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

Kapitel 1
Blockchain – eine Einführung

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`.

Um eine Manipulation des Netzwerks zu verhindern, sind Blockchains nicht nur dezentral, sondern verwenden oft auch eine *Kryptowährung*. Blockchain-Netzwerke generieren

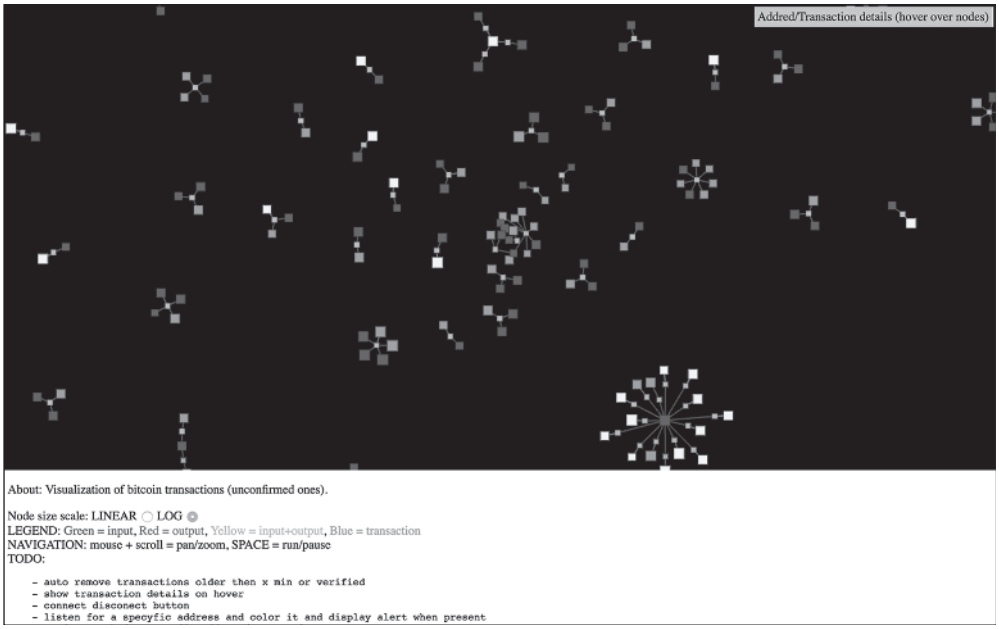

Abbildung 1.1: Der Aufbau des Blockchain-Netzwerks Bitcoin

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.

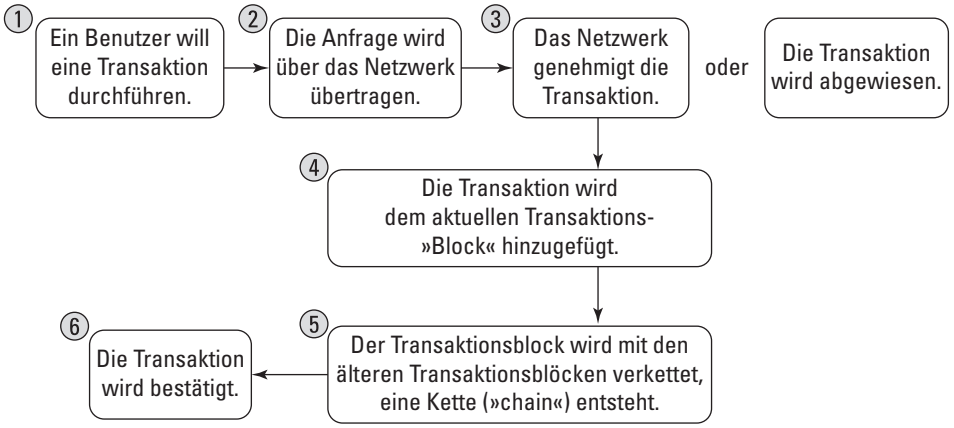

Abbildung 1.2: Wie Blockchains arbeiten

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.