ausweises oder Dokuments kontrolliert und durch einen Blockchain-Eintrag nachweist). Blockchain-Spiele nutzen oft auch Dinge wie selbstreplizierende digitale Assets (digitale Güter, durch deren Kombination während des Spiels ein neues Asset entstehen kann); das Krypto-Spiel Cryptokitties ist ein Beispiel für ein solches Asset. In Spielen kommt es oft auch zu winzigen Zahlungen oder Mikrotransaktionen. Spiele öffnen das gesamte Potenzial der Blockchain-Technologie für durchschnittliche Benutzer.

Inzwischen laufen viele neue Spiele auf der EOS-Blockchain. EOS ist eine attraktive Option, da die eingebauten Funktionen neue Arten von Games ermöglichen. Blockchains sind von Natur aus zensurresistent. Es kann nicht nur jeder spielen, sondern es ist auch schwer zu verhindern, dass ein Spiel auf globaler Ebene abläuft. Einige Spiele sind in Ihrer Region vielleicht nicht legal (zum Beispiel ist Glücksspiel oft verboten oder stark reglementiert).

Blockchains ermöglichen auch digitales Eigentum, das über die Standards zentralisierter Spieleunternehmen hinausgeht. Ihre Ingame-Objekte, wie Skins für Ihren Avatar, sind nun nicht mehr im Besitz und unter der Kontrolle einer Firma, sondern Sie ganz alleine sind dafür verantwortlich. Blockchains verfügen auch über eigene Kryptowährungen, die Zahlungen erleichtern und Rückbuchungen reduzieren. Das ist für Entwickler sehr attraktiv. Außerdem sind die Gebühren für Blockchain-Transaktionen teilweise geringer als bei Kreditkartenunternehmen.

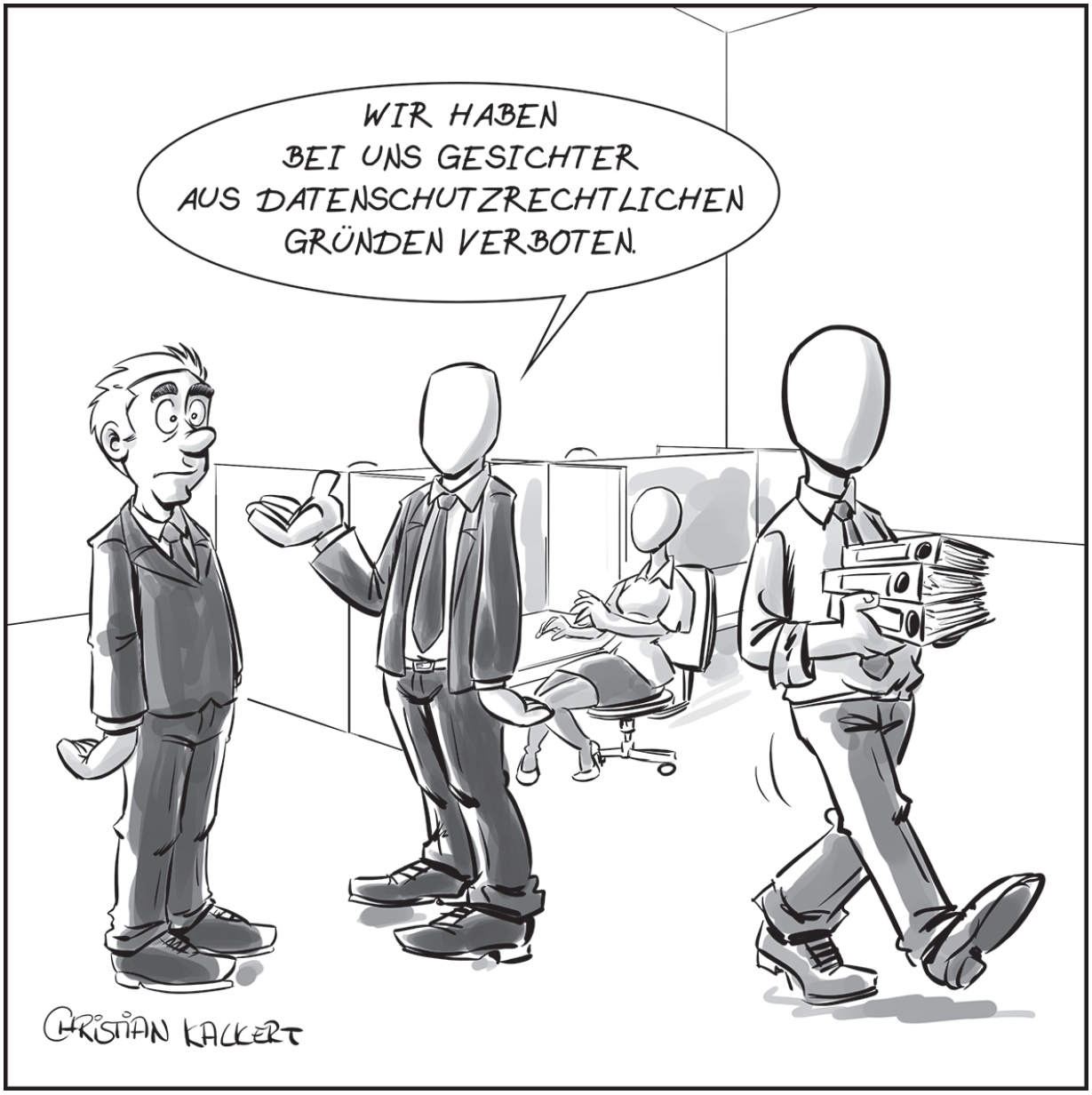
Die EOS-Blockchain hat sich aufgrund ihrer hohen Geschwindigkeit und der geringen Transaktionskosten als bevorzugte Lösung für die Spieleentwicklung etabliert. Das bedeutet, dass die Smart Contracts (auch bekannt als Chaincode) auf EOS schneller und kostengünstiger laufen – ein sehr wichtiger Aspekt bei der Spieleentwicklung.

Auf DappRadar finden Sie immer die neuesten EOS-Games: https://dappradar.com/rankings/protocol/eos/category/games.

Die Blockchain-Technologie lässt einige Vorteile von zentralisierten Diensten vermissen. Wenn ein Spiel ausfällt, gibt es keinen Kundendienst. Wenn Sie Ihr Inventar verlieren, ist es für immer weg. Und wenn sich ein anderer Spieler unfair verhält, kann man auch nicht viel ausrichten. Der Blockchain-Bereich ist immer noch wie der Wilde Westen, und Spiele bringen Rivalität, Egoismus und Gier zum Vorschein.

Teil III

Leistungsstarke Blockchain-Plattformen



IN DIESEM TEIL …

Lernen Sie Hyperledger, das größte Unternehmenskonsortium im Blockchain-Bereich, kennen, und erfahren Sie, welche Vorteile und Auswirkungen es für Ihre Branche und Ihr Unternehmen mit sich bringt.

Erfahren Sie mehr über die Blockchain-Projekte und die wichtigsten Werkzeuge von Microsoft.

Entdecken Sie das IBM-Projekt Bluemix, und erfahren Sie, welche Bedeutung die Kombination von Blockchain-Technologie und künstlicher Intelligenz hat.

Kapitel 9

Hyperledger

IN DIESEM KAPITEL

- Die Hyperledger-Foundation
- Wichtige Hyperledger-Projekte erkunden
- Eine Asset-Tracking-Plattform aufbauen
- Chaincode-Smart-Contracts erstellen

Hyperledger ist eine Initiative, die eine Gemeinschaft aus Softwareentwicklern und Technologiebegeisterten dabei unterstützt, Normen für Blockchain-Frameworks und -Plattformen zu schaffen. Die Arbeit von Hyperledger ist entscheidend, weil dadurch Blockchain-Lösungen entstehen, die den Bedürfnissen von Wirtschaftsunternehmen entsprechen. Kryptowährungen auf öffentlichen Blockchains unterliegen regulatorischen Pflichten, die viele Unternehmen daran hindern, diese Netzwerke zu nutzen. Hyperledger bietet viele der Vorteile einer öffentlichen Blockchain, kommt aber ohne Kryptowährung aus. Mit großen Unterstützern wie Intel und IBM ist Hyperledger die »vertrauenswürdige« Bereitstellungsplattform für Unternehmen.

Hyperledger und sein einzigartiges Projekt wachsen täglich weiter. Zum Zeitpunkt der Drucklegung dieses Buchs hat Hyperledger mehr als 100 Mitgliedsunternehmen und verschiedene Blockchain-Anwendungen in Planung. Zu den ersten Projekten gehören Fabric, Iroha und Sawtooth. Dies sind Frameworks, mit denen Entwickler private Blockchains und Smart Contracts erstellen und die Identität von Menschen und Dingen dezentral verwalten.

In diesem Kapitel erfahren Sie, wie Sie mit dem Composer-Tool von Hyperledger eine Asset-Tracking- und eine Smart-Auction-Anwendung erstellen. Ich stelle Ihnen außerdem auch die Fabric-, Iroha- und Sawtooth-Projekte vor. Sie erfahren, was die Zukunft der kommerzialisierten Blockchain für Ihr Unternehmen und Ihre Branche bringen wird. Dieses Wissen wird Ihnen helfen, wenn Sie darüber nachdenken, welche Technologien Sie einsetzen sollen oder auf welche Sie verzichten sollen. Damit sparen Sie Entwicklungszeit und Ressourcen.

Hyperledger kennenlernen

Ende 2105 rief die Linux Foundation das Hyperledger-Projekt ins Leben, um ein dezentrales, quelloffenes Ledger-Framework der Enterprise-Klasse zu entwickeln. Man hoffte, die Blockchain-Gemeinschaft darauf ausrichten zu können, robuste, branchenspezifische Anwendungen, Plattformen und Hardwaresysteme zu entwickeln, und damit die Wirtschaft voranzubringen.

Die Linux Foundation hatte erkannt, dass sich viele verschiedene Gruppen mit Blockchain-Technologie beschäftigten, ohne dabei eine gemeinsame Stoßrichtung zu verfolgen. Diese »Stammeszugehörigkeit« führte nicht selten dazu, dass Teams dasselbe Problem zweimal lösten. Die Mitglieder der Foundation erkannten Parallelen zwischen der Geburtsstunde des Internets und der aufkommenden Blockchain-Technologie: Um das volle Potenzial dieser Technologie zu erschließen, bedurfte es unbedingt einer Entwicklungsstrategie mit Open-Source-Code und gemeinschaftlicher Softwareentwicklung.

Das Hyperledger-Projekt wird vom Geschäftsführer Brian Behlendorf geleitet, der über jahrzehntelange Erfahrung verfügt und aus der ursprünglichen Linux Foundation und Apache Foundation stammt. Darüber hinaus war er CTO des World Economic Forums. Es ist also kaum überraschend, dass Hyperledger gut ankam. Viele führende Unternehmen schlossen sich dem Projekt an, unter anderem Accenture, Cisco, Fujitsu

Limited, IBM, Intel, J. P. Morgan und Wells Fargo, außerdem viele wichtige Blockchain-Organisationen.

Die technischen Lenkungsausschüsse von Hyperledger stellen Robustheit und Interoperabilität zwischen diesen unterschiedlichen Technologien sicher. Man hofft, dass die branchenübergreifende Zusammenarbeit an diesem Open-Source-Projekt die Blockchain-Technologie voranbringen und Milliarden von Dollar an wirtschaftlichen Werten schaffen wird, indem die Kosten für Forschung und Entwicklung auf viele Organisationen aufgeteilt werden.

Hyperledger identifiziert und berücksichtigt wichtige Funktionen und Anforderungen, die im Blockchain-Technologieökosystem fehlen. Außerdem fördert es einen branchenübergreifenden offenen Standard für verteilte Ledger und bietet Entwicklern Raum, um zu besseren Blockchain-Systeme beizutragen.

Hyperledger hat einen Projektlebenszyklus, der mit dem der Linux Foundation vergleichbar ist. Es werden Vorschläge unterbreitet, und die akzeptierten Vorschläge werden in Planung genommen. Wenn ein Projekt einen stabilen Zustand erreicht hat, wird es in einen aktiven Zustand überführt. Derzeit befinden sich alle Hyperledger-Projekte in der Vorschlags- oder Planungsphase. Jedes Projekt wird von einem großen Unternehmen oder Start-up geleitet. Beispielsweise wird Fabric von IBM geleitet, Sawtooth von Intel und Iroha vom Start-up Soramitsu.

Hyperledger nutzt wie viele Open-Source-Projekte GitHub (www.github.com/hyperledger) und Slack (https://slack.hyperledger.org), um die Projektteams miteinander zu verbinden. Dort erhalten Sie Neuigkeiten und können sich über den Fortschritt bei der Entwicklung der Projekte informieren.

Wichtige Hyperledger-Projekte

Hyperledger hat mehrere revolutionäre Projekte in der Pipeline. In diesem Abschnitt informiere ich Sie über die drei

herausragendsten und am weitesten entwickelten Projekte. Zu diesen Blockchain-Technologien gehören Frameworks für dezentrale Konten, Smart-Contract-Engines, Kundenbibliotheken, grafische Schnittstellen, Utility-Bibliotheken und Beispielanwendungen.

Fabric

Fabric war die erste Blockchain-Implementierung auf Hyperledger und wurde zur Grundlage für die Entwicklung der meisten Blockchain-Anwendungen. Fabric ist einzigartig im Blockchain-Ökosystem, weil Entwickler Fabric-Stücke nutzen können, ohne sich auf die gesamte Funktionalität festzulegen - ein echtes Plug-and-Play-Erlebnis. Fabric ermöglicht auch Smart Contracts mit der Bezeichnung *Chaincode*.

Fabric kommt als Blockchain-Berechtigungsplattform ohne eigene Kryptowährung aus. Das bedeutet, dass alle Teilnehmer bekannt sind (im Gegensatz zur typischen öffentlichen Blockchain, deren Teilnehmer standardmäßig anonym sind). Fabric funktioniert wie die meisten Blockchains und führt ein Kontobuch (Ledger) über digitale Ereignisse. Diese werden als Transaktionen angelegt und zwischen den verschiedenen Teilnehmern geteilt. Die Transaktionen werden ohne Kryptowährung ausgeführt. Im Gegensatz dazu setzt eine öffentliche Blockchain mit ihrer nativen Kryptowährung Anreize für die Aufrechterhaltung des Netzwerks und um die Anonymität aller Beteiligten zu gewährleisten. Mehr über Fabric erfahren Sie unter https://trustindigitallife.eu/wp-content/uploads/2016/07/marko_vukolic.pdf.

Alle Transaktionen sind abgesichert, privat und vertraulich. Fabric bewahrt seine Integrität, indem es Aktualisierungen nur mit Zustimmung der Teilnehmer erlaubt. Einmal eingetragene Datensätze sind unveränderlich.

Fabric ist eine Enterprise-Lösung, bei der es um Skalierbarkeit sowie die Einhaltung der Vorschriften geht. Alle Teilnehmer müssen einen Identitätsbeleg bei den Mitgliedsservices vorlegen,

um Zugriff auf das System zu erhalten. Fabric stellt Transaktionen mit abgeleiteten Zertifikaten aus, die nicht mit dem ausstellenden Teilnehmer in Verbindung gebracht werden können. Damit bietet es Anonymität im Netzwerk. Darüber hinaus werden alle Transaktionsinhalte verschlüsselt, um sicherzustellen, dass nur die vorgesehenen Teilnehmer sie sehen können.

Fabric ist modular aufgebaut. Sie können Komponenten hinzufügen oder entfernen, indem Sie Fabrics Protokollspezifikation implementieren. Seine Containertechnologie unterstützt die meisten Mainstream-Sprachen zur Entwicklung von Smart Contracts.

Das Iroha-Projekt

Das Iroha-Projekt von Hyperledger baut auf dem Fabric-Projekt auf. Es soll Fabric, Sawtooth Lake und die anderen Projekte unter Hyperledger ergänzen. Hyperledger fügte der Planung das Iroha-Projekt hinzu, weil die anderen Projekte keine Infrastrukturprojekte in C++ beinhalteten. Ein C++-Projekt war wichtig, damit mehr Anwender von Hyperledger profitieren und damit mehr Entwickler zu dem Projekt beitragen konnten.

Darüber hinaus wurde ein Großteil der Blockchain-Entwicklung bisher auf niedrigster Infrastrukturebene durchgeführt, und es floss wenig bis keine Entwicklungsarbeit in Benutzeroberflächen oder mobile Anwendungen. Deshalb hält das Hyperledger-Konsortium Iroha die Popularisierung der Blockchain-Technologie für notwendig. Hier sind mehr Entwickler an der Entwicklung von Bibliotheken für mobile Benutzeroberflächen beteiligt.

Zum Zeitpunkt der Drucklegung dieses Buchs ist Iroha ein sehr neues Projekt und wurde noch nicht in Fabric oder Sawtooth Lake integriert. Hyperledger plant, die Funktionalität zu erweitern und bald mit den anderen Blockchain-Projekten zusammenzuarbeiten. Seine iOS-, Android- und JavaScript-Bibliotheken stellen unterstützende Funktionen bereit, beispielsweise zur digitalen Signatur von Transaktionen. Es wird für die Entwicklung kommerzieller Apps sehr praktisch sein. Außerdem bringt es neue

Sicherheitsebenen und Geschäftsmodelle ins Spiel, die nur mit der Blockchain-Technologie möglich sind.

Sumeragi: Der neue Konsensalgorithmus

Blockchains enthalten Systeme, mit denen man sich zuerst auf eine einzige Version der Wahrheit einigt, die dann im Ledger aufgezeichnet wird. Ein Vereinbarungssystem wird als *Konsensmechanismus* bezeichnet.

Ein Konsensmechanismus ist kompliziert. Die Feinheiten, wie und warum sich Konsensmechanismen so verhalten, wie sie es tun, können in diesem Buch nicht erklärt werden. Als Anwender werden Sie diese Informationen auch sehr wahrscheinlich nicht benötigen. Sie müssen jedoch die Konsequenzen der verschiedenen Methoden zur Konsensbildung kennen und wissen, wie sie sich auf Ihre Arbeit mit der betreffenden Blockchain auswirken. Ich erkläre hier Sumeragi, den Konsensmechanismus von Iroha, weil er sich von den traditionellen Blockchains maßgeblich unterscheidet.

Hier einige Dinge, die Sumeragi so anders machen:

- ✔ **Sumeragi verwendet keine Kryptowährung.**
- ✔ **Knoten, die an der Konsensfindung mitwirken, werden dem System durch den Fabric-Mitgliederservice hinzugefügt.** Knoten erarbeiten sich mit der Zeit einen gewissen Ruf, je nachdem, wie sie in der Vergangenheit mit dem Ledger zusammengearbeitet haben. Es handelt sich um eine Berechtigungs-Blockchain, die von bekannten Teilnehmern betrieben wird.
- ✔ **Neue Einträge werden dem Ledger auf einzigartige Weise hinzugefügt.** Der erste Knoten, der die Konsensfindung startet, der sogenannte *Leader*, überträgt den Eintrag an eine Gruppe anderer Knoten. Diese Knoten führen dann eine Überprüfung durch. Wird der Eintrag nicht von ihnen genehmigt, überträgt ihn der erste Knoten nach einer vordefinierten Zeitdauer erneut.

Ja nach Anwendungsfall kann Iroha für Sie Vor- oder Nachteile haben. Wenn Sie sich Sorgen um Zensur machen, ist Iroha wahrscheinlich nicht das Richtige für Sie. In diesem Fall sollten Sie besser nach einer zensurresistenten Blockchain suchen. Wenn Sie nicht wollen, dass andere Mitglieder des Netzwerks Arbitrage betreiben, ist Iroha womöglich auch nicht das Richtige für Sie; eine weitere Recherche ist notwendig. Wenn Sie alle Teilnehmer Ihrer Blockchain kennen wollen, ist Iroha wahrscheinlich genau das, was Sie suchen.

Entwicklung mobiler Apps

Diesen Abschnitt können Sie überspringen, wenn Sie keine Apps entwickeln wollen.

Iroha ist auf Web- und Mobilgeräte-App-Entwickler zugeschnitten, die damit auf die Stärken des Hyperledger-Systems zugreifen können. Das Iroha-Team hat erkannt, dass ein verteiltes Ledger nichts bringt, wenn es nicht auch von Anwendungen genutzt wird.

Iroha hat einen Entwicklungspfad für die folgenden eingekapselten C++-Komponenten:

- ✔ Sumeragi-Konsensbibliothek
- ✔ Ed25519-Bibliothek für digitale Signaturen
- ✔ HA-3-Hashing-Bibliothek
- ✔ Iroha-Bibliothek für die Transaktionsserialisierung
- ✔ P2P-Broadcast-Bibliothek
- ✔ API-Server-Bibliothek
- ✔ iOS-Bibliothek
- ✔ Android-Bibliothek
- ✔ JavaScript-Bibliothek
- ✔ Blockchain-Explorer/Datenvisualisierungspaket

Eine der größten Hürden für die Blockchain-Branche war es, die Systeme benutzerfreundlich zu machen. Iroha hat Open-Source-

Softwarebibliotheken für iOS, Android und JavaScript eingeführt und den Aufruf allgemeiner API-Funktionen vereinfacht. Diese befinden sich immer noch in einer frühen Entwicklungsphase, aber Iroha ist eine gute Quelle, um weitere Informationen für Anwendungsfälle in Unternehmen zu erhalten.

Sawtooth Lake

Sawtooth Lake von Intel ist ein weiteres Projekt in Hyperledger. Es ist als höchst modulare Plattform ausgelegt, um neue dezentrale Ledger für Unternehmen zu erstellen.

Zum Zeitpunkt der Drucklegung dieses Buchs *simuliert* die Software der veröffentlichten Version den Konsensprozess nur. Sie bietet keine Sicherheit für Ihr Projekt und sollte nur eingesetzt werden, um neue Ideen auszuprobieren.

Sawtooth Lake verzichtet auf eine Kryptowährung. Die Sicherheit der Plattform wird durch Unternehmen gewährleistet, die private Blockchains erstellen können. Diese Betreiber privater Blockchains teilen dann den Rechenaufwands im Netzwerk unter sich auf. In der Dokumentation von Sawtooth Lake wird erklärt, dass dieses Design eine universelle Einigung über den Status des gemeinsamen Ledgers sicherstellt.

Sawtooth Lake hat das grundlegende Modell der Blockchains auf den Kopf gestellt. Die meisten Blockchains bestehen aus drei Elementen:

- einer frei zugänglichen Aufzeichnung des aktuellen Status der Blockchain,
- einer Möglichkeit, neue Daten einzugeben,
- einer Methode, sich auf diese Daten zu einigen.

Sawtooth Lake kombiniert die beiden ersten Elemente zu einem einzigen Prozess, der als *Transaktionsfamilie* bezeichnet wird. Dieses Modell ist am besten für Anwendungsfälle geeignet, in

denen alle beteiligten Parteien von einer korrekten Aufzeichnung profitieren.

Intel hat seine Software flexibel genug gemacht, um benutzerdefinierte Transaktionsfamilien zu unterstützen, die die speziellen Anforderungen aller Unternehmen berücksichtigen, und zudem drei Vorlagen für die Erstellung digitaler Anlagevermögen erstellt:

- **EndPointRegistry:** ein Ort, an dem Elemente in einer Blockchain aufgezeichnet werden,
- **IntegerKey:** ein gemeinsames Ledger für Lieferkettenmanagement,
- **MarketPlace:** eine Blockchain-Handelsplattform für den Kauf, den Verkauf und den Handel mit digitalem Anlagevermögen.

Der Konsensalgorithmus: Proof of Elapsed Time

Der Konsensalgorithmus für Sawtooth Lake heißt *Proof of Elapsed Time* (PoET). Er kann in einem absicherten Bereich des Hauptprozessors Ihres Computers ausgeführt werden, dem sogenannten *Trusted Execution Environment* (TEE). PoET nutzt die Sicherheit von TEE, um die vergangene Zeit zu belegen, indem Transaktionen einen Zeitstempel erhalten.

Andere Konsensalgorithmen nutzen ebenfalls eine Zeitstempelkomponente. Indem sie ihre Blockchains öffentlich machen, belegen sie zugleich, dass sie nicht verändert wurden. Das veröffentlichte Ledger kann jedermann nachschlagen und überprüfen. Das ist etwa so, als würde man eine Anzeige in einer Zeitung veröffentlichen, um mitzuteilen, dass etwas passiert ist.

PoET beinhaltet auch ein Auswahlsystem, das sich etwas anders als bei Proof-of-Work-Blockchains verhält. Aus dem Pool der zur Überprüfung berechtigten Knoten wird ein zufälliger Teilnehmer ausgewählt. Die Wahrscheinlichkeit dafür nimmt proportional dazu zu, wie viel Rechenleistung ein Knoten zum gemeinsamen Ledger beigetragen hat. Es können Maßnahmen ergriffen werden, die

verhindern, dass Knoten das System betrügen und das Ledger verfälschen.

Bereitstellung von Sawtooth

Intel hat unter https://intelledger.github.io eine fantastische Dokumentation und Tutorials zusammengetragen. Sie führen Sie durch den Prozess, eine virtuelle Entwicklungsumgebung für eine Blockchain einzurichten. Es gibt sogar eine Umgebung für den Aufbau einer Blockchain für Tic-Tac-Toe. Sie müssen Vagrant und VirtualBox kennen, um das Angebot nutzen zu können.

Ein eigenes System in Fabric erstellen

Es wurde viel Arbeit investiert, um Fabric zugänglich zu machen. Der Hyperledger Composer ist ein leicht zu bedienendes Werkzeug, um *Proof of Concepts* (POCs) für Blockchain-Anwendungen zu erstellen. Das Beste daran ist, dass Sie Ihr Unternehmensnetzwerk darin mit JavaScript definieren können, einer der weltweit beliebtesten Entwicklungssprachen. Alleine dies wird Ihren Bedarf an spezialisierten Blockchain-Entwicklern deutlich senken.

Der Hyperledger Composer reduziert Zeit und Kosten für die Entwicklungsarbeit und lässt Sie schneller zur Produktionsreife gelangen. Ein weiterer Vorteil des Composers ist der Einsatz von LoopBacks, die digitale Datenströme zurück an Ihr bestehendes IT-System übertragen und Ihre Abläufe synchron halten. Sie benötigen zwar immer noch ein gutes Entwicklungsteam, können Ihre unternehmerischen Anwendungen aber leicht abbilden.

Ein LoopBack ist ein Codeabschnitt in Ihrer Software, der einen digitalen Datenstrom ohne zusätzliche Verarbeitung oder Änderung an eine Quelle zurückgibt.

Vermögenswerte mit Hyperledger Composer verfolgen

Sie können den Hyperledger Composer in Ihrem Browser ausprobieren, ohne dafür eine besondere Software herunterladen zu müssen. Falls Sie offline arbeiten wollen oder den kompletten Funktionsumfang des Composers zur Anwendungsentwicklung nutzen möchten, gibt es auch eine Download-Variante, die hervorragend funktioniert.

Für dieses kurze Tutorial brauchen Sie nur einen Webbrowser mit Internetverbindung. In den folgenden Abschnitten zeige ich Ihnen, wie Sie Ihr eigenes Netzwerk bereitstellen, eine Tracking-Demo einrichten und Assets von A nach B verschieben. Dazu genügen größtenteils nur Mausklicks, aber Sie müssen auch ein paar Code-Schnipsel kopieren und einfügen.

Als Framework verwenden Sie das Animal Tracking Business Network. Es wurde als Anwendungsbeispiel für die britische Regierung und Landwirte entwickelt. In dieser Demo kann ein Landwirt Tiere zwischen verschiedenen Feldern bewegen, und die britische Regulierungsbehörde kann die Standorte der Kühe verfolgen. Die Assets in dieser Demo sind zufälligerweise Tiere, aber sie könnten jede Art von Objekt darstellen, dessen Position von einer Drittpartei, wie etwa einer Aufsichtsbehörde oder einem Versicherungsunternehmen, verfolgt werden muss.

Schritt 1: Ein Netzwerk zur Nachverfolgung einrichten

Zuerst müssen Sie Ihr Tracking-Netzwerk einrichten. Befolgen Sie dazu diese Schritte:

1. **Gehen Sie auf die Website von Hyperledger Composer: https://composer-playground.mybluemix.net/login.**
2. **Klicken Sie auf DEPLOY A NEW BUSINESS NETWORK.**
3. **Nennen Sie Ihr Netzwerk ANIMAL-TRACKING.**
4. **Geben Sie eine Beschreibung für Ihr Netzwerk ein.**

5. **Vergeben Sie einen Namen für die zu erstellende Admin-Card.**
6. **Wählen Sie für Ihr Business-Netzwerk unter SAMPLES ON NPM die Vorgabe ANIMALTRACKING-NETWORK aus.**
7. **Klicken Sie auf DEPLOY.**

Schritt 2: Eine Test-Demo einrichten

Nachdem Sie ein Tracking-Netzwerk erstellt haben, können Sie eine Test-Demo einrichten. Befolgen Sie diese Schritte:

1. **Klicken Sie auf CONNECT NOW.**
2. **Öffnen Sie einen weiteren Browser-Tab.**
3. **Kopieren Sie die URL aus dem ersten Tab, und fügen Sie sie in den zweiten Tab ein.**
4. **Klicken Sie im ersten Tab auf DEFINE.**
5. **Klicken Sie im zweiten Tab auf TEST.**
6. **Öffnen Sie das DEFINE-Fenster.**
7. **Kopieren Sie diesen Befehl:**

```
{
"$class": "com.biz.SetupDemo"
}
```

8. **Öffnen Sie das TEST-Fenster.**
9. **Klicken Sie auf ALL TRANSACTIONS.**
10. **Klicken Sie auf SUBMIT TRANSACTION.**
11. **Wählen Sie SETUPDEMO aus dem Dropdown-Menü.**
12. **Fügen Sie diesen Befehl ein:**

```
{
"$class": "com.biz.SetupDemo"
}
```

13. **Klicken Sie auf SUBMIT.**

Schritt 3: Ihre Kuh verschieben

In diesem Abschnitt verfolgen Sie digital die Bewegung Ihres Vermögenswerts von einem Standort zum nächsten. Vermögenswerte werden häufig an andere Orte verschoben, und es ist von Vorteil, wenn Sie und andere Personen, mit denen Sie zusammenarbeiten, den Standort jederzeit feststellen können.

1. **Öffnen Sie das DEFINE-Fenster.**
2. **Kopieren Sie diesen Befehl:**

```
{
"$class": "com.biz.AnimalMovementDeparture",
"fromField": "resource:com.biz.Field#FIELD_1",
"animal": "resource:com.biz.Animal#ANIMAL_1",
"from": "resource:com.biz.Business#BUSINESS_1",
"to": "resource:com.biz.Business#BUSINESS_2"
}
```

3. **Öffnen Sie das TEST-Fenster.**
4. **Klicken Sie auf ALL TRANSACTIONS.**
5. **Wählen Sie ANIMALMOVEMENTDEPARTURE.**
6. **Fügen Sie diesen Befehl ein:**

```
{
"$class": "com.biz.AnimalMovementDeparture",
"fromField": "resource:com.biz.Field#FIELD_1",
"animal": "resource:com.biz.Animal#ANIMAL_1",
"from": "resource:com.biz.Business#BUSINESS_1",
"to": "resource:com.biz.Business#BUSINESS_2"
}
```

7. **Klicken Sie auf SUBMIT.**

Schritt 4: Ihre Kuh erhalten

In diesem Abschnitt schließen Sie den Transfer des Vermögenswerts ab, indem Sie den neuen Standort akzeptieren.

Durch diese Doppelerfassung wird die Rechenschaftspflicht der Teammitglieder gewährleistet.

1. **Öffnen Sie das DEFINE-Fenster.**
2. **Kopieren Sie diesen Befehl:**

```
{
"$class": "com.biz.AnimalMovementArrival",
"arrivalField": "resource:com.biz.Field#FIELD_2",
"animal": "resource:com.biz.Animal#ANIMAL_1",
"from": "resource:com.biz.Business#BUSINESS_1",
"to": "resource:com.biz.Business#BUSINESS_2"
}
```

3. **Öffnen Sie das TEST-Fenster.**
4. **Klicken Sie auf ALL TRANSACTIONS.**
5. **Wählen Sie ANIMALMOVEMENTDEPARTURE.**
6. **Fügen Sie diesen Befehl ein:**

```
{
"$class": "com.biz.AnimalMovementArrival",
"arrivalField": "resource:com.biz.Field#FIELD_2",
"animal": "resource:com.biz.Animal#ANIMAL_1",
"from": "resource:com.biz.Business#BUSINESS_1",
"to": "resource:com.biz.Business#BUSINESS_2"
}
```

7. **Klicken Sie auf SUBMIT.**

Herzlichen Glückwunsch! Sie haben nun die Bewegung Ihrer Kuh von einem Standort zum nächsten auf einer Plattform dokumentiert, über die ein Dritter die Position und Identität dieses Tieres überprüfen kann.

Smart-Contracts auf Hyperledger verwenden

Ein *Smart Contract* ist ein in einem Blockchain-Protokoll verfasster Computercode. Smart Contracts sollen im Vorfeld ausgehandelte Bedingungen zwischen zwei oder mehr Parteien festschreiben, überprüfen oder durchsetzen. Das Blockchain-Protokoll selbst sorgt hier für die Erfüllung der Verträge. Mithilfe von Smart Contracts können zwei oder mehr Parteien auch ohne gegenseitiges Vertrauen oder übergeordnete Vermittlerinstanzen zusammenarbeiten, auch wenn etwas schiefgeht. Zumindest in der Theorie. Viele verschiedene Plattformen unterstützen Smart Contracts. In Hyperledger heißen sie *Chaincode*.

Chaincode wird praktischerweise in Go, node.js und Java geschrieben und in einem sicheren Docker-Container ausgeführt. Im Gegensatz zu anderen Smart-Contract-Plattformen, bei denen der Vertrag in einem öffentlichen Netzwerk ausgeführt und durchgesetzt wird, läuft Chaincode getrennt vom Verifikationsprozess der öffentlichen Blockchains. Auf diese Weise können Sie Ihre Geschäftsvereinbarungen unter Verschluss halten.

Ein weiteres Merkmal, mit dem sich Chaincode von vielen anderen Plattformen unterscheidet, ist, dass jeder Chaincode-Contract für sich alleine steht. Andere Unternehmen, die Hyperledger einsetzen, können ohne Genehmigung nicht direkt auf Ihren Chaincode zugreifen. Angriffsvektoren auf Ihre Verträge werden durch hierdurch reduziert, weil Dritte keinen Zugriff darauf haben.

Eine *Smart Auction* ist eine bestimmte Art von Smart Contract. Dabei wird das Eigentum an einem Gegenstand übertragen, nachdem die vorgegebenen Parameter der Vereinbarung erfüllt sind. In dieser Demo werden Sie eine Auktion für Autos erstellen. Sie bieten Vermögenswerte zum Verkauf an, legen einen Mindestpreis fest und testen, was passiert, wenn die Objekte am Ende des Auktionszeitraums den Mindestpreis erreicht oder überschritten haben.

Da Sie Hyperledger Composer verwenden, benötigen Sie keine Programmierkenntnisse, um diese Demo abzuschließen. Sie

müssen auch keine spezielle Software herunterladen. Ein Chrome-Browser und eine gute Internetverbindung reichen aus.

Schritt 1: Ein Auktionsnetzwerk einrichten

Befolgen Sie diese Schritte, um ein Auktionsnetzwerk einzurichten:

1. **Gehen Sie auf die Website von Hyperledger Composer:** https://composer-playground.mybluemix.net/login.
2. **Wählen Sie für Ihr Business-Netzwerk unter SAMPLES ON NPM die Vorgabe CARAUCTION-NETWORK aus.**
3. **Klicken Sie für das CARAUCTION-NETWORK auf CONNECT NOW.**

Schritt 2: Ein Auktionsfenster einrichten

Befolgen Sie diese Schritte, um ein Auktionsfenster einzurichten:

1. **Öffnen Sie einen weiteren Browser-Tab.**
2. **Kopieren Sie die URL aus dem ersten Tab, und fügen Sie sie in den zweiten Tab ein.**
3. **Klicken Sie im ersten Tab auf DEFINE.**
4. **Klicken Sie im zweiten Tab auf TEST.**

Schritt 3: Einen Auktionator erstellen

Befolgen Sie diese Schritte, um einen Auktionator zu erstellen:

1. **Öffnen Sie das DEFINE-Fenster.**
2. **Kopieren Sie diesen Befehl:**

```
{
"$class": "org.acme.vehicle.auction.Auctioneer",
"email": "auction@acme.org",
"firstName": "Jenny",
"lastName": "Jones"
}
```

3. **Öffnen Sie das TEST-Fenster.**
4. **Klicken Sie auf CREATE NEW PARTICIPANT.**
5. **Fügen Sie diesen Befehl ein:**

```
{
"$class": "org.acme.vehicle.auction.Auctioneer",
"email": "auction@acme.org",
"firstName": "Jenny",
"lastName": "Jones"
}
```

6. **Klicken Sie auf CREATE NEW.**

Schritt 4: Zwei Teilnehmer erstellen

Befolgen Sie diese Schritte, um zwei Teilnehmer zu erstellen:

1. **Öffnen Sie das DEFINE-Fenster.**
2. **Kopieren Sie diesen Befehl:**

```
{
"$class": "org.acme.vehicle.auction.Member",
"balance": 5000,
"email": "memberA@acme.org",
"firstName": "Amy",
"lastName": "Williams"
}
```

3. **Öffnen Sie das TEST-Fenster.**
4. **Klicken Sie auf MEMBER.**
5. **Klicken Sie auf CREATE NEW PARTICIPANT.**
6. **Fügen Sie diesen Befehl ein:**

```
{
"$class": "org.acme.vehicle.auction.Member",
"balance": 5000,
"email": "memberA@acme.org",
"firstName": "Amy",
```

```
"lastName": "Williams"
}
```

7. **Klicken Sie auf CREATE NEW.**
8. **Wiederholen Sie die Schritte 1 bis 6 für den zweiten Teilnehmer.**

Schritt 5: Einen neuen Vermögenswert anlegen

Befolgen Sie diese Schritte, um einen neuen Vermögenswert anzulegen:

1. **Öffnen Sie das DEFINE-Fenster.**
2. **Kopieren Sie diesen Befehl:**

```
{
"$class": "org.acme.vehicle.auction.Vehicle",
"vin": "vin:1234",
"owner":
"resource:org.acme.vehicle.auction.Member#memberA@acme.or
g"
}
```

3. **Öffnen Sie das TEST-Fenster.**
4. **Klicken Sie auf VEHICLE.**
5. **Klicken Sie auf CREATE NEW ASSET.**
6. **Fügen Sie diesen Befehl- ein:**

```
{
"$class": "org.acme.vehicle.auction.Vehicle",
"vin": "vin:1234",
"owner":
"resource:org.acme.vehicle.auction.Member#memberA@acme.or
g"
}
```

7. **Klicken Sie auf CREATE NEW.**

Schritt 6: Ein neues Angebot erstellen

Befolgen Sie diese Schritte, um ein neues Angebot zu erstellen:

1. **Öffnen Sie das DEFINE-Fenster.**
2. **Kopieren Sie diesen Befehl:**

```
{
"$class": "org.acme.vehicle.auction.VehicleListing",
"listingId": "listingId:ABCD",
"reservePrice": 3500,
"description": "Arium Nova",
"state": "FOR_SALE",
"vehicle":
"resource:org.acme.vehicle.auction.Vehicle#vin:1234"
}
```

3. **Öffnen Sie das TEST-Fenster.**
4. **Klicken Sie auf VEHICLELISTING.**
5. **Klicken Sie auf CREATE NEW ASSET.**
6. **Fügen Sie diesen Befehl ein:**

```
{
"$class": "org.acme.vehicle.auction.VehicleListing",
"listingId": "listingId:ABCD",
"reservePrice": 3500,
"description": "Arium Nova",
"state": "FOR_SALE",
"vehicle":
"resource:org.acme.vehicle.auction.Vehicle#vin:1234"
}
```

7. **Klicken Sie auf CREATE NEW.**

Herzlichen Glückwunsch! Sie haben nun eine Smart Auction erstellt, ein Auto zum Verkauf angeboten und die drei Parteien angelegt, die zur Ausführung des Vertrags erforderlich sind. Jetzt ist alles vorbereitet, und Sie können die Smart Auction starten und das Auto vom Besitzer auf den Käufer übertragen.

Schritt 7: Das Auto versteigern

Befolgen Sie diese Schritte, um das Auto zu versteigern:

1. **Öffnen Sie das DEFINE-Fenster.**
2. **Kopieren Sie diesen Befehl:**

```
{
"$class": "org.acme.vehicle.auction.Offer",
"bidPrice": 3500,
"listing":
"resource:org.acme.vehicle.auction.VehicleListing#listing
Id:ABCD",
"member":
"resource:org.acme.vehicle.auction.Member#memberB@acme.or
g"
}
```

3. **Öffnen Sie das TEST-Fenster.**
4. **Klicken Sie auf SUBMIT TRANSACTION.**
5. **Wählen Sie OFFER aus dem Dropdown-Menü.**
6. **Fügen Sie diesen Befehl ein:**

```
{
"$class": "org.acme.vehicle.auction.Offer",
"bidPrice": 3500,
"listing":
"resource:org.acme.vehicle.auction.VehicleListing#listing
Id:ABCD",
"member":
"resource:org.acme.vehicle.auction.Member#memberB@acme.or
g"
}
```

7. **Klicken Sie auf SUBMIT.**

Schritt 8: Die Auktion beenden

Befolgen Sie diese Schritte, um die Auktion zu beenden:

1. **Öffnen Sie das DEFINE-Fenster.**
2. **Kopieren Sie diesen Befehl:**

```
{
"$class": "org.acme.vehicle.auction.CloseBidding",
"listing":
"resource:org.acme.vehicle.auction.VehicleListing#listing
Id:ABCD"
}
```

3. **Öffnen Sie das TEST-Fenster.**
4. **Klicken Sie auf SUBMIT TRANSACTION.**
5. **Wählen Sie CLOSEBIDDING aus dem Dropdown-Menü.**
6. **Fügen Sie diesen Befehl ein:**

```
{
"$class": "org.acme.vehicle.auction.CloseBidding",
"listing":
"resource:org.acme.vehicle.auction.VehicleListing#listing
Id:ABCD"
}
```

7. **Klicken Sie auf SUBMIT.**

Sie haben eine Smart Auction erstellt, einen Vermögenswert zum Verkauf angeboten, einen Käufer angelegt und den Vermögenswert verkauft. Nicht schlecht! Weitere Informationen finden Sie in der Hyperledger-Community unter https://hyperledger.github.io/composer/latest/support/support-index.html.

Kapitel 10

Microsoft Azure

IN DIESEM KAPITEL

- Neue Anwendungen erstellen
- Ihre Systeme verknüpfen
- Neue Systeme authentifizieren
- Ein privates Ethereum einsetzen

In diesem Kapitel erhalten Sie einen Überblick über die attraktiven Innovationen, die auf der Azure-Plattform von Microsoft stattfinden, und erfahren, wie diese Änderungen die Effizienz Ihres Unternehmens steigern und neue Gelegenheiten für Produkte und Services schaffen können.

Dieses Kapitel hilft Ihnen, weltweit Kunden zu gewinnen, mit ihnen zusammenzuarbeiten und sie zu beliefern. Die Blockchain-Technologie eröffnet neue Märkte und sorgt für völlig neue Geschäftsmodelle. Microsoft arbeitet nachdrücklich daran, die Technologie auch traditionellen Unternehmen zugänglich machen.

Dieses Kapitel erklärt auch innovative Blockchain-Schnittstellen, mit denen Sie Ihre vorhandenen Systeme ankoppeln und skalieren können. Sie werden erfahren, wie Sie Ihre eigene Blockchain in Azure bereitstellen und was Sie auf jeden Fall brauchen, um in Ihrem Unternehmen einen sicheren und unkomplizierten Umstieg auf Blockchain-Systeme vorzunehmen.

Bletchley: Die modulare Blockchain-Struktur

Das Projekt Bletchley bietet hauptsächlich Bausteine für Unternehmenskunden innerhalb eines *Consortium Blockchain Ecosystems* an. Das sind Netzwerke, in denen nur berechtigte Mitglieder Verträge ausführen können. Die Blockchain-Struktur von Bletchley basiert auf Azure, der Cloud-Computing-Plattform von Microsoft. Beim Projekt Bletchley geht es um Folgendes:

- ✔ digitale Identität,
- ✔ Verwaltung privater Schlüssel,
- ✔ Datenschutz für Kunden,
- ✔ Datensicherheit,
- ✔ Betriebsverwaltung,
- ✔ Systeminteroperabilität.

Im Projekt Bletchley stellt Azure die Cloud-Ebene für Blockchains bereit. Azure dient weltweit in 24 Regionen als Plattform zur Erstellung und Bereitstellung von Anwendungen. Es kombiniert traditionelle Produkte wie etwa hybride Cloud-Funktionen, ein umfangreiches Compliance-Zertifizierungsportfolio und professionelle Datensicherheit mit verschiedenen Blockchains. Microsoft will Bestandskunden die schnelle Integration der Blockchain-Technologie einfacher machen, besonders in regulierten Bereichen wie dem Gesundheitswesen, Finanzdienstleistungen und Regierungsstellen.

Abbildung 10.1 zeigt Blockstack Core v14 aus dem Bletchley-Projekt, ein neues, dezentrales Netz serverloser Anwendungen, in dem Benutzer ihre Daten kontrollieren können.

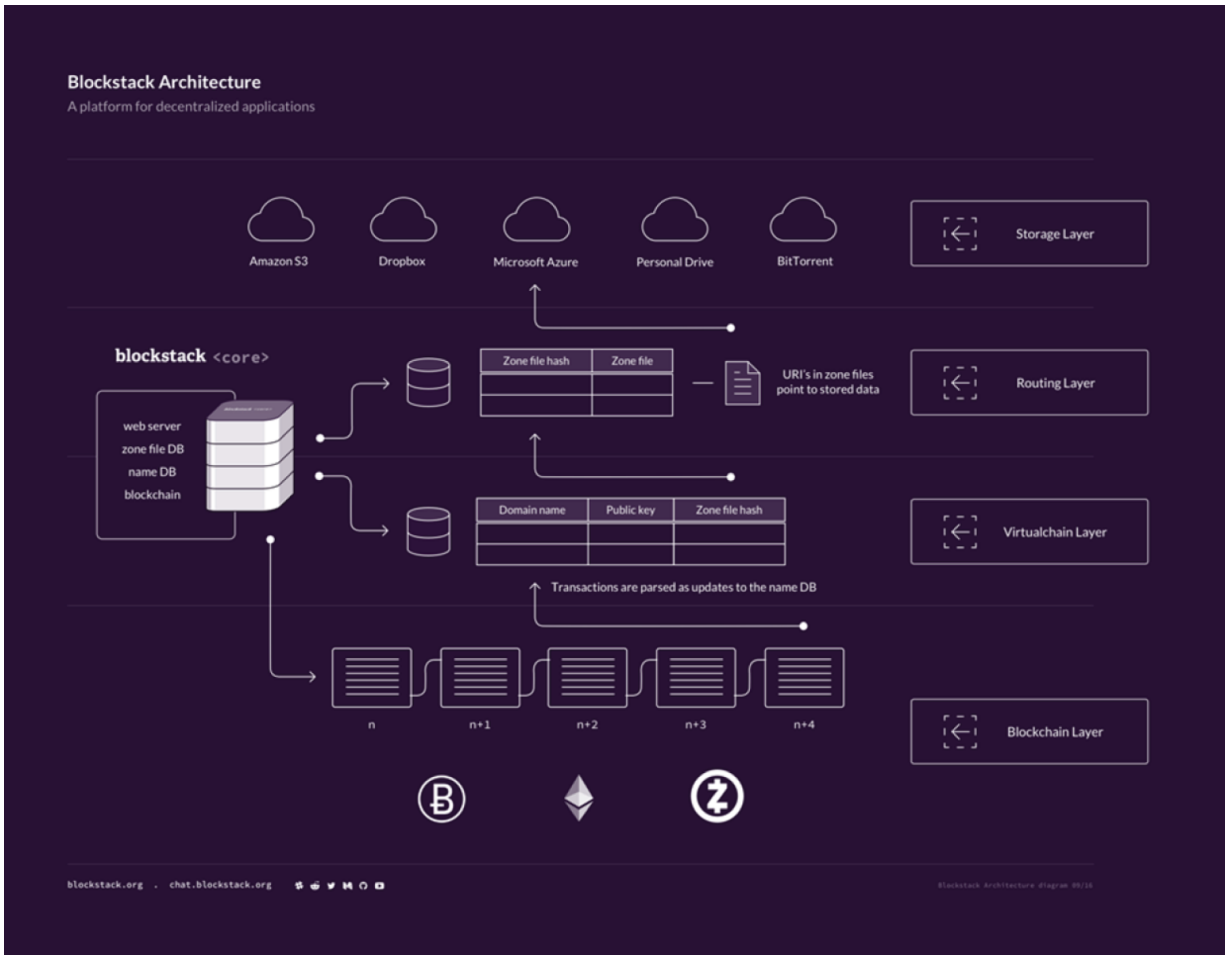


Abbildung 10.1: Blockstack Core v14

Azure arbeitet mit mehreren Blockchain-Protokollen. Sie sind Teil des Hyperledger-Projekts und UTXO-basierter Protokolle (Unspent Transaction Output). Das bedeutet, dass die Azure-Plattform keine Kryptowährung verwendet und möglicherweise für Unternehmenskunden attraktiver ist. Außerdem gibt es eine Integration für komplexere Protokolle, wie beispielsweise Ethereum, die zur Sicherung des Netzwerks eine Kryptowährung verwenden.

Cryptlets für die Verschlüsselung und Authentifizierung

Das Projekt Bletchley wurde um zwei Ideen herum aufgebaut:

- **Blockchain-Middleware:** Cloud-Speicher, Identitätsverwaltung, Analyse und Maschinenlernen,
- **Cryptlets:** sichere Ausführung für die Zusammenarbeit und Kommunikation zwischen Microsoft Azure, dem Bletchley-Ökosystem und Ihrer eigenen Technologie.

Cryptlets sind in einer beliebigen Sprache geschriebene Komponenten, die nicht zum Chaincode gehören und in einem vertrauenswürdigen Container ausgeführt und über einen sicheren Kanal übertragen werden. Cryptlets können in Smart Contracts und UXTO-Systemen zum Einsatz kommen, falls zusätzliche Funktionen oder Informationen benötigt werden.

Cryptlets schließen die Sicherheitslücke zwischen der Ausführung von Programmen innerhalb und außerhalb der Chain. Sie werden eingesetzt, wenn zusätzliche sichere Informationen benötigt werden. Damit können Sie beispielsweise Ihr CRM-System oder Ihre Handelsplattform mit Ihrem Cloud-Speicher verknüpfen und diese Verbindung mit Ethereum absichern.

Die Middleware von Bletchley arbeitet mit Cryptlets und vorhandenen Azure-Services zusammen, beispielsweise Active Directory (AD) und Key Vault, außerdem mit anderen Blockchain-Technologien. So kann eine vollständige Lösung präsentiert und ein zuverlässiger Betrieb Ihrer Blockchain-Integration gewährleistet werden.

Tabelle 10.1 zeigt den Unterschied zwischen einem Orakel und einem Cryptlet aus der Präsentation von Bletchley von Devcon 2.

	Cryptlets	***Orakel***
Prüfanforderungen	Fordert Vertrauen, mit einer Überprüfung eines vertrauenswürdigen Hosts (HTTPS), eines vertrauenswürdigen Cryptlet-Schlüssels und einer vertrauenswürdigen Enclave-Signatur.	Fordert Vertrauen, aber keine formelle Überprüfung.

	Cryptlets	*Orakel*
Infrastruktur	Standardinfrastruktur. Sie erzielen eine auf der Hardware basierende Isolierung und Bestätigung über Enclaves, die in Azure allgemein verfügbar sind. Es stehen Blenchley Cryptlet SDK Frameworks (Software Development Kit; Utility und Contract) zur Verfügung, die Ihnen helfen, schnell Cryptlets zu erstellen und zu verbrauchen.	Benutzerdefinierte Infrastruktur. Sie können separat schreiben und hosten. Der Aufbau von Vertrauen ist schwierig. Orakel sind plattformspezifisch, und es gibt nur sehr wenig Dokumentation.
Verwendung durch den Entwickler	Es werden zahlreiche Sprachoptionen unterstützt, Blockchains sind egal.	An die eigene Blockchain gebunden, wenige Sprachoptionen.
Verfügbarkeit eines Marktplatzes	Für die Veröffentlichung und den Abruf steht ein Marktplatz zur Verfügung.	Für die Veröffentlichung und den Abruf steht kein allgemeiner Marktplatz zur Verfügung.

Tabelle 10.1: Cryptlets im Vergleich zu Prognosen

Cryptlets werden von Entwicklern erstellt und auf dem Marktplatz von Bletchley verkauft. Sie unterstützen viele verschiedene Funktionsmengen, wobei es im Wesentlichen darum geht, verteilte, auf Ledgern basierende Anwendungen zu erstellen. Der Markt wächst, um die Anforderungen von Kunden zu erfüllen, die die entsprechende Funktionalität benötigen, beispielsweise sichere Ausführung, Integration, Datenschutz, Verwaltung, Interoperabilität und eine ganze Palette an Datenservices.

Utility- und Contract-Cryplets und CryptoDelegates

Es gibt zwei Arten von Cryptlets:

- **Utility:** Utility-Cryptlets unterstützen Verschlüsselung, Zeitstempel, externen Datenzugriff und Authentifizierung. Sie erzeugen korrektere und vertrauenswürdigere Transaktionen.
- **Contract:** Contract-Cryptlets sind vollständige Delegations-Engines. Sie können als autonome Agenten oder Bots eingesetzt werden. Sie bieten die gesamte Ausführungslogik, die ein Smart Contract normalerweise benötigt, aber außerhalb einer Blockchain.

Contract-Cryptlets sind mit Smart Contracts verknüpft und werden erzeugt, wenn Ihr Smart Contract veröffentlicht wird. Sie werden parallel zu Ihrer virtuellen Maschine ausgeführt und bieten eine bessere Leistung als herkömmliche Smart Contracts innerhalb von Blockchains, weil für ihre Ausführung keine Mining-Gebühren anfallen. Sie sind vor allem interessant für Benutzer von Blockchains ohne Kryptowährung, wo der Chaincode und Smart Contracts von bekannten Parteien signiert werden.

Abbildung 10.2 zeigt einen Cryptlet-Container und den sicheren Kommunikationspfad zu Ihrem Smart Contract.

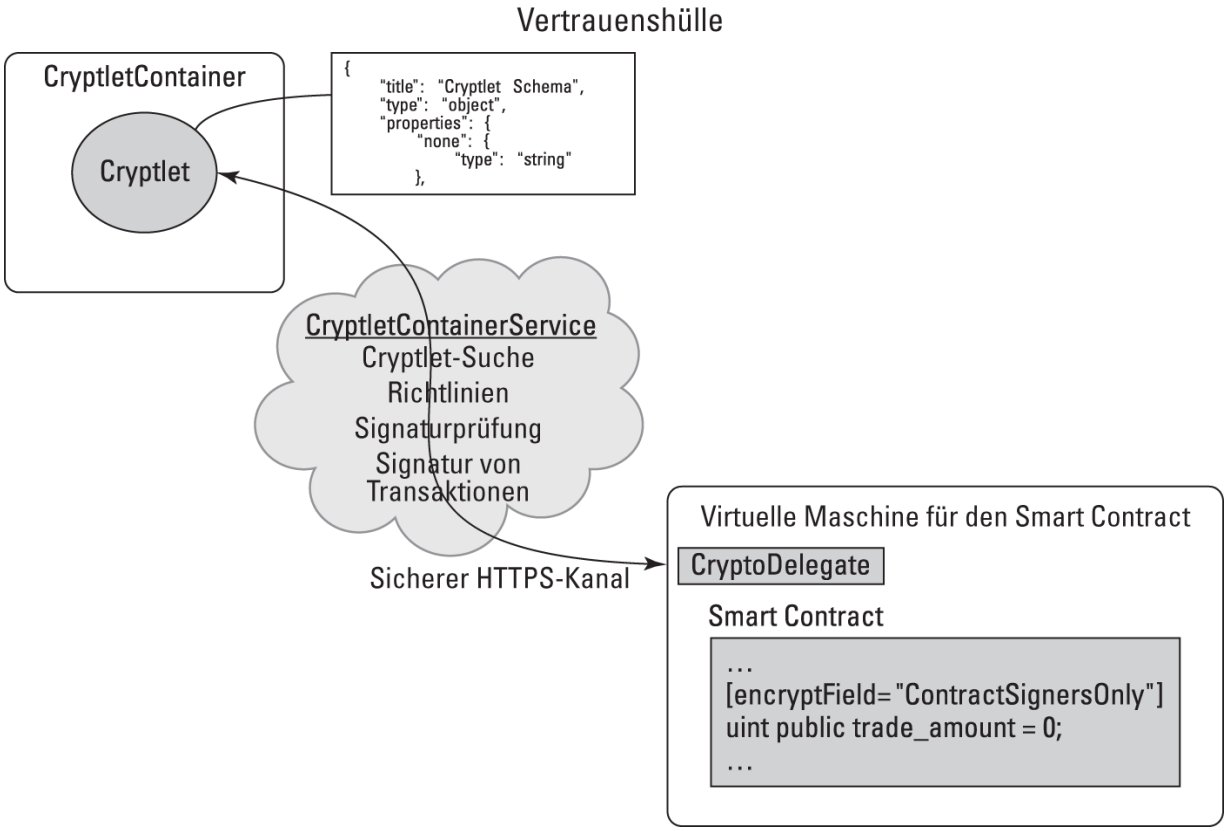


Abbildung 10.2: Ein Cryptlet-Container

CryptoDelegates unterstützen Utility- und Contract-Cryptlets. Sie verhalten sich wie Zwischenstücke, indem sie Funktionshooks für Ihre virtuellen Maschine mit dem Smart Contract erzeugen. Sie rufen das Cryptlet von dem Code Ihres Smart Contracts aus auf, sodass eine sichere und authentische Hülle für Transaktionen entsteht.

Entwicklung im Azure-Ökosystem

Azure ist ein digitales Ökosystem und eine Cloud-Computing-Plattform. Es verbindet Unternehmen direkt mit ihren Cloud-Partnern und SaaS. Dadurch können Unternehmen wiederum ihre gemeinschaftlichen Daten zuverlässig und sicher übertragen.

Die Cloud-Plattform Azure ist die weltweit zweitgrößte Infrastruktur-als-Service-Plattform (IaaS). Sie stellt einen zuverlässigen und sicheren Ort für Ihr Cloud-Computing und Ihren Datenspeicher dar. In Azure gibt es einen Service, ExpressRoute, der Verbrauchern eine direkte Verbindung mit Azure ermöglicht. Das verhindert die Leistungs- und Sicherheitsprobleme, die es im öffentlichen Internet oft gibt.

2015 hat Microsoft beschlossen, sein Azure-Ökosystem unter Verwendung der Blockchain-Systeme Ethereum und Hyperledger zu erweitern. Das erste Angebot des Blockchain as a Service von Azure wird durch Ethereum gestützt. Ethereum ist ein Turing-vollständiges Blockchain-Netzwerk für die Entwicklung von Anwendungen. In Kapitel 5 oder in *Ethereum For Dummies* von Michael G. Solomon (Wiley) können Sie mehr darüber nachlesen. Microsoft plant weitere Angebote auf Basis von Blockchain-Technologie und Hyperledger. Außerdem erweitert es den Azure-Marktplatz, indem es auf ein Kundenportal für Azure umsteigt.

Das Azure-Stack-Programm von Microsoft enthält Azure Quickstart Templates, die über den Azure Resource Manager verschiedene Azure-Ressourcen bereitstellen, die Ihre Produktivität steigern sollen. Der Azure Resource Manager gestattet Kunden, mit ihren Geschäftspartnern als Gruppe zusammenzuarbeiten und alle Ressourcen in ihrer Lösung in einer einzigen koordinierten Aktion bereitzustellen, zu löschen oder zu aktualisieren.

Azure Quickstart Templates können in unterschiedlichen Umgebungen eingesetzt werden, beispielsweise in der Produktion, für die Beschaffung und zu Testzwecken. Über den Azure Resource Manager erhalten die Kunden verschiedene Funktionen für Kennzeichnung, Prüfung und Sicherheit, mit denen sie ihre Ressourcen nach der Bereitstellung besser verwalten können.

Das Bletchley-Projekt von Microsoft ist eine Blockchain-Architektur, die mit etablierten Enterprise-Technologien kombiniert

wird, die Microsoft bereits anbietet. Azure erhält dadurch ein Backend und einen Marktplatz für Blockchain-Lösungen.

Das Bletchley-Ökosystem ist der von Microsoft gewählte Ansatz, Blockchains und verteilte Ledger-Netzwerke einem größeren Publikum sicher und effektiv näherzubringen. Microsoft will dazu beitragen, authentische Lösungen zu erzeugen und auf aktuelle Geschäftsprobleme einzugehen.

Wählen Sie Ihre Vorlage!

Quickstart Template ist ein Tool, mit dem die Benutzer des Bletchley-Projekts leichter private Gruppen einrichten können. Derzeit gibt es etwa ein Dutzend Blockchain-Vorlagen, mit denen Sie Blockchain-Anwendungen in Azure einrichten können. In der Zukunft soll es weitere Vorlagen geben.

Die private Version von Ethereum ist eine der besten, um den Prozess zu automatisieren. Step-it ist ein schrittweiser Prozess, bei dem Sie die Mitglieder Ihres Konsortiums auswählen können, ebenso wie die Anzahl der Knoten für jeden Benutzer im Netzwerk. Anschließend können Sie diese Knoten unter Verwendung der Azure-Cloud geografisch verteilen, um die Ausfallsicherheit zu steigern.

Die ersten Schritte mit Chain auf Azure

Das Unternehmen Chain bietet Blockchain-Technologielösungen an und hat seine Chain Core Developer Edition auf Azure veröffentlicht. Die Chain Core Developer Edition ist eine kostenlose Open Source-Version der verteilten Ledger-Plattform des Unternehmens. Sie ermöglicht es Ihnen, Werte in autorisierten Blockchain-Netzwerken auszustellen und zu übertragen.

Über ein Testnetzwerk können Ihre Entwickler einem Blockchain-Netzwerk beitreten oder ein solches erstellen. Sie erhalten darin Zugriff auf technische Tutorials und Dokumentationen, und sie können Finanzanwendungen erstellen. Die Entwickler können

auch ihre eigenen Prototypen im Testnetzwerk von Chain ausführen oder ein eigenes persönliches Netzwerk auf Azure erstellen.

Installation des verteilten Ledgers von Chain

Die Chain Core Developer Edition umfasst Codebeispiele, ein Java SDK sowie Anleitungen für den Schnellstart. Darüber hinaus gibt es eine Dashboard-Oberfläche und Installationsprogramme für Linux, Mac und Windows.

Gehen Sie wie folgt vor, um Ihre Chain Core Developer Edition zu installieren:

1. **Gehen Sie unter** https://chain.com/docs/core/get-started/install **auf die Installationsseite von Chain.**
2. **Wählen Sie Ihr Betriebssystem aus der Liste aus.**
3. **Klicken Sie auf DOWNLOAD.**
4. **Öffnen Sie das Chain-Programm.**
5. **Führen Sie das Installationsprogramm Chain Core aus.**

Chain stellt ein SDK breit, das Ihnen und Ihren Entwicklern die Softwareentwicklungstools bereitstellt, mit denen Blockchain-Anwendungen und Werte erstellt werden können.

Ein eigenes privates Netzwerk erstellen

Sie können ein privates Ethereum-Consortium-Blockchain-Netzwerk in Azure erstellen. Dazu brauchen Sie noch nicht einmal die Hilfe eines Entwicklers. Gehen Sie einfach wie folgt vor:

1. **Richten Sie ein Azure-Konto ein, oder melden Sie sich mit Ihrem Azure-Konto an.**

   Es gibt die Möglichkeit, eine kostenlose Testversion zu erhalten sowie in einem Guthabenmodus zu arbeiten, wodurch

es ganz einfach ist, Azure auszuprobieren.

2. **Öffnen Sie** https://goo.gl/YtqnKa**.**
3. **Klicken Sie auf DEPLOY TO AZURE (an Azure senden).**

 Die Mitglieder der Azure-Community haben Azure-Resource-Manager-Vorlagen erstellt. Microsoft überprüft diese nicht auf Sicherheit, Kompatibilität oder Leistung.

4. **Füllen Sie das Formular aus.**
5. **Klicken Sie auf PURCHASE (kaufen).**

Herzlichen Glückwunsch! Sie haben jetzt ein privates Ethereum-Consortium-Blockchain-Netzwerk.

Finanzdienstleistungen von Azure Chain nutzen

Chain stellt eine kostenlose Open-Source-Entwicklerplattform bereit. Diese umfasst ein Testnetzwerk, das von Microsoft, Chain und der Initiative for Cryptocurrencies and Contracts (IC3) betrieben wird. Chain Core ist die von Chain veröffentlichte Plattform, die Blockchain-Technologielösungen bereitstellt. Mit der Chain Core Developer Edition können Einzelpersonen und Unternehmen mit der Technik experimentieren und Prototypen bauen.

Chain Core ermöglicht es Ihnen, Vermögenswerte in authentifizierten Blockchain-Netzwerken auszustellen und zu übertragen. Dies ist ein Projekt von führenden Finanzeinrichtungen und Chain. Über Chain Core können verschiedene Finanzanwendungen entwickelt werden.

Es sind bereits viele innovative Produkte geplant, die auf dieser Plattform veröffentlicht werden sollen. Dabei geht es unter anderem um Zahlungen, Bankwesen, Versicherungen und Kapitalmärkte. Darüber hinaus hat Visa in Zusammenarbeit mit Chain eine sichere, schnelle und einfache Methode entwickelt, B2B-Zahlungen weltweit zu verarbeiten.

Bereitstellung von Blockchain-Tools auf Azure

Azure bietet weitere praktische Implementierungen der Blockchain-Technologie, außerdem Tools, die Sie vielleicht interessant finden. Ich stelle in diesem Abschnitt vier der wichtigsten Blockchain-Tools und -Projekte von Azure vor, unter anderem seine Ethereum-Implementierung, ein Tool für analytisches maschinelles Lernen namens Cortana, Power BI, das Datenvisualisierungstool von Azure, und sein AD-Tool (Active Directory). Bei den drei zuletzt genannten Projekten handelt es sich nicht um spezifische Blockchain-Tools, sie können jedoch für Ihr Azure-Blockchain-Projekt nützlich sein.

In diesem Abschnitt erhalten Sie einen Eindruck, was Sie mit Azure und den verfügbaren Tools entwickeln können, um Ihr Projekt erfolgreich zu machen.

Ethereum auf Azure

Die Ethereum- Blockchain steht jetzt als Service auf der Azure-Plattform von Microsoft zur Verfügung. Dieser Service wird gemeinsam von ConsenSys und Microsoft angeboten. Eines ihrer neuen Projekte ist Solidity. Mit ihm können Sie Ihre dezentrale Anwendung auf Ethereum entwickeln. Weitere Informationen finden Sie unter https://marketplace.visualstudio.com/items?itemName=ConsenSys.Solidity.

Ethereum Blockchain as a Service (EBaaS) ermöglicht Unternehmensentwicklern und Kunden, mit einem Klick eine Blockchain-Umgebung in der Cloud einzurichten.

Wenn Sie die Ethereum-Blockchain auf Azure bereitstellen, bietet Ihnen Azure zu Beginn zwei Tools an:

- ✔ **BlockApps:** eine Ethereum-Blockchain-Umgebung,
- ✔ **Ether.Camp:** eine eingebaute Entwicklerumgebung.

BlockApps kann auch in der öffentlichen Umgebung von Ethereum bereitgestellt werden. Dieses Tool gestattet eine schnelle Entwicklung von Anwendungen basierend auf einem Smart Contract.

Ethereum ist ein flexibles und offenes System, das an die verschiedenen Bedürfnisse der Kunden angepasst werden kann. Weitere Informationen über Ethereum finden Sie in Kapitel 5.

Cortana: Ihr Tool für analytisches maschinelles Lernen

Cortana ist ein leistungsstarkes Tool für analytisches maschinelles Lernen, das auf Cloud-Systemen basiert. Es handelt sich dabei um einen vollständig verwalteten Cloud-Service, dessen Benutzer schnell und einfach prädiktive analytische Lösungen erstellen, organisieren und teilen können. Es bietet dem Verbraucher zahlreiche Vorteile.

Dank der von Cortana Intelligence angebotenen Analyse können Sie schneller agieren als Ihre Wettbewerber, weil Sie die nächste große Entwicklung schon vorhersehen können. Diese flexible und schnelle Software gestattet Ihnen, schnelle Lösungen für Ihre Branche zu finden, die genau auf Ihre speziellen Anforderungen zugeschnitten sind.

Darüber hinaus ist das Cortana-Lerntool sicher und skalierbar. Cortana bietet Mehrwert, unabhängig von der Komplexität und der Größe der Daten. Vor allem gestattet Ihnen Cortana jedoch, mit Smart Agents zusammenzuarbeiten, sodass Sie näher an Ihre Kunden herankommen – auf natürlichere, praktischere und nützlichere Art und Weise. Die Cortana Intelligence Suite ist in verschiedenen Bereichen sehr hilfreich, unter anderem in der Produktion, bei Finanzdienstleistungen, im Einzelhandel und Gesundheitswesen.

Mit Power BI Daten visualisieren

Power BI von Microsoft ist ein leistungsstarker, cloudbasierter Service. Er deckt die neuesten Business-Intelligence-Services

und -Tools von Microsoft ab. Der Dienst hilft Datenwissenschaftlern, Einblicke aus den Daten ihrer Unternehmen visuell darzustellen und zu teilen.

Der Kurs zur Datenvisualisierung mit Power BI, der online von edX bereitgestellt wird, gehört zum Microsoft Professional Program Certificate im Bereich Datenwissenschaft. Dieser auf der Cloud basierende Service gewinnt schnell an Beliebtheit bei Fachleuten aus dem Bereich der Datenwissenschaft.

Power BI hilft Ihnen, Ihre Daten zu visualisieren und in Verbindung zu bringen. In diesem Kurs erfahren die Teilnehmer, wie sie ihre Daten für Business Intelligence verknüpfen, importieren, transformieren und formen. Darüber hinaus lernen Sie im Power-BI-Kurs, wie Sie Dashboards erstellen und Business-Anwendern über mobile Geräte und das Internet zur Verfügung stellen.

Verwaltung Ihrer Vermögenswerte mit Active Directory von Azure

Azure Active Directory (AD) ist eine allgemeine Lösung für die Zugangs- und Identitätsverwaltung. Sie unterstützt zahlreiche Funktionen, mit denen Sie den Zugriff auf die Cloud sowie Ressourcen und Anwendungen innerhalb des Unternehmens überwachen können. Dazu gehören unter anderem verschiedene Online-Services von Microsoft, beispielsweise Office 365, außerdem zahlreiche SaaS-Anwendungen, die nicht von Microsoft stammen.

Eine der wichtigsten Funktionen von Azure AD ist, dass Sie den Zugriff auf seine Ressourcen steuern können. Diese Ressourcen können außerhalb des Verzeichnisses liegen, wie beispielsweise SaaS-Anwendungen (Software as a Service), es kann sich um Ressourcen innerhalb des Unternehmens oder um SharePoint-Sites handeln, ebenso wie um Azure-Services. Sie können aber auch intern im Verzeichnis vorliegen, wie beispielsweise die Zugriffsberechtigungen durch Verzeichnisrollen.

Kapitel 11

IBM Bluemix

IN DIESEM KAPITEL

- Blockchain-Apps mit künstlicher Intelligenz
- Ihr IBM Fabric erstellen
- Smart Contracts erstellen
- Eine IoT-Lösung bereitstellen

In diesem Kapitel stelle ich Ihnen die Blockchain-Initiativen von IBM vor, die das Unternehmen mit seinen anderen bahnbrechenden Technologien kombiniert. Dazu gehören etwa Bluemix, eine vollständigen PaaS (Platform as a Service) für die Anwendungsentwicklung, und der Supercomputer Watson.

Die Blockchain-Technologie sorgt für einen nahezu reibungslosen Werteaustausch. Künstliche Intelligenz beschleunigt die Analyse riesiger Datenmengen. Die Kombination der beiden Funktionen bewirkt einen Paradigmenwechsel, der sich auf unser Art, Geschäfte zu machen, und auf die Absicherung unserer vernetzten elektronischen Geräte auswirken kann.

Wenn Sie mit dem Internet der Dinge (Internet of Things, IoT) zu tun haben, im Gesundheitswesen tätig sind oder in der Lager-, Transport- oder Logistikbranche angehören, werden Sie von den Informationen in diesem Kapitel profitieren. Aber auch für Unternehmer, der mehr über die neuen Funktionen durch die Integration von künstlicher Intelligenz (KI) und Blockchains auf einer skalierbaren App-Plattform erfahren möchten, ist dieses Kapitel gut geeignet.

Unternehmens-Blockchains auf Bluemix

IBM bietet heute eine Blockchain-Technologie an, die sich in die traditionellen Angebote des Unternehmens einfügt, wie beispielsweise IBM Bluemix. Bluemix ist ein cloudbasierter PaaS mit offenem Standard zur Erstellung und Verwaltung von Anwendungen. IBM hat einen Blockchain-Stack aus Hyperledger integriert, das Teil der Linux Foundation ist und Best Practices für die Blockchain-Technologie einrichtet.

Sie sollten sich auf schnelle und maßgebliche Änderungen innerhalb der Blockchain-Initiativen von IBM vorbereiten. Die Technologie ist sehr neu und befindet sich noch in Entwicklung – sowohl bei IBM als auch bei Hyperledger.

Hyperledger entwickelt gerade mehrere Unterprojekte. Zum Zeitpunkt der Drucklegung dieses Buchs verwendet IBM Fabric, könnte Bluemix aber auch für andere Projekte öffnen. Fabric ist Open Source und wird in Hyperledger aktiv weiterentwickelt

Sie können Fabric auf Bluemix mit Hyperledger Fabric v0.6 testen. IBM warnt allerdings davor, Werttransaktionen direkt auf Fabric v0.6 oder früheren Versionen auszuführen.

Ihre isolierte Umgebung

Bluemix ist das neueste Cloud-Angebot von IBM. Es handelt sich dabei um eine Implementierung der offenen Cloud-Architektur von IBM auf Basis von Cloud Foundry, einer Open-Source PaaS.

Mit Bluemix können Sie schnell und einfach Anwendungen erstellen, bereitstellen und verwalten. Bluemix bietet Services der Enterprise-Klasse, die sich ohne besondere Installation oder Konfiguration in Anwendungen einfügen.

Abbildung 11.1 zeigt, wie IBM unterschiedliche Aspekte von Blockchains und IBM-Systemen verknüpft. Weitere Informationen finden Sie unter https://goo.gl/12Q6no.

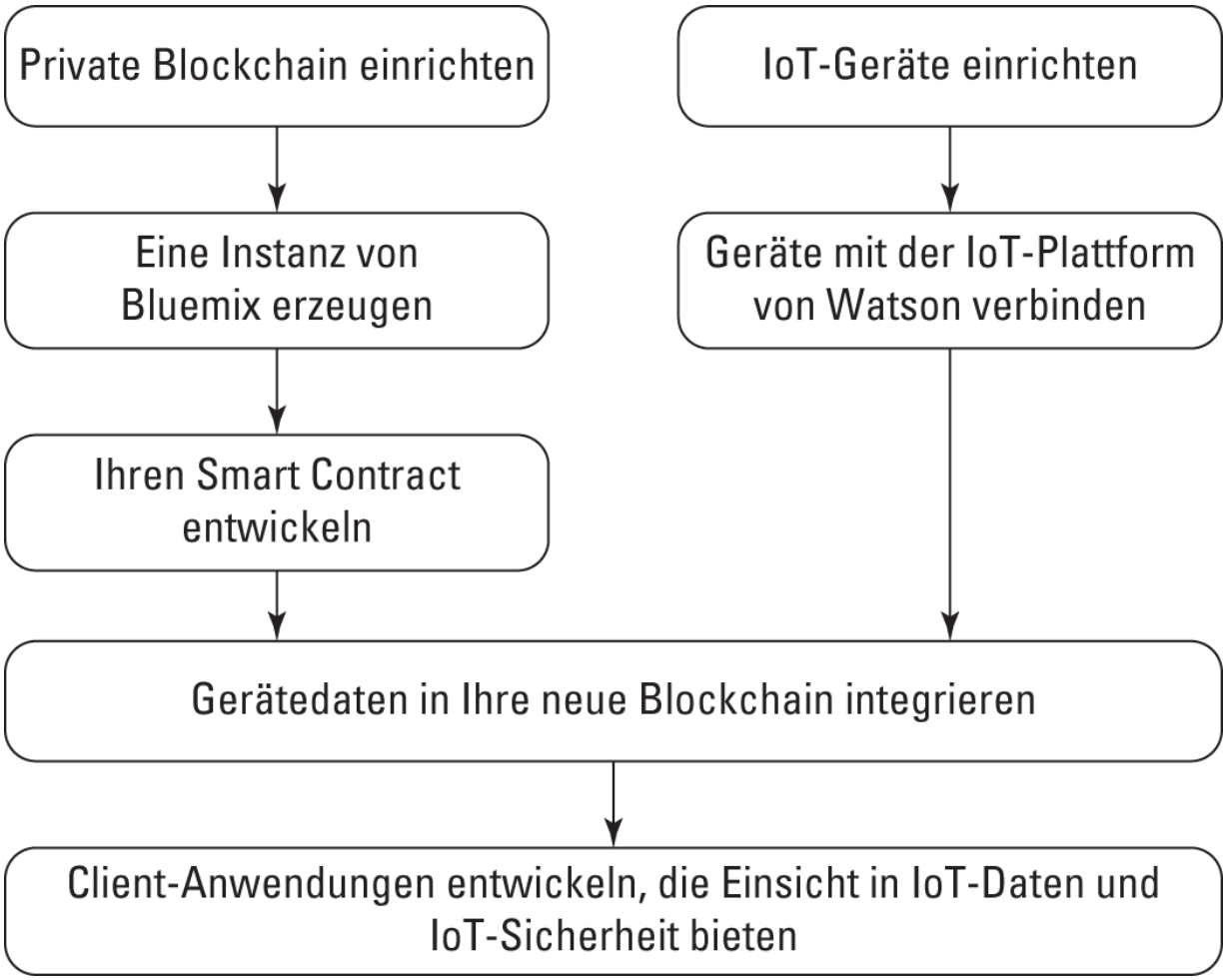


Abbildung 11.1: Wie IBM Bluemix und IoT mit IBM Watson kombiniert werden

IBM Bluemix bietet vier wichtige Dinge:

- ✔ Recheninfrastruktur auf Basis der architektonischen Anforderungen Ihrer Apps,
- ✔ die Möglichkeit, Apps in einer öffentlichen oder spezifischen Bluemix-Cloud bereitzustellen,
- ✔ Entwicklungstools, wie beispielsweise Codeeditoren und -verwaltungssysteme,
- ✔ Zugriff auf Open-Source-Tools von Drittanbietern im Servicebereich.

Bluemix gibt Ihnen alles an die Hand, was Sie für die Entwicklung Ihrer App benötigen. Mittlerweile bietet es auch eine Blockchain-

Infrastruktur zum Testen an.

Es gibt einen Service für die Integration Ihrer Anwendungen in die Bluemix-Blockchain. Derzeit existieren zwei Preismodelle. Mit einem kostenlosen Zugang bekommen Sie alles, was Sie zum Testen Ihrer Idee benötigen. Sie erhalten vier Peers und eine Zertifizierungsautorität, um Transaktionen zu signieren, weiterhin ein Dashboard mit Protokollen, Kontrollen und APIs.

Der Unternehmenstarif beträgt 10.000 US-Dollar pro Monat und bietet eine höhere Sicherheit und Geschwindigkeit als das kostenlose Modell.

Anwendungsfälle für Bluemix

Zwei bemerkenswerte Unternehmenspioniere verwenden Bluemix und die Integration von Hyperledger Fabric:

- **Wanxiang:** Wanxiang, der größte chinesische Automobilteilezulieferer, realisiert mithilfe von IBM eine private Blockchain. Er verankern Eigentumsrechte etwa in Elektroautos. Ziel ist es, die Leasingkosten für Kunden zu senken. Wanxiang verwendet die Blockchain-Technologie, um die Lebensdauer von Komponenten nachzuverfolgen und gebrauchte Batterien aufzubereiten. Bluemix kümmert sich um den Rest.
- **KYCK!:** Das Finanztechnologie-Start-up KYCK! nutzt die Blockchain-Integration von IBM als neue Herangehensweise an die KYC-Anforderungen (*Know Your Customer*) für Maklergeschäfte. Diese erfordern einen hohen Aufwand von Banken und anderen Finanzdienstleistern. KYC soll Geldwäsche und illegalen Handel eindämmen und den Terrorismus bekämpfen. KYCK! baut eine Plattform für Videokonferenzen und verschlüsselte Dokumentenübertragungen, die es den Brokern erlaubt, mit Kunden zusammenzuarbeiten und diese zu authentifizieren, obwoh das Unternehmen diese noch nicht persönlich getroffen hat.

IBM hat außerdem drei einfache Chaincode-Anwendungen erstellt, mit denen Sie mit dem IBM-Blockchain-Netzwerk experimentieren können:

- **Marbles:** Marbles ist eine Anwendung, die zeigt, wie Murmeln zwischen zwei Benutzern übertragen werden. Dies demonstriert, wie Sie Vermögenswerte auf einer Blockchain transferieren können.
- **Commercial Paper:** Commercial Paper ist ein Blockchain-Handelsnetzwerk auf Basis der IBM-Blockchain. Sie können neue Handelspapiere anlegen, vorhandene Handelspapiere kaufen und verkaufen und das Netzwerk überprüfen.
- **Car Lease:** Car Lease ist der Marbles-Demo sehr ähnlich. Hier haben Sie die Möglichkeit, mit Vermögenswerten zu interagieren. Sie können Vermögenswerte erstellen, aktualisieren und übertragen. Außerdem können Drittparteien den Verlauf einsehen.

Die intelligente Watson-Blockchain

Watson, der Supercomputer von IBM, steht ebenfalls auf der Bluemix-Plattform zur Verfügung. Watson ist ein kognitiv arbeitendes Computersystem mit künstlicher Intelligenz. Er kann strukturierte und – was besonders eindrucksvoll ist – unstrukturierte Daten mit einer unglaublichen Geschwindigkeit analysieren.

Diese Technologie befindet sich noch in der Entwicklungsphase, und manche Kunden haben sich darüber beschwert, dass sie keine unstrukturierte schriftliche Sprache versteht.

Watson kann Fragen beantworten, die ihm in natürlicher Sprache gestellt werden, und lernt dabei immer weiter, indem er weitere

Informationen aufnimmt. Die Kombination dieser Technologie mit der Blockchain-Technologie ist erstaunlich. Eine der ersten Implementierungen gab es im IoT-Bereich. Es besteht ein großer Bedarf, von diesen Geräten erzeugte Daten zu sichern und sie in intelligente Handlungen umzusetzen.

Die kognitive Programmierung von Watson simuliert menschliche Denkprozesse und nutzt das MQTT-Protokoll. Wie ein menschliches Gehirn wächst sie mit der Zeit. Die selbstlernenden Systeme verwenden Data Mining, Mustererkennung und Sprachverarbeitung, um die Arbeitsweise des menschlichen Gehirns nachzubilden. Watson arbeitet mit einer Geschwindigkeit von 80 Teraflops pro Sekunde (ein Teraflop sind eine Billion Fließkommaoperationen). Zum Vergleich: Dies entspricht der Fähigkeit eines sehr intelligenten Menschen, Fragen zu beantworten – und übertrifft sie bisweilen. Watson greift dazu auf 90 Server mit einem kombinierten Datenspeicher von mehr als 200 Millionen Seiten mit Informationen zu, die er anhand von sechs Millionen Logikregeln verarbeitet. Watson hat etwa die Größe von zehn Kühlschränken, wird jedoch immer kleiner und schneller.

Abbildung 11.2 zeigt, wie IBM Watson unterschiedliche Aspekte von Blockchains und IBM-Systemen verknüpft. Weitere Informationen erhalten Sie von IBM unter https://goo.gl/12Q6no.

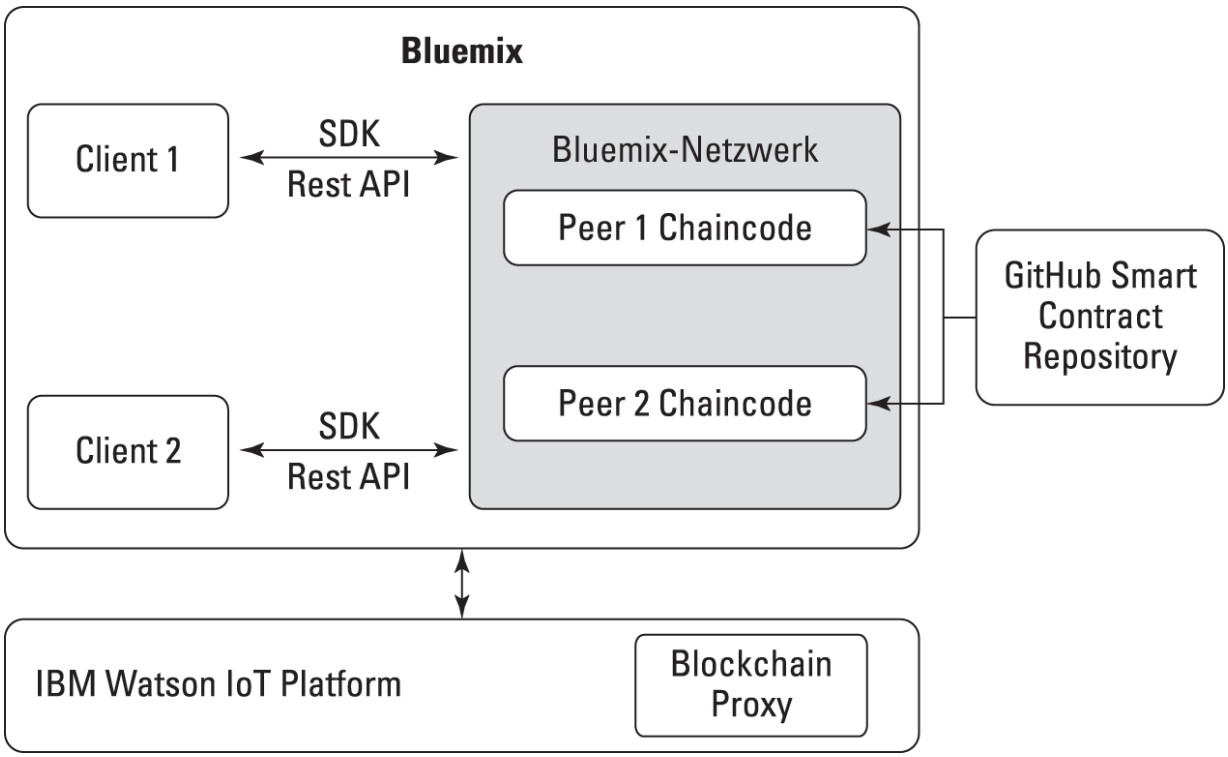


Abbildung 11.2: Wie Bluemix Clients, Peers und IBM Watson integriert

IBM wendet diese Analysefähigkeiten auf IoT-Datenfeeds an, die eine Chaincode-Implementierung verwenden. Chaincode ist das Smart-Contract-System von Hyperledger. Und so funktioniert die watsonfähige Blockchain für IoT-Geräte:

- ✔ IoT-Geräte senden Daten an Ihre privaten Blockchain-Ledger, um sie als fälschungssicheren Datensatz mit Zeitstempel aufzunehmen.
- ✔ Partner und externe Serviceanbieter können ebenfalls IoT-Daten auslesen und bereitstellen, ohne dass eine zentrale Kontrolle oder eine Verwaltung erforderlich ist.
- ✔ Alle Parteien können Daten signieren und überprüfen. Dadurch werden Streitigkeiten begrenzt, und es wird sichergestellt, dass jeder Partner seine individuelle Leistung verantworten muss.

Dies ist eine einfache Implementierung, die nicht die gesamte Funktionalität von Watson nutzt. Die Fähigkeit von Watson, zu

lernen und Vorschläge zu machen sowie veraltete Informationen zu aktualisieren, wird in der Zukunft eine leistungsstarke blockchainfähige Anwendung daraus machen.

Sie können die IoT-Plattform von Watson in Hyperledgers Fabric integrieren. Mit dieser Integration können Sie Chaincode-Verträge durch KI-gestützte Orakel ausführen. Die IoT-Plattform von Watson besitzt eine eingebaute Funktion, mit der Sie Ihrer eigenen privaten Blockchain ausgewählte IoT-Daten hinzufügen können, um ein Orakel zu erzeugen. Auf diese Weise können Sie verhindern, dass unberechtigte Dritte Ihre Daten sehen.

Wenn Sie einen Bluemix-Arbeitsbereich eingerichtet haben, können Sie ausgewählte Services hinzufügen, wie beispielsweise die IoT-Plattform, die mehrere Technologien beinhaltet. Fabric ist die Blockchain-Technologie, die die private Blockchain-Infrastruktur für verteilte Peers bereitstellt, die Gerätedaten repliziert und die Transaktionen durch sichere Verträge überprüft.

Die IoT-Plattform von Watson übersetzt vorhandene Gerätedaten von einem oder mehreren Gerätetypen in das Format, das die Smart-Contract-APIs benötigen. Sie filtert irrelevante Gerätedaten aus und sendet nur die benötigten Daten an den Contract. Abbildung 11.3 zeigt, wie IBM Watson in IoT-Geräte und APIs integriert wird. Watson fungiert als Chaincode-Orakel und lässt Sie entscheiden, welche Informationen den am Smart Contract beteiligten Parteien bekannt sein sollen. Diese Funktionalität ist wichtig für den Datenschutz.

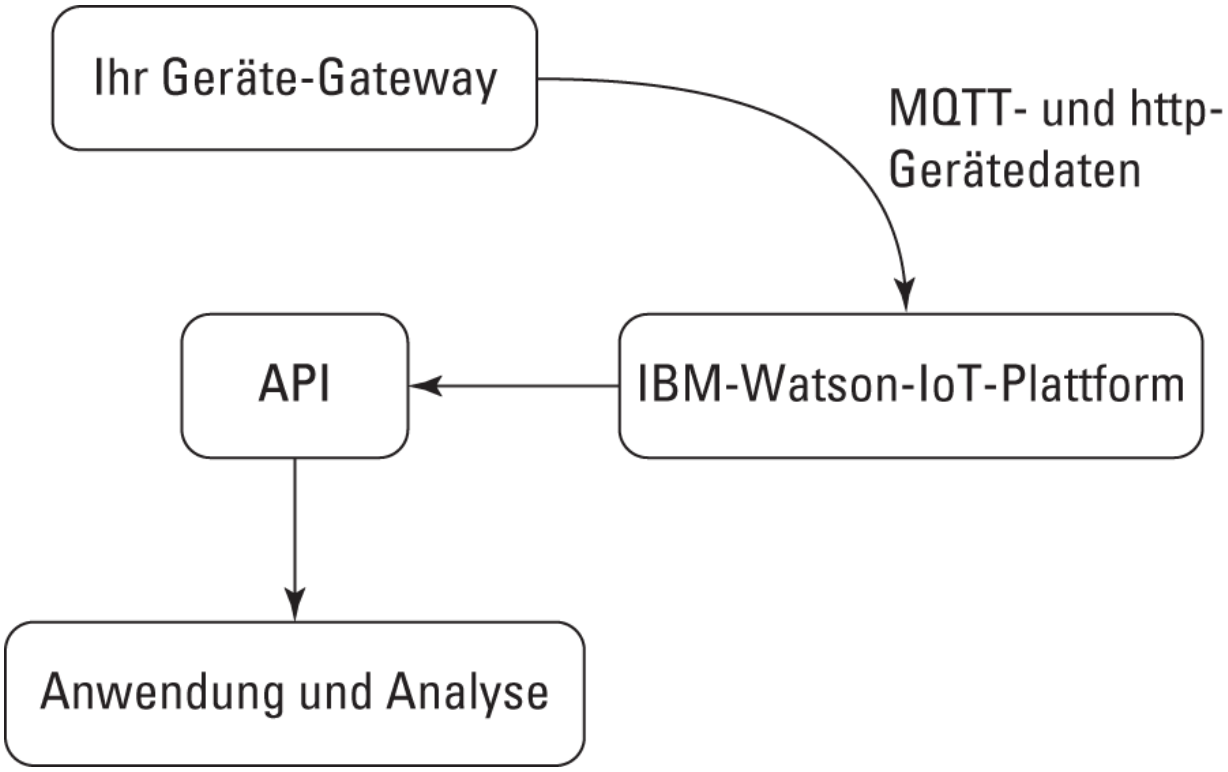


Abbildung 11.3: Der Watson/API/Gerät-Ablauf

Ihr erstes Netzwerk auf Big Blue

Die Blockchain-Technologie von IBM und die IoT-Plattform bieten neue, vielversprechende Tools. Sie können für viele Problemstellungen eingesetzt werden, denen Unternehmen bei der Skalierung gegenüberstehen:

- **Sicherheit:** Das riesige Datenvolumen, das von Millionen Geräten erfasst wird, führt zu datenschutzrechtlichen Bedenken. Gehackte IoT-Geräte wurden bereits von böswilligen Organisationen verwendet, um Websites mit DDoS-Angriffen zu überziehen.
- **Kosten:** Das hohe Nachrichtenvolumen, die von den Geräten erzeugte Datenmenge sowie analytische Prozesse nehmen zu, je mehr Geräte online gehen und diese Daten nutzen.

- ✔ **Architektur:** Zentrale Cloud-Plattformen bleiben ein Flaschenhals und zentraler Angriffspunkt von Ende-zu-Ende-IoT-Lösungen.

Die auf offenen Standards basierenden IoT-Netzwerke von IBM können viele der Probleme lösen, die zentralisierten, cloudbasierten IoT-Lösungen von heute zugeordnet werden. Vernetzte Geräte kommunizieren direkt mit dezentralen Ledgern. Die Daten dieser Geräte werden dann von Dritten verwendet, um Smart Contracts auszuführen, was die Notwendigkeit einer menschlichen Überwachung reduziert.

Die IBM-Watson-IoT-Plattform mit Fabric-Integration repliziert Daten über ein privates Blockchain-Netzwerk. Es müssen daher nicht mehr sämtliche IoT-Daten zentral erfasst und gespeichert werden. Dezentrale Blockchain-Netzwerke verbessern zudem die Sicherheit von IoT-Gräten. Im Laufe der Zeit erhält jedes Gerät eine eindeutige digitale Identität, die extrem schwer zu fälschen ist.

Dank dieser neuen Blockchain-Identitäten können IoT-Geräte Transaktionen signieren, die die Ausführung von Smart Contracts ermöglichen. Eine praktische Anwendung wäre etwa ein Versicherungsprodukt, das von einem Smart Car mit Daten über das Fahrverhalten verschiedener Personen gespeist wird. Das Auto würde Daten senden, die in Fabric veröffentlicht werden. Das Chaincode-basierte Versicherungsprodukt würde die neuen Daten und die Identität Ihres Autos erkennen und Ihre Police aktualisieren.

Es gibt unzählige Möglichkeiten. Das IoT hat interessante Gelegenheiten für Unternehmen und Verbraucher mit sich gebracht, besonders in den Bereichen Gesundheitswesen, Lagerhaltung, Transport und Logistik.

Die cloudgestützten IoT-Lösungen von IBM haben drei Hauptebenen, die verschiedene Probleme im Umgang mit IoT lösen:

- ✔ **Device Gateway:** Das Device Gateway ist für intelligente Geräte oder Sensoren vorgesehen, die Daten über die physische Welt sammeln. Dabei kann es sich etwa um Wettersensoren, eine Temperaturüberwachung für Kühlcontainer oder Gesundheitsdaten eines Patienten handeln. Diese IoT-Geräte versenden ihre Daten über das Internet zur Analyse und Verarbeitung.
- ✔ **IBM-Watson-IoT-Plattform:** IBM kombiniert seinen Supercomputer und seine IoT-Plattform, um Daten von IoT-Geräten zu erfassen, die Daten anschließend zu analysieren und nachfolgend Maßnahmen zur Problemlösung zu ergreifen. Watson unterstützt maschinelles Lernen, maschinelle Beweisführung, Sprachverarbeitung und Bildanalyse. All dies trägt zur besseren Verarbeitung der unstrukturierten Sensordaten bei.
- ✔ **IBM Bluemix:** Bluemix ist eine auf offenen Standards basierende Cloud-Plattform zur Erstellung, Ausführung und Verwaltung von Anwendungen und Diensten. Sie unterstützt IoT-Anwendungen, indem sie die Einbindung analytischer und kognitiver Funktionen in diese Anwendungen vereinfacht.

Mehr über die IBM-Lösung erfahren Sie auf https://developer.ibm.com/technologies/blockchain.

Teil IV

Auswirkungen auf die Wirtschaft

IN DIESEM TEIL …

Erfahren Sie, wie Finanzdienstleister in Zukunft per Blockchain-Technologie schnell und kostengünstig weltweit Geld übertragen werden.

Erweitern Sie Ihr Wissen über den globalen Immobilienmarkt in Bezug auf Blockchain-Technologie.

Erkennen Sie Chancen in der Versicherungsbranche, durch neue Instrumente Betrug zu erschweren und Gewinne zu steigern.

Untersuchen Sie die Auswirkungen auf Regierungsstellen und Rechtsordnungen.

Klären Sie andere globale Trends in der Blockchain-Technologie und wie diese die Welt, in der Sie leben, und Ihre im Alltag genutzten Tools verändern werden.

Kapitel 12

Finanztechnologie

IN DIESEM KAPITEL

- Weltweite Banking-Trends der Zukunft entdecken
- Neue Investitionsinstrumente kennenlernen
- Risiken in der Banking-Blockchain erkennen
- Neue Finanzierungsstrategien entwickeln

Banken, Regierungsstellen und andere Finanzeinrichtungen entdeckten die Blockchain-Technologie für sich als Erstes, und entsprechend nimmt die Anzahl der Blockchain-Benutzer in diesen Bereichen auch am schnellsten zu. Die leistungsstarken Tools zur Verwaltung und zum Transfer von Geldern werden unsere Welt auf neue und unerwartete Weise verändern. Es ist also kaum verwunderlich, dass die Fintech-Branche auf den Zug aufspringt.

Dieses Kapitel zeigt, was die Regierungen derzeit im Hinblick auf die Blockchain-Technologie unternehmen und wie sich dies auf Sie auswirkt. Sie kommen täglich mit Finanztechnologie in Berührung – bewusst oder unbewusst.

In diesem Kapitel stelle ich Ihnen Banking-Trends der Zukunft vor, neue Vorschriften sowie die neuen Tools, mit denen Sie Ihr Geld schneller und kostengünstiger transferieren können. Außerdem erkläre ich neue Investmentinstrumente und andere Blockchain-Innovationen. Abschließend warne ich Sie vor potenziellen Risiken bei Investitionen mit virtuellen Währungen und neuen, blockchainbasierten Fintech-Produkten.

Holen wir die Kristallkugel heraus: Banking-Trends der Zukunft

Das Bankwesen erkannte als erste Branche die Bedrohung durch Bitcoin – und kurze Zeit später auch das Potenzial von Blockchains, die Branche umzugestalten. Der Bankensektor wird streng reguliert, und die Kosten für die Gründung und den laufenden Betrieb einer Bank sind enorm. Die strengen Vorschriften dienten der gesamten Branche schon immer als Schutzschild, aber sie waren auch eine schwere Last. Der Einsatz von schnellem, effizientem, digitalem Geld, das nicht die Kosten von Bargeld verursacht und auf seinem gesamten Weg durch das Finanzsystem nachverfolgbar ist, war eine faszinierende und zugleich bedrohliche Vorstellung. Das Konzept, dass sich Werte der Kontrolle zentraler Obrigkeiten entziehen, hat außerdem auch Finanzeinrichtungen und staatliche Stellen aufmerksam werden lassen, die sich auf Fiat-Währungen stützen.

Anfänglich versuchten Finanzeinrichtungen und Regierungen daher, Blockchains durch Vorschriften zu klein zu halten. Heute sind sie alle begeistert von Blockchains und investieren in diesen Bereich.

2013 und 2014 sprach die US-amerikanische Securities and Exchange Commission (SEC) eine Warnung an Investoren zu den potenziellen Risiken bei Investitionen mit virtueller Währung aus. Die Warnung bezog sich darauf, dass Investoren aufgrund der hohen Renditeversprechungen vielleicht nicht skeptisch genug an das neue Investitionsfeld herangingen, für das es noch keine Erfahrungswerte gab. Laut SEC gehörten digitale Währungen zu den zehn größten Bedrohungen für Investoren. Heute unterstützt die SEC Unternehmen und Investoren, nachdem die Kryptowährung in allen Branchen Fuß gefasst hat.

Nicht einmal zwei Jahre später begannen Länder auf der ganzen Welt, einschließlich Großbritannien, Kanada, Australien, Japan und China, zu untersuchen, wie sie ihre eigenen digitalen Währungen ausgeben könnten. Sie wollten selbst Kryptowährungen nutzen und Geld in die Blockchain übertragen. 2018 führte Venezuela eine eigene Kryptowährung namens Petro ein. Dies ist ein bezeichnender Wendepunkt im Kryptobereich. Erstmals hatte damit ein souveräner Staat eine eigene Kryptowährung herausgegeben. Das Bitcoin-Versprechen eines unveränderbaren Kontobuchs machte das System auch für Staaten attraktiv, die Betrug reduzieren und die Vertrauenswürdigkeit erhöhen wollten. Durch Innovationen in der Blockchain-Technologie schien es möglich zu werden, eine hohe Transaktionsanzahl im Milliardenbereich zu erreichen, sodass die Kryptowährung auch für den größeren Maßstab geeignet wurde.

Blockchains zeichnen alle darin festgehaltenen Transaktionen dauerhaft und unveränderbar auf. Die Geldmenge eines Landes in eine von der Zentralbank kontrollierte Blockchain zu übertragen, wäre eine riesige Veränderung, weil damit irgendwo in den Blockchain-Aufzeichnungen eine permanente Aufzeichnung aller Finanztransaktionen vorläge, selbst wenn diese für die Öffentlichkeit vielleicht nicht einsehbar wäre. Die Blockchain-Technologie und digitale Währungen würden das Risiko und die Betrugswahrscheinlichkeit senken und eine ultimative Kontrolle über die Geldpolitik und das Steuerwesen ermöglichen. die Bloclchain wäre überhaupt nicht mehr anonym wie Bitcoin zu Anfang, vielmehr wäre das Gegenteil der Fall: Sie würde eine vollständige und überprüfbare Aufzeichnung aller digitalen Transaktionen von Einzelpersonen und Unternehmen schaffen. Auf diese Weise könnten Zentralbanken sogar die Rolle der Geschäftsbanken bei der Geldausgabe übernehmen.

Die Zukunft des Bankwesens kann aus heutiges Sicht spannend und unheimlich zugleich wirken. Endanwender können ihren Freunden fast unmittelbar und in jeder Währung oder Kryptowährung Geld per Mobiltelefon schicken. Auch immer mehr Einzelhändler akzeptieren Kryptowährungen für ihr

Warensortiment. In Kenia wäre es fast schon ungewöhnlich, ohne Kryptowährung zu bezahlen. Aber so weit sind wir heute noch nicht. Die westlichen Märkte sind noch in einer sehr frühen Nutzungsphase.

Das Vermögen der meisten Menschen steckt in von Regierungen gestützten gesetzlichen Zahlungsmitteln oder in Vermögenswerten, die dem Rechtssystem dieser Regierungen unterliegen. Fintech-Innovationen müssten daher nahtlos mit diesen vorhandenen Systemen verzahnt werden, ehe Blockchains oder digitale Währungen ganz selbstverständlich genutzt werden können. Wenn die Gesetzgeber Regeln und Methoden zur Besteuerung und Registrierung von Konten finden, ist innerhalb von zwei bis drei Jahren mit der großflächigen Verbreitung von Kunden-Wallets für digitale Token zu rechnen.

Im B2B-Markt werden sich Blockchains schon sehr viel früher durchsetzen. Ein produktionsreifes, ausreichend geschütztes System mit entsprechenden Richtlinien und Operationen wird bereits getestet: Die Unternehmen Ripple und R3 haben zusammen mit vielen anderen hart an einer entsprechenden Umsetzung gearbeitet. Das System konzentriert sich zunächst darauf, Finanzinstituten die Darstellung von Werteinlagen durch digitale Token zu ermöglichen, also IOUs (Schuldverschreibungen) zwischen internen Kostenstellen und vertrauenswürdigen Partnern, wie etwa Lieferanten. Regulierungsbehörden, Zentralbanken und Währungshüter investieren viel, um dies zu ermöglichen. Sehr schnell haben Kanada und Singapur gehandelt.

KYC-Vorschriften (Know Your Customer) und Gesetze zur Prävention von Geldwäsche fordern von den Banken, dass sie ihre Geschäftspartner überprüfen und sicherstellen, dass sie nicht in Geldwäsche oder Terrorismus verwickelt werden. Banken, die Kryptowährungen ausgeben wollen, müssen vorher beträchtliche Hürden überwinden. Um den KYC- und Geldwäschevorschriften zu entsprechen, müssen sie die Identität aller Einzelpersonen kennen, die ihre Währung verwenden. Häufig unterstützen Bankkonten bereits Aus- und Einzahlungsfunktionen für

Transaktionen, so wie dezentrale Ledger in Blockchains, aber sie sind natürlich zentralisiert. Die ersten Kandidaten in diesem Bereich werden Regionen sein, deren Gesetzgeber, Banken und Zentralbanken bereits zusammenarbeiten. Singapur und Dubai mit ihren Blockchain-Initiativen stehen dabei an erster Stelle.

Geld schneller und über Grenzen hinweg bewegen

Das Transaktionsvolumen, das eine Blockchain zum Umschlag der Währung einer gesamten Volkswirtschaft wie der Großbritanniens oder der USA bewältigen muss, ist schwer abzuschätzen. In den USA allein fallen täglich Milliarden von Transaktionen mit einem Wert von über 17 Billionen US-Dollar pro Jahr an. Das ist eine riesige Verantwortung für eine neue Technologie! Das Land wäre ruiniert, wenn die gesamte verfügbare Geldmenge verloren ginge.

Der Internationale Währungsfonds, die Weltbank, die Bank für Internationalen Zahlungsausgleich und Zentralbanker aus der ganzen Welt sind zusammengekommen, um die Blockchain-Technologie zu diskutieren. Der erste Schritt zu schnellerem und billigerem Geld wäre, ein Blockchain-Protokoll für Banküberweisungen und den Interbankenzahlungsausgleich einzusetzen und diese damit zu vereinfachen. Offizielle digitale Währungen, die ganz normale Bürger im Alltag nutzen können, würden sehr viel später eingeführt.

Die einzelnen Verbraucher würden die Kostensenkung durch die Verwendung einer Blockchain für den Interbankenzahlungsausgleich nicht direkt wahrnehmen. Die Einsparungen würden sich in den Bankbilanzen als Kostenreduzierung für Gebühren von Vermittlungsinstanzen niederschlagen.

Die Mehrzahl der Verbraucher wünscht sich auch in absehbarer Zukunft noch Bankfilialen und Geschäftsbanken. Die Millenials der Generation Y akzeptieren dagegen bereits vollumfänglich appgestützte Zahlungsweisen wie PayPal, Venmo, Cash und

weitere. Eine neue Zahlungsmethode über ihre Smartphones würde sie nicht beunruhigen.

Wenn das gesamte Geld digitalisiert ist, kann ein Angriff katastrophale Folgen haben. Dies ist die große Herausforderung. Auch wenn die Architektur von Blockchain-Systemen stark genug ist, besteht vielleicht immer noch die Gefahr, dass der Code im System auf unerwartete Weise ausgeführt wird, wie im Hacker-Angriff auf The DAO (dezentrale autonome Organisation) im Ethereum-Netzwerk (siehe Kapitel 5). Würde die Kryptowährung auf einer traditionellen öffentlichen Blockchain liegen, müssten sich 51 Prozent der Knoten im Netzwerk darauf einigen, das Problem zu beheben. Eine solche Einigung könnte sehr lange dauern und wäre nicht praktikabel für Unternehmen und Einzelpersonen, die zu jeder Zeit stabiles und sicheres Geld brauchen.


Viele Blockchains funktionieren wie Demokratien. Eine Mehrheit (51 Prozent) der Knoten einer Blockchain werden benötigt, um eine Änderung vorzunehmen.

Einen permanenten Verlauf erstellen

Die Datenhoheit und der Schutz privater Daten werden in Zukunft große Themen sein. Betrügereien sind einfacher zu verhindern, denn wenn die gesamte Wirtschaft eine Kryptowährung verwendet, gibt es immer eine nachvollziehbare Aufzeichnung in der Blockchain, die die Währung absichert. Für Vollzugsbehörden ist das wundervoll, für Datenschützer jedoch ein Alptraum.

Aus Kundensicht gibt es bereits eine Aufzeichnung aller Käufe, die mit Kredit- oder EC-Karte getätigt werden. Institutionen profitieren von nachverfolgbaren Aufzeichnungen, weil sie die Transparenz und den Asset-Lebenszyklus verbessern, dem Handel mit Anlagevermögen mehr Legitimität verleihen und den Konformitätsnachweis der täglichen Transaktionen ermöglichen.

Die europäischen Gesetze im Hinblick auf das »Recht auf Vergessenwerden«, die den Bürgern das Recht einräumen, dass

ihre Daten nicht ewig im Internet weitergegeben werden dürfen, sind eine schwierige Herausforderung für Blockchains, denn Blockchains vergessen nie. Regierungen und öffentliche Verwaltungen hätten dauerhafte Verlaufsaufzeichnungen über alle Transaktionen, was sich verheerend auf die nationale Sicherheit auswirken könnte, wenn sie der Öffentlichkeit zugänglich würden. Im Falle von Unternehmen könnten deren Wettbewerber zum Beispiel herausfinden, in was sie investieren.

Die größte Herausforderung beim Einsatz einer öffentlichen Blockchain wie Ethereum oder Bitcoin wäre zu garantieren, dass kein Geld an ein OFAC-Land gesendet wird, um den Terrorismus nicht zu unterstützen. Das ist unmöglich, weil diese Blockchains anonym sind und jeder eine Wallet einrichten kann. Es ist möglich, Algorithmen zur Überwachung von Transaktionsbewegungen zu erstellen – die US-Regierung tut dies seit Jahren –, aber in einer berechtigungsfreien Welt kann jeder Werte an eine beliebige Stelle verschieben.

Das US-amerikanische Office of Foreign Asset Control (Amt für Kontrolle von Auslandsvermögen, OFAC) verhängt Sanktionen für bestimmte Unternehmen oder Einzelpersonen, die aus Ländern kommen, von denen man eine starke Bedrohung vermutet. Die Regierung kann den Transaktionsverlauf letztlich nicht bis zum Empfänger nachverfolgen, wenn berechtigungsfreie Plattformen anonym eingesetzt werden.

Die Notwendigkeit, KYC- und Geldwäschevorschriften zu erfüllen, spricht für Permissioned Blockchains. Das Softwareunternehmen R3 hat Corda entwickelt, eine private und mit Berechtigungen arbeitende, blockchainähnliche Plattform, die viele dieser Herausforderungen erfüllt. Insbesondere werden die Daten der Teilnehmer nicht weltweit übertragen. Die Daten in der Corda-Blockchain bleiben also unter Verschluss. Das war eine der wichtigsten Grundanforderungen der über 75 Banken, die zur Einführung der Blockchain-Technologie mit R3 zusammengearbeitet haben. Datensicherheit ist für sie sehr

wichtig, und sie müssen sich an strenge gesetzliche Vorschriften einhalten.

Es wird international: Globale Finanzprodukte

Blockchains werden zu vielen neuen Wertpapieren und Investmentprodukten führen. Es werden neue Märkte mit effizienteren Methoden zur Risikoberechnung entstehen, weil Kreditsicherheiten über Institutionen hinweg sehr viel transparenter und fungibler werden, wenn sie in einem Blockchain-System nachgewiesen werden können.

Es gibt auch Blockchain-Anwendungen, um Betrügereien im weltweiten Warenverkehr durch mehrfach verkaufte Waren einzudämmen. Anhand von Blockchain-Einträgen können Hersteller und Regulierungsbehörden die Herkunft von Produkten zweifelsfrei dokumentieren. Käufer können wiederum die Authentizität der gekauften Waren verifizieren. Dazu sind bereits mehrere Lösungen auf dem Markt, wie etwa Everledger und Provenance.

Hernando de Soto, der berühmte Wirtschaftswissenschaftler aus Peru, schätzt, dass 9,3 Billionen US-Dollar an Vermögenswerten erschlossen würden, wenn die Armen der Welt Eigentumsrechte für ihr Land, ihr Heim und nicht registrierte Unternehmen erhielten. Dies ist das sogenannte *tote Kapital*.

Man stelle sich vor, dass Länder ihr totes Kapital freisetzen können, nämlich die Liegenschaften, die sie besitzen, die aber keine Rendite abwerfen. Sie könnten die Anteile an diesen Vermögenswerten zusammenfassen und auf einem globalen Marktplatz verkaufen. Dies wären praktisch transparente, hypothekenbesicherte Wertpapiere etwa für neue Immobilienprojekte in Kolumbien oder Peru.

In Zukunft werden Länder in der Lage sein, ihr totes Kapital zu erschließen. Die Eigentümer von Grundstücken, nicht-entwickeltem Land und Liegenschaften, die nichts abwerfen, werden dann die Möglichkeit bekommen, Anteile an diesem Anlagevermögen auf einem globalen Markt zu verkaufen.

Diese Vermögenswerte werden sehr attraktiv sein, weil Anlageverwalter dank der Transparenz der Blockchain aktiv nach erlösschwachen Assets suchen und diese durch solche mit besserer Performance ersetzen können. Dank der Blockchain-Technologie können Anlageverwalter stets erlösstarke Wertpapiere halten, »faule Äpfel« entfernen, sie neu klassifizieren und als neue Wertpapiere verkaufen.

Für Privatkunden sind Mikroinvestitionen eine attraktive Option, die durch Blockchain-Handelsplattformen global und lokal ermöglicht werden. Dank Blockchain-Technologie werden sie die Möglichkeit bekommen, auch ohne Mindesteinlage oder kostspielige Vermittler in Unternehmen und deren Aktivitäten zu investieren.

Es gibt bereits dezentrale autonome Organisationen (DAO), die einen DAO-Investitionspool für einige wenige risikotolerante und technisch bewanderte Investoren bilden. Es kann eine Weile dauern, bis ein institutionalisierter Investor einen solchen nutzt oder bis ein Portfolio-Manager seinen Kunden empfiehlt, Geld in ein auf DAOs basierendes Instrument zu stecken.

DAOs sparen bei Investitionen jede Menge Papierkram und Bürokratie ein, weil sie auf einem blockchaingestützen Abstimmungssystem basieren und Anteile an diejenigen ausgeben, die in ihr Produkt investieren. Eine Blockchain vergisst nichts, denn der Code gilt hier als Gesetz. Die Risiken sind vielfacher Natur, besonders bei nachlässig geschriebenem Code, der auf unbeabsichtigte Weise ausgeführt wird. Hacking-Angriffe auf solche Systeme können verheerend sein. Die Transparenz des Systems bietet Hackern bei mangelhafter Programmierung eine breitere Angriffsfläche und gestattet auch mehrfache

Angriffe, für die sie nach und nach immer mehr Informationen erhalten.

Im folgenden Abschnitt beschreibe ich die Wirkungen und Vorteile der Blockchain-Technologie auf die Weltwirtschaft.

Grenzüberschreitende Gehaltszahlungen

Unsere Welt ist globalisiert, und Unternehmen haben keine Grenzen. Sofortige und nahezu kostenlose Gehaltszahlungen klingen bestechend und würden Unternehmen viel Kopfzerbrechen ersparen. Es gibt jedoch auch Nachteile.

Das größte Risiko ist der Verlust von Geldern durch Hacker-Angriffe. Wenn Sie Ihr Gehalt in Kryptowährung ausgezahlt bekommen und gehackt werden, sehen Sie Ihr Geld nie wieder. Es gibt kein Gericht, vor dem Sie Klage einreichen könnten. Es gibt keinen Kundenservice, bei dem Sie sich beschweren könnten. Kryptodiebe können weltweit zuschlagen und bleiben anonym. Der Hacker könnte überall sitzen.

Die aktuelle Blockchain-Struktur überträgt die gesamte Sicherheitsverantwortung auf den Benutzer. Heutzutage liegt die Hauptlast, sich gegen einen Verlust zu schützen, nicht beim Kunden. Größere Unternehmen und Regierungsstellen sichern Verbraucher schon seit sehr langer Zeit ab. Durchschnittsbürger können auf diese Vorsichtsmaßnahmen verzichten, weil sie schon seit dem Mittelalter kein eigenes Gold mehr einlagern (okay, das gilt für die meisten).

Diese Probleme halten Unternehmen nicht davon ab, Gehaltszahlungen per Kryptowährung abzuwickeln. Bitwage und BitPay buhlen um Marktanteile für die Gehaltsabrechnung in Bitcoin. Mit Bitwage können Arbeitnehmer und Vertragsarbeiter einen Teil ihrer Arbeitsvergütung in Kryptowährung erhalten, auch wenn ihre Arbeitgeber diese Option nicht anbieten. BitPay dagegen integriert die Gehaltsabrechnungsdienstleister Zuman und Incoin in seine Zahlungs- und Gehaltsabrechnungs-APIs.

Und wieder: Die frühe Anwendung der Technologie findet vor allem dort statt, wo es bisher keine oder nur unzureichende Lösungen gab.

Schnellerer und besserer Handel

Blockchains vereinfachen einen schnelleren und möglicherweise auch inklusiveren Handel. Die globale Handelsfinanzierung wurde in den letzten Jahren beschnitten. Einige Banken, wie etwa Barclays, haben sich sogar aus den afrikanischen Wachstumsmärkten zurückgezogen. Sie hinterlassen ein Vakuum für die Handelsfinanzierung. Die Unternehmen benötigen nach wie vor Kapital für den Verkauf ihrer Waren.

DAOs und Mikroinvestitionen könnten diesen Bedarf decken und den Investoren gleichzeitig überdurchschnittliche Renditen verschaffen. Die Transparenz aller verkauften Warten, eine gesicherte Identität sowie die nahtlose weltweite Nachverfolgbarkeit in Verbindung mit einer Blockchain würde diese Chance für kleine Investoren eröffnen.

Die Interoperabilität von Währungen, die Unternehmen wie Ripple ermöglicht, stützt ebenfalls den Handel, weil sie flexiblere Methoden zur Berechnung von Wechselkursen bietet als herkömmliche Überweisungsmechanismen. Der Einzug populärerer Kyptowährungen in den Devisenverkehr wird die Anpassungsfähigkeit und die Integration unterversorgter Märkte befördern.

Das Unternehmen BitPesa wandelt kenianisches M-Pesa-Telefonguthaben in Bitcoin um. Mit dieser Technologie bietet es Geschäftstreibenden eine schnellere und kostengünstigere Möglichkeit, Zahlungen zwischen Afrika und China abzuwickeln. Das Handelsvolumen zwischen Afrika und China beträgt über 170 Milliarden US-Dollar im Jahr. Grenzüberschreitende Zahlungen dauern mehrere Tage und sind zudem sehr teuer. Beim Einsatz von BitPesa erfolgen die Zahlungen unmittelbar und sehr kostengünstig.

Garantierte Zahlungen

Durch Blockchain-Transaktionen garantierte Zahlungen werden den Handel auch dort vorantreiben, wo der Vertrauensvorschuss gering ist. Innerhalb dieser Systeme können ärmere Länder direkt mit reicheren Staaten in Konkurrenz treten. All dies wird in den nächsten zehn Jahren passieren und die Weltwirtschaft wird sich dabei verändern: Die Kosten für Güter und menschliche Arbeit werden möglicherweise steigen.

Globale Konzerne zahlen ihren Mitarbeitern konkurrenzfähige Gehälter, die auch von ihrem bisherigen Lohnniveau abhängen. Blockchains ermöglichen zwar Gleichberechtigung über wirtschaftliche Gefälle hinweg, aber dies wird nicht über Nacht passieren. Softwareentwickler und andere Wissensarbeiter sind hier die Ausnahme, weil es für sie leichter ist, mit anonymer Arbeit Geld zu verdienen.

Finanzielle Inklusion und ein gleichberechtigter Welthandel sind wichtige Themen für Regierungen. Der umfassende Übergang zu digitalen Währungen wird in kleinen Ländern und Schwellenländern wahrscheinlich schneller passieren. Die meisten großen Länder haben dezentrale Machtstrukturen, die schnelle Veränderungen an lebenswichtigen Systemen wie Geld verhindern.

Ihre zentralen Machtstrukturen ermöglichen es kleinen Ländern, herkömmliche Infrastruktur und Bürokratie einfach auszulassen. Beispielsweise gibt es in den meisten afrikanischen und südamerikanischen Ländern keine Festnetzanschlüsse oder Adressen, aber alle haben Smartphones und die Möglichkeit, Kryptowährungs-Wallets einzurichten. Das fehlende Teilstück sind ausreichend liquide Märkte und die Fähigkeit, mit Kryptowährungen für Grundbedürfnisse wie Energie, Miete und Lebensmittel zu bezahlen.

Mikrozahlungen: Die neue Transaktionsform

Mikrozahlungen sind eine neue Transaktionsform. Kreditkartenunternehmen könnten die Blockchain-Technologie einsetzen, um die Transaktion abzurechnen, Betrügereien zu reduzieren und ihre eigenen Kosten zu senken.

Globale Institutionen wie Visa und MasterCard, die den Vorteil eines späteren Zahlungsziels bieten, werden in kapitalistischen Gesellschaften von Verbrauchern immer benötigt. Auch wenn sich das Backend ändert, bleibt der Zugang für Kunden weiterhin gleich. Die eigentlichen Karten in ihrer physischen Form werden jedoch verschwinden. Das ist heute schon zu beobachten, selbst ohne Blockchain-Technologie. Mit der Blockchain-Technologie werden die Kundenidentitäten hinter den Zahlungen besser gegen Diebstahl geschützt sein.

Kredite werden weiterhin benötigt, um Unternehmen am Laufen zu halten oder persönliche Anschaffungen zu tätigen. Kreditkartenunternehmen verdienen weiterhin Geld an Transaktionsgebühren. Kredite halten die Welt in Schwung, und in unserer derzeitigen Sozialstruktur wird es immer Kapitalmärkte geben. Die Kosten, Geld zwischen Gruppen zu versenden, werden sinken, was für Finanzinstitute sehr gut ist. Sie sollten sich darauf konzentrieren, ihren Kunden die besten Investment- oder Bankingprodukte anzubieten.

Dem Betrug ein Ende setzen

Bitcoin wurde als Reaktion auf die Finanzkrise entwickelt, nachdem Betrug und andere unmoralische Handlungen den Zusammenbruch der Weltwirtschaft verursacht hatten. Dabei findet ein Paradigmenwechsel von »vertrauen oder nicht vertrauen« hin zu einem System statt, das überhaupt kein Vertrauen mehr benötigt. Dieser feine Unterschied wird häufig übersehen. Bei einem *vertrauenslosen System* vertrauen und misstrauen Sie jeder Person im Netzwerk gleichermaßen. Das Wichtige daran ist, dass Blockchains ein Umfeld schaffen, in dem Transaktionen auch ohne jedes Vertrauen abgewickelt werden können.

Und diese Netzwerke eignen sich nicht nur für den Austausch von Werten. Das folgende Beispiel hilft Ihnen, das Potenzial zu verstehen:

Ich gehe in eine Bar, und der Türsteher hält mich auf, um meinen Ausweis zu überprüfen. Ich greife in meine Brieftasche und zeige ihm meinen Führerschein. Mein Führerschein enthält zahlreiche Informationen, die der Türsteher nicht benötigt, und er braucht auch keinen Zugriff auf Daten wie etwa meine Adresse. Er muss nur sehen, dass ich über 18 bin. Er muss nicht einmal mein genaues Alter kennen, er muss nur wissen, dass ich hinsichtlich der gesetzlichen Bestimmungen alt genug bin.

In Zukunft werden Sie mit Blockchain-ID-Systemen festlegen können, welche Informationen Sie welchen Personen auf welcher Ebene mitteilen. Je mehr anonyme Daten sie enthalten, desto sicherer sind sie. Blockchain-Systeme werden dazu beitragen, den Diebstahl von Identitäten und Daten einzudämmen, indem Sie keine Informationen mehr an Dritte weitergeben, die diese nicht brauchen oder die dafür keine Berechtigung haben.

Ein anderer Aspekt der Blockchain-Technologie ist, dass sie den Fokus auf Betrugsfälle aus der Vergangenheit in die unmittelbare Gegenwart holen wird. In unserem aktuellen System sind Nachprüfungen eine partielle Rückschau auf das, was bereits geschehen ist. Externe Prüfer wählen ein paar zufällige Dateien aus und sehen nach, ob alles in Ordnung ist. Alles Weitere wäre zu teuer und zeitaufwendig.

Aufzeichnungssysteme mit Blockchain-Technologie werden es ermöglichen, neue Dateien in Echtzeit zu überprüfen und bei unvollständigen oder ungewöhnlichen Daten sofort Alarm zu schlagen. So können die Daten sofort proaktiv korrigiert werden, bevor es überhaupt zu Problemen kommt.

Ein weiteres Merkmal von Blockchain-Systemen ist die Möglichkeit, Daten transparent mit Dritten zu teilen. In Zukunft wird man Daten so einfach teilen, wie man eine ZIP-Datei per E-Mail versendet, nur dass der Empfänger dann Zugriff auf das Original hat und nicht auf eine Kopie wie beim E-Mail-Anhang.

Wenn jemand eine Datei sendet, hat er eine Version auf seinem Computer, und der Empfänger hat ebenfalls eine Version. Mithilfe der Blockchain-Technologie teilen sich die beiden Parteien nur noch eine Version.

Blockchains verhalten sich wie ein unabhängiger Zeuge für das Alter und die Erstellung der Dateien. Sie können auf sehr detaillierte Weise aufzeigen, wer in den Systemen mit einer Datei gearbeitet hat, sowohl intern als auch extern. Sie können darauf hinweisen, was aus einer Datei entfernt wurde, und nicht nur die aktuell darin enthaltenen Daten anzeigen. Blockchain-Dateien können auch redigiert geteilt werden, ohne dass dadurch die Gültigkeit der Dokumente beeinträchtigt wird.

Das heißt, dass Sie das Alter einer Datei und ihren vollständigen Versionsverlauf über die Zeit hinweg erkennen. Darüber hinaus sehen Sie auch, ob etwas aus der Datei gelöscht wurde, was eine noch interessantere Eigenschaft ist. Dieses Konzept wird auch als *Negativbeweis* bezeichnet. Die meisten Dateisysteme können aktuell nur zeigen, was sich in ihnen befindet. Jetzt sind sie aber auch in der Lage zu erkennen, was sich *nicht* in einer Datei befindet.

Prüfungen werden damit billiger und vollständiger. Auditierungsregeln könnten an zentraler Stelle aktualisiert werden. Wenn zur Regulierung berechtigte Knoten in einem Blockchain-Netzwerk gemeinsamen und transparenten Einblick in die Transaktionen von Vermögenswerten haben, kann die Berichterstattung über diese Transaktionen direkt am Standort des Regulierers stattfinden, ohne dass Hunderte weiterer Institutionen dieselbe Regelmenge anwenden müssten.

Auf Blockchains basierende Systeme, die komplett in ein Unternehmen integriert sind, können die Ausgabe jedes Cents belegen. Am schwierigsten sind Geldströme dort nachzuvollziehen, wo sie ein Unternehmen oder eine Regierungsstelle verlassen. Und weil diese Ausgaben so schwierig zu erfassen sind, finden potenzielle Veruntreuer hier die benötigten Schlupflöcher.

Diese »letzten Meter« könnten für Unternehmen die größte Chance bieten, Ressourcenverschwendung einzudämmen oder korrupte Mitarbeiter zu identifizieren. Gemeinnützige Unternehmen, die strenge Richtlinien für die Ausgabe ihrer Gelder haben, könnten von einem solchen System am meisten profitieren. Sie könnten Anforderungen hinsichtlich Nachvollziehbarkeit und Rechenschaft gegenüber ihren Spendern erfüllen, ohne dass ihre gemeinnützige Arbeit dadurch beeinträchtigt wird.

Eines der Systeme, die hierfür infrage kommen, integriert sich direkt in den Arbeitsablauf der Helfer. Es wurde ursprünglich zur Aufzeichnung von Patientendaten entwickelt, kann aber auch alle bei der Behandlung eingesetzten Versorgungsgüter nachvollziehen. Die Vorteile eines solchen Systems wären enorm, weil es gerade im NGO-Bereich häufig zu Betrug und Unterschlagung kommt.

Kapitel 13

Immobilien

IN DIESEM KAPITEL

- Globale Immobilientrends bewerten
- Totes Kapital erkennen – und Möglichkeiten, es zu erschließen
- Entdecken, wie Fannie Mae in die Blockchain-Welt passt
- Chinas Entwicklungspotenzial durch Blockchain-Technologie erkennen

Der Immobiliensektor gehört zu den Bereichen, die von den Innovationen der Blockchain-Technologie am meisten beeinflusst werden. Das wird sich in jedem Land etwas anders auswirken. In der westlichen Welt bekommen wir vielleicht transparente hypothekengesicherte Wertpapiere, die an blockchainfähigen Börsen gehandelt werden. In China wird die Blockchain-Integration bereits bei Beurkundungen umgesetzt – einer maßgeblichen Komponente von Immobilientransaktionen. In den Schwellenländern sind Blockchains besonders vielversprechend, weil sie Kapital freigeben und den Handel befördern können.

Dieses Kapitel betrachtet die Innovationen, die in der Immobilienbranche auf der ganzen Welt bereits stattfinden. Außerdem weise ich Sie auf möglicherweise bevorstehende Veränderungen und die wichtigsten Auswirkungen der Blockchain-Technologie hin.

Immobilien zeichnen weltweit für einen Großteil des Reichtums und der wirtschaftlichen Stabilität verantwortlich. Die Branche wird sich in den kommenden Jahren sehr schnell verändern. Es ist von Vorteil zu wissen, wo diese Änderungen stattfinden werden und wie Sie und Ihr Unternehmen davon profitieren können.

Wegfall der Rechtstitelversicherung

Eine Rechtstitelversicherung sorgt etwa in den USA für eine Entschädigung für finanzielle Verluste bei Problemen mit dem Grundbucheintrag einer gekauften Immobilie. Sie brauchen sie, wenn Sie eine Hypothek auf Ihr Haus aufnehmen oder diese refinanzieren wollen. Die Rechtstitelversicherung schützt die Investition der Bank vor Problemen mit Grundbucheintragungen, die in den öffentlichen Aufzeichnungen möglicherweise nicht vorhanden sind, die bei der Grundbuchrecherche übersehen wurden oder durch Betrug oder Fälschung entstanden sind.

Die Rechtstitelversicherung ist vielen englischsprachigen Ländern notwendig, wo das Grundbuchsystem nach dem Common Law (Gewohnheitsrecht) geregelt wird. Der Käufer muss sicherstellen, dass der Grundbucheintrag des Verkäufers in Ordnung ist. Innerhalb solcher Rechtskreise wird eine Grundbuchrecherche durchgeführt und eine Versicherung abgeschlossen. In Regionen, die ein Torrens-Grundbuchsystem verwenden, kann sich ein Käufer auf die Informationen im Grundbuch verlassen und muss keine weiteren Nachforschungen betreiben.

Die Blockchain-Technologie bietet eine Möglichkeit, den Verbrauchern bei Grundbuchsystemen nach dem Common Law zu helfen. Die Idee dahinter ist ganz einfach: Blockchains sind fantastische öffentliche Aufzeichnungssysteme. Und sie können nicht zurückdatiert oder geändert werden. Theoretisch könnten Blockchains die Gewohnheitsrechtssysteme in dezentrale Torrens-Grundbuchsysteme umwandeln.

Dazu müssen jedoch zuerst mehrere Hürden überwunden werden. Jeder Bezirk in einem Bundesland mit Gewohnheitsrechtssystem hat ein eigenes Liegenschaftsamt, wo alle Urkunden oder Rechtstitel für ein Grundstück oder einem Grundstücksanteil aufgezeichnet werden. Allein die USA hat Tausende von Bezirken. Die einzelnen Ämter dort erzeugen

tonnenweise Daten. Blockchains werden das Gesetz oder die Struktur der Aufzeichnungen nicht ändern.

Es wären neue Gesetze erforderlich, die vorschreiben, dass alle Grundstücksrechte und ihre Übertragungen in einem einzigen System aufgezeichnet werden müssen, um Gültigkeit zu haben. Dabei entstünde wiederum ein Torrens-System, das die Blockchain-Technologie eventuell überflüssig machen würde, außer in Ländern, in denen es viel Betrug bei Grundbucheintragungen gibt.

In den folgenden Abschnitten gehe ich genauer auf die Immobilienbranche ein und zeige, wo Blockchains von Nutzen sein können.

Kosten senken

Jede Branche hat eigene Schutzmechanismen, die neue Wettbewerber ausschließen sollen. Das können gesetzliche Auflagen, von der Regierung geschützte Monopole oder hohe Anfangskosten sein. Die Immobilienbranche hat sich in den letzten 40 Jahren nicht merklich geändert. Damit ist die Zeit jetzt reif für durchschlagende Veränderungen. Hierzu tragen viele verschiedene Parteien bei.

Die folgenden Geschäftsfelder sind rund um den Kauf und Verkauf von Eigenheimen entstanden:

- **Immobilienmakler:** Ein Immobilienmakler hilft Ihnen, verschiedene Wohngegenden zu vergleichen und ein Eigenheim zu finden. Er hilft Ihnen auch, einen Preis auszuhandeln, und übernimmt für Sie die Kommunikation mit dem Verkäufer. Diese Dienstleistung ist sehr wertvoll und wird wahrscheinlich nicht durch die Blockchain-Technologie ersetzt werden. Auch heute kann man bereits ein Eigenheim ohne Makler kaufen, aber häufig wird einer beauftragt, weil er den gesamten Vorgang erleichtert.
- **Immobiliengutachter:** Immobiliengutachter überprüfen das Haus vor dem Kauf auf Mängel, die Sie später sehr viel Geld

kosten könnten. Vom Gutachter gefundene Mängel sind zudem geeignet, den Verkaufspreis zu drücken. Auch in Zukunft werden Häuser unweigerlich einem natürlichen Verschleiß unterliegen; das wird sich nie ändern. Die Blockchain-Technologie könnte jedoch genutzt werden, um Reparaturen an einer Immobilie und die bei einer Prüfung gefundenen Mängel festzuhalten.

- ✔ **Notar:** Beim Abschluss ist der letzte Schritt die Bezahlung. Der Notar überwacht und koordiniert den Dokumentenverkehr, zeichnet auf und gibt die Gelder für die jeweiligen Parteien frei. Notare könnten durch die Blockchain-Technologie verdrängt werden, ihre Aufgaben könnten auch mit Smart Contracts oder Chaincode erledigt werden.
- ✔ **Hypothekendienstleister:** Hypothekendienstleister stellen die Finanzmittel für eine Hypothek bereit und ziehen die laufenden Hypothekenzahlungen ein. Sie werden durch die Blockchain-Technologie nicht ersetzt, könnten diese aber nutzen, um die Kosten für die Aufzeichnungen und die Überprüfungen zu reduzieren.
- ✔ **Immobilienschätzer:** Ein Immobilienschätzer hat die Aufgabe, eine Immobilie zu besichtigen und festzulegen, wie viel sie wert ist. Die Schätzung wird bei jedem Kauf und bei jeder Neufinanzierung einer Immobilie durchgeführt. Mit einem vertrauenswürdigen Makler ist die Ermittlung des Marktwerts relativ einfach. Allerdings ist jedes Haus einzigartig und muss regelmäßig bewertet werden. Selbst bei der Vergabe von Hypotheken für Immobilien müssen möglicherweise mehrere Meinungen eingeholt werden, um die Bedürfnisse aller Parteien zu befriedigen. Es könnte sinnvoll sein, diese Daten in einer Blockchain aufzuzeichnen, um sie öffentlich zu belegen.
- ✔ **Kreditsachbearbeiter:** Kreditsachbearbeiter prüfen anhand von Informationen über Ihre Kreditwürdigkeit, Ihre finanzielle Lage und Ihre Beschäftigung, ob Sie für eine Hypothek kreditwürdig sind. Anschließend ermitteln sie, welches der von ihnen verkauften Produkte infrage kommt. Wie ein

Immobilienmakler hilft Ihnen ein Kreditsachbearbeiter, die für Sie beste Option auszuwählen. Blockchain-Software kann Kreditsachbearbeitern dabei unterstützen, alle von Ihnen übermittelten Dokumente nachzuverfolgen und zu prüfen, ob die Kreditvergabe gesetzeskonform oder sittenwidrig ist.

- ✔ **Kreditbearbeiter:** Ein Kreditbearbeiter hilft Kreditsachbearbeitern, die Darlehensinformationen für die Hypothek zusammenzustellen und die Unterlagen für das Kreditinstitut aufzubereiten. Aktuell wird Software entwickelt, die Informationen über den Käufer extrahiert. Diese ist zwar nicht blockchainbasiert, könnte diese Art von Arbeitsplatz in Zukunft aber gefährden.
- ✔ **Hypothekenkreditinstitut:** Ein Kreditinstitut stellt fest, ob Sie für ein Hypothekendarlehen infrage kommen. Es genehmigt Ihren Antrag auf ein Hypothekendarlehen oder lehnt diesen ab, abhängig von Ihrem Kreditverlauf, Ihrer Beschäftigung, Ihren Vermögenswerten und Ihren Verbindlichkeiten. Einige Unternehmen erforschen eine Automatisierung dieses Prozesses unter Verwendung künstlicher Intelligenz. Dabei handelt es sich jedoch nicht um Blockchain-Technologie.

Jeder dieser Beteiligten hat eine bestimmte Aufgabe, die jeweils dazu beiträgt, den Käufer, den Verkäufer und den Hypothekengeber zu schützen. In den meisten Branchen sinken die Betriebskosten im Laufe der Zeit. Effizienzverbesserungen aufgrund von Wettbewerb und Innovation tragen ebenfalls zur Kostensenkung bei. Die Hypothekenbranche ist ein attraktiver Kandidat für Blockchain-Innovationen, weil hier genau das Gegenteil der Fall war: Die Kosten in der Branche sind angestiegen. Die Unterlagen für eine typische Hypothek in den USA umfassen mehr als 500 Seiten und verursachen eine Bearbeitungsgebühr von etwa 7.500 US-Dollar. Vor zehn Jahren lagen die Kosten noch bei einem Drittel davon. Die Blockchain-Technologie kann die notwendige Absicherung von Käufer, Verkäufer und Hypothekengeber gewährleisten und zugleich die Kosten dafür reduzieren.

Fannie Mae und die Verbraucher

Die Federal National Mortgage Association (auch als *Fannie Mae* bezeichnet) ist sowohl ein staatlich gefördertes als auch ein Aktienunternehmen. Es ist derzeit der größte Finanzierer von Hypothekengebern und hat den US-Markt seit dem Rückzug privaten Kapitals nach der Rezession dominiert.

Seit der Rezession werden 95 Prozent aller Eigenheimdarlehen in den USA durch Fannie Mae finanziert. Das entspricht etwa fünf Billionen US-Dollar an Hypothekendarlehen. Mit wenigen Ausnahmen sind Darlehen, die nicht über Fannie Mae oder ihren engen Verwandten Freddie Mac finanziert werden, Jumbo-Darlehen (in der Regel mit je mehr als 417.000 US-Dollar). Diese Darlehen werden immer noch durch privates Geld finanziert.

Fannie Mae nutzt ein automatisiertes Programm, mit dem Kreditgeber die Kreditwürdigkeit von Kreditnehmern überprüfen. Es hilft ihnen, Richtlinien für ein herkömmliches Darlehen anzulegen. Die Kreditgeber speisen Ihren Kreditantrag in das Computersystem von Fannie Mae ein. Die Antwort entscheidet, ob Sie Ihr Darlehen erhalten oder nicht. Online-Plattformen tragen diese neue Software direkt an Verbraucher heran, damit sie herkömmliche Vertriebsstrukturen umgehen können. Fannie Mae und Freddie Mac überprüfen gerade den Einsatz von Blockchain-Technologie, um diesen Prozess weiter zu optimieren und Kunden direkt zu erreichen.

Hypotheken in der Blockchain-Welt

Eine Hypothek in der Blockchain-Welt unterscheidet sich nicht sehr von einer Hypothek in der normalen Welt. Sie werden jedoch feststellen, dass der Abschluss einer Blockchain-Hypothek sehr viel kostengünstiger ist.

Die meisten Menschen kaufen im Laufe ihres Lebens nicht allzu viele Häuser, der Unterschied scheint also nicht dramatisch zu

sein. Aber es summiert sich. Die Blockchain-Technologie könnte die Kosten für die Ausstellung einer Hypothek auf ein Niveau von vor 2007 absenken.

Reduzierung der Bearbeitungsgebühren

Die Kosten für die Ausstellung von Hypotheken sind gestiegen. Der Grund dafür ist einfach: Banken haben Angst vor Strafen, die ihnen auferlegt werden könnten, wenn sie bei der Hypothekenvergabe einen Fehler machen. Aus diesem Grund hat die Branche Schritte eingeführt, um sicherzustellen, dass alle Anforderungen zum Zeitpunkt der Ausstellung sowie auch Jahre später – wenn sie irgendwann überprüft werden – erfüllt sind. Große Banken mussten wegen mangelhafter Dokumentation Milliardenstrafen bezahlen. Heute müssen sie nicht nur alle wichtigen Dokumente erfassen, sondern auch belegen, dass sie sich an alle Vorgaben gehalten und Ihnen alle erforderlichen Dokumente ausgehändigt haben.

Blockchainbasierte Produkte verringern die Puffer, die die Banken nach der Finanzmarktkrise in ihre Abläufe eingebaut haben. Die Kosten für Dokumentation und Überprüfung sind seitdem durch die Decke gegangen. Die Blockchain-Technologie könnte diese Kosten wieder senken.

Unternehmen, die die Anforderungen der Banken mithilfe einer Blockchain-Lösung erfüllen wollen, müssten den Nachweis ermöglichen, dass die Banken die höheren Anforderungen erfüllt haben. Die Blockchain würde den Banken zudem helfen zu dokumentieren, warum sie bestimmte Hypothekenentscheidungen getroffen haben, und Dokumente abzulegen, die für die Entscheidung verwendet wurden, selbst wenn sich diese nicht in ihrem Besitz befinden.

Mit Blockchain-Anwendungen könnten bei einem durchschnittlichen Hauskauf bis zu 4.000 US-Dollar eingespart werden. Die Hypothekenbranche ist der Autokreditbranche und der Kreditkartenbranche sehr ähnlich. Vergleichbare

Anwendungen könnten die Verwaltungskosten senken, die diesen Branchen aufgrund von Verbraucherschutzgesetzen entstehen, während die Unternehmen nach wie vor die entsprechenden Anforderungen erfüllen.

Das letzte bekannte Dokument finden

Einer der größten Kostentreiber im Hypothekenausstellungsprozess kommt häufig Jahre nach der anfänglichen Kreditvergabe zum Tragen. Häufig werden von den Sachbearbeitern unnötige Dokumente in die Kundenakte mit aufgenommen, oder es verbleiben alte Akten im Ordner, die nicht für die Ausstellung einer Hypothek verwendet wurden. Teilweise gibt es auch doppelte Aufzeichnungen. Beim Überprüfen der Akte finden sich dort zu viele Informationen, um sie einfach sichten zu können. Banken zahlen externen Anbietern viel Geld, um ihre Aufzeichnungen zu prüfen und festzustellen, welche Dokumente bei der endgültigen Überprüfung eines Kreditantrags schließlich verwendet wurden.

Blockchain-Software kann dieses Problem auf elegante Weise lösen. Blockchains sind dezentrale Aufzeichnungssysteme, die es im zeitlichen Verlauf mehreren Parteien erlauben, gemeinsam an den Daten zu arbeiten, ohne dass aus dem Blick gerät, wie die Daten zu einem beliebigen Zeitpunkt aussahen. All die verschiedenen Stellen, die Sie beim Hauskauf unterstützen, können nun also an derselben Kette mitarbeiten.

In diesem Fall würde die Kette bei Ihnen beginnen. Ihre Kette könnte im Laufe der Zeit mehrere Unterketten erhalten, wie beispielsweise einen Hauskauf. Sie könnten den anderen – beispielsweise Banken, Arbeitgebern, Kreditinstituten, Gutachtern usw. – gestatten, Einträge in Ihre Kette vorzunehmen. Sie würden dann ihre Daten in Ihre Kette eintragen, und die anderen berechtigten Parteien könnten diese Daten lesen und ebenfalls eigene Daten hinzufügen.

Mit Blockchains müssen Daten nicht mehr an einer zentralen Stelle abgelegt werden. Sie automatisieren zum Teil die Verarbeitung von Papierunterlagen und zeichnen immer einen eindeutigen Verlauf Ihres Darlehens auf. Damit entfielen die Notwendigkeit einer Überprüfung und die Aufbereitung der zu überprüfenden Dokumente.

Das beschreibt eine große Idee, aber es muss nicht das gesamte Ökosystem daran arbeiten. Jede Branche, die es tut, würde das System stärken und aufwerten, ähnlich wie jeder zusätzliche Faxteilnehmer den Nutzen eines eigenen Faxgeräts steigert.

Regionale Trends vorhersehen

Blockchain-Software musste auf dem Weg zur allgemeinen Verbreitung schon viele Hürden überwinden. Häufig begegnet man ihr mit Angst, weil viele Menschen nicht verstehen, wie sie funktioniert und welche Auswirkung eine Umstellung hat. Viele der frühen Verfechter wurden belächelt, wie es so oft bei Anwendern ganz neuer Technologien geschieht. Blockchains leiden unter der schlechten Presse von Bitcoin und den illegalen Geschäften, die mit der Technologie gemacht werden.

Das Jahr 2016 stellte jedoch einen Wendepunkt für die Branche dar. Es wurde deutlich, dass Blockchains viele Bereiche erschüttern würden und dass diejenigen, die weiterhin erfolgreich arbeiten wollen, eine Blockchain-Strategie brauchen.

Jede größere Bank begann, Blockchains für sich zu untersuchen und mit ihnen zu experimentieren, oder hat sich einem entsprechenden Konsortium angeschlossen. Oft wurden Blockchains zuerst für ein bankübergreifendes Zahlungssystem und grenzüberschreitende Überweisungen eingesetzt – ganz einfache Anwendungen für Blockchains. Die nächsten und tiefgreifenderen Weiterentwicklungen werden Systeme und Daten sein, die durch Dezentralisierung abgesichert werden.

In den folgenden Abschnitten zeige ich Blockchain-Trends in den USA, Europa, China und Afrika auf.

USA und Europa: Engstellen in der Infrastruktur

Die USA und die europäischen Staaten brauchen möglicherweise länger als andere Länder, um die Blockchain-Technologie zu implementieren. Zwar geben Unternehmen in diesen Ländern Milliarden Dollar für ihre Infrastruktur aus, allerdings nur für deren reinen Erhalt. Für die Probleme, die Blockchain-Projekte lösen können, gibt es bereits Lösungen. Es genügt aber nicht, wenn eine Lösung besser ist als die bereits etablierte. Sie muss zehnmal besser sein als das konventionelle System oder sich in die bestehenden Strukturen leicht integrieren lassen.

Eine der größten Herausforderungen in den USA ist die dezentrale Machtverteilung und Entscheidungsfindung. Jeder Bezirk und jeder Staat stellt seine eigenen Regeln für die Implementierung oder Nutzung der Blockchain-Technologie auf; dieser Prozess hat bereits begonnen.

Die Verwendung von Blockchains könnte auch in Ihrem Land Gesetzen und Vorschriften für den Geldtransfer unterliegen. Da alle wichtigen öffentlichen Blockchains derzeit ein Kryptowährungs-Token als Anreiz zur Bewahrung der Netzwerksicherheit verwenden, gelangen Anwender hier schnell in einen Graubereich. Das hat dazu geführt, dass private und Permissioned Blockchains entstanden sind, die ohne Token auskommen.

Die Lizenzierungsanforderungen sind für Unternehmen, die Blockchains auch über die Zahlungsabwicklung hinaus als Technologie für andere Zwecke verwenden wollen, oftmals unklar. Auch Verbraucherschutzregelungen kommen zum Tragen. In Europa gibt es bereits ein »Recht auf Vergessenwerden«. Die Konformität mit diesen Vorschriften kann kompliziert sein, wenn in Blockchains eingetragene Daten dauerhaft erhalten bleiben und auch auf Wunsch nicht gelöscht werden können.

In vielen Staaten der USA ist es eine Straftat, ohne ordentliche Lizenz Geldüberweisungen zu tätigen. Die harten Konsequenzen

bei Gesetzesüberschreitungen durch innovative Technik veranlasst Blockchain-Unternehmen in den USA, immer mehr Zeit und Geld für die Gesetzeskonformität aufzuwenden – durchschnittlich zwei bis sieben Millionen US-Dollar pro Jahr und Unternehmen. Schließlich müssen sie den gesetzlichen Anforderungen aller 50 Bundesstaaten genügen. Die Gebühren für Rechtsberatung stellen für Technologie-Start-ups eine hohe Belastung dar.

Die Gesetzgebung der verschiedenen US-amerikanischen Staaten im Hinblick auf die Blockchain-Branche sind noch nicht geklärt. New York und Vermont haben begonnen, die Technologie in das Gesetz zu integrieren. New York hat die Anforderungen an die Compliance erhöht und innovative Unternehmen dazu gebracht, in freundlichere Gefilde abzuwandern. Vermont dagegen hat ein Gesetz verabschiedet, das Blockchain-Aufzeichnungen als Beweismittel vor Gericht zulässt.

Luxemburg hat 2011 einen gesetzlichen Rahmen für elektronische Zahlungen eingerichtet und früh das Konzept des »elektronischen Geldes« befürwortet. Luxemburg und Großbritannien sind Heimat vieler Blockchain-Unternehmen geworden, weil das gesetzliche Umfeld dort durchsichtiger ist und weniger Kosten verursacht. In der Europäischen Union können Blockchain-Unternehmen für weniger als eine Million US-Dollar eine Lizenz für ein Zahlungsinstrument erhalten. Diese Lizenz erteilt den Unternehmen Zugang zu 28 Ländern der EU. Mit diesem Ansatz ist die EU den USA im Hinblick auf Fintech-Innovationen weit voraus.

China: Als Erster im Rennen

China hat schnell erkannt, dass seine Bürger die Technologie nutzten, um unbemerkt Werte außer Landes zu schaffen und neues Vermögen in weniger restriktiven Systemen aufzubauen. Aus diesem Grund hat China seine Vorschriften hinsichtlich Kryptowährungen mehrfach überarbeitet, was den Marktpreis für Bitcoins wesentlich beeinflusst hat.

Die chinesische Industrie sieht Blockchains als Lösung für die zahlreichen Probleme, die in anderen Teilen der Welt auftreten. In China hat man Blockchains schnell als Ergänzung zu bestehenden Ansätzen eingesetzt und zusätzliche Sicherheitsebenen etwa für das Internet der Dinge (IoT) und die Beurkundung eingeführt. Während westliche Länder eine eher föderale und dezentrale Machtstruktur besitzen, ist diese in China stärker zentralisiert. Deshalb kann China auf Innovationen schneller mit Gesetzen reagieren.

China Ledger, eine Blockchain-Vereinigung mit Unterstützung der chinesischen Nationalversammlung, ist ein gutes Beispiel für die schnelle Reaktion von Regierungsstellen und Industrie. China Ledger konnte Anthony Di Ioro und Vitalik Buterin gewinnen, zwei der Gründer von Ethereum, sowie den Bitcoin-Core-Entwickler Jeff Garzik und den UBS-Innovationsmanager Alex Baltin.

Ein weiteres zukunftsweisendes chinesisches Blockchain-Projekt ist Distributed Credit Chain (DCC), das dezentrale Banksysteme aufbaut. Das DCC-Netzwerk hat Standards für Geschäftsabläufe, den Kontobuchkonsens, die Vertragszuordnung sowie den Zahlungsausgleich von Finanzdienstleistern ausgegeben.

Entwicklungsländer: Hürden für Blockchains

Die Zukunft ist da – sie hat sich nur noch nicht verbreitet. Dies gilt insbesondere in Entwicklungsländern, in denen oft technologischer Nachholbedarf besteht, es aber an Ressourcen oder der geeigneten politischen Umgebung fehlt, um diese Innovationen auch zu ermöglichen. Einige kleine Länder setzen auf protektionistische Maßnahmen, die den Import von Waren verbieten, die sie selbst produzieren können. Andere Länder misstrauen zudem der Qualität und der Güte von Produkten und Dienstleistungen aus externen Quellen. Und einige politischen Systeme profitieren sogar so sehr von den Ineffizienzen und Unklarheiten ihres Rechtssystems, dass sie überhaupt nichts ändern wollen.

Hernando de Soto Polar ist ein peruanischer Ökonom und Autor, der viel über die sogenannte »informelle Wirtschaft« und die Bedeutung von Unternehmens- und Eigentumsrechten geschrieben hat. Eines der größten Probleme, das den Fortschritt der Entwicklungsländer hemmt, ist das *tote Kapital*. Dabei geht es um Boden- und anderes Eigentum, über das weniger Privilegierte verfügen, das aber nicht formal anerkannt ist, sowie um die mangelnde Vertrauenswürdigkeit der vorhandenen Systeme. Für die Besitzer solchen Eigentums ist es schwierig bis unmöglich, Hypotheken dafür aufzunehmen oder es zu verkaufen. Die rechtliche Unsicherheit verringert auch den Wert ihres Besitzes.

In der westlichen Welt kann man relativ unkompliziert Hypotheken auf Immobilienbesitz aufnehmen und diesen frei verkaufen, wodurch Innovation und wirtschaftlicher Wohlstand gefördert werden. Blockchaingestützte Technologien könnten dies auch in den Entwicklungsländern sehr schnell möglich machen. Eindeutige Eigentumsregister für Landbesitz würden ermöglichen, diesen zu verkaufen oder zu beleihen. Strandgrundstücke in Kolumbien würden dadurch sehr wertvoll. Unumkehrbare Zahlungen und eine echte, bekannte Identität würden dem Kreditwesen und der Wirtschaft völlig neue Wege eröffnen.

Viele Start-ups und Entwickler haben sich zusammengetan, um diese Zukunftsvision Realität werden zu lassen. Selbst globale Player wie etwa die Weltbank haben wiederholt Konferenzen zum Thema Blockchain und deren Einfluss auf die Entwicklungsländer abgehalten. Bitcoin und Blockchains halten Einzug in Afrika, wo ein starkes Misstrauen gegenüber lokalen Währungen und Infrastrukturen herrscht. BitPesa, eine Zahlungs- und Handelsplattform, die viele Länder in Afrika bedient, hat mit der Expansion nach Großbritannien und Europa begonnen. Das Angebot wurde inzwischen auf Gehaltszahlungen ausgeweitet.

Die Entwicklungsländer müssen zwar viele Hürden im Hinblick auf Entwicklung und Innovation nehmen, sie haben aber auch Vorteile, an denen westliche Länder nie vorbeikommen werden. Die fehlende Infrastruktur in Entwicklungsländern erleichtert es beispielsweise, in einem Sprung direkt auf den aktuellen Stand

westlicher Länder zu gelangen. Das machte etwa die Einführung von Smartphones in Entwicklungsländern deutlich. Entwicklungsländer haben außerdem weniger Aufsichtsbehörden und Verbraucherschutz. Das ist vor allem für Blockchain-Start-ups attraktiv, die in westlichen Ländern in die Grauzone fallen. In Entwicklungsländern müssen oft weniger Entscheider beteiligt werden, und dadurch wird es einfacher, genau mit denjenigen Menschen zusammenzutreffen, die den Stein ins Rollen bringen können.

Kapitel 14

Versicherungen

IN DIESEM KAPITEL

- Neue Unternehmen aufbauen
- Individuelle Versicherungen maßschneidern
- Neue Versicherungsmärkte erschließen
- Auf unerwartete Weise Kosten reduzieren

Die Blockchain-Versicherungstechnologie könnte den Versicherungsabschluss und den Erhalt von Versicherungsleistungen durch Unternehmen und Einzelpersonen völlig revolutionieren. Das Ganze wird auch bereits von bekannten Unternehmen getestet, etwa von Toyota. Sie sollten die Auswirkungen dieser neuen Technologien verstehen, die bereits am Horizont auftauchen.

In diesem Kapitel erkläre ich, wie sie funktionieren und wo sie im Wesentlichen ihre Grenzen haben. Ich werde Ihnen zeigen, wie Versicherungsanbieter IOT-Geräte (Internet of Things, Internet der Dinge) nutzen. Außerdem beschreibe ich, wie selbstausführende Blockchain-Verträge Unternehmensstrukturen und -strategien beeinflussen werden.

Dieses Kapitel bereitet Sie auf die grundlegenden technischen Veränderungen vor, die möglicherweise zu einer Beweislastverschiebung führen. Nachdem Sie dieses Kapitel gelesen haben, können Sie besser informierte Entscheidungen über blockchainbasierte Versicherungsleistungen und Zahlungen treffen. Sie werden verstehen, wie sich das auf Ihre Versicherungsbeiträge auswirkt und welche verschiedenen Deckungstypen Ihnen zukünftig zur Verfügung stehen werden.

Präziser, maßgeschneiderter Versicherungsschutz

IoT-Geräte, unveränderbare Daten, dezentrale autonome Organisationen (DAOs) und Smart Contracts haben einen Einfluss auf die Entwicklung von Verbraucherversicherungen. Die Entwicklung im Bereich der Blockchains ermöglicht es, alle diese Technologien zusammenzuführen.

Blockchains können einige Dinge richtig gut, die für zwei wichtige Veränderungen beim künftigen Kauf und Verkauf von Versicherungen sorgen werden: Einzelpersonen erhalten einen individuelleren Versicherungsschutz, und es werden sich völlig neue Märkte auftun, die zuvor aus Kostengründen undenkbar schienen.

Individuelle Versicherung

Eine ganz speziell auf einen Versicherten zugeschnittene Versicherung wird die Prioritäten maßgeblich verschieben. Das Anlagenmanagement wird weniger kritisch; die Versicherer können sich auf die Risikoberechnung konzentrieren und das Angebot an die Nachfrage anpassen.

Sie könnten einen Marktplatz entwickeln, auf dem Kunden ihre Versicherungen abschließen können. Es gibt viele Möglichkeiten, dieses neue Geschäft aufzuziehen. Eine Möglichkeit wäre ein On-Demand-Marktplatz, auf dem Benutzer ihre Anfragen einstellen, entweder standardisiert über einen individuellen Smart Contract oder als Chaincode-Vertrag. Falls Sie diese Arten neuer, selbstausführender digitaler Verträge noch nicht kennen, lesen Sie Kapitel 5 über Ethereum und Kapitel 9 über Hyperledger.

Sie als Versicherer könnten die Prämie für die spezifische Anfrage auf Grundlage historischer Daten und anderer Faktoren Ihres Risikomodells berechnen. Wenn das Angebot Ihrem Kunden zusagt, kann er je nach verwendetem Modell ein Gebot abgeben oder unterzeichnen.

Dieser neue Versicherungstyp könnte von einer Peer-to-Peer- (P2P) oder einer Crowdfunding-Versicherung übernommen werden oder auch von einem herkömmlichen Versicherungsunternehmen, das die Technologie einsetzt. Auf jeden Fall werden beide in einem dezentralen Kryptowährungs-Ledger erstellt. Dazu werden Smart Contracts/Chaincode verwendet, um die Zahlung vom Kunden an den Versicherer zu garantieren und umgekehrt, falls ein Versicherungsfall eintritt. Blockchain ist hier der Schlüssel, weil dadurch einige Dinge möglich werden, die vor ein paar Jahren noch undenkbar oder zu unsicher waren.

Blockchains schaffen einen nahezu reibungslosen Transfer von Werten, das heißt, sie ermöglichen Mikrozahlungen, weil die Transaktionsgebühren so gering sind. Sie können jetzt neue Märkte eröffnen, für die es bisher kein funktionierendes Geld- oder Rechtssystem gab, oder für Situationen, in denen die Kosten für Transaktionen und Streitigkeiten den Vorteil eines Versicherungsangebots weitaus überstiegen.

Sie können DAOs mit Smart Contracts verwenden, um große Gruppen zu einem Bruchteil der Kosten und der Zeit zu verwalten. Sie könnten dieses Modell verwenden, um Ihr neues Unternehmen zu gründen und zu verwalten, möglicherweise mit Versicherungsplattformen, die über Crowdfunding finanziert werden.

Smart Contracts sind selbstausführend, womit auch viele der Kosten für die Schadensregulierung und für Drittanbieter zur Verarbeitung und Einziehung von Beträgen wegfallen könnten.

Allerdings ist noch nicht klar, ob dies gesetzlich zulässig ist. Die daten- und verbraucherschutzrechtliche Seite ist schwierig. Jedes Land hat seine eigenen Vorschriften und Informationspflichten. Wenn diese Vorschriften jedoch erfüllt sind, werden sich die Versicherungsbranche und die Kundenerfahrung in diesem Bereich maßgeblich verändern.

Die neue Welt der Mikroversicherungen

Eine *Mikroversicherung* ist eine Versicherung, die geringverdienende Menschen gegen Risiken wie beispielsweise Unfälle, Krankheiten und Naturkatastrophen versichert. Durch die Blockchain-Technologie lässt sich dies nun besser umsetzen.

Achten Sie bei Mikroversicherungen vor allem auf zwei Kategorien (die Hand in Hand gehen können):

- ✔ Versicherungen für Haushalte mit geringem Einkommen, Landwirte und andere, bei denen die Versicherung auf bestimmte Bedürfnisse ausgerichtet ist – in der Regel eine indexbasierte Versicherung mit geringer Prämie,
- ✔ Versicherung für Produkte oder Dienstleistungen mit geringem Wert.

Das größte Problem dieser Vertragstypen bei herkömmlichen Versicherungsmodellen sind die überproportional hohen Bearbeitungskosten, durch die es unattraktiv wird, diese Märkte zu bedienen.

Blockchains haben sehr geringe Reibungsverluste und können Werte zu äußerst geringen Kosten übertragen, nahezu unmittelbar an jeden Ort der Welt und ohne die Gefahr von Rückbuchungen. Dies eröffnet die Möglichkeit, mehr Menschen zu niedrigeren Kosten zu bedienen.

Der wichtigste Vorteil der Blockchains ist, dass Smart Contracts sichere Transaktionen ohne Mittelsleute ermöglichen. Für die Versicherung entstehen also sehr viel geringere Kosten.

Das Mikroversicherungsprinzip über die Blockchain ist einfach und besteht aus vier Schritten:

1. **Angebot eines Miet-/Versicherungsvertrags**

   Eine Person kann eine Vermietung über ihre Versicherung anbieten, wenn der Mietgegenstand digital registriert ist. Das

Angebot wird entweder über die Kanäle des Versicherungsunternehmens oder eine öffentliche Plattform wie etwa Facebook an den potenziellen Benutzer geschickt.

2. **Überprüfung der Vereinbarung**

   Der Interessent kann das Angebot überprüfen und anschließend annehmen oder ablehnen. Es wird in den öffentlichen Datensätzen gespeichert. Akzeptiert der Interessent, kann er die Versicherung über Standardzahlungskanäle abschließen, und der Vorgang wird im dritten Schritt fortgesetzt.

3. **Unterzeichnung und Beurkundung des Vertrags**

   Wenn sich beide Seiten einig sind, die Versicherung bezahlt wurde und der Interessent den Mietgegenstand erhalten hat, wird der Vertrag in einer Blockchain digital signiert und beurkundet. Damit wird er so gut wie manipulationssicher. Alle Informationen zu der Transaktion werden sicher gespeichert, mit einem klaren Prüfpfad, falls dieser später benötigt werden sollte.

4. **Bestätigungs-Token**

   Beide Parteien erhalten spezielle digitale Token, die als Identitätsbeleg für den betreffenden Vertrag gelten. Diese Token dienen als kryptografischer Beleg, dass beide Parteien den Vertrag unterzeichnet haben.

Neben diesem einfachen Verfahren unterstützen Smart Contracts auch indexbasierte Versicherungen, was im landwirtschaftlichen Bereich sehr sinnvoll ist oder auch in anderen Bereichen, in denen Werte stark von dynamischen Faktoren abhängen, die von vertrauenswürdigen Dritten präzise dokumentiert werden. In diesem speziellen Fall können die versicherten Landwirte automatische Auszahlungen erhalten, wenn bestimmte Bedingungen, wie beispielsweise Dürreperioden, eintreten. Damit werden potenzielle Bearbeitungskosten weiter reduziert.

Das Internet der Dinge als vertrauenswürdige Datenquelle

Blockchains ermöglichen die Erstellung einer neuen Art von Identität für Menschen und Dinge. Sie basiert auf einem herkömmlichen Modell, bei dem eine Behörde ein Zertifikat ausstellt. Bei Menschen könnte dies ein Dokument wie eine Geburtsurkunde oder ein Führerschein sein. Bei »Dingen« gibt es ähnliche Zertifikate, die dem Verbraucher die Kontrolle über Qualität und Authentizität ermöglichen.

Für die Erstellung solcher Zertifikate wurden immer komplexere Sicherheitsmaßnahmen nötig, wodurch die Kosten stiegen. Blockchains ermöglichen die Aufzeichnung dieser herkömmlichen Zertifikate in einem unveränderbaren Verlauf, den jeder einsehen und auf den jeder verweisen kann. Außerdem lassen sich die Datensätze beim Auftreten neuer Ereignisse auch aktualisieren.

IoT-Geräte können mittlerweile alle möglichen Daten autonom in ihren Datensätzen veröffentlichen und ihren Status aktualisieren. IoT-Geräte können jetzt »sprechen« und ihren Verlauf und ihre Identitäten veröffentlichen und mit Dritten teilen. Die Versicherungsbranche wird dabei nur einer der vielen Sektoren sein, die hiervon betroffen sind.

IoT-Projekte in der Versicherung

Das IoT wird maßgeblichen Einfluss auf drei Bereiche Ihres Lebens nehmen: das vernetzte Auto, das vernetzte Heim und die vernetzte Person selbst.

Das IoT ist im Grunde eine disruptive Technologie. Es verändert die unterschiedlichsten Bereiche, beispielsweise Automobilindustrie, Sicherheitstechnik, Breitband- und Mobilfunkanbieter. Dazu gehören auch Versicherungsunternehmen, insbesondere diejenigen, die Schadens- und Unfallversicherungen anbieten.

Die von den Sensoren in den neuen Geräten erfassten Daten werden zusammen mit der Automation und zusätzlichen Steuerungsoptionen völlig neue Möglichkeiten eröffnen. Auch werden neue Unternehmen in der Versicherungsbranche entstehen. Zusammen mit den dezentralen Ledgers der Blockchains und Smart Contracts ließe sich der gesamte Prozess automatisieren, und zwar viel weiter, als es zuvor möglich gewesen wäre.

Der radikale Technologiewechsel führt zu einem neuen Lebensstil. Wir sind ständig online, und einige der bisher vorhandenen Risiken fallen weg, während neue entstehen, besonders im Hinblick auf die Informationssicherheit. Das alles bedeutet, dass die Risikofaktoren neu berechnet werden müssen. Beispielsweise haben selbstfahrende Autos ein geringeres Unfallrisiko, weil keine menschlichen Fehler mehr auftreten können. Aber die Zuverlässigkeit der Technologie bleibt fragwürdig, bis wir genügend Daten aus der realen Anwendung haben werden.

Auswirkungen von Big Data

Big Data ist seit dem Jahr 2000 ein Thema. Heute beschäftigt sich eine 200 Milliarden US-$ schwere Branche damit. Von besonderer Bedeutung ist sie für den Finanzsektor. Die allgegenwärtige Präsenz von Big Data im Alltag bringt aber auch zunehmende Probleme mit sich:

- **Kontrolle:** Für große, multinationale Unternehmen oder Konzerne ist die Weitergabe von Daten ein ziemlich komplexes Thema. Die Versionskontrolle ist nicht perfekt, und es kann manchmal wirklich schwierig sein zu erkennen, welches die neueste und aktuellste Kopie ist.
- **Vertrauenswürdigkeit der Daten:** Wie können Sie belegen, dass Sie die betreffenden Daten erzeugt haben und nicht jemand anders? Was passiert mit fehlerhaften Daten?

- ✔ **Datenmonetarisierung und -übertragung:** Wie können Sie Rechte an Daten übertragen, kaufen oder verkaufen und sicher sein, dass es sich dabei um die einzige Kopie handelt?
- ✔ **Datenänderung:** Wie können Sie sicher sein, dass Daten nicht unberechtigt geändert werden?

All diese Probleme sind mithilfe von Kryptowährungen und Blockchains lösbar. Die große Herausforderung ist bis heute die Skalierung der Blockchain-Technologie, damit sie für die Kosten- und Datenspeicheranforderungen von großen Unternehmen fit wird.

Wegfall der Drittpartei bei Versicherungen

Einer der größten Vorteile der Blockchain-Technologie für die moderne Finanzwelt ist, dass die Smart Contracts für Geschäftstransaktionen ohne Beteiligung von Drittparteien wie Banken oder Vermittlern abgeschlossen werden können. Hierdurch werden zum Beispiel Micropayments oder Kostenreduzierungen durch den Verzicht auf monotone menschliche Arbeit möglich.

Einfach ausgedrückt ist ein *Smart Contract* ein Protokoll, durch das zwei Parteien ihre Transaktion in einer Blockchain aufzeichnen können. Diese Verträge können für so ziemlich alles verwendet werden, vom Handel mit physischen Waren (die digitale Signaturen haben) bis hin zum Austausch von Informationen oder Geld.

Die wichtigste Sicherheitsfunktion ist hier, dass die Informationen anders als bei einer gewöhnlichen Finanzdatenbank an alle Computer im Netzwerk verteilt und von diesen überprüft werden. Sie werden also dezentral gespeichert. Die Daten sind einzigartig und können nicht kopiert werden. Der Prüfpfad ist unveränderbar.

Selbstfahrende Autos sind ein weiterer spannender Anwendungsfall für die Blockchain-Technologie. Es gibt allerdings ein Dilemma bei der Beurteilung der Schuldfrage ohne menschliche Zeugen. Wer trägt die Schuld – die Steuersoftware des Autos, ein verbautes Teil oder der andere Fahrer?

Dezentrale Sicherheit

Den Kern der aktuellen Geschäftsmodelle bildet etwas, was man auch als das *Paradigma des zentralen Vertrauens* bezeichnen könnte. Gemeint ist, dass Mittelsleute wie Banker, Broker oder Rechtsanwälte die Richtigkeit von Finanztransaktionen und dem Warenhandel koordinieren und sicherstellen.

Die Zentralisierung birgt bestimmte inhärente Sicherheitsrisiken, wie beispielsweise die Verfälschung oder den Diebstahl von Daten. Blockchains bekämpfen dies, indem sie ein dezentrales System schaffen, das auf einem wechselseitigen Misstrauen aller Teilnehmer basiert, die einander ständig überprüfen.

Um ein solches System zu erstellen, legen Sie ein verteiltes Kontenbuch (Ledger) an, das eine Kryptowährung verwendet (wie Bitcoin, Ethereum oder Factom). Dabei sind alle Teilnehmer sowohl Nutzer des Systems als auch verantwortlich für dessen Pflege und Erhaltung.

Abdeckung durch Crowdfunding

Ähnlich wie bei standardmäßigen Crowdfunding-Initiativen ist die Idee hier, Ressourcen von mehreren Entitäten oder Personen in einem Pool zusammenzufassen, um unerwartete Unzulänglichkeiten in einem Versicherungsvertrag abzudecken. Beispielsweise könnte eine Rentenversicherung erst ab einem Alter von 65 zahlen, aber die versicherte Person muss aufgrund unvorhersehbarer Umstände früher in Rente gehen. Für diesen unglücklichen Versicherungsnehmer wäre eine zusätzliche Finanzierung notwendig.

Die wirtschaftliche Ungleichheit ist im Laufe der Jahre immer größer geworden. Von einem Crowdfunding-System könnten viele

unterversicherte oder überhaupt nicht versicherte Menschen profitieren. Crowdfunding kann Vorteile für alle drei beteiligten Parteien bieten:

- **Versicherer** machen mehr Umsätze, weil mehr Kunden an ihren Versicherungen interessiert sind. Sie erhalten Zugang zu einem größeren Anteil der unterversicherten Bevölkerung. Darüber hinaus könnte das Versicherungsunternehmen den Erkennungswert seiner Marke steigern: Man würde es als engagiertes Unternehmen wahrnehmen.
- **Geber** könnten von möglichen Steuerbefreiungen profitieren, wenn die Struktur der Kampagne dies erlaubt, oder andere Vorteile wie Rabatte oder kostenlose Services nutzen.
- **Interessenten** (diejenigen, die nach einer Versicherung suchen) profitieren natürlich am meisten, weil sie einen besseren Schutz und eine erschwingliche Versicherung erhalten.

Cognizant hat in seinem Whitepaper interessante Einblicke im Hinblick auf das Crowdfunding aufgezeigt. Sie finden es unter https://goo.gl/u3Kd3U.

Auswirkungen der DAO-Versicherung

Dezentrale autonome Organisationen (DAOs) sind Unternehmenseinheiten ohne reguläre Angestellte, die aber alle Funktionen eines normalen Unternehmens ausführen können. Die Möglichkeit, ein solches Unternehmen einzurichten, ist unmittelbar der Verbesserung der Blockchain-Algorithmen in den letzten Jahren zuzuschreiben. Dadurch ist etwas entstanden, was häufig als Blockchain 2.0 bezeichnet wird.

Eine DAO ist im Wesentlichen eine Art fortgeschrittener Smart Contract. Man kann sich die DAO als Unternehmen vorstellen, in dem alle in die Vertragsbedingungen einwilligenden Mitglieder zugleich Teilhaber sind, während das Unternehmen selbst nie

eine direkte Kontrolle über eine bestimmte Gruppe oder eine Einzelperson ausübt.

Gleichermaßen steht eine DAO nie unter der Kontrolle der Entwickler, die auch keine Richtlinien ausgeben oder verweigern. Es handelt sich um ein strenges Peer-to-Peer-Versicherungsmodell. Es gibt immer noch Schwachpunkte im Hinblick auf die Identitätsüberprüfung, aber dieses System wird stetig verbessert, und dieselben Probleme gibt es in der Realität auch in den bestehenden zentralisierten Versicherungssystemen.

Kapitel 15

Regierung

IN DIESEM KAPITEL

- Blockchain-Dokumente lesen
- Intelligente Städte aufbauen
- Hackingsichere Identitäten erstellen

In diesem Kapitel stelle ich Ihnen einige hochinteressante Innovationen vor, die bei verschiedenen Regierungsstellen gerade eingeführt werden. Außerdem geht es um die Unternehmen, die dies durch innovative Blockchain-Projekte unterstützen.

Betrug und Abzocke sind heute an der Tagesordnung. Dieses Kapitel erklärt, wie staatliche Stellen Cyberkriminalität und Identitätsdiebstahl bekämpfen. Sie werden Initiativen für die Einrichtung intelligenter Städte kennenlernen, die entscheidend für das Wirtschaftswachstum und die Nachhaltigkeit sind. Viele davon setzen dabei auch auf Blockchain-Technologie.

Die intelligenten Städte Asiens

Intelligente Städte oder *Smart Cities* nutzen die moderne Technologie, um die Funktionalität und Sicherheit der Infrastruktur zu verbessern, ebenso Verkehr und Luftqualität. Das Smart-City-Konzept ist heute ein Riesen-Boom, den fast jede größere Kommune verfolgt.

Blockchains sind vor allem dann nützlich, wenn sie in das von Smart Cities genutzte Internet der Dinge (Internet of Things, IoT) integriert sind. Derzeit entstehen mehrere interessante Projekte. Das US-Ministerium für innere Sicherheit überprüft die

Absicherung von IoT-Geräten, die für den Zoll und den Grenzschutz eingesetzt werden (Customs and Border Protection, CBP). Mithilfe von Unternehmen wie Slock.it können vernetzte Gegenstände über die Blockchain in Smart Contracts eintreten. Das erste Produkt war ein blockchainfähiges intelligentes Schloss, das von Airbnb-Kunden verwendet werden konnte. Die Integration dieser Technologien ermöglicht, dass die Geräte ihre Sensoren verwenden, um Smart Contracts einzurichten. Dieselbe Technologie ließe sich auch für Parkuhren in der Stadt einsetzen.

Abbildung 15.1 zeigt die Website des singapurischen Smart-Nation-Projekts. Singapur hat Start-ups aus der ganzen Welt gebeten, in seiner *regulatorischen Sandbox* neue Technologie zu entwickeln. Dies ist eine Einladung für Unternehmen, die Blockchain-Technologien entwickeln und bisher in einer Grauzone ohne klaren Gesetzesrahmen gearbeitet haben. Viele Länder ergreifen ähnlich wie Singapur die Initiative, um das Feld zu definieren und Unternehmen mitzuteilen, was erlaubt ist und was nicht.

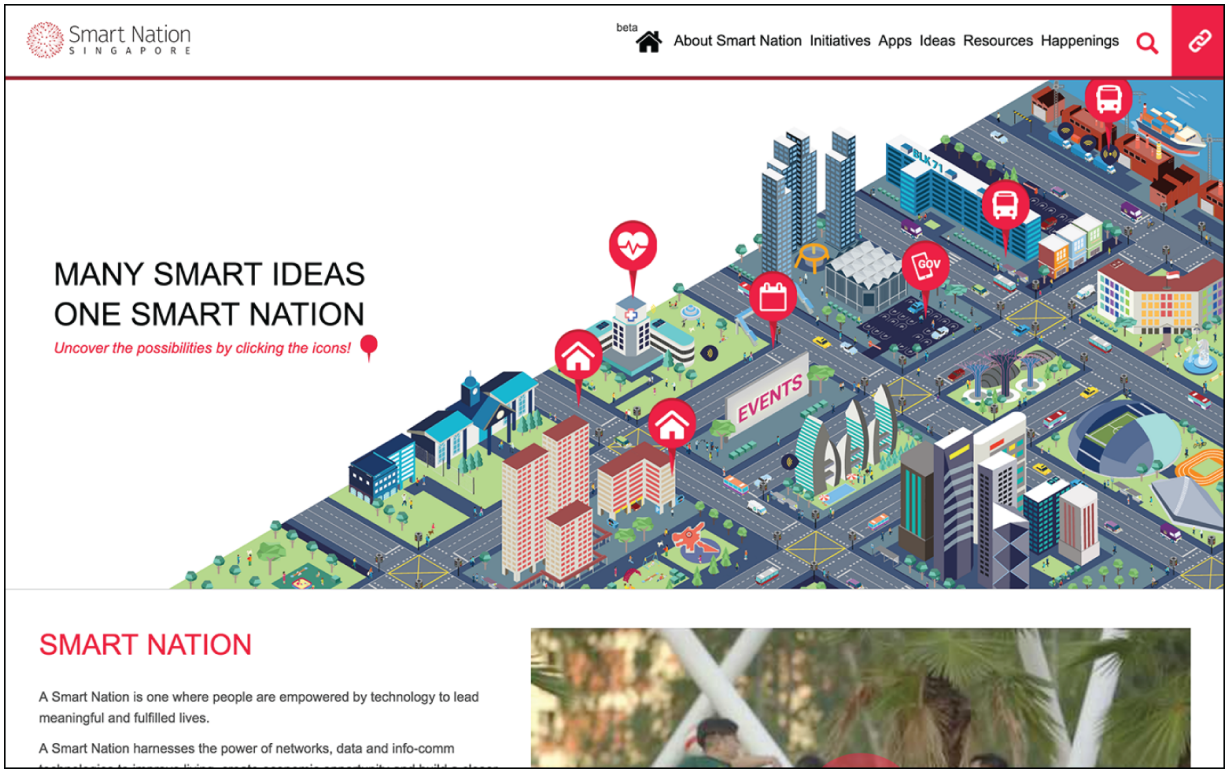


Abbildung 15.1: Das Smart-Nation-Projekt von Singapur

Die Blockchain-Technologie ließe sich auch für den sicheren Informationsaustausch zwischen Netzwerken einer intelligenten Stadt nutzen. Viele Städte überprüfen, wie Blockchains Verkehrsstaus vermeiden könnten. Das Smart-Nation-Projekt von Singapur hofft, die Smartphone-Daten der Bürger nutzen zu können, um die Bedingungen bei Busfahrten zu messen. Die erfassten Daten sollen anschließend analysiert werden, um festzustellen, wo Verkehrswege ausgebaut werden müssen. Singapur ist führend, was die Smart City-Entwicklung betrifft, und hat damit begonnen, intelligente Städte in anderen Ländern zu entwickeln.

In diesem Abschnitt beschreibe ich einige der vielen asiatischen Blockchain-Initiativen.

Singapurs Satellitenstädte in Indien

Die indische Regierung hat 2015 die Mission Smart Cities ins Leben gerufen. Sie hat das Ziel, 100 neue intelligente Städte zu bauen. Viele dieser Entwicklungen finden im Industriekorridor Delhi – Mumbai statt, der sich auf 1.000 Kilometern zwischen Delhi und Mumbai erstreckt. Es wurde bereits Infrastruktur im Wert von elf Milliarden US-Dollar in 33 Städten geplant. Ein Großteil der Entwicklung wird über ein Public-Private-Modell finanziert. Das Projekt soll 90 Milliarden US-Dollar Investitionsgelder aus dem Ausland anziehen. Mit diesen sollen Gewerbegebiete, Produktionsregionen und intelligente Städte gebaut werden, die sich alle entlang eines speziellen Eisenbahntransportkorridors befinden.

Diese Smart Cities werden entwickelt, weil sich die indische Wirtschaft industrialisiert und die Bevölkerung in die Städte wandert. Die Zentralregierung muss hier planerisch eingreifen, um zu verhindern, dass die vorhandenen Städte übervölkert und unbewohnbar werden. Indien ist aufgrund seiner riesigen und verarmten Bevölkerung dem Klimawandel besonders ausgeliefert. Aus diesem Grund ist es wichtig, dass die Städte nachhaltig und intelligent sind. Es müssen Niedrigenergie-Baumaterialien, intelligente Stromnetze, abgestimmten Verkehr, integrierte IT-

Systeme, e-Governance und innovative Wasserspeicherung genutzt werden.

Singapur ist ein hervorragendes Beispiel für eine intelligent geplante Stadt. Trotz der hohen Bevölkerungsdichte besitzt Singapur eine hervorragende Infrastruktur und eine hohe Lebensqualität. Viele der privaten Unternehmen in Singapur haben die Kompetenz und die Ressourcen, die für die Entwicklung der Smart Cities in Indien notwendig sind. In Zusammenarbeit mit der indischen Regierung könnte der private Sektor das Kapital, die Fertigkeiten und die Technologie bereitstellen, die für so riesige Pläne erforderlich sind.

Der südostindische Staat Andhara Pradesh und die Währungsbehörde von Singapur haben eine Innovationspartnerschaft im Bereich Finanztechnik angekündigt. Der Hauptschwerpunkt liegt dabei auf Blockchains und digitaler Zahlungsabwicklung. Singapur hat vor, einen Marktplatz für Fintech-Lösungen in Indien zu entwickeln.

Die Regierung von Singapur bekundet Interesse an einer Partnerschaft mit Indien. Ziel ist die Entwicklung einer intelligenten Stadt sowie einer neuen Hauptstadt für den Staat Andhara Pradesh. Sie richtet Ausschüsse ein, die eine mögliche Mitarbeit an Indiens Plan analysieren, 100 neue Städte zu bauen und die Infrastruktur in 500 vorhandenen Städten und Großstädten weiterzuentwickeln.

Der indische Minister für städtische Entwicklung führte Gespräche mit dem amtierenden Premierminister von Singapur und dessen Vorgänger. Er interessierte sich für die singapurischen Erfahrung im Hinblick auf intelligente Städte, insbesondere intelligente Verkehrssysteme, ein verbessertes Wassermanagement und e-Governance. Außerdem wertete der Minister für städtische Entwicklung die Pläne für öffentliche Gebäude in Singapur aus, ebenso die Vorschriften für den privaten Hausbau. Darüber hinaus beschäftigte man sich mit Finanzierungsmöglichkeiten für die Verkehrsinfrastruktur.

Die indischen Behörden beauftragten ein Expertenteam aus Singapur, die Entwicklung einer Satellitenstadt in Himachal Pradesh zu unterstützen. Das 20 Hektar große Projekt soll Shimla entlasten, eine Stadt mit massivem Bevölkerungsanstieg in den letzten Jahrzehnten. Das Team aus Singapur wird Unterstützung für das Bildungswesen, den Wohnungsbau und die Wirtschaft der entwickelten Stadt bereitstellen.

Sowohl Singapur als auch Malaysia zeigen Interesse an einer Investition in eine weitere Satellitenstadt in der Nähe von Jathia Devi. Die Regierung Singapurs führt eine Studie zur Bewertung verschiedener Optionen durch. Die Regierung von Himachal Pradesh plant die Entwicklung von fünf Satellitenstädten in der Nähe vorhandener Städte unter Verwendung eines öffentlich-privaten Finanzierungsmodells.

Ascendas-Singbridge aus Singapur hat seinen achten IT-Park in Indien ins Leben gerufen. Das 400 Millionen Dollar teure Projekt International Tech Park Gurgaon erstreckt sich über 24 Hektar und soll 74.000 Quadratmeter Geschäftsräume bieten und damit den aufstrebenden IT-Sektor Indiens unterstützen.

Das chinesische Big-Data-Problem

In China wird viel über die Blockchain-Technologie gesprochen, weil damit die Zuverlässigkeit von Big Data erhöht werden soll. Man betrachtet sie als Lösung für das Vertrauensproblem beim Austausch von Daten zwischen zwei oder mehr Parteien, die unterschiedliche Ziele verfolgen. Die Blockchain-Technologie bietet viele neue Lösungen, um Eigentumsverhältnisse, Herkunft und Authentizität nachzuweisen.

Peernova ist ein vielversprechendes US-amerikanisches Unternehmen, das sich mit Big-Data-Problemen beschäftigt. Zuvor hatte es sich auf Bitcoin-Mining konzentriert, ist dann jedoch zur Blockchain-Entwicklung gewechselt und hat vier Millionen US-Dollar vom chinesischen Bauunternehmen Zhejiang Zhongnan Holdings Group erhalten. Peernova will die Blockchain-Technologie einsetzen, um herkömmliche Datenbanken abzufragen und Änderungen nachzuverfolgen.

In der Praxis sollen beispielsweise Änderungen an Untermengen großer Datenspeicher überprüft und statt eines herkömmlichen Prüfers effizientere und umfassendere kryptografische Prüfmethoden eingesetzt werden. Man hofft, Hedgefonds bei der Steuerberechnung für ihre Investitionen unterstützen zu können, indem mithilfe von Blockchains der Verlauf des über die Jahre investierten Geldes nachverfolgt wird.

Dalian Wanda, der größte Immobilienkonzern in China, ist ebenfalls in das Blockchain-Spiel eingestiegen. Gemeinsam mit dem Big-Data-Softwareunternehmen Cloudera rief er das Blockchain-Projekt Hercules ins Leben. Dalian Wanda zeigt das Potenzial der Blockchain-Technologie, Prognosen aus Big Data zu berechnen, mit deren Hilfe das Management Entscheidungen treffen kann. Es soll damit von einer reaktiven in eine proaktive Situation versetzt werden, etwa bei Strategiewechseln. Außerdem lässt sich damit das Nutzerverhalten in abgeschlossenen Systemen beobachten. Dalian Wanda und Cloudera wollen Hercules weiterentwickeln und die Technologie in unterschiedliche Branchen integrieren, die IT und Big Data benötigen. Das Hercules-Projekt ist ein Open-Source-Paket, das sich an den Anforderungen von Unternehmen ausrichtet. Es vereinfacht die Bereitstellung und Verwaltung von Blockchain-Apps für große Datencluster.

Vielleicht finden Sie es seltsam, wenn ein Mining-Unternehmen mit einer traditionellen Baufirma zusammenarbeitet, um Probleme für Hedgefonds zu lösen, oder wenn Immobilienunternehmen Big Data nutzen, um Probleme für Systemadministratoren zu lösen, aber das ist der Wilde Westen der Blockchain-Welt. Es ist der Mangel an Blockchain-Experten und die hohe Nachfrage nach Blockchain-Projekten und Investitionen, die dieses Umfeld prägen.

Der Kampf um das Finanzkapital der Welt

Seit die Blockchain-Technologie 2015 mit unzähligen Nachrichten ins Bewusstsein der Öffentlichkeit rückte, hat sie sich immer weiter entfaltet. Viele Start-ups arbeiten seitdem an Beta- und Pre-Launch-Builds. Allein im Jahr 2016 entstanden quasi über Nacht fast 2.000 neue Blockchain-Start-ups. Seither gingen viele davon in Singapur, Dubai und London auf den Markt. Die Aufsichtsbehörden dieser progressiven Finanzzentren sind sehr aufgeschlossen für Innovationen. Dabei geht es für die in diesem Bereich führenden Länder nicht nur um Fintech und Smart Cities. Es ist ein Wettrennen um Bedeutung in einer Welt, deren Bürger – auch in finanzieller Hinsicht – immer mobiler werden.

Londons früher Weitblick

2016 veröffentlichte die britische Regierung einen Bericht namens *Distributed Ledger Technology: Beyond Block Chain* (https://goo.gl/asIz6L). Darin wurde erklärt, dass verteilte Ledger (Blockchains) genutzt werden könnten, um Korruption, Fehler und Betrug zu reduzieren und verschiedene Abläufe effizienter zu gestalten. Er besagte auch, dass Blockchains die Beziehung der Staatsbürger zu ihrer Regierung ändern könnten, indem sie für mehr Transparenz und Vertrauenswürdigkeit sorgten. London zeigt sich spätestens seit 2014 sehr aufgeschlossen gegenüber der Technologie. Viele frühe Blockchain-Start-ups wurden in London gegründet oder sind dort ansässig, weil es inoffiziell der sicherste Ort für einen Unternehmensaufbau war. Das war damals sehr wichtig, weil 2014 und 2015 viele Kryptowährungsunternehmer verhaftet wurden.

Seit der Veröffentlichung des genannten Berichts wurden Blockchains auch für den behördlichen Einsatz in Großbritannien zugelassen, unter anderem für die Whitehall-Ministerien (nicht ministeriale Abteilungen wie Grundbuchamt, Forstverwaltung und Lebensmittelstandards), lokale Behörden und Regierungsbeauftragte.

Nachfolgend werden einige interessante britische Projekte und Experimente vorgestellt:

- ✔ **Blockchainbasierte Verteilung von Sozialhilfeleistungen:** Das Ministerium für Arbeit und Renten arbeitete mit Barclays, RWE, GovCoin und der Universität von London an einem Experiment, um Sozialhilfeleistungen mithilfe der Blockchain-Technologie über eine Handy-App zu verteilen. Dabei wurde getestet, ob Zahlungen per Blockchain gesendet und nachverfolgt werden können.
- ✔ **Regierungs-DLT:** Credits, ein Anbieter für Blockchain-Plattformen, und die britische Regierung arbeiten gemeinsam an einem Framework, über das die britischen Ministerien mit der Blockchain-Technologie experimentieren können. DLT steht für Distributed Ledger Technology (Verteiltes-Kontobuch-Technologie).
- ✔ **Blockchainbasierte internationale Zahlungen:** Die Santander Bank hat einen Test von blockchainbasierten internationalen Zahlungen gestartet. Das Pilotprogramm umfasst eine App, die eine Verbindung zu Apple Pay einrichtet. Benutzer können die Fingerabdruck-ID verwenden, um Zahlungen zwischen zehn und 10.000 Pfund zu tätigen.
- ✔ **Einsatz der Blockchain-Technologie für den Goldhandel:** Die Königliche Münzanstalt nutzte die Blockchain-Technologie in Zusammenarbeit mit dem Marktbetreiber CME Group für den Aufbau eines Goldmarkts, in der Hoffnung, London zu einer attraktiven Stadt für den Goldhandel zu machen. Beide Seiten nutzten die Blockchain-Technologie, weil sie sie als effizienten digitalen Mechanismus für den Goldhandel betrachten.

Mit all diesen Experimenten soll ermittelt werden, ob Blockchain-Anwendungen als neue Plattform für den Austausch von Werten geeignet sind. Abhängig vom Erfolg oder Misserfolg dieser Experimente wird sich der weitere Weg für Großbritannien und die restliche Welt gestalten.

Die regulatorische Sandbox Singapurs

Singapur setzt genau wie Großbritannien alles daran, die Arbeitswelt so einfach, freundlich und finanziell attraktiv wie möglich zu gestalten. 2015 reisten Regierungsvertreter nach San Francisco, um Unternehmer zu ermuntern, in einer sogenannten *regulatorischen Sandbox* zu arbeiten – eine Abwandlung der aus der Programmierwelt bekannten *Entwicklungs-Sandbox*. Bei dieser handelt es sich eine sichere Umgebung, in der die Entwickler Software erstellen können. Dieselbe Idee hatte Singapur für den Aufbau von Software-Unternehmen.

Damals befanden sich Blockchain-Unternehmen in den USA und an vielen anderen Orten noch in der Grauzone. Das Konzept eines sicheren Orts, an dem man arbeiten und Geld investieren konnte, war für viele Unternehmer sehr attraktiv, auch für mich. Wenn Sie noch nie in Singapur waren, sollten Sie es einmal besuchen! Es ist dort sehr schön, sauber und sicher.

Singapur beschäftigt sich mit der Erkundung der Technologie, und das zahlt sich aus. Die singapurische Bank OCBC nahm mit der Blockchain-Technologie Auslandsüberweisungen an ihre Töchter OCBC Malaysia und Bank of Singapore vor.

Auch das Unternehmen R3 war in Singapur aktiv. Es eröffnete mit der Währungsbehörde von Singapur ein Labor für die gemeinschaftliche Forschung und Entwicklung digitaler Ledger-Technologien. R3 arbeitet an einer Plattform für den Interbankenhandel. Die Banken zahlen Bargeld ein, und es wird eine digitale Währung ausgegeben.

Die Zentralbank von Singapur rief ebenfalls ein Pilotprojekt ins Leben, zusammen mit acht ausländischen und ortsansässigen Banken sowie der Aktienbörse. Diese Machbarkeitsstudie soll die Verwendung der Blockchain-Technologie für den Interbankenhandel auswerten. Das Pilotprojekt hat außerdem das Ziel, grenzüberschreitende Fremdwährungstransaktionen zu überprüfen.

Jede Bank auf der Welt muss wissen, mit wem sie Geschäfte macht. Das gesamte KYC-Konzept (*Know Your Customer*) hilft, die Geldwäsche und den Geldtourismus zu bekämpfen.

In der nächsten Phase werden Fremdwährungstransaktionen definiert, wobei auf den KYC-Bemühungen von Singapur aufgebaut wird. Dies könnte dazu führen, dass das Land auch eine blockchainbasierte Identität einführt. Singapur verwendet bereits ein robustes und modernes digitales Identitätsmanagement, das sich ganz einfach mit einer Blockchain verbinden ließe.

Nicht nur Blockchain-Unternehmen experimentieren in Singapur. Alle wirklich großen Player sind beteiligt: die Bank of America, Merrill Lynch, IBM, Credit Suisse, die Bank von Tokyo-Mitsubishi UFJ Ltd., die DBS Bank Ltd., JP Morgan, die Hong Kong and Shanghai Banking Corp Ltd., die OCBC Bank, die United Overseas Bank und die Börse von Singapur.

Die Initiative Dubai 2020

Die Regierung Dubais hat den ambitionierten Plan, bis 2020 alle Regierungsdokumente und -systeme auf die Blockchain zu legen. Der Plan, papierlos zu arbeiten, ist Teil dieser Initiative, weltweit führend in der Blockchain-Technologie zu werden und die Effizienz in allen Bereichen zu steigern.

Der Minister für Kabinettsangelegenheiten und Zukunft hat erklärt, wie Benutzer mit dem neuen Programm ihre Zugriffsrechte über die Blockchain aktualisieren und überprüfen können. Sie müssen sich nur einmal mit ihren Daten anmelden, um Zugang zu Regierungsstellen und Privatunternehmen wie etwa Versicherungen und Banken zu bekommen. Außerdem ist geplant, die Technologie an andere Länder weiterzugeben, um einen einfacheren Grenzübertritt zu ermöglichen. Statt Ausweisen könnten die Reisenden vorab authentifizierte digitale Wallets und IDs nutzen.

Die Regierung Dubais schätzte, dass ihre Blockchain-Initiative potenziell 25,1 Millionen Stunden Produktivität einsparen könne. Diese Effizienzsteigerung würde auch helfen, den CO2-Ausstoß zu verringern.

Der Global Blockchain Council (GBC) von Dubai hat sieben neue öffentlich-private Gemeinschaftsprojekte angekündigt, bei denen die Kompetenzen und Ressourcen von Start-ups, lokalen Unternehmen und Regierungsstellen kombiniert werden. Sie wenden die Blockchain-Technologie auf Folgendes an:

- ✔ **Gesundheitswesen:** Das Softwareunternehmen Guardtime aus Estland arbeitet mit einem der größten Telekommunikationsanbieter von Dubai, Du, zusammen, um die technologische Erfahrung für die Digitalisierung von Aufzeichnungen aus dem Gesundheitswesen bereitzustellen und sie in der Blockchain zu speichern.
- ✔ **Diamantenhandel:** Ein Pilotprojekt setzt die Blockchain-Technologie für die Authentifizierung und den Transfer von Diamanten ein. Das Dubai Multi Commodities Center wird *Kimberly-Zertifikate* (von den UN ausgestellte Dokumente, die den Handel mit Blutdiamanten einschränken sollen) digitalisieren.
- ✔ **Eigentumsrechtsübertragungen:** Eigentumsrechtsübertragungen werden digitalisiert und in einer Blockchain aufgezeichnet. Das Blockchain-Start-up Dxmarkets aus Singapur hat eine Machbarkeitsstudie durchgeführt.
- ✔ **Unternehmensregistrierung:** Der GBC testet den Einsatz von Blockchains für die Unternehmensregistrierung. Das ist anders als bei den DAOs (dezentrale autonome Organisationen) von Ethereum, könnte aber die Identitätsüberprüfung durch das Flexi-Desk-Programm optimieren. Derzeit befindet sich das Projekt in der Demo-Phase. Mehrere Teilnehmer arbeiten an einer Machbarkeitsstudie.

- **Tourismus:** Dubai Points ist ein Pilotprogramm, das in Zusammenarbeit mit Loyyal, einem weiteren Blockchain-Unternehmen, ins Leben gerufen wurde. Hier soll die Blockchain-Technologie die Tourismusbranche unterstützen. Dabei soll ein Anreiz geschaffen werden, indem Reisenden, die bestimmte Orte besuchen, Punkte gutgeschrieben werden. Dieser Anreiz wird mithilfe von Smart Contracts unterstützt. Die Punkte funktionieren ähnlich wie ein Krypto-Token und können an Börsen gehandelt werden.
- **Versand:** IBM arbeitet mit dem GBC zusammen, um die Blockchain-Technologie zur Optimierung von Versand und Logistik einzusetzen. Das Programm zielt darauf ab, regionale Unternehmen beim Güteraustauch zu unterstützen. Als Lösungen für Compliance- und Zahlungsprobleme werden Smart Contracts verwendet.

Dubai investiert genau wie Singapur Geld und Fachleute, um das Blockchain-Feld schnell dominieren zu können. Diesen Luxus können sich kleine Regierungen mit zentraler Machtstruktur leisten.

Das Bitlicense-Regelwerk: New York City

Wenn Sie ein Blockchain-Start-up in New York City betreiben wollen, machen Sie sich auf zusätzliche Gebühren gefasst. Im Juni 2015 veröffentlichte das New York State Department of Financial Services (NYDFS) die endgültige Version von Bitlicense, einem regulatorischen Rahmenwerk für digitale Währungen, das mehr Klarheit in der Branche schaffen sollte. Tatsächlich hat man damit viele Blockchain-Start-ups aus New York vertrieben. Die eigentliche Lizenz kostet 5.000 US-Dollar und kann bis zu 500 Seiten umfassen. Man benötigt dafür die Fingerabdrücke der Unternehmensführung sowie eine umfangreiche Hintergrundprüfung des antragstellenden Unternehmens. Die größte Hürde sind die hohen Kosten von geschätzt etwa 100.000 US-Dollar pro Bewerbung. Diese Schätzung beinhaltet

Zeitaufwand sowie Anwalts- und Compliance-Gebühren. Bitlicense ist das genaue Gegenteil der Bemühungen, die andere Finanzzentren wie London, Singapur und Dubai unternehmen.

Bitlicense war das Ergebnis von fast zwei Jahren Analysen und Debatten darüber, wie die Technologie geregelt werden solle, nachdem man festgestellt hatte, dass die vorhandenen Vorschriften nicht für Kryptowährungsunternehmen geeignet waren.

Ein positiver Aspekt ist, dass die Blockchain-Unternehmen in New York City keine Genehmigung vom NYDFS für neue Software-Updates oder neue Runden der Venturekapitalfinanzierung benötigen. Das Rahmenwerk besagt, dass Unternehmen mit digitaler Währung nur eine Genehmigung für Änderungen benötigen, die »für ein vorhandenes Produkt, einen Dienst oder eine Aktivität vorgeschlagen werden, die verursachen könnten, dass sich dieses Produkt, der Dienst oder die Aktivität maßgeblich von den zuvor auf dem Antrag für die Lizenzierung durch den Unternehmensleiter aufgelisteten unterscheiden«.

Das erste Unternehmen, das eine Bitlicense erhielt, war der Bitcoin-Wallet-Anbieter Circle. Die Lizenz gestattet ihm, innerhalb des Regelwerks von New York zu arbeiten. Circle ist eines der wenigen Unternehmen, denen dies gesetzlich erlaubt ist. Die meisten Blockchain-Start-ups vermeiden es, in New York zu arbeiten, weil die Kosten und der Aufwand für die Lizenz den Nutzen weit überwiegen. Deshalb engagieren sich hier nur finanzkräftige Start-ups.

Ripple erhielt mittlerweile seine zweite Lizenz. Diese gestattet ihm, XRP, die digitale Währung hinter dem Ripple Consensus Ledger (RCL), zu verkaufen und zu halten. Damit kann Ripple mit Geschäftskunden arbeiten, die seine Technologie für die internationale Übertragung von Geldern nutzen wollen.

Andere Regionen in den USA haben ähnliche Gesetze für die Regulierung von Kryptowährungen festgelegt und fordern eine Lizenzierung. Für Kalifornien sollte das Gesetz AB 1326 verabschiedet werden, was jedoch nach einem Einspruch der

Electronic Frontier Foundation (EFF) fehlschlug. Die EEF ist eine Gruppe mit Sitz in San Francisco, die sich für Verbraucherrechte und neue Technologien einsetzt.

Die freundliche Gesetzesstruktur von Malta

Malta hat als EU-Mitglied drastische und direkte Schritte in Richtung Blockchain-Technologie unternommen. Dieser Staat hat das Potenzial der Blockchain viel schneller als andere Länder erkannt und Maßnahmen ergriffen, um sich als Innovationszentrum zu profilieren. Die meisten Blockchain-Start-ups sahen sich anfangs mit einem feindlichen Umfeld konfrontiert. Viele ließen sich daher in Malta nieder, so auch die Mega-Exchange Binance.

Nach dem Austritt von Großbritannien aus der EU wird Malta eines der wenigen verbleibenden EU-Länder mit englischer Amtssprache sein. Malta hat ein Mischrechtssystem aus dem romanischen Rechtskreis und dem Gewohnheitsrecht (Common Law), wodurch es für die Wirtschaft attraktiv ist. Damit hat Malta eine gute Position inne, um internationale Blockchain- und Kryptowährungsunternehmen bei der Gründung und der Suche nach einer passenden Rechtsform zu unterstützen.

Malta ist eine kleine Insel, die schon viele Fremdherrschaften erlebt hat. Jede hat ihre eigenen Regeln aufgestellt, und einige haben sich verfestigt. Malta verfügt heute über einen gemischten Gesetzesrahmen, der römisches, französisches Recht und britisches Recht sowie eigene Gesetze umfasst, die vom maltesischen Parlament nach der Unabhängigkeit 1964 erlassen wurden. Vor allem ist Malta jedoch für das Zivil- oder Kontinentalrecht (das im Laufe der Jahre kodifiziert wurde) und das Gewohnheitsrecht (das durch Gerichtsurteile festgelegt wird) bekannt.

Malta hat drei bahnbrechende Gesetze verabschiedet, die den rechtlichen Status von Blockchain-Unternehmen und aller von

ihnen hervorgebrachten Innovationen deutlich verbessern. Sie bieten Rechtssicherheit und ein Gerüst, das dezentralisierte Technologie und Blockchains besser reguliert. Hier ist eine Zusammenfassung dieser drei Gesetze:

- ✔ Virtual Financial Assets Act (Gesetz über virtuelle finanzielle Vermögenswerte): Dieses Gesetz regelt Initial Coin Offerings (ICOs). Das Gesetz verpflichtet jedes Unternehmen, das sich über die Ausgabe neuer Coins Kapital beschafft, ein Whitepaper mit einer detaillierten Beschreibung des gesamten Projekts zu veröffentlichen. Beim ICO muss auch die Finanzhistorie des Unternehmens veröffentlicht werden.
- ✔ Malta Digital Innovation Authority Act: Damit wurde ein Regulierungsverfahren für Kryptowährungen und Blockchain-Unternehmen geschaffen. Außerdem wird eine Regulierungsbehörde namens Malta Digital Innovation Authority (MDIA) eingerichtet.
- ✔ Technology Arrangements and Services Bill (Technologievereinbarungs- und Dienstleistungsgesetz): Auf Grundlage des Technology Arrangements and Services Bill können sich Blockchain-Unternehmen und Kryptowährungsbörsen registrieren und von der maltesischen Regierung zertifizieren lassen.

Diese neuen Gesetze haben Malta für neue Technologien geöffnet und werden möglicherweise anderen Regierungen, die ebenfalls Innovationen anziehen wollen, als Vorbild dienen. Der größte Nutzen besteht darin, Unternehmen ein sicheres Umfeld für ihr Wachstum und weitere Experimente zu geben.

Sicherung der Grenzen auf der ganzen Welt

Blockchains werden von vielen Regierungen auf ihre Eignung zur Grenzsicherung untersucht. Großbritannien hat das ambitionierte

Ziel, dass Reisende auf Flughäfen nirgends warten müssen – man kann es sich kaum vorstellen, angesichts der langen Schlangen beim Sicherheitscheck, die man heute auf fast jedem Flughaften sieht. Die größte Hürde, die Großbritannien für reibungsloses Reisen überwinden müsste, wäre, die Identität jedes Passagiers definitiv zu kennen, selbst wenn er aus einem anderen Land stammt. Dies ist im Kampf gegen den Terrorismus seit Langem ein Problem.

Die USA haben ihre Technologie zur Passagieridentifizierung unter dem Global Travel Assessment System (GTAS) auf Github offengelegt, zu finden unter (www.github.com/US-CBP/GTAS).

Computer, Kameras und Sensoren für die nicht invasive Untersuchung und die Authentifizierung aller Passagiere müssen im Interesse der nationalen Sicherheit abgesichert werden. Blockchains sind wegen ihrer Unveränderlichkeit für diesen Einsatz sehr vielversprechend und werden heute daraufhin analysiert.

Ebenfalls interessant sind die biografischen Identitäten, die durch Blockchains realisiert werden können – Identitäten, die im Laufe der Zeit aufgebaut werden. Beliebige Daten können mit einer biografischen Identität verknüpft werden. Der Datenschutz und die Lesbarkeit der zugeordneten Daten können von den Veröffentlichern verwaltet werden. Im Laufe der Zeit wird die Identität durch Hinzufügen zusätzlicher Attribute aufgebaut. Attribute können alles Mögliche sein, von den Daten Ihres persönlichen Geräts bis zur Häufigkeit, mit der Ihre Dokumente bei einem Grenzübertritt kontrolliert wurden. Diese Attribute werden in der Identitätskette einer Person durch Zertifizierungsstellen oder durch von Zertifizierungsstellen bevollmächtigte Organisationen veröffentlicht.

Das US-Ministerium für innere Sicherheit und die Identität von Gegenständen

Die Abteilung für Wissenschaft und Technik des US-Ministeriums für innere Sicherheit beschäftigt sich mit der Absicherung von IoT-Geräten für den US-amerikanischen Grenzschutz. Gemeinsam mit Factom, Inc., einem Blockchain-Start-up mit Sitz im texanischen Austin, arbeitet es an der Weiterentwicklung der Sicherheit digitaler Identitäten für IoT-Geräte.

Factom erzeugt Identitätsprotokolle, die die ID eines Geräts erfassen, seinen Hersteller, Listen verfügbarer Updates, bekannte Sicherheitsprobleme und erteilte Genehmigungen. Zur zusätzlichen Absicherung wird auch die Zeitdimension hinzugefügt. Ziel ist, etwaige Hacker daran zu hindern, die Aufzeichnungen für ein Gerät zu verändern, sodass es schwieriger zu fälschen ist.

Ausweise der Zukunft

ShoCard (www.shocard.com) ist ein Unternehmen für die Anwendungsentwicklung, das mit dem Blockchain-Unternehmen Blockcypher zusammenarbeitet. Seine Prototypen ermöglichen es Ihnen, Ihre Identität innerhalb einer sicheren Blockchain-Umgebung einzurichten. Die ShoCard ID befindet sich in einer App auf Ihrem Smartphone und kann genutzt werden, um verschiedenste Zugangsdaten sicher weiterzugeben.

Die neue Geburtsurkunde

Vielleicht haben Sie noch nichts von Smartrac gehört, aber sehr wahrscheinlich haben Sie täglich mit der Technologie dieses Unternehmens zu tun. Smartrac ist der wichtigste Anbieter von RFID-Tags und anderen ID-Chips, die etwa in Ausweisen und Pässen enthalten sind.

Eine der größten Herausforderungen, der die Länder beim Kampf gegen eine Identitätsfälschung gegenüberstehen, ist die Authentifizierung der Dokumente, die für den Nachweis der Identität verwendet werden. Dabei handelt es sich etwa um Sozialversicherungskarten, Geburtsurkunden und sonstige Zeugnisse, die derzeit einfach und billig zu fälschen sind.

Smartrac kämpft mit immer fortschrittlicherer Technologie gegen dieses Problem. Die neueste Innovation des Unternehmens ist eine Software-Authentifizierungslösung namens dLoc, die es ermöglicht, Geburtsurkunden anhand eines Blockchain-Datensatzes zu überprüfen.

Die Dokumentdaten werden mit einer eindeutigen ID des NFC-Tags (Near Field Communication, Nahfeldkopplung) verknüpft, um einen 32-Bit-Hash-Wert zu erzeugen, der nur von der ausstellenden Behörde unter Verwendung eines privaten Schlüssels erkannt werden kann. Der Hash-Wert wird in Smart Cosmos gespeichert und in einer öffentlichen Blockchain gesichert. Anschließend kann das Dokument mit dem dLoc-Aufkleber mithilfe eines Lesegeräts oder einer mobilen App auf einem NFC-fähigen Smartphone überprüft werden.

Damit werden zwei erstaunliche Dinge erreicht, die mit Papierdokumenten nicht möglich sind:

- ✔ ein unveränderbarer Verlauf des Dokuments, der das korrekte Alter und den Eigentümer anzeigt,
- ✔ die Möglichkeit, die Authentizität eines Dokuments durch Zertifizierungsbehörden kryptografisch zu signieren. Selbst wenn also die Unterlagen für die Erstellung von Dokumenten gestohlen wurden, wären sie nicht richtig signiert. Und wenn ein Dokument nach der Ausstellung gestohlen wird, könnte es als gestohlenes Dokument gekennzeichnet werden.

Kapitel 16

Weitere Branchen

IN DIESEM KAPITEL

- Entdecken, wie Staaten auf der ganzen Welt versuchen, ihre Verwaltungen zu verschlanken
- Einen Vorsprung hinsichtlich verbesserter Internet-Infrastrukturebenen für Unternehmen und die private Nutzung bekommen
- Eine eigene Blockchain-Identität erstellen
- Informationen über Smart Contracts zu Geld machen

Meist konzentrieren wir uns auf die bekanntesten Blockchain-Projekte und ihre wirtschaftlichen Auswirkungen. Die Blockchain-Technologie ist aber inzwischen in alle Gesellschaftsbereiche vorgedrungen.

In diesem Kapitel stelle ich Ihnen einige vielleicht eher unerwartete, interessante und ungewöhnliche Blockchain-Anwendungen vor. Einige der spektakulärsten Umbrüche werden in Regierungssystemen, neuen Vertrauensebenen für das Internet und ganz neuen Blockchains-Branchen stattfinden. Ich zeige Ihnen hier die eindrucksvollsten Änderungen auf, die bereits heute stattfinden. Sie erfahren, wie sie sich auf Ihr Leben und Ihre Branche auswirken, ebenso wie auf die Regierungen und Behörden, unter deren Schutz Sie stehen.

Schlanke Regierungen

Einige kleinere Länder haben erkannt, dass sie mehr bieten müssen, um im globalen Wettbewerb zu bestehen, und zwar ohne

ihre eigenen Bürger dadurch zu belasten. Im Sinne der Wettbewerbsfähigkeit haben sich dabei viele der herkömmlichen Vorstellungen im Hinblick auf die Staatsbürgerschaft verändert. In einer Welt, deren ehemals feste Grenzen immer durchlässiger werden, in der sich die Menschen aussuchen können, wo sie leben und in welchem Land sie zu Hause sein wollen, präsentieren sich diese kleinen Länder als Vorreiter.

Staatsbürgerschaft wird zu einer Ware, die gekauft werden kann, wobei jede Nationalität unterschiedliche Vorteile bietet. Die Länder entfernen sich vom passiven Staatsbürgerschaftsmodell, bei dem man als Bürger eines Landes geboren wird, hin zu einem Modell, bei dem Sie die Staatsbürgerschaft auf Grundlage der von einem Land angebotenen Vorteile auswählen.

In diesem neuen Modell ist Nationalität nicht mehr an einen physischen Standort gebunden. Die Regierung kann ohne Grenzen oder einen physischen Standort existieren. Alte Modelle betrachten eine Nation als einen Standort, in den eine andere Nation einmarschieren kann, um ihn zu übernehmen, oder in dem die eigenen Leute beispielsweise bei einer Revolution die Herrschaft an sich reißen können.

Die Blockchain-Technologie und andere wegweisende Innovationen werden in diesen Bereichen begeistert aufgenommen – erstens, weil sie dieses Modell ermöglichen, und zweitens, weil sie der Regierung eine Last abnehmen, indem sie effizientere Systeme schaffen, auf die die Bürger an jedem Ort der Welt schnell zugreifen können, selbst wenn das geografische Staatsgebiet eingenommen wurde.

Singapur, Estland, die Vereinigten Arabischen Emirate (UAE) und China sind bei solchen Initiativen führend. Das Smart-Nation-Projekt in Singapur und die e-Residency in Estland sind einzigartige Systeme, die versuchen, den Papierkrieg und die Wartezeiten für Bürger zu reduzieren und die Effizienz der gemeinsamen Ressourcen zu steigern. Dubai möchte bis 2020 auf alle physischen Dokumente verzichten und sie durch blockchaingestützte Dokumente oder Systeme ersetzen. Und

Chinas Bemühungen zur Bekämpfung von Betrug haben die Dynamik im Blockchain-Bereich verändert.

Das Smart-Nation-Projekt in Singapur

Smart Nation nennt sich ein singapurisches Projekt, das in Zukunft ein besseres Leben für alle Bürger und Einwohner schaffen soll. Menschen, Unternehmen und Regierung arbeiten gemeinsam daran. Das Projekt erstreckt sich von der digitalen Identität bis hin zu IoT-Sensoren, die öffentliche Aufzeichnungen optimieren.

In Singapur ist man der Meinung, dass technologische Unterstützung ein sinnvolleres und erfüllteres Leben ermöglichen kann. Man nutzt neue Technologien, Netzwerke und Big Data in vollem Umfang und sucht aktiv nach Innovationen durch regelmäßige Sandbox-Projekte, aktive Rekrutierung und Belohnung innovativer Start-up-Unternehmen.

Eine Beschreibung der Smart-Nation-Initiative finden Sie unter https://goo.gl/EGmF4X.

Singapur konnte die neue Technologie wegen der kurzen Entscheidungswege in seiner Regierung schnell testen und einsetzen. Diese koordiniert die Richtlinien und Aufgaben zwischen den Einrichtungen schnell. Smart Nation ist ein ausgezeichnetes Beispiel für die Philosophie, dass neue Technologien die Politik ausstechen.

e-Residency in Estland

Estland ist ein kleines Land mit 1,3 Millionen Einwohnern. Die Ressourcen zur Erfüllung der Bedürfnisse seiner Staatsbürger sind begrenzt, aber mithilfe der Technik übersteigen Estlands Möglichkeiten die von weit größeren Ländern. Estland gibt digitale Ausweise für Online-Dienste heraus und bietet als erstes Land eine *e-Residency* an, eine digitale Identität, die jeder Mensch auf der ganzen Welt beantragen kann, der ein Online-Unternehmen betreiben will.

Die Bewerbung für eine estnische e-Residency dauert nur wenige Minuten, und die Hintergrundprüfung kostet 100 Euro. Eine e-Residency macht Sie nicht zum Esten, aber sie bietet Ihnen eine Menge Vorteile.


Auch Sie können e-Resident von Estland werden. Bewerben Sie sich online unter https://apply.gov.ee.

Nach dem Austritt aus der Sowjetunion investierte Estland viel in neue Technologie. Der traditionelle Verwaltungsapparat wurde größtenteils umgeformt und bietet nun eine einzelne Anlaufstelle für sämtliche bürgerlichen Belange, wie etwa Steuererklärungen und Zollabwicklungen. Hierfür genügt ein einziger sicherer Anmeldevorgang mit weltweitem Zugang. Dieses System ermöglicht einfache und papierlose Transaktionen. Alles kann komplett online erledigt werden, außer Hochzeiten und Immobilienkäufen. Estnische Staatsbürger können Banküberweisungen und Steuerzahlungen innerhalb weniger Minuten durchführen.

Die Esten erwarten, dass ihre Verwaltung immer weiter vereinfacht wird und mehr IT-Lösungen einsetzt. Die aktive Entwicklung von e-Services hat die Besucheranzahl der Steuer- und Zollbehörden zwischen 2009 und 2016 um über 60 Prozent gesenkt, wodurch es im Verwaltungsbereich insgesamt zu Einsparungen kam.

Estland führte 2015 eine Reform im Bereich der Einkommensteuer und Sozialabgaben durch. Die Umsatzsteuereinnahmen stiegen auch aufgrund der Entwicklung und umfassenden Nutzung von e-Services um 125 Millionen Euro gegenüber dem Vorjahr an. Die estnische Regierung führte einen Steuerrechner ein, der Daten aus den eingebundenen Banksystemen der Bürger übernimmt. Außerdem vereinfachte sie das Hochladen von Belegen.

Die Esten haben die Blockchain-Technologien begeistert übernommen. Die nächste große Entwicklung wird eine blockchainfähige Cloud sein. Estland beauftragte Ericsson,

Apcera und Guardtime, gemeinsam eine hybride Cloud-Plattform zu entwickeln und zu betreiben. Diese soll die Skalierbarkeit, Ausfallsicherheit und Datensicherheit für Steuererklärungen und medizinische Online-Dienste verbessern.

Nasdaq entwickelt ebenfalls Blockchain-Dienste in Estland. Das Unternehmen baut einen Markt für private Unternehmen auf, der die von ihnen ausgegebenen Aktien überwacht und Transaktionen unmittelbar verrechnet, und konzentriert sich auf die Verbesserung des Vertreterstimmrechts für Unternehmen.

Gemeinsam mit Estland entwickelt das Bitnation-Projekt für estnische e-Residents ein öffentliches Notariat, über das sie unabhängig von ihrem Wohnort oder ihrem Geschäftsstandort ihre Heirats- und Geburtsurkunden sowie Geschäftsverträge in einer Blockchain beurkunden können. Per Blockchain beglaubigte Dokumente sind weder in der Gerichtsbarkeit von Estland noch in anderen Ländern rechtlich bindend, ermöglichen es den Bürgern aber dennoch, das Alter dieser Dokumente zu belegen.

Bessere Beurkundung in China

China verbindet eine Hassliebe mit Kryptowährungen. Einerseits wurde in China versucht, Token als Mittel zur Geldwäsche zu nutzen und damit Geld außer Landes zu schaffen oder Gewinne vor dem Fiskus zu verbergen. Dies veranlasste die chinesische Regierung, den Gebrauch von Kryptowährungen stärker zu regulieren. Nachdem sich jedoch die Anwendungsbereiche des zugrunde liegenden Blockchain-Konzepts über die reine Bewegung von Werten hinaus entwickelten, machte sich auch China die Blockchain-Technologie zunutze.

Ein interessantes Beispiel für den frühen Einsatz war Ancun Zhengxin Co., ein führendes Unternehmen für den Umstieg auf elektronische Datenbeurkundungsdienste in China. Es pflegt Partnerschaften mit über 100 herkömmlichen Notariaten in 28 Provinzen. Außerdem bietet es elektronischen Datenspeicher und eine Blockchain-Beurkundungslösung über herkömmliche Kanzleien an.

Ancun veröffentlicht Tausende von Datensätzen in einer öffentlich einsehbaren Blockchain, die es den Benutzern gestattet, die Authentizität und das Alter beurkundeter Dokumente zu überprüfen.

Viele Startups in den USA arbeiten an ähnlichen Konzepten. Beispielsweise ermöglicht Ihnen Tierion (www.tierion.com), einen Hash zu erzeugen und mit einem Zeitstempel zu versehen. Anschließend werden die Daten für Sie in der Bitcoin-Blockchain verankert.

Die Vertrauensebene für das Internet

In den letzten 30 Jahren wurde das Internet in Ebenen aufgebaut – eine Ebene über der anderen –, wodurch es für die Benutzer immer einfacher und sicherer wurde. Die Blockchain ist die nächste Ebene im Internet. Sie können sie sich als die Vertrauensebene vorstellen. Irgendwann wird die Öffentlichkeit wahrscheinlich gar nicht mehr darüber nachdenken, und Online-Interaktionen werden einfach angenehmer. Durch die Implementierung der Blockchain-Technologie werden irgendwann all die lästigen Probleme wegfallen, die es online im Moment oft gibt, weil sich die Vertrauenswürdigkeit von Information nicht zufriedenstellend beurteilen lässt.

In zwei Schlüsselbereichen hat die Arbeit bereits begonnen. Sie bekommen das vielleicht nicht mit, werden das Ergebnis aber lieben: E-Mails mit wenig bis überhaupt keinem Spam und eine neue Art der Online-Identität.

Spamfreie E-Mail

Wahrscheinlich gehen Ihnen massenhafte Spam-Mails genauso auf die Nerven wie mir, aber das Problem liegt noch viel tiefer. Die aktuellen E-Mail-Systeme sind nicht mehr sicher. Ende 2016 erlitt Yahoo! einen der größten Hacker-Angriffe der Welt. Eine Milliarde

Benutzerkonten wurden geknackt und die persönlichen Daten der Benutzer dabei offengelegt.

Die Sicherung von E-Mails ist ein überzeugender Anwendungsfall für die Blockchain-Technologie, und die Zeit ist reif, neue Wege in der E-Mail-Technologie einzuschlagen. Eine Legende der Online-Sicherheit hat die Herausforderung angenommen: Dr. John McAfee, der Pionier der Antiviren-Software, entwickelte eine neue, blockchainbasierte E-Mail-Plattform.

John McAfees SwiftMail (www.johnmcafeeswiftmail.com) ist ein auf einer Blockchain basierendes E-Mail-System. Es unterscheidet sich nicht wesentlich von den E-Mail-Systemen, die Sie kennen. Es bietet einfache Navigationsmöglichkeiten und einige Entwickler haben Handy-Apps und webbasierte Apps erstellt, um die Benutzererfahrung noch zu verbessern.

Die Blockchain von SwiftMail bestätigt, dass Ihre E-Mail authentisch ist und dass die von Ihnen gesendeten E-Mails von den gewünschten Parteien empfangen wurden. Es ist also nicht mehr nötig, Ihre Daten einem Drittanbieter wie Yahoo! anzuvertrauen. Außerdem kostet jede versendete E-Mail einen geringen Geldbetrag, was Spammer abschreckt.

SwiftMail legt größten Wert auf Datenschutz, während viele Dienstanbieter eine gleichgültige Haltung an den Tag legen. Dazu John McAfee: »Wenn Datenschutz keine Rolle spielt, würden Sie Ihre Brieftasche dann einer wildfremden Person anvertrauen, die sie durchsehen und sich alles aufschreiben kann, was sie darin findet? Warum in aller Welt sollte es uns dann egal sein, dass jemand unsere Informationen einsehen kann, nur weil wir nichts Verbotenes tun?«

SwiftMail verwendet eine Wallet-Adresse, ähnlich wie eine Bitcoin-Wallet, die in einer Anwendung auf Ihrem Computer gespeichert wird. Sie besteht aus 32 Zufallszahlen ohne Metadaten, und die Benutzer können schnell eine neue erzeugen, genau wie bei Bitcoin. Die E-Mails selbst werden mit einem 256-Bit-Schlüssel vollständig verschlüsselt, sodass abgefangene Daten für Diebe nutzlos sind.

Derzeit stehen Downloads von SwiftMail nur für Android, Linux und Windows zur Verfügung. Bisher bietet die Software keine applefreundliche Version. Achten Sie darauf, dass Sie die für Sie richtige Version herunterladen.

Andere Projekte in diesem Bereich, beispielsweise Earn (https://earn.com), arbeiten an der Entwicklung eines Blockchain-Backends für E-Mails. Earn hat ein E-Mail-System entwickelt, das von Personen außerhalb Ihres Netzwerks eine Gebühr verlangt, wenn sie Ihnen eine E-Mail senden wollen. Sie können das Geld dann entweder behalten oder für wohltätige Zwecke spenden.

Im Besitz der eigenen Identität

Einer der wichtigsten Grundsätze, über den alle Blockchain-Befürworter sprechen, ist die persönliche Verantwortung für den Besitz der Daten, die Sie selbst erstellen und die Sie eindeutig identifizieren. Dieses Konzept scheint ganz einfach zu sein, aber die meisten Menschen üben keine Kontrolle über die Daten aus, die ihre Identität repräsentieren.

Die meisten Daten liegen in zentralen Datenbanken, die anfällig für Angriffe sind. Diese Datenbanken speichern die Informationen, und Zertifizierungsbehörden überprüfen, ob die Informationen korrekt und unverändert sind. Im Informationszeitalter sind Ihre Daten Ihre Identität. Je weiter die Daten verteilt sind, desto wahrscheinlicher ist es, dass sie in die Hände von Angreifern fallen, die sie missbrauchen wollen.

Bei der blockchainbasierten Identität liegt die Kontrolle über die Identität in den Händen der Menschen oder Unternehmen, die die Identität repräsentiert. Zentrale Datenbanken und Zertifizierungsbehörden werden nicht unbedingt ersetzt. Die Daten brauchen immer noch ein sicheres Zuhause, und es ist sinnvoll, dass Drittparteien die Authentizität von Dokumenten überprüfen.

Die Verantwortung für die Identität zurück auf das Individuum zu verlagern, hat den Vorteil, dass es dann schwieriger wird, identitätsstiftende Dokumente zu stehlen, in Geiselhaft zu nehmen oder zu manipulieren. Informationen werden nach Bedarf weitergegeben, ohne unnötige Informationen offenzulegen. Eine unwiderrufliche und global zugängliche Identität muss nicht immer eine gute Sache sein. Die Entwickler von Identitätsplattformen müssen den Schutz der Benutzer etwa hinsichtlich einer Bonitätsprüfung, dem Recht, vergessen zu werden, und der Anonymität bei Wahlen berücksichtigen.

Blockchain-Orakel

Die Blockchain-Technologie löst nicht das Problem für Sie, dass Informationen von irgendwoher kommen müssen. Außerdem müssen die Informationen zuverlässig sein. Diese menschliche Komponente darf in der Gleichung nicht vernachlässigt werden, wenn Sie einen Vertrag in einem Blockchain-System eingehen möchten.

Es gibt keine zentrale Autorität, die Ehrlichkeit in einem Blockchain-System vorschreibt oder erzwingt. Die zukünftige Ehrlichkeit der Verfasser von Informationen lässt sich nicht vorhersagen. Die logische Schlussfolgerung ist, dass jede Transaktion jeweils weniger kosten muss als die Kosten für den Wiederaufbau der Reputation. Die Reputation vertrauenswürdiger Verfasser wird im Laufe der Zeit aufgebaut, und je länger ein Verfasser ehrlich und korrekt ist, desto wertvoller wird seine Reputation. Dieses Konzept ist vergleichbar mit dem Wert eines Markennamens.

In diesem Abschnitt erkläre ich, wie Künstler und Kreative die Blockchain-Technologie nutzen können, um Geld mit ihrer Arbeit zu verdienen.

Vertrauenswürdige Verfasser

Smart Contracts und Chaincode bieten findigen Einzelpersonen und Unternehmen neue Chancen, ihre Informationen zu Geld zu

machen. Diese Systeme brauchen vertrauenswürdige Informationsquellen für ihren Betrieb. Bei solchen zuverlässigen Quellen könnte es sich beispielsweise um Rating-Agenturen handeln.

Sie könnten auch IoT-Geräte mit einer Blockchain-Infrastruktur verbinden und ihnen eigene Stimmen und Identitäten in einem Blockchain-Netzwerk geben. Sie müssen im Laufe der Zeit Vertrauen aufbauen und sind trotzdem jederzeit angreifbar. Ehrliches Verhalten in der Vergangenheit verhindert keine Unehrlichkeit in der Zukunft oder die Unterwanderung einer Informationsquelle.

Nicht jeder Smart Contract oder Chaincode ist in sich abgeschlossen oder wird mit ausfallsicheren Quellen ausgeführt. Praktische unternehmerische Anwendungsfälle brauchen auch Zugriff auf Informationsquellen außerhalb des bekannten Universums eines Blockchain-Netzwerks. Mehrere Start-up-Unternehmen nähern sich diesem Problem auf unterschiedliche Weise an.

Das Start-up-Unternehmen Po.et entwickelt ein dezentrales Protokoll für mediale Inhalte. Das System zeichnet Metadaten und Urheberinformationen über kreative Assets wie Texte und Musik auf und speichert sie mit einem Zeitstempel. Damit lässt sich die Urheberschaft zweifelsfrei belegen, und die spätere Katalogisierung und Vermarktung von Inhalten wird erleichtert.

Factom hat mit Acolyte einen Service entwickelt, mit dem Benutzer im Laufe der Zeit einen Ruf für die von ihnen im Netzwerk bereitgestellten Informationen aufbauen können. Die Entwickler von Smart Contracts können es abonnieren und für die erstellten Orakel bezahlen. Sie können sie auch auf ihre Vertrauenswürdigkeit hin bewerten.

Augur, ein weiteres Blockchain-Start-up, hat sich der Idee der Prognosemärkte von einer völlig anderen Seite her angenähert. Augur ist eine Plattform, die die Benutzer für eine Prognose zukünftiger realer Ereignisse belohnt, wie beispielsweise eine Wahl oder Unternehmensübernahmen. Die Wetten erfolgen durch

den Handel virtueller Anteile am Ergebnis der Ereignisse. Die Benutzer verdienen Geld, indem sie Anteile an den richtigen Ergebnissen kaufen. Die Kosten für die Anteile variieren abhängig davon, was die Gemeinschaft über die Wahrscheinlichkeit des tatsächlichen Ereignisses denkt. Augur ähnelt einem Online-Wettbüro. Jeder kann eine Prognose abgeben. Jeder kann einen Prognosemarkt für ein beliebiges Ereignis erzeugen. Damit könnten Sie als Unternehmenseigentümer beispielsweise eine Umfrage durchführen, um zu erfahren, was die Menschen für am wahrscheinlichsten halten. Dies könnte sogar Insider-Informationen aufdecken, aus denen die Verfasser Gewinn schlagen wollen.

Recht auf geistiges Eigentum

Die Musikindustrie wurde von dem Problem der geistigen Eigentumsrechte besonders schwer getroffen. Top-Interpreten werden von zahlreichen Mittelsleuten, die von ihrer kreativen Arbeit profitieren, wirtschaftlich ausgenutzt. Unbekannte Künstler können nicht ausschließlich von ihrer Musik leben, weil sie nur einen kleinen Teil des Umsatzes erhalten. Megastars verdienen nur aufgrund der riesigen Menge an Fans gut.

Das Internet hat es für Künstler aller Bekanntheitsgrade einfacher gemacht, ihre Arbeit zu verbreiten. Gleichzeitig ist es für sie aber noch schwerer geworden, von ihrer Lieblingsbeschäftigung gut zu leben. Die Nahrungskette in der Musikbranche ist lang, und jeder Mittelsmann nimmt sich ein kleines Stück vom Kuchen und verlängert wiederum die Zeit, die es dauert, bis das Geld endlich den Künstler erreicht hat. Häufig wartet dieser 18 Monate oder mehr, bis er Geld erhält, und mancher bekommt nur 0,000035 US-Dollar pro Streaming-Instanz seiner Musik. Und diese Situation geht nur vom besten Fall aus, dass niemand den Künstler betrügt.

Blockchains wurden als Möglichkeit eingeführt, die massiven finanziellen Belastungen der kreativen Berufsgruppen zu verringern. Mit Kryptowährungen ließen sich Kreditkartengebühren und Betrügereien reduzieren. Außerdem

könnten sie neue Märkte in Entwicklungsländern eröffnen, die keinen großflächigen Zugang zu Kreditkarten haben.

Eine noch interessantere, aber weniger einfache Möglichkeit wäre es, das gesamte Ökosystem der Musikbranche in ein Blockchain-System zu verschieben, das Smart Contracts oder Chaincode verwendet, um eine unmittelbare Bezahlung für die Nutzung zu vereinfachen. Damit könnte auch das Eigentum an Lizenzen geklärt werden, und die Verbraucher hätten es einfacher, Musik für die kommerzielle Verwendung zu lizenzieren.

Mehrere Projekte arbeiten an diesem Problem und versuchen, ein gesundes, nachhaltiges und reibungsloses Ökosystem zu fördern, eines, das keine Marktteilnehmer ausbootet, aber den Künstlern gestattet, etwas mehr mit ihrer harten Arbeit zu verdienen.

Die Plattform von UjoMusic befindet sich in der Beta-Testphase. Auf ihr können die Nutzer Musik direkt verkaufen und lizenzieren. Dabei setzt sie auf das Ethereum-Netzwerk, Smart Contracts für die Ausführung und Ether (die Kryptowährung von Ethereum) für die Zahlung. Sie können ein ganzes Lied herunterladen oder nur die Vokal- oder Instrumentalspuren, die sie für den kommerziellen oder nicht kommerziellen Einsatz brauchen. Die Musiker werden unmittelbar in Ether bezahlt.

Peertracks ist ein weiteres Blockchain-Start-up, das auf einen Umbruch der Musikbranche hinarbeitet. Es handelt sich dabei um eine Streaming-Website für Musik, deren Benutzer Musikstücke herunterladen und neue Künstler entdecken können. Dazu verwendet es sein Peer-to-Peer-Netzwerk MUSE und erstellt individuelle Künstler-Token. Diese Token funktionieren wie andere Kryptowährungen und variieren abhängig von der Popularität des Künstlers im Wert.

Blockchain-Technologie bedeutet nicht, dass man keine Labels und Distributoren mehr benötigt. Aber diese müssen schnell handeln, wenn sie nicht durch neue Unternehmen verdrängt werden wollen, die dieses effizientere Modell anwenden, genauso wie Netflix den Videoverleiher Blockbuster abgelöst hat.

Teil V

Der Top-Ten-Teil

Auf www.fuer-dummies.de finden Sie noch mehr Bücher für Dummies!

IN DIESEM TEIL …

Entdecken Sie zehn kostenlose Blockchain-Ressourcen, mit denen Sie über die Technologie und die ganze Branche auf dem Laufenden bleiben.

Lernen Sie zehn Regeln kennen, gegen die Sie niemals verstoßen dürfen, wenn Sie mit Kryptowährungen und Blockchains arbeiten.

Finden Sie mehr über die zehn besten Blockchain-Projekte und -Organisationen heraus, die die Zukunft der Branche bestimmen.

Kapitel 17

(Ungefähr) zehn kostenlose Blockchain-Ressourcen

IN DIESEM KAPITEL

- Kostenlose Ressourcen mit weiterführenden Informationen zu Blockchains entdecken
- In der Blockchain-Community mitwirken
- Niemals die neuesten Blockchain-News verpassen
- Ihre Kenntnis anderer Blockchain-Ressourcen erweitern

In diesem Kapitel stelle ich Ihnen interessante kostenlose (englischsprachige) Ressourcen aus dem Blockchain-Ökosystem vor. Diese sollen Ihnen helfen, sich weiter zu informieren und sich der Community anzuschließen. Hier finden Sie Videos, die Ihr Wissen erweitern, und Informationen über Unternehmen, die die Zukunft der Branche bestimmen werden.

Ethereum

Ethereum ist ein per Crowdfunding finanziertes Open-Source-Projekt, innerhalb dessen die Ethereum-Blockchain erstellt wurde. Es ist eines der wichtigsten Projekte überhaupt, weil es erstmals eine Programmiersprache in eine Blockchain eingebaut hat. Dank dieser eingebauten Programmiersprache können Sie im Ethereum-Netzwerk Smart Contracts programmieren, dezentrale Organisationen (DAOs) erstellen und dezentrale Anwendungen bereitstellen.

Ethereum 101 (www.ethereum101.org) ist eine Website der Mitglieder der Ethereum-Community. Ihr Inhalt wird laufend gepflegt, und Sie finden dort hochqualitative Informationen über die Blockchain-Technologie und das Ethereum-Netzwerk. Dieses Projekt wird von Anthony D'Onofrio geleitet, dem Director of Community bei Ethereum.

DigiKnow

DigiByte ist ein von Bitcoin inspiriertes, dezentrales Zahlungsnetzwerk. Es ermöglicht Ihnen, Geld über das Internet zu übertragen, und bietet kürzere Transaktionszeiten und niedrigere Gebühren als Bitcoin. Das Netzwerk steht auch allen Mining-Interessenten offen.

Der Gründer von DigiByte, Jared Tate, hat auf YouTube die Videoreihe DigiKnow erstellt, die Ihnen alles erklärt, was Sie für die Verwendung von DigiByte wissen müssen. Hier der Link zu seinem ersten Video, in dem er die Grundlagen von Blockchains erklärt und auf den Mehrwert eingeht, der durch das DigiByte-Netzwerk geschaffen wird: https://youtu.be/scr6BzFddso.

Blockchain University

Blockchain University ist eine Website, die Entwicklern, Managern und Unternehmern Informationen über die Blockchain-Welt bereitstellt. Sie bietet öffentliche und private Schulungsprogramme, Hackathons und Demo-Veranstaltungen. Die Programme enthalten lösungsorientiertes Design-Thinking und praktische Schulungen. Sie finden die Blockchain University in Mountain View, Kalifornien, oder unter http://blockchainu.co.

Bitcoin Core

Die Bitcoin-Core-Adresse (https://bitcoin.org) wurde ursprübglich von Satoshi Nakamoto genutzt, um sein Whitepaper über das Bitcoin-Protokoll zu hosten. Sie finden dort interessante

Informationen über das Bitcoin-Kernprotokoll und können verschiedene Versionen der originalen Bitcoin-Software herunterladen.

Die Website verfolgt das Ziel, Bitcoin dezentral und für jeden zugänglich zu halten.

Es handelt sich um ein Community-Projekt; deshalb wird nicht der gesamte Inhalt vom Programmierteam verwaltet. Denken Sie daran, wenn Sie Informationen dieser Website nutzen.

Blockchain Alliance

Die Blockchain Alliance wurde von der Blockchain Chamber of Digital Commerce und der Nachrichtenorganisation Coincenter gegründet. Es handelt sich dabei um eine öffentlich-private Zusammenarbeit der Blockchain-Community, der Strafverfolgungsbehörden und der Regulierer. Sie verfolgen das gemeinsame Ziel, die Blockchain-Welt sicherer zu machen und technische Entwicklungen in diesem Bereich zu fördern. Dazu bekämpft die Blockchain Alliance kriminelle Aktivitäten auf der Blockchain, indem sie Informationen, technische Unterstützung und regelmäßige Informationsveranstaltungen zu Bitcoin und anderen digitalen Währungen für die Benutzer von Blockchain-Technologie bereitstellt.

Weitere Informationen über ihre Veranstaltungen finden Sie unter www.blockchainalliance.org. Hier können Sie der Alliance auch beitreten.

Multichain Blog

Multichain ist ein Unternehmen, das Organisationen dabei hilft, schnell blockchainbasierte Anwendungen zu erstellen. Es bietet eine Plattform, die Millionen von Vermögenswerten auf einer privaten Blockchain erstellen kann. Sie können über seine Tools

zudem auch Aktivitäten in Ihrem Netzwerk nachverfolgen und überprüfen. Es stellt nicht nur sein Toolset und seine Plattform bereit, sondern ist gleichzeitig führender Vordenker im Blockchain-Bereich.

Hier meine Lieblingsbeiträge im Multichain-Blog (www.multichain.com/blog):

- ✔ Vier echte Blockchain-Anwendungsbeispiele (www.multichain.com/blog/2016/05/four-genuine-blockchain-use-cases/)
- ✔ Vorsicht vor dem unmöglichen Smart Contract (www.multichain.com/blog/2016/04/beware-impossible-smart-contract/)
- ✔ Smart Contracts und die DAO-Implosion (www.multichain.com/blog/2016/06/smart-contracts-the-dao-implosion/)
- ✔ Zero-Knowledge-Blockchains verstehen (www.multichain.com/blog/2016/11/understanding-zero-knowledge-blockchains/)

HiveMind

Paul Sztorc ist der Gründer von Truthcoin, einem Peer-to-Peer-Orakelsystem und Prognosemarktplatz für Bitcoin. Es verwendet eine Proof-of-Work-Sidechain, die Daten über den Status der Prognosemärkte speichert. Bitcoin unterstützt Finanzderivate und Smart Contracts über HiveMind, die Plattform, die sich aus dem Truthcoin-Whitepaper entwickelt hat. Weitere Infos und Lernmaterialien finden Sie unter http://bitcoinhivemind.com.

Smith + Crown

Smith + Crown ist ein Blockchain-Forschungsinstitut, das sich auf globale Trends, Branchenanalysen und die Struktur von Blockchain-Systemen konzentriert. Die Analysewerkzeuge von

Smith + Crown ermöglichen Blockchain-Projekten eine konstante Weiterentwicklung und Verbesserung. Der größte Teil der Forschungsergebnisse ist öffentlich und kostenfrei zugänglich. Sie können von den Recherchetools, unzähligen Berichten und Datenbanken über viele namhafte Projekte im Blockchain-Bereich profitieren. Smith + Crown agieren als Analysten und Berater für verschiedene bekannte Blockchain-Projekte und –Gruppen, wie die Chamber for Digital Commerce, die Token Alliance und Social Alpha. Besuchen Sie die Seite unter https://www.smithandcrown.com .

Die Podcast-Reihen Unchained und Unconfirmed

Die Podcast-Reihen Unchained und Unconfirmed präsentieren erstaunliche und aktuelle Interviews mit hochrangigen Branchenvertretern aus dem Blockchain- und Kryptobereich. Unchained ist ein wöchentlicher, einstündiger Podcast von Laura Shin, einer ehemaligen Forbes-Redakteurin. Sie ist die erste Mainstream-Reporterin, die in Vollzeit über Krypto-Assets berichtet. Shin befasst sich eindrucksvoll, gut durchdacht und tiefgründig mit den Menschen und Unternehmen, die das dezentrale Internet aufbauen. Mit ihrer Hilfe können Sie ein besseres Verständnis für Regulierungs-, Sicherheits- und Datenschutzprobleme erlangen, die der Blockchain-Technologie innewohnen. Sie können ihren Podcast unter https://unchainedpodcast.com anhören.

Dies sind einige hörenswerte Folgen:

- ✔ **Ledger on How Consumers and Institutions Should Be Safeguarding Their Private Keys:** https://unchainedpodcast.com/ledger-on-how-consumers-and-institutions-should-be-safeguarding-their-private-keys-ep-101/

- ✔ **How Donating Crypto Can Help You Save on Taxes:** https://unchainedpodcast.com/how-donating-crypto-can-help-you-save-on-taxes-ep-94/
- ✔ **Naval Ravikant On How Crypto Is Squeezing VCs, Hindering Regulators, and Bringing Users Choice:** https://unchainedpodcast.com/naval-ravikant-on-how-crypto-is-squeezing-vcs-hindering-regulators-and-bringing-users-choice/
- ✔ **How Binance Became the Most Popular Crypto Exchange in 5 Months:** https://unchainedpodcast.com/how-binance-became-the-most-popular-crypto-exchange-in-5-months-ep-84/

Kapitel 18

Zehn Blockchain-Regeln, die Sie niemals brechen dürfen

IN DIESEM KAPITEL

- Gesetzliche Schwachstellen erkennen
- Die technischen Unzulänglichkeiten von Blockchains verstehen
- Die besten Angriffspunkte von Dieben in Ihren Systemen identifizieren
- Die sichersten Vorgehensweisen entwickeln

In diesem Kapitel geht es darum, was Sie beim Umgang mit Blockchains und ihren Kryptowährungen berücksichtigen sollten.


Fragen Sie Ihren Steuerberater oder Anwalt, bevor Sie Finanzentscheidungen treffen. Diese Technologie ist neu, und ihre Regeln sind noch nicht vollständig ausgearbeitet.

Verwenden Sie Kryptowährungen oder Blockchains nicht, um das Gesetz zu umgehen

Die Legalität und die gesetzliche Regulierung von Kryptowährungen unterscheiden sich an vielen Orten der Welt. Es

ist kein Scherz, wenn ich Sie auffordere, Ihren Steuerberater oder Anwalt zu fragen. Das Geld ist gut angelegt und wird Sie vor Ärger bewahren.

Diese drei dummen Fragen werden mir erschreckend häufig gestellt:

- **Kann ich Kryptowährungen verwenden, um Schwarzgeld zu verstecken?** Das ist eine riskante Idee. Denken Sie daran: Blockchains zeichnen alle Transaktion für alle Ewigkeit auf. Selbst wenn Sie also denken, eine geschickte Methode zum Verbergen von ein paar Token gefunden zu haben, kann man Ihnen später jederzeit noch auf die Schliche kommen.
- **Kann ich Blockchains verwenden, um Geld außer Landes zu bringen?** Viele Länder legen Obergrenzen fest, wie viel Geld ihre Bürger außer Landes bringen dürfen. Auch dies sollten Sie aus den oben genannten Gründen nicht versuchen. Blockchains zeichnen alle Transaktionen für immer auf. Selbst die DEA-Ermittler, die Bitcoins vom berüchtigten Darknet-Marktplatz Silk Road entwendeten, wurden erwischt.
- **Kann ich mit Kryptowährungen illegale Waren kaufen?** Die Antwort lautet. Sie ahnen es: Nein! Blockchains zeichnen Ihre Transaktionen wirklich *für immer* auf!


Tun Sie mit Kryptowährungen und Blockchains nichts, was auch mit herkömmlichem Geld illegal wäre!

Halten Sie Ihre Contracts so einfach wie möglich

Dezentrale autonome Organisationen (DAOs), Smart Contracts und Chaincode sind im Moment in aller Munde. Vielen Unternehmen gefällt die Möglichkeit, Verwaltungs- und Gerichtskosten zu reduzieren. Eine bisweilen unterschätzte Besonderheit dieser Technologie ist, dass es sich einfach nur um

Code handelt. Das bedeutet, dass nirgendwo ein Mensch sitzt und die Regeln interpretiert, die Sie festgelegt haben und denen alle folgen müssen. Der Code wird zum Gesetz, und das Gesetz erstreckt sich nur darauf, was in dem Blockchain-Contract enthalten ist. Deshalb kann es sehr wichtig sein, alles sehr übersichtlich zu halten.

Niemand interpretiert den Code. Das bedeutet: Wenn der Code auf unerwartete Weise ausgeführt wird, gibt es niemanden, der die Absicht des Smart Contracts durchsetzen würde. Der Code ist das Gesetz, und somit ist nichts Ungesetzliches passiert. Sie sollten also Ihre Smart Contracts einfach und modular anlegen, um die Ergebnisse der Ausführung präzise einzugrenzen und vorhersehbar zu machen. Außerdem ist es sinnvoll, sie von anderen Entwicklern gründlich auf Schwachstellen überprüfen zu lassen.

Darüber hinaus ist auch die Reichweite der Blockchain entscheidend, auf der Sie Ihr Projekt aufbauen. Sie können sich das wie Gerichtsbezirke vorstellen. Natürlich kann ein Smart Contract auf externe Dateneingaben reagieren, aber er kann keine Finanzmittel von Konten anfordern, auf die er keinen Zugriff hat.

Was Sie ebenfalls berücksichtigen sollten, ist die Informationsquelle, auf die Ihr Smart Contract zugreift. Wenn es sich um Wetterdaten beispielsweise für einen landwirtschaftlichen Versicherungsvertrag handelt: Vertrauen Sie der Quelle? Könnten die Quelldaten vielleicht manipuliert werden? Vor der Implementierung sollten Sie die Vorhersagequelle sehr sorgfältig begutachten. Beachten Sie beim Programmieren eines Smart Contracts, dass sich Ihre Datenkanäle verändern könnten. Beispielsweise werden APIs häufig aktualisiert, und wenn Ihr Vertrag eine veränderte API aufruft, lässt er sich womöglich nicht mehr korrekt ausführen.

Veröffentlichungen nur mit größter Vorsicht

Daten, die in eine Blockchain gelangt sind, sind schwer wieder daraus zu entfernen. Das ist der ganze Sinn von Blockchains. Wenn Sie etwas hineingeschrieben haben, wird es also für sehr lange Zeit dort bleiben. Wenn Sie verschlüsselte sensible Informationen veröffentlichen, müssen Sie davon ausgehen, dass die Verschlüsselung eines Tages geknackt wird, sodass die von Ihnen verschlüsselten Informationen plötzlich von jedermann gelesen werden können.

Stellen Sie sich folgende Fragen, bevor Sie etwas veröffentlichen:

- ✔ Hätte ich ein Problem damit, wenn diese Informationen irgendwann entschlüsselt würden?
- ✔ Will ich diese Informationen für alle Ewigkeit mit beliebigen Dritten teilen?
- ✔ Sind diese Daten schädlich für Dritte, und könnte ich bei einer Veröffentlichung für irgendetwas haftbar gemacht werden?

Derzeit arbeitet man an der Quantenkryptografie, um eine quantensichere Verschlüsselung zu erhalten, aber weil sowohl Quantencomputer als auch die quantensichere Verschlüsselung noch in den Kinderschuhen stecken, ist schwer zu sagen, was die Technologie in 20 Jahren leisten kann.

Sichern Sie Ihre privaten Schlüssel! Unbedingt!

Blockchains sind äußerst konsequent. Ihnen ist es egal, ob Sie Ihre privaten Schlüssel oder Passwörter verloren haben. So mancher Krypto-Nerd hat unzählige Token in den Weiten der Blockchains verloren – Vermögen, das sich nicht wieder zurückholen lässt.

Die privaten Schlüssel, die Ihre Kryptowährung absichern, befinden sich häufig in Ihren Wallet-Dateien, deshalb müssen Sie diese schützen und sichern. Seien Sie vorsichtig mit Online-Diensten, die Ihr Geld für Sie aufbewahren. Bei vielen Kryptowährungsbörsen und Online-Wallets wurde bereits das gesamte Guthaben gestohlen. Screenshots oder Fotos zu machen und sie in der Cloud zu speichern, ist übrigens dasselbe, wie sich selbst eine E-Mail schicken. Was immer Sie tun, lassen Sie das bitte bleiben. Sie bringen damit Ihre Schlüssel in Gefahr. Legen Sie sich einen Plan zurecht, wie Ihre Liebsten auf Ihre Schlüssel zugreifen können, falls Ihnen etwas zustößt. Ein 30-jähriger, gesunder CEO einer Kryptobörse starb und blockierte dabei Coins im Wert von 190 Millionen Dollar, weil er keinen Nachfolgeplan hatte. Übersehen Sie auch keine mögliche Bluetooth-Verbindung als Hintertür zu Ihrer Offline-Wallet. Stellen Sie sicher, dass Ihr Gerät komplett vom Internet getrennt ist.

Speichern Sie nur kleine Mengen von Token für den täglichen Gebrauch online oder auf einem Gerät mit Internetzugang. Sie können sich Kryptowährungs-Wallets genau wie Portemonnaies vorstellen. Bewahren Sie darin nicht mehr Geld auf, als Sie jederzeit als Verlust verschmerzen können. Unzählige Malware-Apps sind darauf abgerichtet, Ihre privaten Schlüssel auszuspähen und Ihre Token zu stehlen.

Bewahren Sie den Rest Ihrer Kryptowährung im sogenannten *Cold Storage* auf – vollständig offline und ohne Internetzugriff. Dabei könnte es sich um eine Paper-Wallet handeln, um einen Computer, der keine Verbindung zum Internet hat, oder um eine

spezielle Hardware-Wallet, die für die Absicherung von Kryptowährung vorgesehen ist.

Wenn Sie für die Sicherung Ihrer Kryptowährung eine Paper-Wallet verwenden, laminieren Sie diese, und erstellen Sie sich Kopien. Beachten Sie dabei, dass Drucker und Kopierer oft Internetzugang oder interne Bildspeicher haben und ihre Daten von Dritten ausgelesen werden könnten. Wirklich paranoide Anwender nutzen Drucker ohne Internetzugang. Bewahren Sie Ihre Paper-Wallet-Kopien an unterschiedlichen Orten auf, beispielsweise in einem Schließfach oder an einem sicheren Ort bei Ihnen zu Hause.

Sichern Sie Ihre digitalen Wallets, und bewahren Sie sie an einem sicheren Ort auf. Das Backup ist für den Fall vorgesehen, dass Ihr Computer ausfällt oder Sie irrtümlicherweise die falsche Datei löschen. Hiermit können Sie Ihre Wallet wiederherstellen, falls Ihr Gerät kaputtgeht oder gestohlen wurde. Denken Sie außerdem daran, die Wallet zu verschlüsseln. Mit der Verschlüsselung können Sie ein Passwort für den Transfer von Token festlegen.

Tools, mit denen Sie Ihre Token sicher aufbewahren

Sie könnten in Betracht ziehen, die BitGo-Wallet zu verwenden, um Ihre Bitcoins abzusichern. Dabei handelt es sich zwar um eine Online-Wallet, aber BitGo fordert eine Online- und eine Offline-Signatur, um Zugriff auf die Token zu gewähren. Dank dieser Funktion ist sie sicherer als standardmäßige Online-Wallets.

BitGo-Wallets verwenden drei Schlüssel. Die Wallet hat einen, Sie haben einen, und ein weiterer wird für Sie von einem externen Service für die Wiederherstellung von Schlüsseln Key Recovery Service; KRS) aufbewahrt. Für jede Transaktion werden zwei Schlüssel angefordert. Normalerweise geschieht dies durch BitGo und durch Sie, es sei denn, Sie verlieren einen Ihrer Schlüssel. In diesem Fall hilft Ihnen der KRS weiter. Die BitGo-Wallet ist nicht umsonst – Sie müssen für jede Transaktion eine kleine Gebühr entrichten.

Weitere Informationen über die BitGo-Wallet finden Sie unter www.bitgocom/wallet.

Mit Verschlüsselung können Sie sich gegen Diebe schützen, aber nicht gegen Keylogging-Software. Nutzen Sie immer ein sicheres Passwort, das Buchstaben, Zahlen und Interpunktionszeichen enthält und mindestens 16 Zeichen lang ist. Die sichersten Passwörter werden von Programmen erstellt, die genau für diesen Zweck entwickelt wurden. Starke Passwörter kann man sich schlecht merken. Sie könnten sich Ihr Passwort aufschreiben und es laminieren, genau wie Ihre privaten Schlüssel. Es gibt nur begrenzte Möglichkeiten, Passwörter für Kryptowährung zurückzuerhalten, und ein vergessenes Passwort kann verlorene Token bedeuten.

Überprüfen Sie Adressen dreimal, bevor Sie Geld senden

Kryptowährung hat schon viele Gauner angezogen. Seien Sie also vorsichtig, wenn Sie Geld versenden. Sobald das Geld Ihre Wallet verlassen hat, ist es für immer weg, und Sie können es nicht mehr zurückholen. Es gibt keine Rückbuchungen und keinen Kundensupport. Das Geld ist tatsächlich verloren.

Überprüfen Sie die Empfängeradresse dreimal, bevor Sie Geld senden. Stellen Sie immer sicher, dass Sie es an die richtige Adresse schicken. Achten Sie auch beim Kopieren und Einfügen sehr genau auf die Adresse. Es gibt Schadsoftware, die Ihre Adresse beim Verwenden der Tastenkürzel Strg+C und Strg+V gegen eine andere austauscht.

Seien Sie vorsichtig bei der Verwendung von Börsen

Börsen für Kryptowährung sind zentrale Angriffspunkte für Hacker, die es auf Ihre Token abgesehen haben. Sie betrachten sie als Goldgrube, die sie nur anzapfen müssen. Über 150 Börsen wurden bereits geknackt. Das sollten Sie beachten, wenn Sie solche Handelsplätze aufsuchen. Befolgen Sie die in diesem Buch beschriebenen Verfahren, um Ihre Token zu sichern. Sehen Sie sich die jeweilige Börse genau an, um ihre Sicherheitsmaßnahmen zu evaluieren.

Eine Zwei-Faktor-Authentifizierung ist unerlässlich. Vielleicht können Sie bei Ihrem Mobilfunkanbieter auch ein geheimes Passwort einrichten, um Social Engineering zu verhindern. Sie wollen schließlich nicht zum Opfer eines SIM-Kartentauschs werden. Die Handynnummer muss aber nicht unbedingt Ihr Back-up sein; Google und einige andere Unternehmen bieten auch eine Zwei-Faktor-Authentifizierung an (suchen Sie nach der Google Authenticator App).

Nutzen Sie Börsen nur, um Ihre Geldmittel einzuzahlen oder abzurufen. Verwenden Sie sie nicht, um Werte zu speichern. Größere Mengen Kryptowährung bewahren Sie am besten in einer vom Internet abgeschnittenen Cold-Wallet oder in einer laminierten Paper-Wallet mit mehreren Kopien auf.

Hüten Sie sich vor WLAN

Wenn Ihr Router nicht korrekt eingerichtet wurde, kann jeder ein Protokoll all Ihrer Aktivitäten einsehen. Wenn Sie an einem ungesicherten öffentlichen Internetzugang arbeiten, könnten Sie zudem auch Schadsoftware ausgesetzt sein. Gehen Sie davon aus, dass der Netzwerkbetreiber Ihre Aktivitäten sehen kann.

Nutzen Sie nur vertrauenswürdige WLAN-Netzwerke, und stellen Sie sicher, dass das Passwort für Ihren Router möglichst sicher ist. Die meisten Passwörter für WLAN-Router sind auf die Werkseinstellung »admin« gesetzt und können von Dritten ganz leicht erraten werden.

Wählen Sie Ihren Blockchain-Entwickler sorgfältig aus

Die Blockchain-Technologie ist noch ganz neu, und es gibt noch nicht viele Entwickler, die sich mit Blockchain-Anwendungen auskennen.

Wenn Sie einen Entwickler engagieren wollen, der Sie bei Ihrem Projekt unterstützt, sollten Sie in GitHub nachforschen und sich seine bisherigen Projekte ansehen, ehe Sie ihn beauftragen. Möglicherweise hat er noch keine spezifischen Blockchain-Erfahrungen, ist aber außerhalb der Blockchain-Welt ein sehr fähiger Entwickler.

Es gibt nicht viele Ressourcen, die Entwicklern weiterhelfen, wenn sie nicht mehr weiterwissen. Unerfahrene Entwickler haben möglicherweise ihre Probleme, und momentan sind die meisten noch unerfahren, was die Entwicklung Ihrer Anwendung verzögern kann.

Lassen Sie sich nicht entmutigen

Die Blockchain-Branche als Ganzes verfügt nicht über denselben Schutz und die Sicherheitsmaßnahmen wie Banken oder andere Finanzeinrichtungen, und es gelten nicht dieselben Gesetze für Ihren persönlichen Schutz und Ihr finanzielles Wohlergehen. Hier gibt es keinen staatlichen Verbraucherschutz und keine

Einlagensicherung. Wenn Sie bestohlen wurden, können Sie niemanden um Hilfe bitten.

Die Branche erfuhr in den letzten Jahren einen riesigen Hype, ohne dass irgendwelche Ergebnisse von größerem Wert entstanden wären. Im Jahr 2016 wurden über Nacht Tausende neuer Blockchain-Unternehmen aus der Taufe gehoben, die alle behaupteten, Erfahrung zu besitzen. Sie wollen ein Projekt entwickeln und möchten feststellen, ob es die Investition überhaupt wert ist? Dann denken Sie immer zuerst einen Moment nach, ob es überhaupt sinnvoll ist. Stellen Sie sich dabei die folgenden Fragen:

- ✔ Wird realer Mehrwert geschaffen?
- ✔ Ist dieser Mehrwert für Sie von Vorteil?
- ✔ Warum gibt es das nicht schon?
- ✔ Gibt es andere, erprobtere Technologien, die dasselbe ebenso effizient oder noch besser bewerkstelligen?

Die Blockchain-Technologie ist sehr vielversprechend und kann viel leisten. Gerade deshalb sollten Sie sich ihr wohlüberlegt und vorsichtig nähern.

Handeln Sie keine Token, wenn Sie nicht wissen, was Sie tun

Kryptowährungen sind extrem volatil, und ihr Marktwert kann jederzeit und aus teilweise unerfindlichen Gründen stark schwanken. Viele Kryptowährungen haben eine geringe Markttiefe, sodass beim Verkauf größerer Mengen der ganze Markt einbrechen kann. Wenn Sie mit öffentlichen Blockchains arbeiten, müssen Sie aber wahrscheinlich einen gewissen Betrag in ihrer Währung halten, um sie überhaupt nutzen zu können.

Handeln Sie nicht mit Token, wenn Sie den Markt nicht gut genug verstehen. Wenn Sie bisher noch keine traditionellen Anlagen wie

Aktien gehandelt haben, sollten Sie sich besonders viel Zeit nehmen, um Kryptowährungen zu verstehen. Sie müssen genauso tief in die Materie eintauchen, wie Sie es am Aktienmarkt tun würden, bevor Sie zu handeln anfangen. Überlegen Sie auch, *Cryptocurrency Investing For Dummies* von Kiana Danial (Wiley) zu lesen. Vergessen Sie auch nicht, den Handel von Token und Kryptowährungen mit Ihrem Steuerberater abzusprechen. Möglicherweise müssen Sie die Gewinne oder Verluste in Ihrer Einkommensteuererklärung angeben.

Kapitel 19

Zehn herausragende Blockchain-Projekte

IN DIESEM KAPITEL

- Neue Blockchain-Initiativen kennenlernen
- Weltweite Blockchain-Implementierungen entdecken

Jeden Tag entstehen neue Blockchain-Start-ups. Unternehmer sehen zahllose Gelegenheiten, Kapital aus den leistungsstarken Tools der Blockchains zu schlagen, mit denen Geldtransfers beschleunigt, Computersysteme gesichert und digitale Identitäten erstellt werden können.

In diesem Kapitel stelle ich Ihnen einige meiner bevorzugten Projekte und Unternehmen vor. Nachdem Sie dieses Kapitel gelesen haben, können Sie sich vorstellen, welche faszinierenden Dinge im Universum der Blockchain-Software möglich sind. Und vielleicht bekommen Sie ja sogar selbst eine zündende Idee!

Das R3-Konsortium

Viele Banken haben in den Aufbau von Blockchain-Prototypen investiert – viele aufgrund der KYC-Anforderungen (*Know Your Customer*, eine Legitimitätsprüfung für Neukunden) gegen die Geldwäsche, aber auch, um die Kosten für Geldtransfers zu reduzieren. Sie mussten zahlreiche Hürden überwinden, unter anderem im Hinblick auf die Sicherheit von privaten Informationen und die gesetzliche Grauzone von Kryptowährungen.

R3 (https://www.r3.com) ist ein innovatives Unternehmen, das mit dem Ziel, die neue Blockchain-Technologie zu integrieren und Nutzen daraus zu ziehen, ein Konsortium aus über 75 weltweit führenden Finanzeinrichtungen ins Leben gerufen hat. R3 verbessert den grenzübergreifenden Geldtransfer, senkt die Kosten für Prüfungen und beschleunigt die Kapitalübertragung und den Ausgleich zwischen den Banken.

Die drei Säulen von R3 sind:

- ✔ **Blockchains mit Eignung für die Finanzbranche**: R3 hat die grundlegende Technologie entwickelt, die die Anforderungen der globalen Finanzwirtschaft erfüllt.
- ✔ **Forschung und Entwicklung**: R3 hat ein bilaterales Forschungszentrum eingerichtet, das Industrienormen für die Blockchain-Technologie mit Eignung für die Wirtschaft prüft und erstellt.
- ✔ **Produktentwicklung**: R3 arbeitet eng mit Einrichtungen zusammen, um Produkte zu entwickeln, die Probleme entlang der gesamten Wertschöpfungskette lösen.

R3 hat die Blockchain-Plattform Corda für Finanzinstitutionen entwickelt. Corda ist eine Plattform mit dezentralem Ledger für die Verwaltung und Synchronisierung von Finanzvereinbarungen zwischen regulierten Finanzinstituten. Anders als die meisten Blockchains, die ihre Transaktionen über das gesamte Netzwerk übertragen, können Transaktionen parallel auf verschiedenen Knoten ausgeführt werden, ohne dass ein Knoten über die Transaktionen der anderen informiert wird. Der Verlauf des Netzwerks wird bedarfsabhängig bereitgestellt.

Die wichtigsten Merkmale von Corda sind:

- ✔ **Kontrollierter Zugriff**: Nur Parteien mit legitimem Bedarf dürfen die Daten sehen.
- ✔ **Kein zentraler Controller**
- ✔ **Regelnde und überwachende Beobachterknoten**

- ✔ **Validierung durch Parteien, die an der Transaktion beteiligt sind, statt durch einen allgemeineren Pool unbeteiligter Validatoren**
- ✔ **Unterstützung verschiedenster Konsensmechanismen**
- ✔ **Keine native Kryptowährung, (Corda verwendet nun aber Ripples XRP)**

T ZERO: Blockchains am Aktienmarkt

T ZERO ist eine Plattform, die die Blockchain-Technologie in vorhandene Marktprozesse integriert, um die Zeitdauer und die Kosten des Zahlungsausgleichs zu reduzieren und zugleich die Transparenz, Effizienz und Überprüfbarkeit zu erhöhen. T ZERO kann all dies, weil es modular und anpassbar ist.

T ZERO ist ein Tochterunternehmen von Overstock.com und konzentriert sich auf die Entwicklung und Kommerzialisierung von auf Fintech basierenden Technologien, die mit kryptografisch gesicherten, dezentralen Ledgers arbeiten. Seit seiner Gründung im Oktober 2014 hat T ZERO (www.t0.com) verschiedene funktionierende kommerzielle Blockchain-Produkte eingeführt.

In Zusammenarbeit mit der Keystone Capital Corporation, einem unabhängigen Broker/Händler in Kalifornien, hat T ZERO die ersten öffentlichen Emissionen von Blockchain-Aktien durchgeführt. Gemeinsam bieten die beiden Unternehmen Broker-Services für Benutzer, die Blockchain-Wertpapiere handeln.

Patrick Byrne, Gründer und CEO von Overstock, führte diese Initiative. Die undurchsichtigen Geschäftspraktiken der Wall Street haben den Markt für eine übersichtliche und vertrauenswürdige Handelsplattform geöffnet, auf der die Kunden wissen, was sie kaufen und welche Kosten dabei entstehen. Das SEC erklärte den S-3-Antrag der Muttergesellschaft Overstock.com für zulässig, sodass diese die Möglichkeit hatte, Blockchain-Aktien

öffentlich auszugeben. Außerdem testete es die Plattform in Partnerschaft mit der weltweit größten Bank, der Industrial and Commercial Bank of China (ICBC).

Byrne realisiert dies durch das im Mehrheitsbesitz von Overstock.com befindliche Fintech-Tochterunternehmen Medici. Dieses konzentriert sich darauf, mithilfe der Blockchain-Technologie wichtige Probleme im Zusammenhang mit Finanztransaktionen zu lösen. Sein erstes Projekt soll die Wertpapierabwicklung vereinfachen.

Verteilte Systeme von Blockstream

Blockstream (www.blockstream.com) genießt auf dem Gebiet der Bereitstellung von Blockchain-Technologie einen hervorragenden Ruf. Das Unternehmen konzentriert sich hauptsächlich auf verteilte Systeme. Blockstream bietet Hard- und Softwarelösungen für Organisationen, die blockchainbasierte Netzwerke verwenden.

Blockstream Elements ist die Software-Kernplattform des Unternehmens und Teil eines Open-Source-Projekts. Es bietet verschiedene Ressourcen und ein höchst produktives Protokoll für Blockchain-Entwickler.

Das größte Innovationsfeld von Blockstream sind Sidechains, die den Nutzen vorhandener Blockchains erhöhen, indem sie ihren Datenschutz und die Funktionalität durch neue Merkmale wie etwa Smart Contracts und vertrauliche Transaktionen verbessern. Sidechains vermeiden Liquiditätsengpässe, die bei Kryptowährungen auftreten können. Außerdem ermöglichen es Sidechains, digitale Vermögenswerte zwischen verschiedenen Blockchains zu übertragen.

Mit Sidechains können Sie Unternehmensaktien über eine Blockchain handeln, ohne sich Gedanken über Transaktionskosten oder langsame Netzwerke machen zu

müssen. Die verteilte Infrastruktur für die Vermögensverwaltung kann auch das Bitcoin-Netzwerk verwenden, sodass Einzelpersonen und Organisationen unterschiedliche Anlagekategorien ausgeben können.

Blockstream hat außerdem zur Einrichtung von Lightning Network beigetragen, einem System, über das Bitcoin Mikrozahlungen unterstützen kann, ohne dass das Netzwerk verlangsamt wird. Das Lightning Network unterstützt große Volumina von kleinen Zahlungen unter Verwendung proportionaler Transaktionsgebühren und mit einer hohen Geschwindigkeit. Das Unternehmen entwickelt weitere Bitcoin-Lightning-Prototypen und schafft Konsens und Interoperabilität.

MadHive

Das von Tom Bolich und Adam Helfgott gegründete MAD-Netzwerk zielt darauf ab, eine neue Art von Internetwerbung zu schaffen. Das Internet basiert auf Prinzipien wie Pay-per-Click und Social-Media-Marketing, und Google und Facebook wären ohne Werbung längst nicht so mächtig, wie sie es heute sind. MadHive ist deshalb mit seiner neuen blockchainbasierten Werbeengine sehr interessant. Nutzer können dabei ihre Privatsphäre wahren, und Werbetreibende erhalten dennoch in mehrfacher Hinsicht bessere Ergebnisse.

In der Online-Werbung werden häufig Anzeigen auf Ergebnisseiten von Suchmaschinen geschaltet, die wiederum auch die Suchhistorie der Nutzer miteinbeziehen. Hierbei kommen sogenannte Ad-Engines zu Einsatz.

Das Unternehmen MadHive betrachtet den Datenschutz als Menschenrecht; dadurch unterscheidet es sich von anderen Werbe-Engines auf dem Markt, die auf private Informationen der Verbraucher angewiesen sind und alles dafür tun, um diese Informationen zu erhalten und miteinander zu verknüpfen.

Das MadHive-Team ist auch der Ansicht, dass die Bemühungen der Werbebranche niemals im Widerspruch zu den Rechten der Kunden stehen sollten. Indem MadHive die Privatsphäre der Kunden respektiert, löst es den Interessenkonflikt, den Werbetreibende haben, wenn sie Daten mit Wettbewerbern austauschen müssen. Die Blockchain-Technologie ermöglicht einen kontrollierten und verifizierbaren Datenaustausch und bietet eine einfache Lösung für ein komplexes Problem. Das MAD-Netzwerk macht die Online-Werbebranche durch schnelle Transaktionsabwicklung außerdem auch effizienter.

Das MAD-Netzwerk ist derzeit noch in der Entwicklungsphase, hat aber bereits zahlende Kunden. Mehr erfahren Sie auf der Website https://madhive.com/.

Blockdaemon

Blockdaemon ist das Docker für die Blockchain-Entwicklung. Mit Blockdaemon bekommen Sie schnell eine eigene dezentrale Anwendung (DApp) ans Laufen. Sie müssen dann nicht mehr unbedingt jedes Protokoll mit seinen nativen Programmiersprachen verstehen. Stattdessen erstellen Sie einfach die gewünschte App. Mit dem Blockdaemon-System können Sie Ihre Blockchain-Netzwerke über mehrere Clouds und Rechenzentren hinweg orchestrieren und eigene Test- oder Mainnetze aufbauen. Wenn Sie eine Blockchain-Anwendung anlegen oder eine Blockchain-Funktionalität in Ihrer App nutzen möchten, ohne selbst alles über die Entwicklung und den Betrieb von Blockchain-Software zu lernen, ist Blockdaemon eine gute Alternative. Mehr erfahren Sie auf https://blockdaemon.com .

Gemini-Dollar und -Börse

Gemini operiert seit mehreren Jahren als Kryptowährungsbörse. Die Gründung durch die berühmten Winklevoss-Zwillinge lief anders ab als bei anderen Börsen. Da sie im US-Bundesstaat New York lizenziert und beheimatet ist, muss sie strengere

Auflagen erfüllen. Eine aufregende Entwicklung ist der neue, 2018 von Gemini eingeführte Stablecoin namens Gemini-Dollar. Dabei handelt es sich um einen ERC20-Token auf Ethereum-Basis, der den Wert des US-Dollar abbildet.

Hier können Sie den Smart-Contract einsehen: https://etherscan.io/token/0x056Fd409E1d7A124BD7017459dFEa2F387b6d5Cd.

Im Gegensatz zu vielen anderen Stablecoins legt Gemini Wert auf Regulierung. Die US-Dollar-Einlagen, die die Salden des Gemini-Dollars stützen, werden jeden Monat von der registrierten Wirtschaftsprüfungsgesellschaft BPM, LLP geprüft. Das Verhältnis von US-Dollar zu Gemini-Dollar muss dabei immer 1:1 betragen. Gemini ließ zudem auch den Code auf Sicherheit auditieren. Da sich Smart-Contracts als anfällig für unerwartete Ausführungsfälle erwiesen haben, schafft dies etwas mehr Sicherheit, dass die Gelder nicht verschwinden werden.

Decentraland

Decentraland ist ein Virtual-Reality-Spiel, das auf der Ethereum-Blockchain basiert. Die Spieler können in einer virtuellen Welt Land kaufen und bewirtschaften. Sie können Inhalte und Anwendungen erstellen, erleben und monetarisieren. Decentraland ist eine umfangreiche Plattform, deren Nutzer auch eigene Spiele im Zusammenhang mit Decentraland erstellen können. Innerhalb des Spiels finden Sie etwa Casinos, Musik, Workshops und mehr.

Decentraland startete 2015 als kleiner Konzeptnachweis. Eigentumsrechte an digitalen Immobilien wurden unter den Nutzern verteilt. Zuerst wurde das Land als Pixel in einem 2-D-Raster dargestellt. Jedes Pixel hatte einige Daten, die es beschrieben und die Eigentumsverhältnisse auswiesen. Ende 2017 begann das Decentraland-Team mit der Arbeit an einer virtuellen 3-D-Welt, die in Pakete statt in Pixel unterteilt ist. Der

Eigentümer eines Grundstücks kann es mit einem Hash-Verweis auf eine Datei verknüpfen.

Der neue virtuelle 3-D-Raum innerhalb von Decentraland heißt nun »LAND« und fungiert als Token. LAND ist ein knappes, nicht beliebig austauschbares digitales Gut. Ein Ethereum-Smart-Contract setzt die Regeln von LAND durch. LAND ist in Pakete unterteilt, die sich im Besitz der Nutzer befinden und in einer Spielwährung namens »MANA« gekauft wurden. Das Software Development Kit (SDK) von Decentraland bietet alles, was Sie benötigen, um interaktive Spiele oder statische 3-D-Szenen zu erstellen. Mehr über Decentraland erfahren Sie unter https://decentraland.org.

TransferWise

TransferWise ist ein Peer-to-Peer-Geldtransferdienst, mit dem Sie Geld zwischen verschiedenen Konten und Währungen umbuchen können. Zum Zeitpunkt, als dieses Buch erscheint, werden ungefähr 300 Währungen angeboten. TransferWise ist kein ausdrückliches Blockchain-Projekt, aber es könnte in Zukunft mit Berechtigungs-Blockchains wie Ripple zusammenarbeiten. TransferWise bietet ein sogenanntes grenzenloses Konto, zu dem auch eine Mastercard-Debitkarte gehört. So können Sie sich mühelos überall auf der Welt bewegen und Ihr Geld ausgeben. TransferWise wirbt mit niedrigen Wechselgebühren und keinen Transaktionskosten.

TransferWise wurde 2010 von zwei Esten gegründet und hat über vier Millionen Kunden, die jeden Monat über vier Milliarden Dollar transferieren. Das Unternehmen wird auch von Branchendisruptoren wie Richard Branson, Max Levchin und Peter Thiel unterstützt.

Mehr über die Angebote von TransferWise erfahren Sie unter https://transferwise.com.

Lightning Network

Lightning Network bildet eine zweite Ebene über dem Bitcoin-Netzwerk, das die Transaktionen der Blockchain übernimmt und zusammenfasst. Mit Lightning Network können Bitcoin-Transaktionen fast verzögerungsfrei und kostengünstig erfolgen. Da es sich dabei um Off-Chain-Transaktionen handelt, wird die Sicherheit durch Smart Contracts zwischen Ihnen und Ihrem Geschäftspartner gewährleistet. Wegen seiner Auslegung als Peer-to-Peer-Netzwerk kann sich Lightning beliebig an die Marktnachfrage anpassen und die Kapazität der alten Zahlungsprotokolle vervielfachen.

Das Lightning Network funktioniert auch blockchainübergreifend. Sie können damit also Token oder Kryptowährungen zwischen verschiedenen Blockchains austauschen. Solche Transaktionen werden als *Atomic Swaps* bezeichnet und nutzen heterogene Blockchain-Konsensregeln, bei denen jeder Einzelknoten gleichberechtigt ist. Als Einschränkung müssen beide Blockchains die gleiche kryptografische Hash-Funktion haben.

Mehr über das Lightning-Network erfahren Sie unter https://lightning.network.

Bitcoin Cash

Bitcoin Cash oder BCH ist eine jüngere Bitcoin-Fork mit Fokus auf eine schnellere und günstigere Transaktionsabwicklung. Das Bitcoin-Projekt und seine Community teilten sich im Jahr 2017 auf. Das Team von Bitcoin Cash war bestrebt, die Nutzung von Bitcoin als alltägliches Zahlungsmittel für jedermann zu vereinfachen. BCH ist ein frei zugängliches, dezentrales Peer-to-Peer-Zahlungssystem, das ohne Vermittler oder Zentralbanken auskommt. Deren Funktionen übernimmt das zugrunde liegende Bitcoin-Cash-Protokoll.

Bitcoin Cash wird an den meisten Börsen mit dem Tickersymbol BCH gehandelt. Im Bitcoin-Cash-Protokoll ist auch verankert, dass es niemals mehr als 21 Millionen BCH-Coins geben wird. Mit Bitcoin Cash können Sie jederzeit an jeden weltweit Geld

versenden. Das Protokoll schläft nie. Die Gebühren sind niedrig, deshalb ist keine Überweisung zu groß oder zu klein. Und Sie brauchen niemals die Einwilligung oder Zustimmung von Dritten. Wie bei anderen Kryptowährungen sind Sie Ihre eigene Bank und müssen daher dieselben Vorsichtsmaßnahmen treffen wie bei jedem anderen digitalen Vermögenswert. Das bedeutet auch, dass niemand Ihr Geld beschlagnahmen, Ihr Konto einfrieren oder Ihre Transaktionen blockieren kann. Mehr erfahren Sie unter www.bitcoincash.org.

Stichwortverzeichnis

Symbole

5-Algorithmen-System
    Mining 1

A

Acolyte 1
Active Directory 1, 2
AD 1, 2
Afrika 1
Altcoin-Börse 1
Ancun Zhengxin 1
Andhara Pradesh 1
Anforderungen an Blockchains 1
Anwendungen 1
Anwendungen von Blockchains 1
Apache Foundation 1
API
    Factom 1
App
    mobile entwickeln 1
ASIC 1
Asset, digitales 1
Atomic Swaps 1
Augur 1

Australien 1
Auswahl einer Blockchain 1
Ausweispapiere 1
Azure 1, 2
    Active Directory 1, 2
    Bletchley 1
    BlockApps 1
    Blockchain-Tools 1
    Blockstack Core v14 1
    Chain 1
    Cortana 1
    Cryptlets 1
    Ether.Camp 1
    Ethereum 1
    ExpressRoute 1
    Finanzdienstleistungen 1
    privates Netzwerk erstellen 1
    Quickstart Templates 1
    Stack-Programm 1

B

Badbitcoin.org 1
Bankenwesen 1
Bank für Internationalen Zahlungsausgleich 1
BCH 1
Berechtigungsplattform 1
Betriebsprüfungen 1

Betrug 1, 2, 3
    Bitcoin 1
    dLoc 1
Beurkundung 1, 2
Big Data 1, 2
    Versicherung 1
Binance 1
Bitcoin 1, 2
    Betrug 1, 2
    Colored Coin 1
    Einschränkungen 1
    Erpressung 1
    Geschichte 1
    Hacking 1
    illegale Ware 1
    Investition 1
    in Waves umtauschen 1
    Limit 1
    Mining 1
    Missverständnisse 1
    Protokoll 1
    Schneeballsystem 1
    Skalierungsprobleme 1
    Weiterentwicklung 1
    Wettbewerbsdruck 1
    Whitepaper 1
Bitcoin Bloat 1
Bitcoin Cash 1

Bitcoin Core 1
Bitcoin kaufen 1
Bitcoin-QT 1
BitGo-Wallet 1
Bitlicense 1
BitPay 1
BitPesa 1, 2
Bitwage 1
Bletchley 1
    Blockchain-Middleware 1
    Blockstack Core v14 1
    Cryptlets 1
Block 1
BlockApps 1
Blockchain Alliance 1
Blockchain Chamber of Digital Commerce 1
Blockchain (Definition) 1, 2
Blockchain University 1
Blockdaemon 1
Block.one 1
Blockstack Core v14 1
Blockstream 1
Blockstream Elements 1
Bluemix 1, 2
    KYCK! 1
    Wanxiang 1
    Watson 1
Blutdiamanten 1

Brave-Webbrowser 1
Byzantinische Generäle 1, 2

C

Car Lease 1
CGminer 1
Chain 1, 2, 3
    Finanzdienstleistungen 1
    Ledger installieren 1
Chaincode 1
Chain Core 1
Chain Core Developer Edition 1
China 1, 2, 3, 4
    Immobilien 1
China Ledger 1
Circle 1
Cloud
    Azure 1
    Bletchley 1
    Bluemix 1
Cloudera 1
Cloud-Mining 1
Coincenter 1
Cold Storage 1
Colored Coin 1, 2
    erstellen 1
Colored-Coin-Generator 1

Commercial Paper 1
Common Law 1, 2
ConsenSys
    Solidity 1
Contract-Cryptlet 1
Corda 1, 2
    Merkmale 1
Cortana 1
C++ 1, 2
Crowdfunding 1
Cryptlet 1
    Contract 1
    Utility 1
CryptoDelegate 1
CryptoKitties 1
Cyberkriminalität 1

D

Dalian Wanda 1
DAO 1, 2, 3
    Funktionsweise 1
    Investition 1
    Versicherung 1
    Zukunft 1
DApp 1
Darlehensvertrag 1
Datenbank, verteilte 1

Datenintegrität 1
Datenschutz 1
Datenvisualisierung 1
Decentraland 1
delegated proof-of-stake 1
Device Gateway 1
DEX 1
Dezentrale autonome Organisation 1
Dezentrale Autonome Organisation 1, 2
Dezentrale Exchanges 1
Diamanthandel 1
DigiByte 1
DigiKnow 1
Digitale Identität 1, 2, 3, 4
Digitales Asset 1
Distributed Credit Chain 1
Distributed Ledger Technology 1
dLoc 1, 2
DLT 1
Docker 1
Docker Quick Start Terminal 1
Docker Toolbox 1
Dokumentenauthentifizierungssystem 1
DPOS 1
Dubai 1
Dubai 2020 1
Dubai Points 1

E

EBaaS 1
Eigentumsrechtsübertragung 1
E-Mail 1
EndPointRegistry 1
Entry Credits 1
Entscheidungsbaum 1
Entscheidungsmatrix 1
Entscheidungsprozess 1
Entwicklungsländer 1–2
EOS 1
EOS-DApp-Sammlung 1
EOS-Delegates 1
EOS-Spiele 1
ERC20-Token 1
e-Residency 1–2
Erfolgsanalyse 1
Erpressung 1
Estland 1
Ether 1, 2
    Mining 1
Ether.Camp 1

Ethereum 1, 2, 3, 4, 5, 6
Azure 1
Blockchain 1
Blockchain as a Service 1
Bugs 1
Classic 1
DAO 1
Foundation 1
Frontier 1
Gas 1
Geschichte 1
Hacking 1
Hard Fork 1
Homestead 1
Knoten 1
Kryptowährung 1
Metropolis 1
Mining 1
Programmiersprache 1
Serenity 1
Smart Contract 1
Zukunft 1
Everipedia 1
Everledger 1
ExpressRoute 1

F

Fabric 1–2, 3
Bluemix 1
Skalierbarkeit 1
Watson 1
Factoids 1, 2
Entry Credits 1
Factom 1, 2
API 1
Blockchain 1
digitale Identität 1, 2
dLoc 1
Dokumentenauthentifizierungssystem 1
Explore 1
Factoids 1
Harmony 1–2
Kettenstruktur 1
Publishing-Plattform 1
Unternehmen 1
Vorteile 1
Fake-Websites 1
Fannie Mae 1
Federal National Mortgage Association 1
Finanzbranche 1
Finanzprodukte, globale 1
Finanztechnologie 1
Fintech 1
FPGA-Prozessor 1

G

Geburtsurkunde 1
Gehaltszahlungen, grenzüberschreitende 1
Geistiges Eigentum 1
Geldwäsche 1, 2, 3
Gemini-Dollar 1
Gesetze 1
Gesundheitswesen 1, 2
Gewichtete Entscheidungsmatrix 1
Gewohnheitsrecht 1, 2
GitHub 1
GitHub-Konto einrichten 1
Global Blockchain Council 1
Globale Finanzprodukte 1
Global Travel Assessment System 1
Grenzsicherung 1
Greymass 1, 2
Großbritannien 1, 2
Grundbuchsystem 1

H

Hacker-Angriff 1
Hacking 1
    Bitcoin 1
    Ethereum 1
    The DAO 1
Hard Fork 1, 2

Harmony 1
Harte Abspaltung 1, 2
Hash 1
Hash-Baum 1, 2
Hashing 1, 2
Hash-Schlüssel 1
Hercules-Projekt 1
HiveMind 1
Homestead 1
Hyperledger 1
    C++ 1
    Iroha 1
    Sawtooth Lake 1
Hyperledger Composer 1
Hypothek 1
    Bearbeitungsgebühren 1
Hypothekendienstleister 1
Hypothekenkreditinstitut 1

I

IBM 1, 2, 3
Bluemix 1
Car Lease 1
Commercial Paper 1
Device Gateway 1
Fabric 1
Marbles 1
Supercomputer 1
Watson 1
IC3 1
ICO 1
Identität 1, 2
Identitätsdiebstahl 1
ID-System 1
Illegale Waren 1
Immobilien 1
China 1
Entwicklungsländer 1
Europa 1
Fannie Mae 1
Grundbuchsystem 1
Hypothek 1
Money Transmitter 1
Rechtstitelversicherung 1
Trends 1
USA 1
Immobilien
Immobiliengutachter 1

Immobilienmakler 1
Immobilienschätzer 1
Indexbasierte Versicherung 1
Industrial and Commercial Bank of China 1
Industrienormen für die Blockchain-Technologie 1
Initial Coin Offerings 1
IntegerKey 1
Intel 1
Intelligente Stadt 1
Internationaler Währungsfond 1
Internet of Things (IoT) 1, 2, 3, 4
    Gerät 1
    Watson 1
IoT-Geräte 1, 2
Iroha 1–2

J

Jaxx-Wallet 1

K

Kanada 1
Kapital, totes 1
Kenia 1
KETH 1
Kette 1
Keylogging-Software 1
Keystone Capital Corporation 1

Key Vault 1
KI 1
Knoten 1
    Leader 1
    vollständiger 1, 2, 3
Know Your Customer 1, 2, 3
Konsens 1, 2
    Sumeragi 1
Konsensalgorithmus 1
Konsensmodell 1
Kontobuch 1, 2, 3
Kreditsachbearbeiter 1
Kriterien für Projektbewertung 1
Kryptografie 1
Kryptokonto 1
Kryptowährung 1, 2, 3, 4, 5
    Ether 1, 2
    Factoids 1
    Gesetze 1
    illegale Waren 1
    Schwarzgeld 1
    Securities and Exchange Commission 1
    Staaten 1
Kryptowährungsbörse 1, 2
Künstliche Intelligenz 1
KYC 1, 2, 3
KYCK! 1
KYC-Konzept 1

L

Lagerbranche 1
Leader 1
Ledger 1, 2, 3
Legalität 1
Legitimitätsprüfung 1
Lightning Network 1, 2
Linux Foundation 1
Logistikbranche 1
Loyyal 1
Luxemburg 1

M

MadHive 1
Malaysia 1
Malta 1
Marbles 1
MarketPlace 1
Maschinenlernen 1
MasterCard 1
Medici 1
Merkle-Root 1
MetaMask 1–2
Metropolis 1

- Microsoft
  - Azure 1
  - Cortana 1
  - Online-Dienste 1
  - Power BI 1
  - Solidity 1
- Mikroinvestition 1
- Mikroversicherung 1
- Mikrozahlung 1
- Mining 1, 2
  - ASIC 1
  - Bitcoin 1
  - Bitcoin-QT 1
  - CGminer 1
  - Cloud 1
  - Cloud-Service 1
  - Computersystem 1, 2
  - Ethereum 1
  - Farm 1
  - Multiminerapp 1
  - Software 1, 2
- Mining-Pool 1
- Mobile App entwickeln 1
- Money Transmitter 1
- M-pesa-Telefonguthaben 1
- MQTT-Protokoll 1
- Multichain 1
- Multiminerapp 1

Musikindustrie 1

N

Nahfeldkopplung 1
Nationalität 1
Near Field Communication 1
Negativbeweis 1, 2
Netzwerk 1
    verteiltes 1
New York City 1
NFC 1
    Kommunikationsprotokoll 1
Notar 1
Nxt-Protokoll 1

O

OCBC 1
OFAC-Länder 1
Öffentliche Blockchain 1, 2
Office of Foreign Asset Control 1
Orakel 1
Overstock.com 1

P

Paper-Wallet 1, 2
Passwort, sicheres 1
Peernova 1

Peer-to-Peer-System 1
Peertracks 1
Permissioned Blockchain 1, 2
Podcasts 1
Po.et 1
PoET 1
Poloniex 1, 2
Polymath 1
POW 1
Power BI 1
Private Blockchain 1, 2, 3
    erstellen 1, 2
Privater Schlüssel 1, 2
Problem der byzantinischen Generäle 1
Prognose vs. Cryptlet 1
Programmierung 1
Projektabschluss 1
Projektbewertung 1
Projektplan 1
Projektziel definieren 1
Proof of Elapsed Time 1
Proof of Stake 1
Proof of Work 1, 2
ProtonVPN 1–2
Provenance 1
Publishing-Engine 1
Publishing-Plattform 1

Q

Quickstart Template 1

R

R3 1, 2, 3
Recht auf Vergessenwerden 1
Rechtstitelversicherung 1
Regierungen, schlanke 1
Reisepass 1
Ressourcen 1
Root-Hash 1

S

Sandbox, regulatorische 1
Satellitenstadt 1
Sawtooth 1–2
    Anwendungsfälle 1
    Dokumentation 1
Sawtooth Lake 1–2
Schlüssel
    privater 1
    sichern 1
Schneeballsystem 1
Schwarzgeld 1
Schwellenländer 1
SEC 1

Secure Hash Algorithm 1
Securities and Exchange Commission 1
Serenity 1
SHA-256 1, 2
ShoCard 1
Sicherheit 1
    Bugs 1
    Cryptlets 1
    DAO 1
    IBM 1
    Smart Contract 1
Sidechains 1
Singapur 1, 2, 3, 4
Skalierbarkeit 1
    Fabric 1
    Factom 1
Slock.it 1
Smart Auction 1
Smart Car 1
Smart Cities 1
Smart Contract 1, 2, 3
    Sicherheit 1
Smart-Nation-Projekt 1
Smartrac 1, 2, 3
Smith + Crown 1
Softwareentwickler auswählen 1
Solidity 1
Soramitsu 1

Sozialhilfeleistungen 1
Spam-Mail 1
Spiel
    Tic-Tac-Toe 1
Spiele 1
Staatsbürgerschaft 1
Stablecoin 1
Stadt, intelligente 1
step-it 1
Struktur einer Blockchain 1
Sumeragi 1
Supercomputer 1
SwiftMail 1

T

TEE 1
The DAO 1
Tierion 1
Torrens-Grundbuchsystem 1
Totes Kapital 1, 2
Tourismus 1
Transaktion 1
Transaktionsfamilie 1
TransferWise 1
Transportbranche 1
Trends 1, 2
Trusted Execution Environment 1

Truthcoin-Whitepaper 1
Turing-vollständige Programmiersprache 1
Typen von Blockchains 1, 2
T ZERO 1

U

UjoMusic 1
Umgebung, sichere 1
Unchained (Podcast) 1
Unconfirmed (Podcast) 1
Unternehmensregistrierung 1
US-Ministerium für innere Sicherheit 1
Utility-Cryptlet 1

V

Vereinigte Arabische Emirate 1
Vermögenswert, digitaler 1
Verschlüsselte Informationen 1
Versicherung 1
    Big Data 1
    Crowdfunding 1
    DAO 1
    dezentrale Sicherheit 1
    indexbasierte 1
    IoT 1
    landwirtschaftliche 1
    Mikroversicherung 1

Verteilte Datenbanken 1
Vertrauen 1
Vertrauensebene 1, 2
Vertrauensloses System 1
Virtual Private Network 1
Virtuelle Währung 1
Visa 1
Vollständiger Knoten 1, 2, 3
VPN 1

W

Wallet
    BitGo 1
    sichere 1
Wanxiang 1
Watson 1
    Fabric 1
    Geschwindigkeit 1
    IoT-Plattform 1, 2
    Lernfähigkeit 1
Waves-Blockchain 1
    Smart-Contracts 1
    Unterschiede zu anderen Blockchains 1
Waves-DEX 1
Waves-Netzwerk 1

Waves-Wallet 1
Assets transferieren 1
einrichten 1
nutzen 1
sichern 1
Weltbank 1
Weltwirtschaft 1
WLAN 1

Y

Yahoo!, Hacker-Angriff 1
YouTube-Videos 1

Z

Zahlungen, internationale 1
Zhejiang Zhongnan Holdings Group 1

WILEY END USER LICENSE AGREEMENT

Besuchen Sie www.wiley.com/go/eula, um Wiley's E-Book-EULA einzusehen.