KRYPTO WÄHRUNGEN FÜR EINSTEIGER

EINE REISE IN DIE TECHNOLOGIE VON BITCOIN, DEZENTRALEM FINANZWESEN UND NFT, UM EIN FÜR ALLE MAL ZU VERSTEHEN, WIE KRYPTOWÄHRUNGEN FUNKTIONIEREN

BEN SCHULZ

KRYPTOWÄHRUNGEN FÜR EINSTEIGER

Eine Reise in die Technologie von Bitcoin, dezentralem Finanzwesen und NFT, um ein für alle Mal zu verstehen, wie Kryptowährungen funktionieren

Ben Schulz

Inhaltsverzeichnis

Vorwort

Bitcoin und Kryptowährungen wecken das Interesse einer wachsenden Zahl von Menschen. Die meisten von ihnen nähern sich dieser Welt jedoch mit völlig realitätsfremden Verdienstaussichten, nur um dann enttäuscht zu werden, wenn die „Investitionen“ nicht den Erwartungen entsprechen.

Die einzige Möglichkeit, diesen Sektor richtig und nachhaltig anzugehen, besteht darin, die technologischen und wirtschaftlichen Strukturen zu verstehen, die ihn bestimmen. Das Ziel dieses Buches ist es, die Konzepte hinter Kryptowährungen und Blockchain klar zu erklären und praktische Beispiele für ihre Funktionsweise und Anwendungen zu liefern. Jedes Thema wird so neutral wie möglich behandelt, damit sich der Leser eine fundierte Meinung über diese Welt bilden kann.

Zunächst werden wir die Grundlagen von Bitcoin, der Blockchain und den wichtigsten Kryptowährungen erörtern. Danach wird der Schwerpunkt darauf liegen, wie man digitale Vermögenswerte richtig kauft, verkauft und hält. Es handelt sich also um einen Lehrpfad, der diejenigen Schritt für Schritt begleiten will, die sich zum ersten Mal dieser Branche nähern (oder für diejenigen, die mit den verworrenen Vorstellungen aufräumen wollen, die durch die Lektüre anderer selbsternannter „Leitfäden“ entstanden sind).

Viel Spaß!

TEIL 1 - BITCOIN

„Bitcoin ist Gold für Computerfreaks.“
Stephen Colbert (TV-Moderator)

Kapitel 1

Was ist Bitcoin?

Wenn Sie sich der Welt der Kryptowährungen zum ersten Mal nähern, sollten Sie Ihre Lernreise am besten mit dem Studium von Bitcoin beginnen. Dafür gibt es im Wesentlichen zwei Gründe. Erstens ist es die erste Kryptowährung, die geschaffen wurde, und bietet daher einen Ausgangspunkt. Zweitens ist seine technologische Infrastruktur viel einfacher als die anderer Kryptowährungen und bietet daher die Möglichkeit, sich diesem Sektor zu nähern, ohne in allzu komplexe technische Abläufe zu verfallen.

Wir beginnen diese Reise mit einer ersten Definition von Bitcoin, die in den folgenden Kapiteln weiterentwickelt und genauer formuliert wird.

Definition: Der Bitcoin ist eine digitale Form von Geld.

Eine Besonderheit, die sofort hervorgehoben werden sollte, ist, dass es im Gegensatz zu den gesetzlichen Zahlungsmitteln, die wir gewohnt sind, keine Zentralbank gibt, die Bitcoin kontrolliert und verwaltet. Tatsächlich wird das gesamte Finanzsystem von Bitcoin von Tausenden von Computern auf der ganzen Welt verwaltet. Jeder kann zum Bitcoin-Ökosystem beitragen, indem er die Open-Source-Software herunterlädt und ausführt. Wenn Ihnen dieses Konzept nicht klar ist, machen Sie sich keine Sorgen: Wir legen das Fundament, auf dem wir den Diskurs aufbauen können.

Menschen nutzen Bitcoin aus unterschiedlichen Gründen. Viele schätzen sie wegen ihrer Freiheit und der fehlenden zentralen Kontrolle: Jeder, der einen Internetanschluss hat, kann Bitcoin senden und empfangen. Für diese Menschen ist diese Kryptowährung ein bisschen wie Bargeld, denn niemand kann ihre Verwendung verhindern oder eine Transaktion blockieren. Die digitale Präsenz von Bitcoin bedeutet jedoch, dass er weltweit transferiert werden kann, was ihn vielseitiger macht als physische Banknoten oder Münzen.

Fügen wir also der obigen Definition eine weitere komplexe Ebene hinzu.

> **Definition: Bitcoin ist eine digitale Form von dezentralem, Zensur-resistentem, sicherem und grenzenlosem Geld.**

Diese Eigenschaften haben Bitcoin für eine Vielzahl von Fällen attraktiv gemacht, z. B. für internationale Zahlungen und Transaktionen, bei denen Einzelpersonen ihre Identität nicht preisgeben wollen.

All diese Personen tragen zur transaktionalen Dimension von Bitcoin bei. Wie wir in späteren Kapiteln sehen werden, gibt es auch diejenigen, die Bitcoin als eine Form der Investition betrachten.

Kapitel 2

Wer hat Bitcoin erfunden?

Die Antwort auf diese Frage wird wahrscheinlich nie mit Sicherheit zu finden sein. Der Schöpfer von Bitcoin verwendete das Pseudonym Satoshi Nakamoto, aber wir wissen nichts über seine Identität. Bei Satoshi könnte es sich um eine Einzelperson oder eine Gruppe von Personen handeln; auch seine Herkunft ist nicht bekannt. Der Name ist japanischen Ursprungs, aber Satoshis Englischkenntnisse, wie sie in dem Forum zu sehen sind, in dem er das Bitcoin-Whitepaper veröffentlichte, haben viele zu der Annahme veranlasst, dass er aus einem englischsprachigen Land stammt. Satoshi veröffentlichte 2008 das Bitcoin-Whitepaper und brachte 2009 die erste Version der Software heraus. Der mysteriöse Schöpfer verschwand dann 2010 und überließ die Entwicklung und Verbreitung der Kryptowährung der Community.

Bitcoin kombiniert eine Reihe von Technologien, die bereits zum Zeitpunkt ihrer Erfindung existierten. Das Konzept der Blockchain selbst stammt zum Beispiel nicht aus der Zeit von Bitcoin. Die Verwendung ähnlicher technologischer Strukturen lässt sich sogar bis in die frühen 1990er-Jahre zurückverfolgen, als Stuart Haber und W. Scott Stornetta ein System zur Zeit-Kennzeichnung von Dokumenten vorschlugen.

Interessant ist, dass im Bitcoin-Whitepaper nirgends der Begriff "Blockchain" verwendet wird, obwohl diese Technologie, wie wir noch sehen werden, die Grundlage für das Funktionieren von Kryptowährungen bildet.

Vielen ist nicht bewusst, dass Bitcoin nicht der erste Versuch war, digitales Geld zu schaffen. In der Tat gab es im Laufe der Geschichte immer wieder Projekte, die genau dies zum Ziel hatten. Diese sind jedoch alle innerhalb kurzer Zeit gescheitert.

Ein eindrucksvolles Beispiel ist der Fall von DigiCash. DigiCash war ein Unternehmen, das Ende der 1980er-Jahre von dem Kryptografen und Informatiker David Chaum gegründet wurde. Dieses „digitale Geld“ wurde auf der Grundlage eines von Chaum selbst verfassten Paper als datenschutzorientierte Lösung für Online-Transaktionen vorgestellt. Im Gegensatz zu Bitcoin war das Modell von DigiCash jedoch ein zentralisiertes System. Das Unternehmen scheiterte relativ schnell, und Chaum führte diesen Misserfolg darauf zurück, dass die Welt noch nicht bereit für eine solche Technologie war. Schließlich wussten in den 1980er-Jahren nur wenige Menschen von der Existenz des Internets, und Online-Zahlungen waren noch eine ferne Idee.

Kapitel 3

Wie Bitcoin funktioniert

Lassen Sie uns nun versuchen, ein wenig mehr ins Detail zu gehen und zu verstehen, wie Bitcoin und damit verbundene Transaktionen funktionieren. Ein guter Ansatz ist es, gleich ein konkretes Beispiel zu verwenden. Nehmen wir an, es gibt zwei Personen, Frank und Anna, die Bitcoins tauschen wollen.

Wenn Anna eine Transaktion an Frank tätigt, schickt sie das Geld nicht so, wie man es erwarten würde. In der Tat ist es nicht das digitale Äquivalent zur Übergabe einer Banknote an Frank. Es ist so, als würde Anna auf ein Stück Papier schreiben (das jeder sehen kann), dass sie Frank einen bestimmten Geldbetrag gibt. Dieses Stück Papier sammelt alle Transaktionen, die jemals zwischen allen Teilnehmern des Bitcoin-Netzwerks stattgefunden haben, nicht nur die zwischen Anna und Frank.

Ein Detail dieses Papiers ist, dass die Namen von Anna und Frank sowie die der anderen Teilnehmer nicht explizit aufgeführt sind. Was tatsächlich erscheint, sind die öffentlichen Schlüssel der Adressen von Annas und Franks Geldbörsen. Jede Adresse besteht aus zwei Teilen: dem öffentlichen Schlüssel und dem privaten Schlüssel. Bevor wir fortfahren, wollen wir daher einige Definitionen geben.

Definition: Bei Kryptowährungen ist die Adresse der Ort, von dem und an den Geldmittel gesendet werden.

Definition: Ein öffentlicher Schlüssel ist der Teil der Adresse, der die Geldbörse eines Nutzers öffentlich identifiziert.

Definition: Ein privater Schlüssel ist der Teil der Adresse, der nur seinem Besitzer bekannt ist und der die Durchführung von Transaktionen ermöglicht.

Um einen Vergleich mit dem traditionellen Finanzwesen zu ziehen, kann man sich den öffentlichen Schlüssel wie die IBAN vorstellen.

Umgekehrt kann man sich den privaten Schlüssel wie ein Passwort für den Zugang zum Homebanking vorstellen. Es ist daher sofort klar, dass man sein Homebanking-Passwort nicht weitergeben sollte, ebenso wie der private Schlüssel geheim bleiben sollte.

Dieses Papier ist eine besondere Art von Datenbank und wird im Fachjargon als Blockchain bezeichnet. Alle Teilnehmer des Netzes haben eine identische Kopie auf ihren Geräten gespeichert und verbinden sich miteinander, um neue Transaktionen zu synchronisieren. Transaktionen werden in Blöcken gruppiert, die bei Bitcoin alle 10 Minuten gespeichert werden. Diese Blöcke werden nacheinander in chronologischer Reihenfolge katalogisiert. Aus diesem Grund sprechen wir von Blockchain.

Wir können daher eine erste Definition von Blockchain geben.

Definition: Die Blockchain ist eine für alle sichtbare Datenbank, in der alle Transaktionen aufgezeichnet werden.

Die Transaktionen werden in Blöcken gruppiert; diese Blöcke werden chronologisch katalogisiert.

Eine Besonderheit der Blockchain ist, dass es sich um eine Datenbank handelt, in der Daten hinzugefügt, aber nicht entfernt werden können. Einmal hinzugefügte Informationen können nur sehr schwer, wenn überhaupt, geändert oder gelöscht werden. Auf technischer Ebene ist dies dank einer Funktion möglich, die in jedem Block eine Funktion einprägt, die im nächsten Block eine Art Fingerabdruck erzeugt. Da es sich um eine Funktion handelt, kann es nur einen Fingerabdruck geben, der die beiden Blöcke verbindet. Wenn der Wert dieser Funktion auch nur geringfügig verändert wird, sieht der Fingerabdruck des nächsten Blocks völlig anders aus. Da die Blöcke chronologisch geordnet sind, gibt es keine Möglichkeit, einen alten Eintrag zu ändern, ohne alle nachfolgenden Blöcke zu ändern. Diese Struktur ist eine der Komponenten, die die Blockchain sicher machen und böswillige Personen daran hindern, vergangene Transaktionen zu verändern und sich selbst Gelder zu berechnen, die ihnen nicht gehören.

Wenn ein Nutzer eine Zahlung vornimmt, überträgt er sie also direkt an das Netz, ohne den Umweg über eine Zentralbank oder ein Institut, das Überweisungen bearbeitet. Um neue Transaktionen hinzuzufügen, verwendet die Bitcoin-Blockchain einen Mechanismus namens Mining (Bergbau). Durch diesen Prozess werden neue Transaktionsblöcke in der Blockchain aufgezeichnet. Geben wir also auch eine Definition von Mining.

Definition: Mining ist der Prozess, durch den die Bitcoin-Blockchain neue Transaktionsblöcke zur Bitcoin-Blockchain

hinzufügt.

Schauen wir uns nun an, wie dieser Prozess funktioniert.

Mining

Beim Mining fügen die Teilnehmer der Blockchain Blöcke von Transaktionen hinzu. Dazu müssen sie Rechenleistung aufwenden, um ein kryptografisches Problem zu lösen. Als Anreiz für diese Arbeit und für die Lösung des Problems gibt es eine Belohnung in Bitcoin, die an die erste Person vergeben wird, die die Lösung findet, die den Block validiert.

Die Belohnung für das Mining besteht aus zwei Komponenten: den Provisionen für die Transaktionen des Blocks und der Belohnung für die Validierung des Blocks. Die Belohnung für die Validierung des Blocks ist die einzige Möglichkeit, neue Bitcoins auf den Markt zu bringen. Mit jedem validierten Block wird dem zirkulierenden Pool eine bestimmte Menge Bitcoin hinzugefügt. Außerdem erhält derjenige, der einen bestimmten Block validiert, auch Provisionen für alle darin enthaltenen Transaktionen.

Die Software passt sich dem Schwierigkeitsgrad des Minings so an, dass es etwa zehn Minuten dauert, einen neuen Block zu validieren. Das bedeutet: Je mehr Rechenleistung den Minern zur Verfügung steht, desto schwieriger ist das kryptografische Problem zu lösen. Die Schwierigkeitsanpassung erfolgt alle zwei Wochen, sodass es Zeiten geben kann, in denen die für die Validierung eines Transaktionsblocks benötigte Zeit deutlich unter oder über dem 10-

Minuten-Zielwert liegt. Im Durchschnitt ist dies jedoch die benötigte Zeit.

Die Belohnungen für die Block-Validierung und die im Block enthaltenen Transaktionsgebühren werden automatisch der Adresse des Miners gutgeschrieben.

Beispiel für eine Transaktion

Nachdem nun alle Elemente, die Bitcoin zum Funktionieren bringen, geklärt sind, ist es an der Zeit, die Teile anhand eines konkreten Transaktionsbeispiels zusammenzufügen.

Nehmen wir an, Anna möchte Frank 2 Bitcoins zum Geburtstag schicken. So wird es ablaufen:

- Anna wird Frank bitten, ihr den öffentlichen Schlüssel zu seiner Adresse zu geben. Im Bitcoin-Ökosystem wird der öffentliche Schlüssel durch eine alphanumerische Zeichenfolge mit einer Länge zwischen 26 und 35 Zeichen dargestellt. Der Einfachheit halber wird dieser oft in einen QR-Code umgewandelt, damit er leicht weitergegeben werden kann.
- Sobald Frank diese Information an Anna weitergegeben hat, wird sie die Transaktion für 2 Bitcoins einleiten. In diesem Stadium hat Anna auch die Möglichkeit, eine Nachricht für Frank einzugeben; eine Art Grund für diese „Überweisung“.
- Anna bestätigt die Transaktion mit ihrem privaten Schlüssel, und die Transaktion wird in die Warteschlange

für den nächsten Block gestellt, zusammen mit allen anderen.

- Die Miner lösen das kryptografische Problem des Blocks, in dem Annas Transaktion enthalten ist, und erhalten im Gegenzug die Belohnung und die Gebühren für alle in dem Block enthaltenen Transaktionen.
- Sobald der Block validiert wurde, werden die 2 Bitcoins auf Franks Adresse gutgeschrieben.

Dies ist ein recht unkomplizierter Prozess, wenn man die verschiedenen beteiligten Parteien versteht. An dieser Stelle wird sich der aufmerksame Leser jedoch eine Frage stellen: Wie leitet Anna die Transaktion ein und bestätigt sie Frank? Die Antwort ist einfach: über ein Wallet.

Kapitel 4

E-Wallets

Ein Wallet ist ein Werkzeug, das zur Interaktion mit einem Blockchain-Netzwerk verwendet werden kann. Es gibt verschiedene Arten von Wallets, die sich in zwei Hauptgruppen unterteilen lassen: Software-Wallets und Hardware-Wallets. Je nach ihren Funktionsmechanismen lassen sie sich in Hot Wallets und Cold Wallets unterteilen.

Die meisten Anbieter von Wallets sind softwarebasiert, was ihre Nutzung einfach und intuitiv macht. Hardware-Wallets sind jedoch die sicherste Alternative für diejenigen, die ihre Bitcoins (oder andere Kryptowährungen, die sie halten möchten) nicht kurzfristig ausgeben wollen.

Im Gegensatz zu dem, was man denken könnte, speichern Wallets keine Kryptowährungen, sondern stellen die Werkzeuge zur Verfügung, die für die Interaktion mit der Blockchain benötigt werden, auf der diese Kryptowährungen gespeichert sind. Mit anderen Worten: Sie können die Informationen generieren, die zum Senden und Empfangen von Kryptowährungen erforderlich sind. Deshalb musste Anna im obigen Beispiel ein Wallet benutzen, um die 2 Bitcoins an Frank zu schicken.

Diese Informationen bestehen unter anderem aus einem oder mehreren öffentlichen und privaten Schlüsselpaaren. In einem Wallet

kann es also mehrere Adressen geben. Ähnlich wie bei den Girokonten, bei denen man „Unterkonten“ einrichten kann, um sein Geld aufzuteilen.

Ein Hot Wallet ist auf irgendeine Weise mit dem Internet verbunden. Im Gegensatz dazu hat ein Cold Wallet keine Verbindung zum Internet. Cold Wallets verwenden ein physisches Medium, um öffentliche und private Schlüssel offline zu speichern und so Hacking-Versuche an der Quelle zu verhindern. Daher sind Cold Wallets in der Regel eine viel sicherere Alternative zum Schutz Ihrer Kryptowährungen als Hot Wallets.

Die Software-Wallets

Software-Wallets sind in den meisten Fällen Hot Wallets. Sehr beliebt in dieser Kategorie sind Web-Wallets, die den Zugang zu Blockchains über eine Browser-Schnittstelle ermöglichen, ohne dass Software heruntergeladen oder installiert werden muss.

Dann gibt es noch Desktop-Wallets, die den Web-Wallets sehr ähnlich sind, mit dem einzigen Unterschied, dass ein Programm installiert werden muss. Auch wenn dies in der Praxis wie eine Kleinigkeit erscheinen mag, so ist es doch ein wichtiges Sicherheitsmerkmal. Desktop-Wallets speichern private Schlüssel in der Regel auf dem Computer, auf dem die Software installiert ist, und nicht auf einem Online-Server. Dies bietet ein höheres Maß an Sicherheit und Schutz vor möglichen Hackerangriffen.

Es gibt auch Mobile-Wallets, die speziell für den Einsatz auf Smartphones konzipiert sind. Diese Art von Wallet wird vor allem von

Personen genutzt, die Kryptowährungen in ihrem täglichen Leben verwenden und in der Lage sein müssen, Transaktionen mit einer gewissen Geschwindigkeit durchzuführen.

Das am besten geeignete Software-Wallet für Anfänger ist Exodus (exodus.com).

Achtung: Wenn Sie ein Software-Wallet herunterladen, sollten Sie dies ausschließlich von der offiziellen Website tun.

Software-Wallets neigen dazu, die Benutzerfreundlichkeit der Sicherheit vorzuziehen. Das genaue Gegenteil sind Hardware-Wallets.

Hardware-Wallets

Hardware-Wallets sind physische Geräte, die einen Zufallszahlengenerator verwenden, um die öffentlichen und privaten Schlüssel einer Adresse zu erstellen. Die Schlüssel werden dann auf dem Gerät selbst gespeichert, das nicht mit dem Internet verbunden ist. Es handelt sich also um eine Art Cold Wallet und gilt als eine der sichersten Alternativen.

Obwohl diese Wallets ein höheres Maß an Sicherheit bieten, können sie Risiken bergen, wenn die Firmware-Implementierung nicht ordnungsgemäß durchgeführt wird. Außerdem sind Hardware-Wallets in der Regel weniger intuitiv und der Zugriff auf das Geld ist schwieriger als bei Software-Wallets.

Das am besten geeignete Software-Wallet für Anfänger ist das Ledger Nano S (ledger.com).

Achtung: Wenn Sie ein Hardware-Wallet kaufen, sollten Sie dies nur und ausschließlich auf der offiziellen Website tun.

Kapitel 5

Bitcoin-Knappheit und Halving

Eine der Besonderheiten von Bitcoin ist, dass es eine begrenzte Höchstmenge an Coins gibt. Die Software setzt das maximale Angebot auf einundzwanzig Millionen Bitcoins fest. Im August 2021 sind bereits mehr als 90 % der Bitcoins in Umlauf gebracht worden. Allerdings wird es mehr als 100 Jahre dauern, bis die restlichen Coins abgebaut sind. Dies ist auf periodische Ereignisse zurückzuführen, die als „Halving“ bekannt sind und die Belohnung der Miner schrittweise reduzieren. Lassen Sie uns ein wenig mehr ins Detail gehen, denn dieses Konzept ist sowohl für das Verständnis der wirtschaftlichen Struktur von Bitcoin als auch für das Verständnis, warum wir über „Investitionen“ in diese Kryptowährung sprechen, von entscheidender Bedeutung.

Nach jeweils 210 000 Blöcken, also etwa alle vier Jahre, wird die Blockbelohnung, die Bitcoin-Miner für die Verarbeitung von Transaktionen erhalten, halbiert. Dadurch wird natürlich auch die Geschwindigkeit, mit der neue Bitcoins in Umlauf gebracht werden, halbiert. Mit anderen Worten: Bitcoin schafft auf diese Weise eine kontrollierte Form der Inflation, die sich alle vier Jahre halbiert, bis alle Bitcoins in Umlauf gebracht sind.

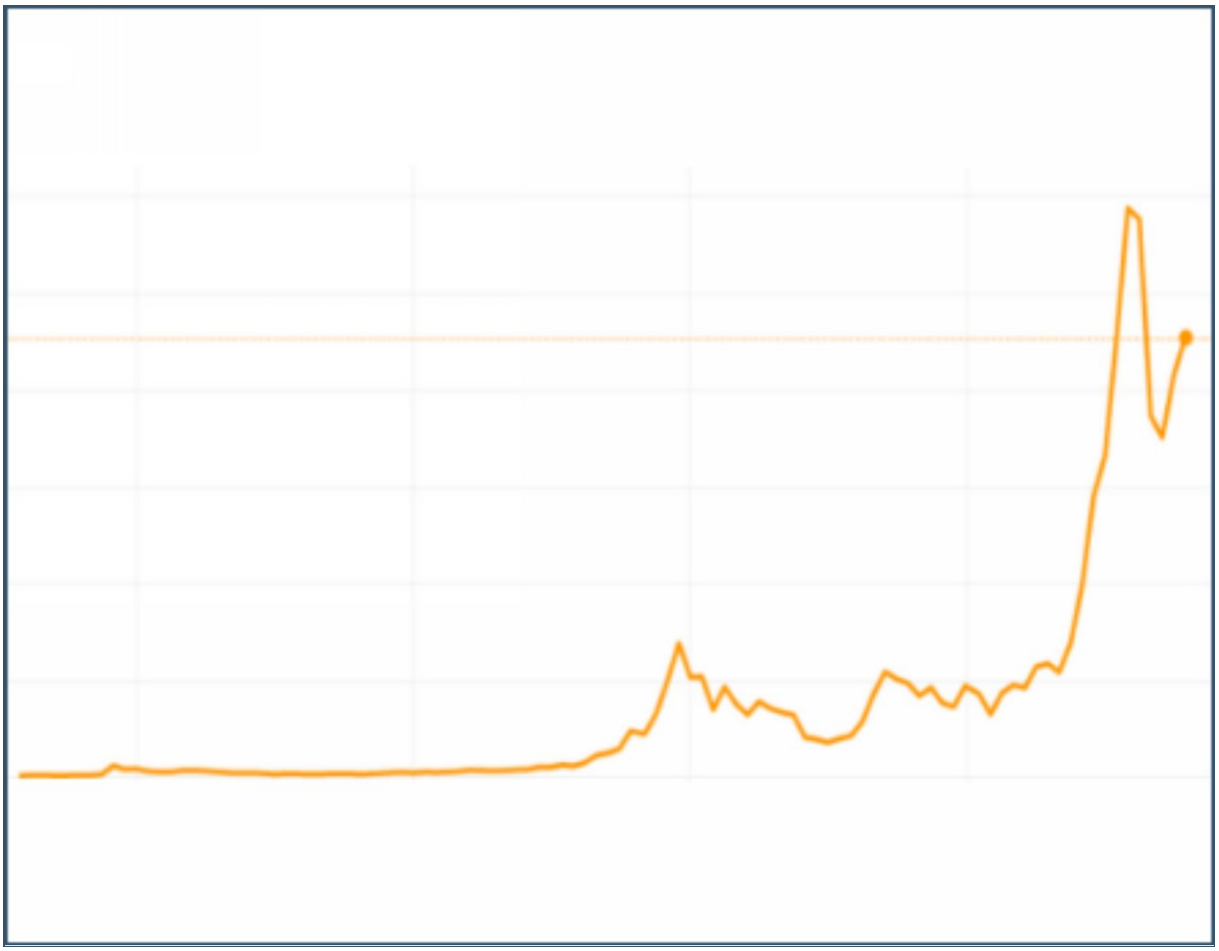
Dieses System der Halbierung der Belohnung wird bis etwa zum Jahr 2140 fortgesetzt. An diesem Punkt werden die Miner nur noch mit Transaktionsgebühren belohnt. Die Provisionen an diesem Punkt werden sicherstellen, dass die Miner weiterhin einen Anreiz haben, abzubauen und das Netzwerk am Laufen zu halten. Daraus folgt, dass der Erfolg oder Misserfolg von Bitcoin von der Anzahl der Nutzer abhängt, die diese verwenden. Wenn die Zahl der Transaktionen im Laufe der Zeit nicht steigt, wird Halving dazu führen, dass die Miner keinen Anreiz mehr haben, Blöcke zu validieren.

Halving ist wichtig, weil es einen Rückgang des ohnehin schon begrenzten Angebots an Bitcoins bedeutet. Diesem Angebotsrückgang muss jedoch auch eine gleichbleibende oder steigende Nachfrage gegenüberstehen, um den Wert des Netzes zu erhöhen.

Im Jahr 2009 betrug die Belohnung für die Validierung jedes Blocks 50 Bitcoins. Nach dem ersten Halving waren es 25, dann 12,5 und schließlich 6,25 Bitcoins pro Block ab dem 11. Mai 2020. Um dieses Konzept besser zu verstehen, stellen Sie sich vor, was passieren würde, wenn sich die Menge des geförderten Goldes alle vier Jahre halbieren würde. Da der Wert von Gold auf seiner Knappheit beruht, würde ein „Halving“ der Goldproduktion seinen Preis erhöhen.

Die zweite Gruppe von Teilnehmern am Bitcoin-Netzwerk basiert genau auf diesem Konzept. Wir sprechen von denjenigen, die sich entscheiden, ihre Bitcoins nicht auszugeben, sondern sie langfristig als eine Form der Investition zu behalten. Diese Leute glauben, dass Bitcoin eine Form von digitalem Gold ist, da Bitcoin nur begrenzt verfügbar ist und immer weniger neue Coins auf den Markt kommen.

Diese Investoren sehen Bitcoin als Wertaufbewahrungsmittel. Sie sind der Meinung, dass diese Eigenschaften sie zu einem idealen Mittel machen, um Vermögen über lange Zeiträume zu speichern. Sie glauben, dass der Wert von Bitcoin im Laufe der Zeit weiter steigen wird, und im Moment haben sie recht. Lassen wir einmal die Zahlen beiseite. Dies ist eine Grafik der Kursentwicklung von Bitcoin gegenüber dem Dollar seit 2009.



Wie man sieht, steigt der Wert von Bitcoin langfristig gesehen stetig an. Wir können dann eine weitere Definition von Bitcoin geben.

Definition: Bitcoin ist digitales Gold.

Diejenigen, die Bitcoin als Anlageform nutzen, merken es sich unter dem Ticker BTC. Von nun an wird diese Abkürzung verwendet, wenn über den Preis von Bitcoin gesprochen wird. Außerdem wird der Preis von Bitcoin immer in Dollar angegeben, da dies die international verwendete Maßeinheit ist.

Kapitel 6

Der Preis und der Wert von Bitcoin

Seit seiner Einführung im Jahr 2009 ist der Bitcoin-Kurs starken Schwankungen unterworfen. BTC wies in den letzten 10 Jahren eine kumulierte jährliche Wachstumsrate von 196,7 % auf. Diese misst die jährliche Wachstumsrate eines Vermögenswerts unter Berücksichtigung seiner Kapitalisierung. Der Bitcoin-Preis ist viermal in die Höhe geschnellt, von nur 1 Dollar im Jahr 2011 bis zu einem Allzeithoch von 65 000 Dollar im Mai 2021. Werfen wir einen Blick auf diese Höchststände des Bitcoin-Preises.

- Juni 2011: Von einem Preis von wenigen Cents im Jahr zuvor stieg der Bitcoin auf $32. Dies war die erste echte Hausse von Bitcoin, die dann ihren ersten Bärenmarkt erlebte, mit einem Absturz auf $2,10.
- April 2013: Nachdem der Bitcoin zu Beginn des Jahres bei etwa $13 gelegen war, stieg er am 10. April 2021 auf $260. In den folgenden zwei Tagen brach der Preis dann ein und stabilisierte sich bei $45.
- Dezember 2013: Gegen Ende des Jahres verzeichnete Bitcoin zwischen Oktober und Dezember einen fast 10-fachen Preisanstieg. Anfang Oktober wurde BTC bei $125 gehandelt, während es im Dezember seinen Höchststand bei $1160

erreichte. Am 18. Dezember war der Preis wieder auf $380 gefallen.

- Dezember 2017: Nachdem Bitcoin das Jahr bei etwa $1000 begonnen hatte, erlebte er einen kometenhaften Aufstieg und erreichte am 17. Dezember 2017 knapp $20 000. Diese Hausse hat die Position von Bitcoin als Anlageobjekt gefestigt und die Aufmerksamkeit von institutionellen Investoren und Regierungen auf sich gezogen.
- April 2021: Auf der Börsen- und Kryptowährungskrach im März 2020 folgt ein nachhaltiger Kursanstieg auf $64 000 am 13. April 2021. Angesichts der wirtschaftlichen Instabilität, die durch die Pandemie verursacht wurde, wurde Bitcoin von einigen als Wertaufbewahrungsmittel angesehen. BTC und der Kryptowährungsmarkt erlebten dann im Mai 2021 einen deutlichen Rückschritt, bevor sie sich bei $40 000 stabilisierten.

Die fundamentalen und technischen Modelle, die wir im Folgenden zur Erklärung der Bitcoin-Kursentwicklung heranziehen werden, können nicht immer das Verhalten beschreiben, das auf den Charts zu sehen ist. Externe Faktoren, einschließlich politischer und wirtschaftlicher Ereignisse, spielen eine wichtige Rolle und müssen einzeln analysiert werden. Ein interessantes Beispiel dafür ist ein berühmter Hack, der in den ersten Jahren der Geschichte von Bitcoin stattfand. Die Rede ist von dem Hack der Mt. Gox-Börse.

Dieses Ereignis, das im Jahr 2014 stattfand, war signifikant und führte zu einem vorübergehenden Rückgang des Bitcoin-Preises und einem allgemeinen Misstrauen gegenüber der Kryptowährungswelt.

Bevor wir analysieren, was passiert ist, brauchen wir eine sehr wichtige Definition.

> **Definition: Eine Börse ist eine Plattform, die den Kauf, Verkauf und Besitz von Kryptowährungen ermöglicht.**

2014 war Mt.Gox die größte Kryptowährungsbörse auf dem Markt, mit einem Handelsvolumen von rund 70 % des gesamten Bitcoin-Angebots. Seit seiner Gründung im Jahr 2010 war Mt.Gox Opfer zahlreicher Hacks geworden, hatte aber weiter überlebt. Beim Hack im Jahr 2014 wurden jedoch rund 850 000 BTC gestohlen, wodurch ein Großteil der Münzen, die sich auf der Börse befanden, verschwanden. Mt. Gox setzte am 14. Februar 2014 die Abhebungen aus, was zu einem Preisverfall von etwa 20 % führte, wodurch der Bitcoin-Preis auf etwa $680 fiel, nachdem er die meiste Zeit der Woche bei $850 gehandelt wurde.

Am Ende stahlen die Hacker 450 000 000 Dollar an Benutzergeldern und Mt.Gox ging in Konkurs. Einige ehemalige Nutzer behaupten, dass es Probleme mit dem Code der Website gab, die nicht rechtzeitig behoben wurden und den Diebstahl ermöglichten. Die Gründe für den Hack sind bis heute unklar und waren der Grund für mehrere Klagen gegen Mark Karpelès, den CEO der Börse.

Langfristig haben zufällige Ereignisse weniger Einfluss auf den Preis als die wirtschaftliche Struktur, die durch die geplante Knappheit des Halvings gegeben ist.

Aus diesem Grund ist es interessant, nach anderen Wegen zu suchen, um die insgesamt positive Entwicklung von Bitcoin zu erklären.

Eines der interessantesten und bisher zuverlässigsten Modelle zur Erklärung der Bitcoin-Preisentwicklung ist das „Stock-to-Flow“-Modell. Schauen wir uns das im Detail an.

Das Stock-to-Flow-Modell

Das Stock-to-Flow-Modell ist eine Methode zur Messung des Vorkommens einer bestimmten Ressource. Das Verhältnis ist die Gesamtmenge einer Ressource, geteilt durch die jährlich produzierte Menge.

Dieses Modell wird im Allgemeinen auf natürliche Ressourcen und Rohstoffe angewandt. Nehmen wir das Beispiel des Goldes. Obwohl die Schätzungen variieren, schätzt der World Gold Council, dass etwa 190 000 Tonnen Gold gefördert wurden. Diese Zahl können wir als Bestand bezeichnen. Gleichzeitig werden jedes Jahr zwischen 2500 und 3200 Tonnen Gold abgebaut. Diese Menge können wir als „Flow“ bezeichnen.

Im Wesentlichen zeigt dieses Modell, wie viel Angebot jedes Jahr für eine bestimmte Ressource im Verhältnis zum Gesamtangebot auf den Markt kommt. Je größer das Verhältnis zwischen Bestand und Flow ist, desto weniger neue Angebote kommen im Vergleich zum Gesamtangebot auf den Markt. Daher sollte ein Vermögenswert mit einem höheren Stock-Flow-Verhältnis theoretisch seinen Wert langfristig erhalten und steigern.

Im Gegensatz dazu haben Konsumgüter und Industrierohstoffe im Allgemeinen einen niedrigen Stock-/Flowwert. Das ist richtig, denn ihr Wert ergibt sich aus ihrem Verbrauch, und die Vorräte sind in der

Regel nur zur Deckung der Nachfrage vorhanden. Diese Ressourcen haben nicht notwendigerweise eine hohe Wertbeständigkeit, sodass sie sich als Investitionsformen eher schlecht eignen. In einigen Ausnahmefällen kann der Preis schnell ansteigen, wenn für die Zukunft eine Verknappung erwartet wird, aber ansonsten hält die Produktion mit der Nachfrage Schritt.

Es ist wichtig zu beachten, dass Knappheit allein nicht unbedingt bedeutet, dass eine Ressource wertvoll sein muss. Gold zum Beispiel ist gar nicht so knapp: Es sind immerhin 190 000 Tonnen verfügbar. Das Verhältnis zwischen Stock und Flow deutet darauf hin, dass es wertvoll ist, weil die jährliche Produktion im Verhältnis zum vorhandenen Bestand relativ gering und konstant ist.

In der Vergangenheit wies Gold das höchste Stock-Flow-Verhältnis unter den Edelmetallen auf. Um dies zu berechnen, nehmen wir die Daten, die wir bereits erwähnt haben. Teilt man das Gesamtangebot von 190 000 Gesamttonnen durch 3200 Tonnen pro Jahr, so ergibt sich ein Verhältnis von Vorrat zu Durchfluss von etwa 59. Dieser Wert besagt, dass es bei der derzeitigen Förderrate etwa 59 Jahre dauern würde, alle 190 000 Tonnen Gold zu fördern.

Es ist jedoch zu bedenken, dass Schätzungen darüber, wie viel neues Gold jedes Jahr gefördert werden wird, nur Schätzungen sind. Wenn wir die jährliche Produktion (den „Flow“) auf 3500 erhöhen, würde das Stock-Flow-Verhältnis nur 54 betragen.

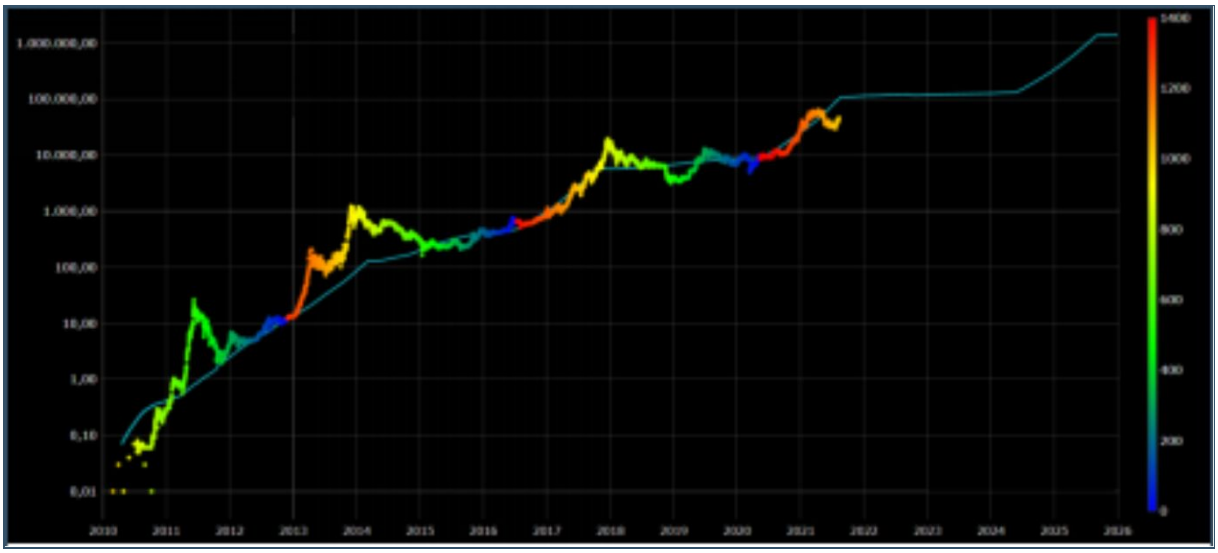
Nach Ansicht der Befürworter des Stock-to-Flow-Modells ist Bitcoin eine Ressource, die mit Gold vergleichbar ist. Sie ist knapp, relativ teuer in der Herstellung und ihr Höchstbestand ist auf 21 Millionen Münzen begrenzt. Außerdem gibt es bei Kryptowährungen einen

konstanten „Flow“, da Blöcke bekanntermaßen etwa alle 10 Minuten validiert werden und Halving die Einführung neuer Münzen schrittweise reduziert.

Den Befürwortern dieses Modells zufolge schaffen diese kombinierten Eigenschaften eine knappe digitale Ressource mit allen Merkmalen, um den Wert langfristig zu erhalten. Den Prognosen des Modells zufolge wird der Bitcoin-Preis im Laufe der Zeit aufgrund des kontinuierlich sinkenden Bestandsverhältnisses voraussichtlich deutlich steigen.

Aber lassen Sie uns nun das Stock-to-Flow-Verhältnis für Bitcoin berechnen. Derzeit befinden sich etwa 18 Millionen Bitcoins im Umlauf, und jedes Jahr werden etwa 0,7 Millionen ausgegeben. Zum Zeitpunkt des Verfassens dieses Buches liegt das Verhältnis bei etwa 50. Es ist klar, dass dieser Wert bei dem nächsten Halving, das 2024 stattfinden wird, erheblich steigen wird. Beachten Sie, dass ein höherer Wert des Verhältnisses mit einer größeren Knappheit der Ressource einhergeht.

Wenn man sowohl den Bitcoin-Bestand als auch den Bitcoin-Flow im Voraus kennt, kann man ein Diagramm erstellen, in dem der tatsächliche Preis mit dem Preis überlagert wird, der idealerweise entstehen würde, wenn er dem sich ändernden Verhältnis folgen würde. Der beliebte Twitter-Nutzer Plan B (@100trillionUSD) hat genau das getan. Wie Sie sehen können, folgt der Preis von Bitcoin mit einer gewissen Toleranz dem Trend des Stock-to-Flow-Verhältnisses.



Wie immer gilt: Es ist nicht alles Gold, was glänzt. Dies ist zwar ein interessantes Modell zur Messung der Bitcoin-Knappheit, aber es berücksichtigt keine externen Ereignisse. Schließlich sind die Modelle nur so gut wie ihre Annahmen.

Erstens basiert das Stock/Flow-Modell auf der Annahme, dass Knappheit Wert schaffen sollte. Einigen Kritikern zufolge würde dieses Modell scheitern, wenn Bitcoin außer der Knappheit des Angebots keine nützlichen Eigenschaften hätte. Auch hier zeigt sich die Bedeutung des transaktionalen Aspekts von Bitcoin. Der Wert dieses Vermögenswertes sollte sich auch aus seiner Verwendung als Währung ergeben, nicht nur aus seiner geplanten Knappheit.

Außerdem sollten wir die Volatilität nicht vergessen. Auch bei der Bewertung eines Vermögenswerts muss dieser Faktor berücksichtigt werden. Wenn die Volatilität bis zu einem gewissen Grad vorhersehbar ist, kann das Bewertungsmodell zuverlässiger sein. Der Bitcoin ist jedoch für seine großen Kursschwankungen bekannt. Wie wir gesehen haben, gab es bis heute nicht weniger als 5

Höchststände, gefolgt von starken Rückgängen. Dies deutet auf eine hohe und unvorhersehbare Volatilität hin.

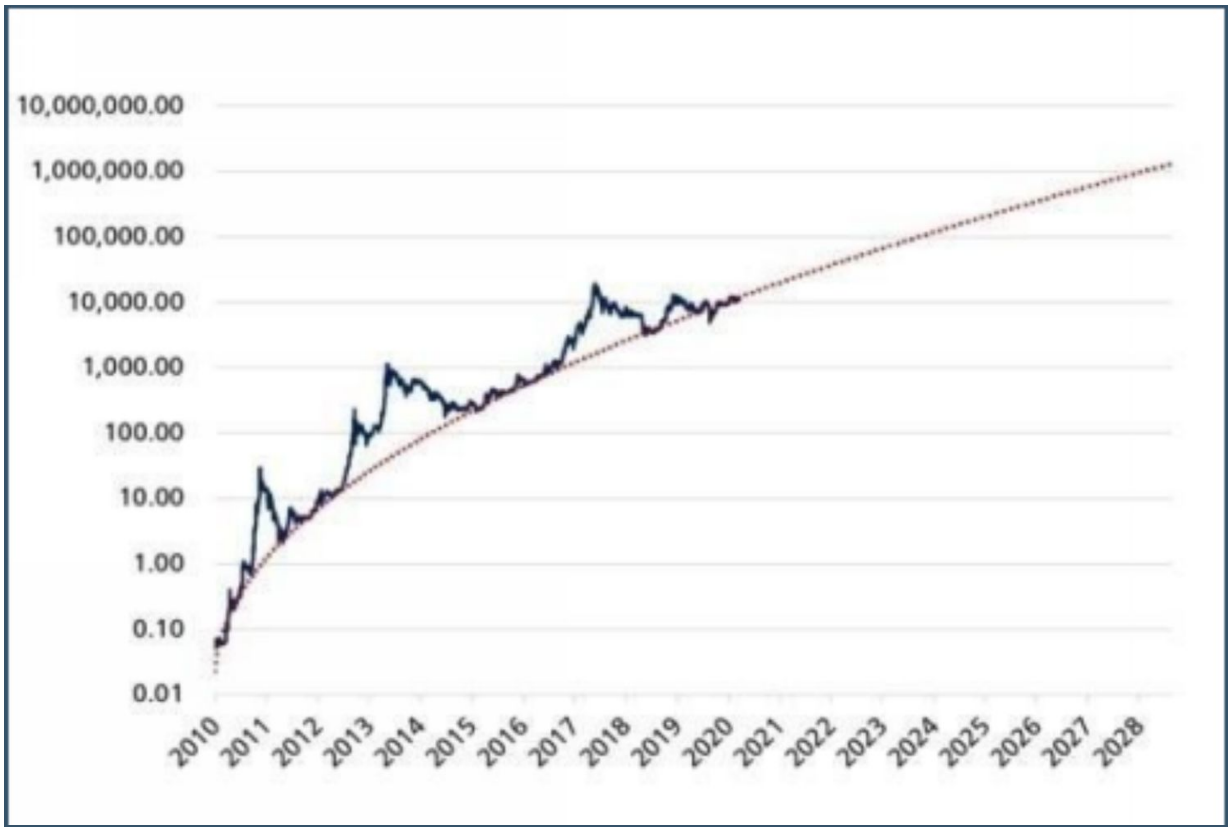
Andere externe Faktoren, wie unvorhersehbare makroökonomische Ereignisse, könnten dieses Modell ebenfalls untergraben. Es ist jedoch anzumerken, dass dasselbe im Wesentlichen für jedes Modell gilt, das versucht, den Preis eines Vermögenswerts auf der Grundlage historischer Daten vorherzusagen. Ein unvorhersehbares Ereignis hat per Definition einen Überraschungseffekt. Nichtsdestotrotz muss gesagt werden, dass das Stock/Flow-Modell bisher besonders gut für Bitcoin funktioniert.

Das Metcalfesche Gesetz

Ein weiteres interessantes Modell zum Verständnis der Bitcoin-Kursentwicklung ist das Metcalfesche Gesetz.

Das Metcalfesche Gesetz ist ein allgemeines Rechenprinzip, das auch auf Bitcoin angewendet werden kann. Diese Regel besagt, dass der Wert eines Netzes proportional zum Quadrat der Anzahl der Nutzer ist, die ihm angehören. Was bedeutet das genau? Ein leicht zu verstehendes Beispiel ist das Telefonnetz. Je mehr Menschen Telefone besitzen, desto exponentiell wertvoller wird das Netz. Wenn nämlich zwei Personen ein Telefon besitzen, kann jede Person nur eine andere Person hören. Wenn jedoch drei Personen ein Mobiltelefon besitzen, kann jede Person mit den beiden anderen in Kontakt treten. Die Zahl der Kontakte nimmt also exponentiell zu, je mehr Menschen ein Telefon besitzen.

Bei Bitcoin können Sie den Metcalfesche-Wert anhand der Anzahl der aktiven Bitcoin-Wallet-Adressen und anderer öffentlicher Informationen in der Blockchain berechnen. Wenn Sie den Metcalfesche-Wert gegen den BTC-Preis auftragen, können Sie eine gute Überlappung sehen.



Dies deutet darauf hin, dass mit der Anzahl der aktiven Adressen auch der Wert des Bitcoin-Netzwerks zunimmt.

Kapitel 7

Das Problem der Skalierbarkeit von Bitcoin

Im vorangegangenen Kapitel wurde erkannt, dass der Wert von Bitcoin nicht allein in seiner programmierten Knappheit liegen kann. Er muss sich auch aus der transaktionalen Verwendung von Kryptowährungen ergeben. Der aufmerksame Leser wird sich eine grundlegende Frage stellen: Wenn man bedenkt, dass Transaktionsblöcke alle 10 Minuten verarbeitet werden, wie ist es dann möglich, Bitcoin täglich zu benutzen? Dies ist eine berechtigte Frage. Schließlich können wir nicht 10 Minuten warten, um einen Kaffee zu bezahlen.

Dieser kritische Punkt ist als Skalierbarkeit-Problem bekannt. Das heißt, wie kann Bitcoin so verbessert werden, dass er in großem Umfang für alltägliche Ausgaben verwendet werden kann?
Eine der vielversprechendsten Lösungen ist das Lightning-Netzwerk. Mal sehen, was es damit auf sich hat.

Das Lightning-Netzwerk

Das Lightning-Netzwerk (im Folgenden auch LN) ist ein Netzwerk, das auf einer separaten Blockchain basiert, um schnelle alltägliche Transaktionen zu ermöglichen. Wir können bereits vorwegnehmen, dass es sich dabei nicht um eine Technologie handelt, die nur bei Bitcoin zum Einsatz kommt: Andere Kryptowährungen wie Litecoin haben es ebenfalls integriert.

Das Lightning-Netzwerk ist eine sogenannte Off-Chain-Lösung oder Sekundärlösung. Sie ermöglicht es, Transaktionen durchzuführen, ohne dass jede Transaktion auf der Haupt-Blockchain registriert werden muss.
Dieses Netzwerk ist vom Bitcoin-Netzwerk getrennt. Es hat seine eigenen Knoten und seine eigene Software, kommuniziert aber dennoch mit der Haupt-Blockchain. Um dem Lightning-Netzwerk beizutreten oder es zu verlassen, müssen Sie spezielle Transaktionen auf der Bitcoin-Blockchain erstellen.
Mit Ihrer ersten Transaktion bauen Sie eine Art privates Hauptbuch mit einem anderen Nutzer auf. In diesem privaten Hauptbuch werden Ihre Transaktionen mit dem anderen Nutzer festgehalten. In dieses Ledger können mehrere Transaktionen geschrieben werden, die nur für die beiden Gegenparteien sichtbar sind. Dieses Register wird auch als „Kanal“ bezeichnet.

Nehmen wir an, dass Anna und Frank jeweils 5 BTC in ihren Kanal im Lightning-Netzwerk eingezahlt haben. In ihrem Kanal hätten sie nun beide jeweils ein Guthaben von 5 BTC. Anna könnte dann eine Transaktion in das Hauptbuch schreiben und 1 BTC an Frank zahlen. Jetzt hat Frank 6 BTC und Anna hat 4 BTC. So könnte Frank zu

einem späteren Zeitpunkt 2 BTC an Anna schicken, wodurch sich der Kontostand auf 6 BTC für Anna und 4 BTC für Frank ändern würde. Sie können über einen bestimmten Zeitraum hinweg weiter handeln, und der Kanal wird ihren jeweiligen Kontostand im Auge behalten.

Beide können jederzeit den aktuellen Stand des Kontos auf der Haupt-Blockchain veröffentlichen. Zu diesem Zeitpunkt werden die jeweiligen Guthaben den jeweiligen Partien in der Blockchain zugeordnet. Auf diese Weise erscheint eine Handelsbeziehung, die mehrere Transaktionen umfasst, in der Haupt-Blockchain als eine einzige Geldbewegung. Das bedeutet, dass Sie nicht 10 Minuten auf jeden der Wechsel zwischen Anna und Frank warten müssen.

Wie der Name schon sagt, sind Lightning-Transaktionen tatsächlich blitzschnell. Es gibt keine Blockchain-Bestätigungen, auf die man warten muss: Zahlungen können mit der Geschwindigkeit erfolgen, die die Internetverbindung der Teilnehmer zulässt.

Bislang scheint das Lightning-Netzwerk der vernünftigste Ansatz zur Skalierung der Bitcoin-Blockchain zu sein. Die Koordinierung von Veränderungen in einem so großen Ökosystem ist kompliziert. In der Tat besteht immer die Gefahr, dass es zu katastrophalen Fehlern kommt. Da so viel auf dem Spiel steht, ist das Experimentieren unglaublich gefährlich, weshalb es in sekundären Netzen durchgeführt wird. Level-2-Lösungen untergraben keine der Sicherheitsvoraussetzungen, die das Bitcoin-Netzwerk seit über 10 Jahren am Laufen halten.

Die Nutzung des Lightning-Netzwerks hat mehrere Vorteile. Der erste und wichtigste Vorteil ist zweifellos die Skalierbarkeit. Wie bereits erwähnt, werden Blöcke etwa alle zehn Minuten erstellt und können nur eine begrenzte Anzahl von Transaktionen enthalten. Speicherplatz ist daher eine knappe Ressource. Dies bedeutet, dass die Nutzer bereit sind, immer höhere Gebühren zu zahlen, damit ihre Transaktion vor anderen bearbeitet wird. Dieses Auktionssystem existiert, weil es den Minern wichtig ist, zuerst bezahlt zu werden, und sie deshalb Transaktionen mit höheren Gebühren zuerst einbeziehen. Denken Sie daran, dass die Provision an den Miner geht, der den Block validiert.
Wenn nicht viele Nutzer gleichzeitig versuchen, Geld zu überweisen, sind die Gebühren relativ niedrig. Bei vielen Transaktionen kann die durchschnittliche Gebühr jedoch erheblich steigen. In einigen Fällen lag sie bei über 5 USD. Auf dem Höhepunkt des Haussemarkts im Jahr 2017 lag sie sogar bei über 50 USD pro Transaktion. Dies ist natürlich ein Problem, das zusätzlich zur Transaktionszeit auftritt. Niemand würde jemals ein Produkt oder eine Dienstleistung mit einer Zahlungsmethode bezahlen, bei der so hohe Gebühren anfallen.
Während dies für Transaktionen, bei denen Tausende von Dollar in Bitcoin bewegt werden, unbedeutend erscheinen mag, ist es für kleinere Zahlungen nicht tragbar.

Beim Lightning-Netzwerk zahlen Sie nur zwei Gebühren: eine, um den Kanal zu öffnen, und eine, um ihn zu schließen. Doch sobald der Kanal geöffnet ist, können die beiden Kontrahenten Tausende von Transaktionen kostenlos durchführen. Sobald der Handel abgeschlossen ist, müssen Sie nur noch den endgültigen Status in der Blockchain veröffentlichen.

Wenn mehr Nutzer auf zweitrangige Lösungen wie das Lightning-Netz zurückgreifen, wird der Blockraum effizienter genutzt. In den Zahlungsverkehrskanälen könnten Überweisungen mit geringem Wert und hoher Frequenz getätigt werden, während der Blockraum für größere Transaktionen und für das Öffnen und Schließen von Kanälen genutzt werden könnte. Dies würde das System einer viel breiteren Nutzerbasis zugänglich machen, sodass Bitcoin langfristig skalieren könnte.

An diesen letzten Punkt knüpft die Frage der Kleinstbeträge an. Es gibt einen Mindestbetrag an Bitcoins, der in einer Transaktion verschickt werden kann. Dieser Betrag entspricht etwa 0,00000546 BTC. Dies ist ein kleiner Betrag, aber das Lightning-Netzwerk ermöglicht es Ihnen, die Grenzen zu überschreiten und die kleinste derzeit verfügbare Bitcoin-Einheit zu tauschen: 0,00000001 BTC. Dieser Wert wird auch als „Satoshi“ bezeichnet.
Es hat sich herausgestellt, dass das Lightning-Netzwerk für Kleinstzahlungen viel attraktiver ist. Die Gebühren für regelmäßige Transaktionen machen es unpraktisch, kleine Beträge über die Hauptkette zu versenden. Innerhalb eines Kanals ist es jedoch möglich, den Bruchteil eines Bruchteils eines Bitcoins kostenlos zu versenden.
Ein dritter Vorteil des Lightning-Netzwerks besteht darin, dass es den Nutzern ein hohes Maß an Vertraulichkeit bieten kann. Die Parteien müssen ihre Kanäle dem Hauptnetz nicht bekannt geben. Sie können sich zwar die Blockchain ansehen und feststellen, welche Transaktion einen Kanal geöffnet hat, aber Sie können nicht feststellen, was in

diesem Kanal vor sich geht. Wenn sich die Teilnehmer dafür entscheiden, ihren Kanal privat zu halten, wissen nur sie, welche Transaktionen stattfinden.

Wenn Anna einen Kanal mit Frank und Frank einen Kanal mit Paola hat, können Anna und Paola über Frank Zahlungen austauschen. Wenn Fabio mit Paola verbunden ist, kann Anna ihm Zahlungen schicken. Sie können sich vorstellen, dass sich dies zu einem weitläufigen Netz miteinander verbundener Zahlungskanäle ausweitet. In einer solchen Konfiguration konnten Sie nicht sicher sein, an wen Anna Geldmittel schickte, sobald der Kanal geschlossen wurde. Es handelt sich um ein äußerst leistungsfähiges System, das jedoch von den staatlichen Stellen nicht gern gesehen wird.

TEIL 2 - DIE BLOCKCHAIN

„Die Erfindung der Blockchain gibt den Menschen noch mehr Macht und stellt die heimtückische Kultur des Eigentums und der Kontrolle infrage.“
Julian Assange (US-amerikanischer Journalist und Aktivist)

Kapitel 8

Unterschiede zwischen Bitcoin und Blockchain

Wer sich zum ersten Mal mit der Welt der Kryptowährungen befasst, ist vielleicht verwirrt über die Unterschiede zwischen Bitcoin und Blockchain. In den vorangegangenen Kapiteln wurden alle Anstrengungen unternommen, um zwischen beiden zu unterscheiden. Bevor wir jedoch diesen Weg weitergehen, ist es gut, diese Begriffe zu klären.

Vielleicht ist eine Analogie angebracht.

So wie:

- Websites sind eine Technologie, die dem Informationsaustausch dient.
- Suchmaschinen sind eine der beliebtesten und bekanntesten Methoden zur Nutzung der Website-Technologie.
- Google wiederum ist eines der beliebtesten und bekanntesten Beispiele für eine Suchmaschine.

Ist es gleichermaßen so:

- Die Blockchain ist eine Technologie, die zur Speicherung von Informationen verwendet wird.
- Kryptowährungen sind eine der beliebtesten und bekanntesten Möglichkeiten, die Blockchain zu nutzen.
- Bitcoin wiederum ist die beliebteste Kryptowährung.

Somit kann Bitcoin als praktischer Ausdruck der Blockchain angesehen werden. Bitcoin basiert auf der Blockchain, aber es ist nicht die Blockchain. Bitcoin hat seine eigene Blockchain, genauso wie andere Kryptowährungen ihre eigene Blockchain haben.

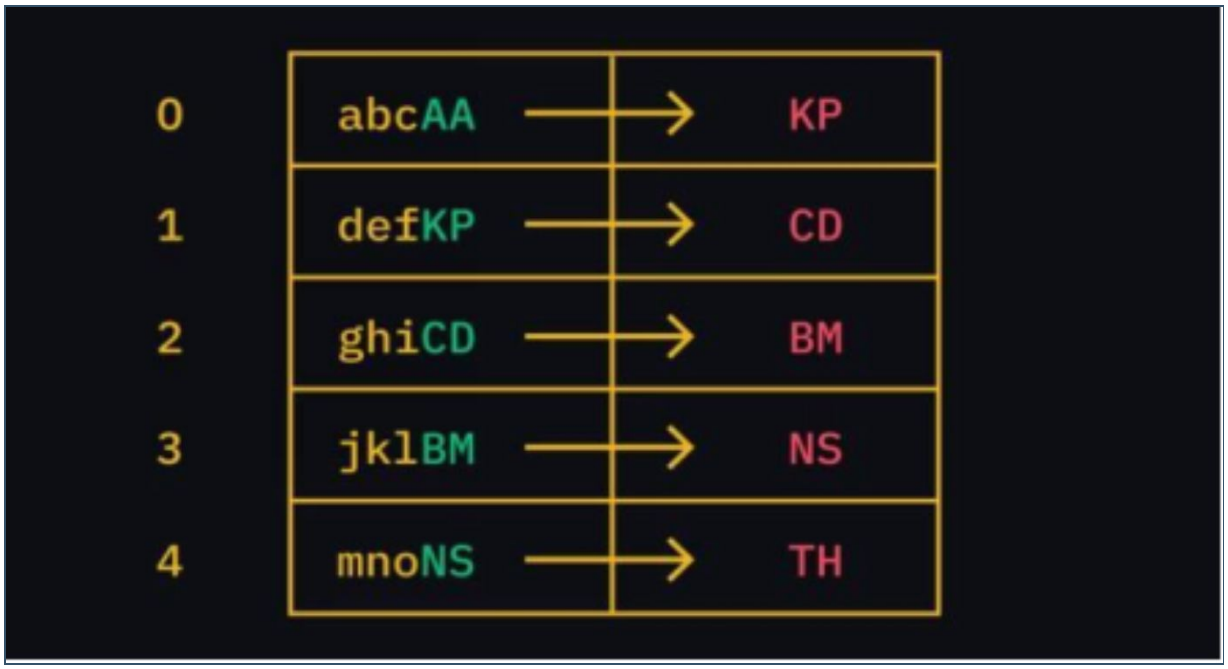
Kapitel 9

Wie die Blockchain funktioniert

Wie wir gesehen haben, hat die Blockchain einige besondere Eigenschaften. Es gibt Regeln für das Hinzufügen von Daten, und wenn die Daten einmal gespeichert sind, ist es praktisch unmöglich, sie zu ändern oder zu löschen. Auf den folgenden Seiten werden diese Eigenschaften näher erläutert.

Wie bereits erwähnt, werden Daten in Strukturen, die Blöcke genannt werden, hinzugefügt. Jeder Block enthält Informationen, die auf den vorhergehenden Block verweisen. Anhand des letzten Blocks können Sie also überprüfen, ob er tatsächlich nach dem vorangegangenen Block erstellt wurde. Wenn man die Kette rückwärts durchläuft, gelangt man zum ersten Block, dem sogenannten „Entstehungsblock“. Angenommen, wir haben ein Blatt mit zwei Spalten. In die erste Spalte der ersten Zeile geben Sie alle Daten ein, die Sie behalten möchten.
Die Daten in der ersten Spalte werden in eine aus zwei Buchstaben bestehende Kennung umgewandelt, die dann als Teil der nächsten Spalte verwendet wird. In diesem Beispiel soll die aus zwei Buchstaben bestehende Kennung KP zum Ausfüllen der nächsten Spalte in der zweiten Zeile (defKP) verwendet werden. Das heißt,

wenn Sie die ersten Daten (abcAA) ändern, erhalten Sie in jeder anderen Spalte eine andere Buchstabenkombination.



In Zeile 4 sehen wir, dass der jüngste Bezeichner TH ist. Angenommen, wir ändern die Daten in der ersten Kolonne. Dies würde zu einer anderen Kennung führen, was bedeutet, dass der zweite Block andere Daten enthält, was wiederum zu einer anderen Kennung in Zeile 2 führt und so weiter. TH ist im Wesentlichen ein Produkt aller Informationen, die ihr vorausgehen, und nicht nur der Informationen, die ihr unmittelbar vorausgehen. Genau aus diesem Grund wird eine Blockchain mit der Zeit immer zuverlässiger: Je mehr Transaktionen aufgezeichnet werden, desto schwieriger ist es für böswillige Personen, Änderungen vorzunehmen.

Die Tabelle, die wir gerade gesehen haben, ist eine vereinfachte Analogie dafür, wie eine Blockchain Hashfunktionen verwendet. Geben wir also eine Definition.

Definition: Hashing ist der Klebstoff, der die Blöcke zusammenhält.

Beim Hashing werden Daten beliebiger Größe durch eine mathematische Funktion geleitet, um eine Ausgabe (Hash genannt) zu erzeugen, die immer die gleiche Länge hat. Die in Blockchains verwendeten Hashes sind insofern interessant, als die Wahrscheinlichkeit, dass zwei Hashes exakt gleich sind, praktisch null ist. Diese Eigenschaft ist entscheidend, denn sie garantiert, dass eine Änderung der Daten auch eine Änderung des Hashes nach sich zieht. Wäre dies nicht der Fall, wäre es möglich, Änderungen an der Blockchain vorzunehmen, ohne dass es jemand merkt. Dies würde natürlich die Sicherheit des gesamten Netzes untergraben.

Bitcoin verwendet SHA256 als Hashfunktion. Wie Sie in der folgenden Abbildung sehen können, erzeugt eine kleine Änderung der Eingabe eine völlig andere Ausgabe.

Als autonome Datenstrukturen sind Blockchains an sich nur in Nischenanwendungen nützlich. Interessant wird es, wenn sie in Verbindung mit der Spieltheorie verwendet werden, um verteilte Hauptbücher zu schaffen, die von niemandem kontrolliert werden.
Das bedeutet, dass es keine Instanz gibt, die die Macht hat, Einträge außerhalb der Regeln der Blockchain selbst zu ändern. In diesem Sinne könnte man sagen, dass die Blockchain allen gehört, denn die Teilnehmer einigen sich darauf, welche Daten in welcher Reihenfolge eingetragen werden sollen.
Der Aufbau einer dezentralen Blockchain ist jedoch aufgrund des Problems des byzantinischen Fehlers keineswegs einfach.

Byzantinischer Fehler

Dieses in den 1980er Jahren theoretisch entwickelte Problem beschreibt eine Situation, in der isolierte Teilnehmer miteinander

kommunizieren müssen, um ihre Aktionen zu koordinieren. In dem konkreten Dilemma geht es um einige Generäle der byzantinischen Armee, die eine Stadt umzingeln und entscheiden müssen, ob sie diese angreifen sollen oder nicht. Die Generäle können nur durch Boten kommunizieren.

Jeder General muss entscheiden, ob er angreifen oder sich zurückziehen will. Es spielt keine Rolle, ob sie angreifen oder sich zurückziehen, solange sich alle Generäle auf eine gemeinsame Entscheidung einigen. Wenn sie sich für einen Angriff entscheiden, werden sie nur dann Erfolg haben, wenn sie gleichzeitig angreifen. Wenn sie beschließen zu fliehen, werden sie nur überleben, wenn sie dies gemeinsam tun. Wie können sie also sicherstellen, dass sie Erfolg haben?

Sicher, sie konnten durch Boten kommunizieren. Was aber, wenn der Bote mit einer Nachricht abgefangen wird, in der es heißt: „Wir werden im Morgengrauen angreifen“ und diese Nachricht durch „Wir werden in der Abenddämmerung angreifen“ ersetzt wird? Was ist, wenn einer der Generäle böse ist und die anderen absichtlich täuscht, um sicherzustellen, dass sie besiegt werden?

Es muss eine Strategie geben, bei der ein Konsens erreicht werden kann, unabhängig von der Güte der Generäle und der Fähigkeit der Boten, nicht abgefangen zu werden.
Wenn es niemanden gibt, der die Blockchain überwacht und den Nutzern „korrekte“ Informationen gibt, müssen die Nutzer auch in der Lage sein, miteinander zu kommunizieren.

Um das potenzielle Versagen eines (oder mehrerer) Nutzer auszugleichen, müssen die Blockchain-Mechanismen sorgfältig konzipiert werden. Wie wir im nächsten Kapitel sehen werden, werden Konsensverfahren verwendet, um strenge Regeln aufzustellen und die Korrektheit der Daten, die von Block zu Block übertragen werden, zu gewährleisten.

Bevor wir jedoch fortfahren, ist es notwendig, ein wichtiges Konzept einzuführen: die Knoten.

Knoten sind einfach die an das Netz angeschlossenen Computer. Sie speichern Kopien der Blockchain und tauschen Informationen mit Computern aus. Die Benutzer müssen diese Prozesse nicht manuell verwalten. Normalerweise müssen sie nur die entsprechende Blockchain-Software herunterladen und starten, der Rest wird automatisch vom Computer erledigt.

Wir haben also eine wichtige Definition zu geben.

Definition: Ein Blockchain-Knoten ist ein Computer, der eine Kopie der gleichen Blockchain speichert und gemeinsam nutzt.

Kapitel 10

Konsensverfahren

Konsensverfahren sind Regeln, die das ordnungsgemäße Funktionieren der Blockchain ermöglichen. Sie regeln, wie Blöcke validiert werden und wie Informationen aufgezeichnet werden. Es gibt mehrere Konsensmechanismen, von denen einige effizienter sind als andere. Die beiden beliebtesten Systeme sind Proof of Work (PoW) und Proof of Stake (PoS).

Der Proof of Work (PoW)

Der PoW ist das System, das auch von Bitcoin verwendet wird. Bei PoW wird mithilfe von Rechenleistung versucht, ein im Protokoll festgelegtes kryptografisches Problem zu lösen.
Das Problem erfordert, dass die Benutzer den Hashwert von Transaktionen und andere im Block enthaltene Informationen berechnen. Damit der Hash als gültig angesehen wird, muss er unter einer bestimmten Zahl liegen. Da es keine Möglichkeit gibt, eine bestimmte Ausgabe vorherzusagen, müssen die Miner die Daten so lange den Hashwert berechnen, bis sie eine gültige Lösung finden.
Es liegt auf der Hand, dass das wiederholte Hashing von Daten rechnerisch und wirtschaftlich teuer ist. Bei Proof-of-Work-Blockchains müssen die Miner Geld in Computer und den zu deren

Betrieb benötigten Strom investieren. Wie wir im Fall von Bitcoin gesehen haben, tun sie dies in der Hoffnung, die Belohnungen von Blöcken und Transaktionsgebühren zu erhalten. Wenn ein Miner einen neuen Block an den Rest des Netzwerks sendet, verwenden alle anderen Knoten ihn als Eingabe für eine Hashfunktion. Sie müssen ihn nur einmal ausführen, um zu überprüfen, ob der Block nach den Regeln der Blockchain gültig ist. Ist dies nicht der Fall, erhält der Miner die Belohnung nicht und hat umsonst Strom verschwendet.

Die wichtigsten Vorteile einer Blockchain mit einem PoW-Konsensverfahren sind:

- Langlebigkeit: Proof of Work ist das bis heute am weitesten verbreitete Konsensverfahren und das einzige, das sich über die Zeit bewährt hat.
- Offen für alle: Jeder kann am Mining teilnehmen oder einfach einen Validierung-Knoten betreiben.
- Dezentralisierung: Miner konkurrieren miteinander um die Validierung von Blöcken, was bedeutet, dass die Hash-Power nie von einer einzelnen Person kontrolliert wird.

Wie immer behalten wir einen neutralen Ansatz bei und weisen auch auf die Nachteile dieses Konsensmechanismus hin:

- Teuer: Mining verbraucht eine große Menge Strom.
- Zunehmend hohe Eintrittsbarrieren: Je mehr Miner dem Netzwerk beitreten, desto schwieriger wird das Problem (im Falle von Bitcoin findet die Anpassung alle zwei Wochen statt). Um wettbewerbsfähig zu bleiben, müssen die Miner in immer bessere Ausrüstung investieren. Im

Falle von Bitcoin sind die Kosten für Computer, die beim Mining mithalten können, sehr hoch und für den Normalbürger unerschwinglich.

- 51%ige Angriffe: Obwohl das Mining die Dezentralisierung fördert, besteht die Möglichkeit, dass ein Miner den größten Teil der Hashing-Power übernimmt. Wenn dies geschieht, könnte er theoretisch Transaktionen zunichtemachen und die Sicherheit der Blockchain beeinträchtigen. Im Falle von Bitcoin überwiegen die Kosten für eine solche Operation jedoch bei Weitem die Vorteile.

Der Proof of Stake (POS)

In Proof-of-Work-Systemen ist der Anreiz für die Miner, ehrlich zu handeln, das Geld, das sie für den Kauf der Computer und den Strom zur Lösung des kryptografischen Problems bezahlt haben.
Im Gegensatz dazu gibt es beim Proof of Stake (PoS) Konsensverfahren keine externen Kosten. Anstelle von Minern gibt es Validatoren, die das Recht erwerben, neue Blöcke zu erstellen, indem sie eine bestimmte Menge an Geldmitteln blockieren. Natürlich ist auch in diesem Fall die Belohnung für die Erstellung der Blöcke eine finanzielle Belohnung.

Das Staking erfolgt mit einem vordefinierten Betrag der Kryptowährung der Blockchain, gemäß den Regeln des jeweiligen Protokolls. Verschiedene Implementierungen haben unterschiedliche Varianten, aber sobald ein Validator die erforderliche Menge blockiert, kann er vom Protokoll zufällig ausgewählt werden, um den

nächsten Block zu erstellen und die Belohnung zu erhalten. Es könnten auch mehrere Validatoren ausgewählt werden, um den Block zu erstellen, und in diesem Fall würde die Belohnung proportional zur Menge der von jedem Validator blockierten Kryptowährung verteilt werden.

Wie wir weiter unten sehen werden, befindet sich Ethereum, die nach Bitcoin am meisten kapitalisierte Kryptowährung, im Übergang von PoW zu PoS.
Auch hier betrachten wir die Vor- und Nachteile des Proof of Stake.

Die Vorteile sind wie folgt:

- Umweltfreundlich: Der CO_2-Fußabdruck des POS ist nur ein Bruchteil desjenigen des Minings. Staking macht ressourcenintensive Hashing-Operationen überflüssig und ist damit ein nachhaltigeres Konsensverfahren.
- Schnellere Transaktionen: Da keine zusätzliche Rechenleistung für die kryptografischen Probleme des Protokolls aufgewendet werden muss, ermöglicht der PoS schnellere Transaktionen.
- Belohnungen und Zinsen: Die Belohnungen für den Schutz des Netzwerks gehen nicht an die Miner, sondern werden direkt an die Inhaber der Kryptowährung ausgezahlt. In einigen Fällen ermöglicht der PoS den Nutzern, passives Einkommen in Form von Zinsen zu erzielen, indem sie ihre Gelder einfach fest anlegen.

Die Nachteile hingegen lassen sich wie folgt zusammenfassen:

- Relativ junge Technologie: PoS-Protokolle müssen erst noch in großem Maßstab getestet werden. Es könnte einige unentdeckte Schwachstellen in ihrer Implementierung geben.
- Plutokratie: Es wird befürchtet, dass PoS ein Ökosystem fördert, in dem „die Reichen noch reicher werden“, da Validatoren mit hohen Einsätzen tendenziell mehr verdienen als diejenigen, die weniger Coins zu blockieren haben.

Proof of Work und Proof of Stake sind die gebräuchlichsten Konsensverfahren, aber es gibt noch viele andere. Einige sind Mischformen und kombinieren Elemente beider Systeme, andere wiederum sind völlig unterschiedliche Methoden. Da es sich um ein Einführungsbuch handelt, werden andere Konsensmechanismen nicht untersucht. Es sollte jedoch darauf hingewiesen werden, dass es bis heute keinem anderen Konsensverfahren gelungen ist, die Popularität von PoW und PoS zu erreichen.

Kapitel 11

Die Forks

Wenn Sie aufgefordert werden, die App Ihrer Bank auf Ihrem Smartphone zu aktualisieren, denken Sie wahrscheinlich nicht zweimal darüber nach, dies zu tun. Es ist sogar wahrscheinlich, dass sich Ihr Handy automatisch aktualisiert, ohne dass Sie es bemerken. Das ist auch notwendig, denn wenn Sie nicht die neueste Version der Software installieren, besteht die Gefahr, dass Ihnen der Zugang zu Bankdienstleistungen verweigert wird.

Bei den Kryptowährungen ist das ganz anders. Man muss nicht jede Zeile des Bitcoin-Codes lesen, um ihn zu nutzen, aber die Möglichkeit dazu ist für Entwickler und Enthusiasten wichtig. Da es keine zentrale Stelle gibt, kann niemand einfach Aktualisierungen verschicken und Dinge nach Belieben ändern. Daher kann die Implementierung neuer Funktionen in Blockchain-Netzwerke eine Herausforderung darstellen.

Grundsätzlich gibt es zwei Arten von Aktualisierungen: Hard Forks und Soft Forks.

Um zu verstehen, wie Forks funktionieren, ist es wichtig, die Teilnehmer am Entscheidungsprozess des Netzes zu kennen. Dieser Prozess wird als „Governance“ bezeichnet, und jede Blockchain hat

ihre eigene. Bei Bitcoin zum Beispiel können wir grundsätzlich zwischen drei Untergruppen von Teilnehmern unterscheiden: Entwickler, Miner und Knoten. Dies sind die Parteien, die tatsächlich zum Netz beitragen. Die Entwickler sind für die Erstellung und Aktualisierung des Codes verantwortlich, der die Bitcoin-Software zum Laufen bringt. Bei den meisten Kryptowährungen kann jeder zu diesem Prozess beitragen, indem er Verbesserungen vorschlägt und auf Fehler hinweist. In der Tat ist der Code für fast alle Kryptowährungen öffentlich zugänglich und daher sehr einfach zu bearbeiten.

Wie an dieser Stelle klar sein sollte, sind die Miner diejenigen, die das Netzwerk schützen. Sie führen den Code der Kryptowährung aus und sind für das Hinzufügen neuer Blöcke zur Blockchain zuständig. Im Bitcoin-Netzwerk geschieht dies, wie wir gesehen haben, durch ein „Proof of Work“- Konsensverfahren.

Schließlich bilden die Knoten das Rückgrat einer Blockchain. Sie verifizieren, senden und empfangen Blöcke und erhalten eine vollständige Kopie der Blockchain.

In diesen drei Kategorien gibt es häufig Überschneidungen. Beispielsweise kann ein Entwickler zur gleichen Zeit einen Knoten haben oder eine Mining-Aktivität durchführen. Außerdem gibt es Netzwerkteilnehmer, die keine dieser drei Rollen innehaben. Viele, die als Nutzer einer Kryptowährung angesehen werden, halten keine dieser Positionen.

In Anbetracht dessen, was wir gerade gesagt haben, sollte man meinen, dass die Entwickler und Miner selbst Entscheidungen für das

Netzwerk treffen können. Schließlich sind es die Entwickler, die den Code erstellen, und ohne sie gäbe es keine lauffähige Software. Außerdem schützen die Miner das Netzwerk und ohne ihre Anwesenheit könnte die Blockchain angegriffen werden oder zum Stillstand kommen.

Wenn diese beiden Kategorien jedoch versuchen würden, den Rest des Netzes zu zwingen, ihrem Willen zu folgen, würde das nicht gut ausgehen. In vielen Fällen liegt die eigentliche Macht bei den Knoten und Nutzern, die keine aktive Rolle spielen. Denn es sind die Knoten und die Menschen, die eine Kryptowährung verwenden, die ihren Wert durch ihre Transaktionen und ihre Verwendung validieren.

Entwickler und Miner sind keine allmächtigen Herren: Sie sind Dienstleister. Wenn die Menschen das Netz nicht nutzen, verliert die Währung an Wert. Der Wertverlust wirkt sich direkt auf die Miner aus, die sofort einen Rückgang der Belohnungen für die Block-Validierung feststellen würden. Was die Entwickler betrifft, so können ihre Vorschläge von den Endnutzern einfach ignoriert werden.

Ein Software-Fork entsteht, wenn Software verändert wird. Das ursprüngliche Projekt hat überlebt, ist aber jetzt von dem neuen Projekt getrennt, das eine andere Richtung einschlägt. Die Projekte basieren auf einer gemeinsamen Grundlage und teilen einen Teil ihrer Geschichte. Wie eine einzige Straße, die sich nach einer Weile in zwei teilt und eine Abzweigung vom Hauptweg bildet.

Forks sind bei Open-Source-Projekten sehr verbreitet, vor allem bei den populärsten, wie Bitcoin und Ethereum. In der Abbildung unten sehen Sie zum Beispiel alle Forks, die bei Bitcoin stattgefunden haben, seit der erste Block geschürft wurde.

Betrachten wir nun speziell die Merkmale von Hard Forks und Soft Forks.

Hard Fork

Hard Forks sind Software-Updates, die mit früheren Versionen nicht kompatibel sind. Diese treten in der Regel auf, wenn Knoten neue Regeln hinzufügen, die im Widerspruch zu früheren Regeln stehen. Die neuen Knoten können nur mit anderen kommunizieren, die die neu eingeführten Regeln verwenden. Infolgedessen spaltet sich die Blockchain und es entstehen zwei getrennte Netzwerke: eines mit den alten und eines mit den neuen Regeln.

Nach einem Hard Fork gibt es zwei parallel arbeitende Netzwerke. Beide Netzwerke werden weiterhin Blöcke und Transaktionen hinzufügen, aber nicht mehr auf der gleichen Blockchain arbeiten.

Da ein Teil der Geschichte der beiden Netzwerke gemeinsam genutzt wird, werden Nutzer, die vor dem Fork Coins besaßen, am Ende in beiden Netzwerken die gleiche Anzahl von Coins besitzen. Ein Beispiel mag helfen. Nehmen wir an, wir hatten 5 BTC, als ein Fork beim 600 000er-Block stattfand. Nehmen wir nun an, dass wir die 5 BTC auf der alten Kette für den nächsten Block, den 600 001, ausgeben. Zu diesem Zeitpunkt werden wir auf der „ursprünglichen“ Blockchain 0 BTC haben. Diese wurden jedoch nicht für den Block 600 001 auf der neuen Blockchain ausgegeben. Unter der Annahme, dass die dem Netzwerk zugrunde liegende Kryptografie durch das Fork nicht verändert wurde, ermöglichen dieselben privaten Schlüssel immer noch den Zugang zu 5 BTC im neuen Netzwerk. Das bedeutet natürlich nicht, dass BTC im neuen Netzwerk genauso viel wert sein werden wie im alten Netzwerk. Der Preis wird immer durch das Zusammentreffen von Angebot und Nachfrage bestimmt. Zur Veranschaulichung sei darauf hingewiesen, dass bisher jedes Fork von Bitcoin und Ethereum zu weniger wertvollen Coins und weniger genutzten Blockchains geführt hat als die Hauptvarianten.

Ein Beispiel für ein Hard Fork war das Fork von 2017, das zur Entstehung von Bitcoin Cash (BCH) führte. Das Fork erfolgte nach einer langen Debatte über den besten Ansatz zur Skalierung von Bitcoin-Blöcken. Die Bitcoin-Cash-Befürworter wollten die Blockgröße erhöhen, während die Bitcoin-Befürworter gegen die Änderung waren.

Eine Vergrößerung der Blöcke erforderte eine Änderung der Regeln. Im Jahr 2017 akzeptierten die Bitcoin-Knoten nur Blöcke, die kleiner als 1 MB waren. Da die Bitcoin-Cash-Befürworter die Blockgröße auf 2 MB erhöhen wollten, wären diese auf der ursprünglichen Blockchain nicht als gültig angesehen worden. Aus diesem Grund musste eine zweite Blockchain geschaffen werden, die Bitcoin Cash-Blockchain, um diese Änderung umzusetzen.

Soft Fork

Ein Soft Fork ist eine Aktualisierung, die mit früheren Versionen kompatibel ist. Das bedeutet, dass aktualisierte Knoten weiterhin mit nicht aktualisierten kommunizieren können. Bei einem Soft Fork wird in der Regel eine neue Regel hinzugefügt, die nicht mit früheren Regeln kollidiert.

So kann beispielsweise eine Verringerung der Blockgröße durch eine Soft Fork erfolgen (im Gegensatz zu einer Vergrößerung der Blockgröße, wie wir es am Beispiel von Bitcoin Cash gesehen haben). Wieder einmal ist es Bitcoin, das uns ein passendes Beispiel bietet. In der Tat gibt es in der Bitcoin-Blockchain keine Grenze, wie klein ein Block sein kann. Wenn ein Knoten nur Blöcke unter einer bestimmten Größe annehmen will, muss er größere Blöcke einfach ablehnen. Dadurch wird die Verbindung zum Netz jedoch nicht automatisch unterbrochen. Er kommuniziert weiterhin mit Knoten, die diese Regel nicht umsetzen, filtert aber einige der von ihnen übermittelten Informationen heraus.
Ein gutes Beispiel für ein Soft Fork war die Einführung von Segregated Witness (SegWit), die kurz nach der Trennung von Bitcoin und Bitcoin

Cash erfolgte. SegWit war eine Aktualisierung, die das Format von Blöcken und Transaktionen änderte, aber sie wurde intelligent durchgeführt. Die alten Knoten konnten zwar noch Blöcke und Transaktionen validieren, hatten aber keinen Zugang zu bestimmten Informationen. Einige Felder waren nur lesbar, wenn die Knoten auf eine neuere Software aktualisiert wurden, die eine genaue Analyse dieser zusätzlichen Daten ermöglichte.

Hard Forks und Soft Forks haben grundsätzlich unterschiedliche Ziele. Die umstrittensten Hard Forks können eine Gemeinschaft spalten, aber die sorgfältig geplanten erlauben es, die Software mit der Zustimmung der Mehrheit des Netzwerks zu ändern.

Soft Forks hingegen sind eine empfindlichere Variante. Im Allgemeinen sind sie in ihren Verbesserungsmöglichkeiten stärker eingeschränkt, da neue Änderungen nicht im Widerspruch zu alten Vorschriften stehen dürfen.

TEIL 3 - VERSCHIEDENE ARTEN VON KRYPTOWÄHRUNGEN

„Virtuelle Währungen können langfristig vielversprechend sein, insbesondere wenn Innovationen ein schnelleres, sichereres und effizienteres Zahlungssystem fördern.“
Ben Bernanke (ehemaliger Vorsitzender der FED)

Kapitel 12

Ethereum

Nachdem wir nun die Grundlagen für das Verständnis der Funktionsweise von Kryptowährungen gelegt haben, wollen wir uns die zweithäufigste Kryptowährung ansehen. Wir sprechen hier ganz klar von Ethereum.

Beginnen wir mit einer Definition.

> **Definition: Ethereum ist eine dezentralisierte Computerplattform.**

Zur Verdeutlichung kann man es sich wie einen Computer vorstellen, der auf Tausenden von Rechnern in der ganzen Welt gleichzeitig läuft. Das bedeutet, dass Ethereum, wie Bitcoin, keinen Eigentümer und keine zentrale Instanz hat, die es kontrolliert.

Ethereum ermöglicht auch den Transfer von digitalem Geld. Es kann jedoch viel mehr als nur Transaktionen durchführen. Der Softwarecode von Ethereum ermöglicht es, mit den von anderen Nutzern erstellten Anwendungen zu interagieren. Aufgrund seiner Flexibilität kann jede Art von Programm auf Ethereum gestartet werden.

Mit anderen Worten: Die Hauptidee hinter Ethereum ist, dass Entwickler Programme erstellen und starten können, die auf einer Blockchain und nicht auf einem zentralisierten Server laufen. Dies bedeutet, dass Anwendungen, die auf Ethereum aufbauen, theoretisch nicht abgeschaltet oder zensiert werden können.
Es mag nicht intuitiv sein, aber die Werteinheiten von Ethereum heißen nicht „Ethereums“ oder ähnlich. Ethereum ist das Protokoll, aber die Währung, die es antreibt, ist als Ether bekannt. Wenn über den Preis von Ether gesprochen wird, wird der Ticker ETH verwendet. Von nun an wird diese Abkürzung auch in diesem Buch verwendet.

Wir haben erklärt, dass Ethereum in der Lage ist, Programme auf seiner Blockchain auszuführen. Daher können diese Anwendungen nicht von außen manipuliert werden. Anwendungen werden der Ethereum-Blockchain hinzugefügt und können so programmiert werden, dass der Code nicht verändert werden kann. Da die Ethereum-Blockchain für jedermann sichtbar ist, können die Nutzer den Code einer Anwendung überprüfen, bevor sie sie verwenden.
Aber wozu dienen diese Anwendungen? Der interessanteste Anwendungsfall sind sicherlich die Smart Contracts. Lassen Sie uns gleich eine Definition geben.

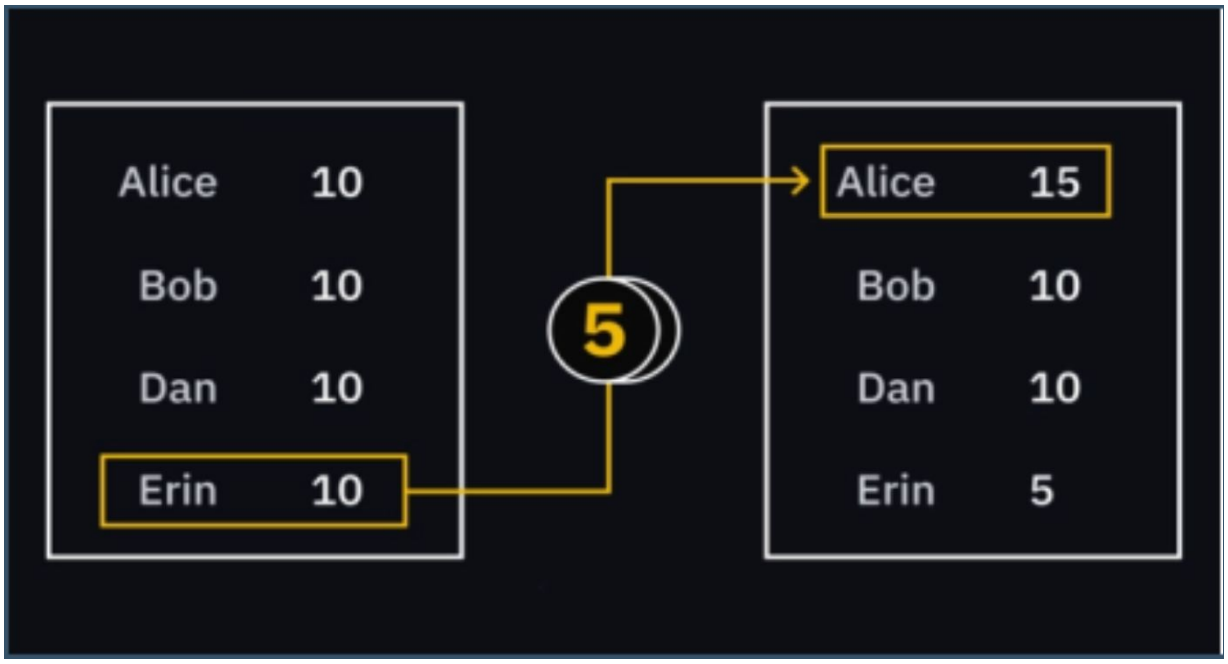
> **Definition: Ein Smart Contract ist ein Vertrag, der automatisch gilt, wenn die Bedingungen für seine Anwendung erfüllt sind.**

Es versteht sich von selbst, dass die Hauptanwendung von Smart Contracts in der Finanzwelt liegt. Aus diesem Grund wird Ethereum von vielen als „programmierbares Geld“ bezeichnet.

Definition: Ethereum ist programmierbares Geld.

Wie Ethereum funktioniert

Zu jeder Zeit kann man eine Momentaufnahme aller Kontostände und Smart Contracts erhalten. Da einige Aktionen eine Statusaktualisierung verursachen, aktualisieren alle Knoten ihre Momentaufnahme, um die Änderung widerzuspiegeln.



Smart Contracts, die auf Ethereum ausgeführt werden, werden durch Transaktionen ausgelöst, die von Nutzern oder von anderen Smart Contracts durchgeführt werden können. Wenn ein Nutzer eine Transaktion an einen Smart Contract sendet, führt jeder Knoten im Netzwerk den Vertragscode aus und zeichnet die Ausgabe auf. Dies geschieht mithilfe der Ethereum Virtual Machine, die Smart Contracts in Anweisungen umwandelt, die die Ethereum-Software lesen kann. Um den Status von Smart Contracts zu aktualisieren, setzt Ethereum derzeit ebenfalls auf Mining, mit einem Proof-of-Work-

Konsensverfahren, der dem von Bitcoin sehr ähnlich ist. Während dieses Buch geschrieben wird, führt Ethereum jedoch langsam Aktualisierungen durch, die es zu einem Proof-of-Stake-Mechanismus machen werden. Der Übergang wird mit der Einführung von Ethereum 2.0 in naher Zukunft abgeschlossen sein.

Smart Contracts

Ein Smart Contract ist einfach ein Stück Code. Der Code selbst ist weder intelligent (Smart) noch ein Vertrag (Contract) im herkömmlichen Sinne. Dennoch wird er als Smart bezeichnet, weil er sich unter bestimmten Bedingungen selbst ausführt und als Vertrag angesehen werden kann, weil er Vereinbarungen zwischen den Parteien vorschreibt.
Das Konzept eines Smart Contracts wurde Ende der 1990er-Jahre von dem Informatiker Nick Szabo vorgeschlagen. Er erläuterte das Konzept am Beispiel eines Getränkeautomaten. In seinem Beispiel handelt es sich um einen einfachen Vertrag in Ausführung: Der Benutzer wirft Münzen ein, und der Automat gibt im Gegenzug das Getränk seiner Wahl aus.

Ein Smart Contract wendet diese Art von Logik in einer digitalen Umgebung an. Im Code könnte etwas Einfaches angegeben werden, z. B. „Hallo, Welt!“, das erscheint, wenn zwei Ether an diesen Vertrag gesendet werden. Auf Ethereum würde der Entwickler diesen Smart Contract so verschlüsseln, dass er von der EVM (Ethereum Virtual Machine) gelesen werden kann. Dazu würde er eine Programmiersprache namens Solidity verwenden. Anschließend wird

der Smart Contract an eine spezielle Adresse gesendet, die ihn in der Ethereum-Blockchain registriert. Von da an kann ihn jeder benutzen.

Der Vertrag hätte also eine Adresse. Um damit zu interagieren, müssten die Nutzer nur 2 ETH an diese Adresse senden. Diese Aktion würde den Code des Vertrags auslösen: Alle Computer im Netzwerk würden ihn ausführen, sehen, dass die Zahlung für den Vertrag erfolgt ist, und seine Ausgabe (Hallo, Welt!) in der Blockchain aufzeichnen. Dies ist vielleicht eines der grundlegendsten Beispiele dafür, was man mit Ethereum machen kann. Es können auch komplexere Anwendungen erstellt werden, die viele Verträge miteinander verbinden. Das Faszinierende an Ethereum ist gerade die Möglichkeit, extrem komplexe Anwendungen zu entwickeln, die die klassischen Strukturen des traditionellen Finanzwesens völlig dezentralisiert nachbilden können. Wir sprechen von der Freiheit, dezentralisierte Handelsplattformen zu schaffen, Immobilien ohne Zwischenhändler zu kaufen oder Zugang zu Krediten zu haben, die nicht von einer Bank genehmigt werden müssen. Aus diesem Grund ist die Definition von „programmierbarem Geld“ für Ethereum sehr passend.

Das Ethereum-Gas

Nehmen wir das Beispiel des einfachen Smart Contracts von vorhin. Das Programm war einfach auszuführen: Sobald 2 ETH an die Vertragsadresse gesendet wurden, wird „Hallo Welt“ in der Blockchain registriert. Es ist überhaupt nicht rechenaufwendig. Der Smart Contract wird jedoch nicht nur von einem PC ausgeführt,

sondern das gesamte Ethereum-Ökosystem wird aufgefordert, ihn auszuführen.
Dies bringt uns zu einer entscheidenden Frage: Was passiert, wenn Zehntausende von Menschen komplexe Smart Contracts ausführen? Wenn jemand seinen Smart Contract so einrichtet, dass er immer wieder denselben Code ausführt, müsste jeder Knoten ihn unendlich oft ausführen. Dies würde die Ressourcen belasten und das System würde wahrscheinlich in kurzer Zeit zusammenbrechen. Um dieses Risiko zu mindern, führte Ethereum das Konzept des „Gas“ ein. So wie ein Auto nicht ohne Treibstoff fahren kann, können auch Smart Contracts nicht ohne Gas laufen. Smart Contracts legen einen Gasbetrag fest, den die Nutzer zahlen müssen, damit sie erfolgreich funktionieren. Wenn nicht genügend Gas vorhanden ist, wird der Vertrag gekündigt.

Es ist zu beachten, dass ETH und Gas nicht dasselbe sind. Der durchschnittliche Gaspreis schwankt und wird weitgehend von den Minern bestimmt. Wenn Sie eine Transaktion durchführen, bezahlen Sie das Gas in ETH. Es ist wie bei den Bitcoin-Provisionen: Wenn das Netzwerk überlastet ist und viele Nutzer versuchen, Transaktionen durchzuführen, wird der Durchschnittspreis für Gas wahrscheinlich steigen. Umgekehrt werden die Kosten sinken, wenn nicht viel los ist.
Während sich der Gaspreis ändert, ist für jede Transaktion eine feste Gasmenge erforderlich. Das bedeutet, dass komplexe Verträge viel mehr kosten als eine einfache Transaktion. Folglich ist Gas auch ein Maß für die Rechenleistung. Damit wird sichergestellt, dass das

System den Nutzern je nach Nutzung der Ethereum-Ressourcen einen angemessenen Tarif anbieten kann.
Gas kostet in der Regel einen Bruchteil des ETH. Daher wird eine kleinere Einheit zur Kennzeichnung verwendet. Diese Einheit ist die „gwei“. Eine gwei entspricht einem Milliardstel ETH.

Lassen Sie uns dieses Konzept anhand eines praktischen Beispiels besser verstehen. Nehmen wir an, dass Anna eine Transaktion für einen Smart Contract durchführt. Über eine Website wie ETH Gas Station (ethgasstation.info) würde Anna herausfinden, wie viel sie ausgeben muss, um Anreize für die Miner zu schaffen, ihre Transaktion so schnell wie möglich durchzuführen. Anna wird auch einen Gasgrenzwert festlegen, der als Schutz dient. Es könnte nämlich etwas mit dem Smart Contract schiefgehen, sodass er mehr Gas verbraucht als erwartet. Der Gasgrenzwert soll sicherstellen, dass der Betrieb eingestellt wird, sobald eine bestimmte Gasmenge verbraucht ist. In diesem Fall würde der Smart Contract nicht aktiviert werden, aber Anna würde am Ende nicht mehr bezahlen als ursprünglich vereinbart.

Kapitel 13

Die Geschichte von Ethereum

Einige Jahre nach der Erfindung von Bitcoin stellte sich ein junger Programmierer namens Vitalik Buterin eine Möglichkeit vor, das Konzept der finanziellen Dezentralisierung auf jede Art von Anwendung zu übertragen. Ethereum wurde von Buterin selbst im Jahr 2013 in einem Beitrag in seinem Blog vorgestellt. Der Artikel trug den Titel „Ethereum: die ultimative Plattform für Smart Contracts und dezentrale Anwendungen“. In seinem Beitrag beschrieb Vitalik Buterin die Idee eines dezentralen Computers, der mit genügend Zeit und Ressourcen jede beliebige Anwendung ausführen könnte. Im Laufe der Zeit werden die Arten von Anwendungen, die auf einer Blockchain implementiert werden können, nur durch die Vorstellungskraft der Entwickler begrenzt sein.

Nach diesem Artikel machte sich Vitalik Buterin an die Programmierung der ersten Version von Ethereum. Die Software wurde 2015 mit einem Anfangsangebot von 72 Millionen Ether eingeführt. Mehr als 50 Millionen dieser Token wurden im Rahmen eines Initial Coin Offering verteilt, bei dem Interessierte Ether im Austausch gegen Bitcoin oder Fiat-Währung kaufen konnten. In der Folge beschlossen viele Kryptowährungen, dem von Ethereum vorgeschlagenen Schema für die Erstausgabe von Coins zu folgen.

DAO

Mit Ethereum sind völlig neue Formen der Zusammenarbeit möglich geworden. Nehmen wir zum Beispiel DAO (dezentralisierte autonome Organisationen). Es handelt sich um Einheiten, die durch Codes gesteuert werden, ähnlich wie ein Computerprogramm.

Einer der ersten und ehrgeizigsten Versuche einer solchen Organisation wurde „The DAO“ genannt. Es hätte aus komplexen Smart Contracts bestanden, die auf Ethereum laufen und als dezentraler und autonomer Investmentfonds funktionieren. DAO-Token wurden auch im Rahmen eines Initial Coin Offering (oft als ICO abgekürzt) verteilt und gaben ihren Besitzern eine Beteiligung an der Organisation und Stimmrechte.

Doch schon kurz nach dem Start nutzten Hacker eine Schwachstelle im Code aus und zogen fast ein Drittel des DAO-Guthabens ab. Es sei daran erinnert, dass zu diesem Zeitpunkt 14 % des gesamten ETH-Angebots der DAO gehörten. Natürlich war dies ein verheerendes Ereignis für das Ethereum-Netzwerk, das noch immer versuchte, seine ersten Schritte zu machen.

Nach diesem Ereignis wurde die Blockchain nach einiger Überlegung in zwei Netzwerke aufgeteilt. In einem dieser Netzwerke wurden die gestohlenen Transaktionen effektiv „rückgängig“ gemacht, um die Gelder wiederherzustellen: Dieses Netzwerk wird als das „echte“ Ethereum angesehen. Die ursprüngliche Blockchain, bei der diese Transaktionen nicht rückgängig gemacht wurden und die

Unveränderlichkeit beibehalten wurde, ist jetzt als Ethereum Classic bekannt.

Dieses Ereignis erinnerte uns eindringlich an die Risiken dieser Technologie und daran, wie gefährlich es sein kann, große Mengen an Vermögenswerten einer Software anzuvertrauen. Es ist auch ein interessantes Beispiel dafür, dass das Treffen kollektiver Entscheidungen erhebliche Herausforderungen mit sich bringen kann. Ungeachtet ihrer Sicherheitslücken veranschaulichte die DAO jedoch das Potenzial der Smart Contracts für eine zuverlässige Zusammenarbeit im großen Maßstab im Internet. Der Beweis, dass dies tatsächlich möglich ist, war der Auslöser für die massive Entwicklung von Anwendungen auf Ethereum

Kapitel 14

Die Token auf Ethereum

Ein großer Teil der Anziehungskraft von Ethereum liegt in der Möglichkeit für die Nutzer, ihre eigenen Token auf der Blockchain zu erstellen. Die für sie geltenden Regeln sind in Smart Contracts festgelegt, die es den Entwicklern ermöglichen, bestimmte Parameter für ihre Token festzulegen. Diese Parameter können die Gesamtmenge der im Umlauf befindlichen Token, ihre Verteilung, Fungibilität und viele andere Aspekte umfassen. Der wichtigste der technischen Standards, die die Erstellung von Token auf Ethereum ermöglichen, heißt ERC-20. Aus diesem Grund werden die Token auf Ethereum im Allgemeinen als ERC-20-Token bezeichnet.

Die Möglichkeit, eigene Token zu erstellen, bietet Innovatoren eine Möglichkeit, innovative Finanz- und Technologieanwendungen zu entwickeln. Von der Ausgabe von Token, die als In-App-Währungen dienen, bis hin zur Herstellung einzigartiger Token, die mit physischen Ressourcen unterlegt sind, ist die Gestaltungsflexibilität praktisch unbegrenzt.

Einmal erstellt, sind neue ERC-20-Token automatisch mit Diensten und Software interoperabel, die den ERC-20-Standard unterstützen. Infolgedessen ist im Laufe der Jahre ein reichhaltiges Ökosystem von

ERC-20-Token entstanden, das ständig erweitert wird. Wir geben daher eine wichtige Definition.

> **Definition: Ein ERC-20-Token ist ein auf Ethereum aufgebauter Token, der einen komplexen Smart Contract abwickelt.**

Wie aus der Definition hervorgeht, verfügen ERC-20-Token also nicht über eine eigene Blockchain. Interessanterweise sind zum Zeitpunkt der Erstellung dieses Buches bereits 3 der 10 am höchsten kapitalisierten Kryptowährungen ERC-20-Token.

Wie man einen ERC-20-Token erstellt

Um dem ERC-20-Standard zu entsprechen, muss der Smart Contract sechs obligatorische Funktionen enthalten. Diese sind: Gesamtangebot, Saldo, Übertragung, Übertragung von, Genehmigung und Zulage. Außerdem können optionale Funktionen angegeben werden, wie Name, Symbol und Dezimalzahl. Was diese Funktionen bewirken, geht vielleicht schon aus ihren Namen hervor. Lassen Sie uns auf jeden Fall mehr ins Detail gehen.

- „Gesamtangebot“ gibt die Gesamtmenge der im Smart Contract enthaltenen Token an.
- Unter „Saldo“ können Sie die Menge der Token sehen, die einer bestimmten Adresse gehören. Denken Sie daran, dass die Adressen im Ethereum-Netzwerk öffentlich sind, sodass Sie den Kontostand jeder Adresse sehen können, solange sie bekannt ist.

- Mit der Funktion „Übertragung“ können Token von einer Adresse zu einer anderen verschoben werden.
- Die Funktion „Übertragen von“ ist eine Alternative zur Funktion „Übertragen“, ermöglicht aber etwas mehr Programmierbarkeit bei dezentralen Anwendungen. Wie die Funktion „Übertragen“ wird auch „Übertragen von“ verwendet, um Token zu verschieben, die jedoch nicht unbedingt der Person gehören müssen, die den Smart Contract ausführt. Mit anderen Worten: Man kann jemanden – oder einen anderen Smart Contract – ermächtigen, im Namen einer dritten Partei Geld zu überweisen. Ein möglicher Anwendungsfall ist die Bezahlung von abonnementbasierten Diensten, bei denen Sie nicht jeden Monat manuell eine Zahlung übermitteln möchten, sondern dies von einem Smart Contract erledigen lassen.
- Die Funktion „Genehmigung“ ist nützlich für die Programmierbarkeit eines ERC-20-Tokens. Mit dieser Funktion können Sie die Anzahl der Token begrenzen, die ein Smart Contract aus dem Guthaben einer Adresse entnehmen kann. Ohne diesen Parameter besteht die Gefahr, dass der Smart Contract nicht ordnungsgemäß funktioniert und es zu einem Verlust von Geldern kommt.
- Die Funktion „Zulage“ ist mit der Funktion „Genehmigung“ verbunden. Wenn Sie einem Smart Contract die Erlaubnis erteilen, seine Token zu verwalten, können Sie mit der Funktion „Zulage“ prüfen, wie viele Token dem Smart Contract noch entnommen werden können.

Nimmt man alle Funktionen zusammen, über die wir gesprochen haben, erhält man einen ERC-20-Token. Die durch diese Funktionen festgelegten Regeln schränken die Entwicklung nicht ein, sodass Entwickler zusätzliche Funktionen implementieren und spezifische Parameter für ihre eigenen Bedürfnisse festlegen können.

Ein interessanter Aspekt ist, dass ERC-20-Token nicht abgebaut werden können. Vielmehr kann man sagen, dass sie geprägt werden, wenn neue Coins geschaffen werden. Wenn ein Smart Contract gestartet wird, verteilen die Entwickler den anfänglichen Vorrat nach ihren Plänen. In der Regel geschieht dies durch ein Initial Coin Offering, ein Initial Exchange Offering oder ein Security-Token Offering. In jedem dieser Fälle senden die Anleger ETH an die Adresse des Smart Contracts und erhalten im Gegenzug Token. Das gesammelte Geld wird zur Finanzierung der weiteren Entwicklung des Projekts verwendet. Die Nutzer erwarten, dass sie ihre Token verwenden oder mit Gewinn verkaufen können, wenn sich das Projekt weiterentwickelt und der Wert der Token steigt.
Werfen wir einen Blick auf einige der Anwendungsfälle für ERC-20-Token.

Stablecoins

Stablecoins, also Token, deren Wert an den Wert eines gesetzlichen Zahlungsmittels gekoppelt ist, verwenden häufig den ERC-20-Token-Standard. Bei einem typischen Stablecoin, der mit einer Fiat-Währung unterlegt ist, hält der Emittent Reserven in Euro, Dollar usw., sodass er für jede Einheit in seiner Reserve einen Token ausgibt. Für jede Einheit in seiner Reserve gibt er also ein Plättchen aus. Das

bedeutet, dass, wenn 10 000 Dollar im Tresorraum einer Bank eingeschlossen wären, 10 000 Token geschaffen werden könnten, die jeweils 1 Dollar entsprechen.

Dies ist auf Ethereum relativ einfach zu implementieren. Der Emittent initiiert einfach einen Vertrag mit 10 000 Token. Diese werden dann an die Nutzer verteilt, mit dem Versprechen, dass sie die Token später für einen entsprechenden Betrag an Fiat-Währung „verkaufen“ können.

Nutzer können mit ihren Token eine Reihe von Dingen tun: Sie können Waren und Dienstleistungen kaufen oder sie in anderen Ethereum-Anwendungen verwenden. Alternativ können sie verlangen, dass der Emittent sie sofort in den Gegenwert der Fiat-Währung umtauscht. In diesem Fall nimmt der Emittent die zurückgegebenen Token vom Markt und entnimmt die entsprechende Menge an Fiat-Währung aus seinen Reserven, um sie dem Nutzer zu geben, der den Umtausch beantragt hat. Der Smart Contract, der dieses System steuert, ist, wie erwähnt, relativ einfach. Die Markteinführung eines Stablecoins erfordert jedoch eine Menge Arbeit in Bezug auf externe Faktoren wie Logistik und Einhaltung von Vorschriften.

Die beliebtesten Stablecoins sind Tether (USDT) und USD Coin (USDC).

Security-Token

Security-Token sind ähnlich wie Stablecoins. Auf der Ebene des Smart Contracts können beide sogar identisch sein, da sie auf

dieselbe Weise funktionieren. Der Unterschied liegt auf der Ebene des Emittenten. Security-Token stellen bankfähige Wertpapiere wie Aktien, Anleihen oder Sachwerte dar. Häufig, wenn auch nicht immer, gewähren sie dem Eigentümer eine Art Beteiligung an einem Unternehmen oder Projekt.

Ein gutes Beispiel für einen Security-Token ist Golem Network. Der Besitzer des Golem Network Token (GNT) hat das Recht, dem Netzwerk die Rechenleistung seines PCs zu leihen, im Austausch für weitere GNT-Token. Natürlich können diese Token dann auf dem Markt gegen Fiat-Währung gehandelt werden.

Utility-Token

Utility-Token sind vielleicht die häufigste Art von Token, die heute auf dem Kryptowährungsmarkt zu finden sind. Im Gegensatz zu den beiden vorhergehenden Arten sind Utility-Token durch nichts gedeckt. Wenn Asset-gestützte Token wie Aktien einer Fluggesellschaft sind, sind Utility-Token wie Treueprogramme: Sie erfüllen eine Funktion, haben aber keinen externen Wert. Sie können eine Vielzahl von Anwendungsfällen abdecken, z. B. als Währung in einem Online-Spiel, als Treibstoff für dezentrale Anwendungen, als Treuepunkte und vieles mehr.

Ein Paradebeispiel für einen Utility-Token ist der Token von Crypto.com, CRO. Mit diesem Token können Sie innerhalb des Ökosystems des Handels bestimmte Operationen durchführen und bestimmte Boni erhalten.

Andere Token-Standards auf Ethereum

ERC-20 war der erste und bis heute populärste Ethereum-Standard, aber er ist keineswegs der einzige. Im Laufe der Jahre sind viele andere aufgetaucht, die Verbesserungen am ERC-20-Standard vorschlagen oder versuchen, ganz andere Ziele zu erreichen.
Einige der weniger verbreiteten Standards sind die, die in Non-Fungible Token, auch bekannt als NFT, verwendet werden. Der ERC-721-Standard wurde zum Beispiel für das CryptoKitties-Projekt verwendet. Es bietet eine API, mit der Nutzer ihre eigenen Non-Fungible Token prägen und deren Metadaten ändern können.

Der ERC-1155-Standard kann als eine Verbesserung von ERC-721 und ERC-20 angesehen werden. Er beschreibt einen Standard, der Fungible und Non-Fungible Token im selben Vertrag unterstützt. Andere Optionen wie ERC-223 oder ERC-621 zielen darauf ab, die Nutzbarkeit von Token zu verbessern. Ersteres implementiert Systeme zur Verhinderung versehentlicher Token-Übertragungen, während Letzteres zusätzliche Funktionen zur Erhöhung und Verringerung des Gesamtangebots an Token enthält.

Kapitel 15

Non-Fungible Token (NFT)

Ein Non-Fungible Token ist eine Art kryptografischer Token, der ein einzelnes Element darstellt. NFTs können „tokenisierte“ Versionen von digitalen oder realen Vermögenswerten sein. Sie dienen als überprüfbarer Nachweis der Authentizität und des Eigentums innerhalb eines Blockchain-Netzwerks. NFTs sind nicht untereinander austauschbar und bringen Knappheit in die digitale Welt.

Unter Fungibilität versteht man das Eigentum an einem Vermögenswert, dessen einzelne Einheiten austauschbar und im Wesentlichen nicht voneinander zu unterscheiden sind. Zum Beispiel sind alle gesetzlichen Währungen fungibel. Um als Tauschmittel zu fungieren, muss jede einzelne Einheit gegen jede andere gleichwertige einzelne Einheit austauschbar sein. Ein Beispiel: Ein Fünf-Euro-Schein ist mit jedem anderen Fünf-Euro-Schein austauschbar.

NFTs können von dezentralen Anwendungen genutzt werden, um die Erstellung und das Eigentum an einzigartigen digitalen Objekten und Sammlerstücken zu ermöglichen. Obwohl NFTs auf Plattformen gehandelt werden können, die Käufer und Verkäufer zusammenbringen, ist zu beachten, dass der Wert eines jeden NFTs

vor dem eigentlichen Kauf oder Verkauf nicht quantifizierbar ist. Um die Ausstellung von NFTs zu erleichtern, wurden verschiedene Standards geschaffen. Der Wichtigste davon ist, wie im vorherigen Kapitel erwähnt, ERC-721, ein Standard für die Ausgabe und den Handel mit nicht-fungiblen Vermögenswerten auf der Ethereum-Blockchain.

Die Standardisierung von NFTs ermöglicht ein hohes Maß an Interoperabilität, was bedeutet, dass einzigartige Ressourcen relativ einfach zwischen verschiedenen Anwendungen übertragen werden können.

NFTs haben das Potenzial, eine der Schlüsselkomponenten einer neuen digitalen Wirtschaft auf der Grundlage der Blockchain zu sein. Sie könnten in vielen verschiedenen Bereichen eingesetzt werden, z. B. für Videospiele, digitale Identitäten, Lizenzen, Zertifikate und sogar für das Bruchteileigentum an teuren Gegenständen.

Das bekannteste NFT ist das Werk „Die ersten 5000 Tage“ des Künstlers Mike Winkelmann, der im Internet als Beeple bekannt ist. Das Werk ist im Wesentlichen eine digitale Collage aus 5000 Werken des Künstlers und wurde für mehr als 69 Millionen Dollar versteigert.

Dieses Ereignis hat zweifellos ein großes Medieninteresse hervorgerufen, und der NFT-Markt hat sich durch diese Käufe und Verkäufe stark vergrößert. Heute gibt es Zehntausende von Künstlern, die ihre Werke in NFTs umsetzen. Einige widmen sich der

Herstellung von Sammelobjekten, andere digitalisieren einfach ihr geistiges Eigentum. Die beiden wichtigsten Börsen, die den Kauf und Verkauf von NFT ermöglichen, sind Opensea (opensea.io) und Rarible (rarible.com).

NFT-Anwendungsfälle

Anhand des Beispiels von Beeple haben wir gesehen, dass NFTs ein hervorragendes Werkzeug für die Digitalisierung von Kunstwerken sind. Es gibt jedoch noch weitere Anwendungsfälle, die es wert sind, in Betracht gezogen zu werden, um einen vollständigeren Überblick zu erhalten.
Ein Anwendungsfall von NFT sind Sammlerstücke. Mit den „NBA Top Shot“ Sammelkarten hat dieser Fall sogar die Mainstream-Medien erreicht. Zusammen mit digitaler Kunst machen diese Non-Fungible Token einen erheblichen Prozentsatz der Verkäufe auf Opensea und Rarible aus.

Auch die Spielindustrie hat einen großen Bedarf an NFT, die gehandelt und gekauft werden können. Die Seltenheit von Videospielobjekten wirkt sich direkt auf ihren Preis aus, und Vielspieler sind bereits mit dem Gedanken an wertvolle digitale Objekte vertraut. Mikrotransaktionen und In-Game-Käufe haben eine Multi-Milliarden-Dollar-Gaming-Industrie geschaffen, die von NFT weiter beflügelt werden könnte. Neben dem wirtschaftlichen Aspekt ist es auch ein spannender Bereich in Bezug auf das, was ein NFT darstellt. Videospiel-Token verbinden Kunst, Sammeln und Nutzen für

die Spieler. Bei den großen Videospielen ist die Einführung von NFT jedoch noch in weiter Ferne.

Tokenisierung realer Objekte

Wer hat gesagt, dass NFTs nur digitale Objekte darstellen sollten? Die Verknüpfung von realen Vermögenswerten mit NFTs kann die Art und Weise, wie Menschen Sachwerte besitzen, digitalisieren. In der Immobilienbranche beispielsweise können durch die Schaffung von tokenisierten digitalen Vermögenswerten hochgradig illiquide Objekte (wie ein Haus oder ein Grundstück) auf die Blockchain übertragen und leicht austauschbar gemacht werden. Dies ist bereits im April 2021 geschehen, als der Immobilienmakler Shane Dulgeroff ein NFT für eine zum Verkauf stehende Immobilie in Kalifornien erstellte, die dann versteigert wurde. Derjenige, der die Auktion gewann, erhielt das NFT, das den Besitz des Hauses bescheinigte. Allerdings ist die Unterstützung durch die Gesetzgeber bisher nicht sehr groß gewesen. Dieser Sektor ist noch in der Entwicklung begriffen, aber er ist ein sehr guter Sektor für die Zukunft.

Kapitel 16

Das dezentrale Finanzwesen

Als wir über Smart Contracts sprachen, erwähnten wir, wie sie zum Aufbau eines neuen Finanzsystems genutzt werden könnten, das

ohne Zwischenhändler funktioniert. Dies ist das Ziel des dezentralen Finanzwesens (oder einfach DeFi). Zunächst einmal eine Definition.

> **Definition: Dezentrales Finanzwesen (DeFi) ist ein Ökosystem von Finanzanwendungen, die auf Blockchain-Netzwerken aufbauen.**

Genauer gesagt kann sich der Begriff dezentrales Finanzwesen auf eine Bewegung beziehen, die darauf abzielt, ein quelloffenes, erlaubnisfreies und transparentes Ökosystem von Finanzdienstleistungen zu schaffen, das allen zur Verfügung steht und ohne eine zentrale Behörde funktioniert. Die Nutzer behalten die volle Kontrolle über ihre Ressourcen und interagieren mit diesem Ökosystem über Smart-Contract-basierte Anwendungen.

Der Hauptvorteil des dezentralen Finanzwesens ist der einfache Zugang zu Finanzdienstleistungen, insbesondere für diejenigen, die vom traditionellen Finanzsystem isoliert sind. Bedenken Sie, dass mehr als 2 Milliarden Menschen auf der Welt keinen Zugang zu Finanzdienstleistungen haben. Der Grund dafür ist, dass das traditionelle Finanzsystem auf Vermittlern beruht, die Gewinne erzielen müssen und daher ihre Dienstleistungen nicht in Ländern mit niedrigem Einkommen anbieten können.
Mit dem dezentralen Finanzwesen soll dieses Problem – zumindest teilweise – gelöst werden.

Ein weiterer Vorteil von DeFi ist die modulare Struktur, auf der es aufbaut: Die Interoperabilität von Anwendungen auf öffentlichen Blockchains schafft völlig neue Finanzmärkte, Produkte und

Dienstleistungen, die viel effizienter und ausgefeilter sind als einzelne Projekte, die einzeln durchgeführt werden.

Das traditionelle Finanzwesen stützt sich bekanntlich auf Institutionen wie Banken oder Makler, die ihre Dienstleistungen anbieten. Im Gegensatz dazu benötigen DeFi-Anwendungen keine Vermittler oder zentralen Stellen. Der Code des Smart Contracts legt die Lösung möglicher Streitigkeiten fest, und die Nutzer behalten jederzeit die Kontrolle über ihr Geld. Dadurch werden die mit der Nutzung dieser Produkte verbundenen Kosten gesenkt und ein leichter zugängliches Finanzsystem ermöglicht.

Da diese neuen Finanzdienstleistungen auf der Blockchain implementiert sind, gibt es keine Fehlerquellen. Tatsächlich sind die Daten über Tausende von Knoten verteilt, was es praktisch unmöglich macht, einen Dienst zu zensieren oder abzuschalten.

Hier sind die wichtigsten Anwendungsfälle für dezentrales Finanzwesen.

Darlehen

Dezentrale Darlehensprotokolle sind eine der beliebtesten Anwendungen im DeFi-Ökosystem. Die dezentrale Darlehensvergabe hat viele Vorteile gegenüber dem traditionellen Darlehenssystem. Dazu gehören die sofortige Abwicklung von Transaktionen und keine Bonitätsprüfung.

Da diese Darlehensdienste auf öffentlichen Blockchains basieren, minimieren sie das erforderliche Vertrauen des Darlehensgebers. Die Darlehensvergabe über DeFi-Anwendungen verringert das Ausfallrisiko und macht die Darlehensvergabe billiger, schneller und leichter zugänglich.

Bankdienstleistungen

Da es sich bei DeFi-Anwendungen per Definition um Finanzanwendungen handelt, sind Bankdienstleistungen ein naheliegender Anwendungsfall für sie. Dazu können die Ausgabe von Stablecoins, Hypotheken und Versicherungen gehören.
In dem Maße, wie der dezentrale Finanzsektor reift, wird der Schaffung von Stablecoins mehr Aufmerksamkeit gewidmet. Da die Preise von Kryptowährungen schnell schwanken können, können Stablecoins für den täglichen Gebrauch und zum Schutz des eigenen Kapitals im Falle eines Marktzusammenbruchs verwendet werden.

Dezentrale Börsen

Diese Plattformen ermöglichen es den Nutzern, Kryptowährungen zu tauschen, ohne dass ein Vermittler erforderlich ist. Der Austausch erfolgt direkt zwischen den Wallets der Nutzer mithilfe von Smart Contracts. Da sie viel weniger Wartungsarbeiten erfordern, sind die Gebühren auf dezentralen Börsen niedriger als auf zentralen Börsen.

Smart Contracts und dezentrales Finanzwesen

Die meisten Anwendungen des dezentralen Finanzwesens beinhalten die Erstellung und Ausführung von Smart Contracts. Die Verwendung von Smart Contracts macht die Erbringung von Dienstleistungen schneller und einfacher und verringert die Risiken für beide Parteien. Andererseits bringen sie auch neue Arten von Risiken mit sich. Da Smart Contracts anfällig für Fehler und Schwachstellen sein können, können Kryptowährungen und die darin enthaltenen vertraulichen Informationen gefährdet sein.

Entscheidende Bedeutung des dezentralen Finanzwesens

Wie alles, was ein hohes Maß an Innovation mit sich bringt, hat auch das dezentrale Finanzwesen seine Tücken. Erstens sind Blockchains exponentiell langsamer als zentrale Lösungen, was zu langsamen Anwendungen führt, die auf ihnen aufbauen. Die Entwickler von DeFi-Anwendungen müssen diese Einschränkungen berücksichtigen und ihre Produkte entsprechend optimieren.

Außerdem übertragen dezentrale Finanzanwendungen die Verantwortung von den Vermittlern auf den Nutzer. Dies kann für viele ein Nachteil sein, insbesondere für diejenigen, die neu in dieser Welt sind. Die Entwicklung von Produkten, die das Risiko von Benutzerfehlern minimieren, ist eine besonders schwierige Herausforderung, wenn diese auf Blockchain basieren. Daher erfordert die Nutzung dezentraler Finanzanwendungen derzeit einen zusätzlichen Aufwand auf Seiten der Nutzer. Damit DeFi-Anwendungen zu einem Kernelement des globalen Finanzsystems werden können, müssen sie einen greifbaren Nutzen bieten, der die

Nutzer dazu veranlasst, sich vom traditionellen System zu lösen, was heute nicht der Fall ist.

Schließlich kann es zum jetzigen Zeitpunkt schwierig sein, die am besten geeignete Anwendung für einen bestimmten Anwendungsfall zu finden. Es gibt so viele dezentrale Finanzanwendungen, dass man leicht den Überblick verlieren kann. Daher besteht die Herausforderung für DeFi nicht nur darin, die Anwendungen zu entwickeln, sondern auch darüber nachzudenken, wie ein funktionales und geordnetes Ökosystem geschaffen werden kann.

TEIL 4 - KAUF, VERKAUF UND BESITZ VON KRYPTOWÄHRUNGEN

„Ich mag Bitcoin wirklich. Ich besitze Bitcoin. Es ist ein Wertaufbewahrungsmittel und eine gute Anlageform, wenn man risikofreudig ist.“
David Marcus (CEO von PayPal)

Kapitel 17

Überwachung von Kryptowährungen

Heutzutage ist es sehr einfach, den Kurs verschiedener Kryptowährungen zu verfolgen, dank Plattformen, die Daten auf einfache und intuitive Weise sammeln und organisieren. Da es über 11 000 Projekte auf der Blockchain gibt, ist die Bedeutung solcher Dienste offensichtlich. Unter ihnen sind CoinMarketCap (coinmarketcap.com) und CoinGecko (coingecko.com) erwähnenswert. Beide bieten einen hervorragenden Service, um den Kryptowährungsmarkt zu überwachen und die Projekte zu verfolgen, die uns am meisten interessieren.

Für diejenigen, die mit Kryptowährungen handeln möchten, ist TradingView (tradingview.com) eine hervorragende Quelle für die Analyse der Charts der meisten Projekte. Häufig ist die TradingView-API direkt in die Börsen integriert.

Da die Blockchains der wichtigsten Kryptowährungen öffentlich und für alle zugänglich sind, haben sich im Laufe der Zeit Plattformen entwickelt, die Blockchain-Daten extrahieren, analysieren und präsentieren. Mit anderen Worten: Diese Dienste liefern Berichte über die Anzahl der aktiven Adressen, die Entwicklung der Provisionen, die Dauer der Sperrung usw. CryptoQuant (cryptoquant.com) und GlassNode (glassnode.com) sind sicherlich zwei Benchmarks für diese Art der Analyse.

Apropos Blockchain-Überwachung: Die effektivste Möglichkeit, Ihre Transaktionen zu verfolgen und zu überprüfen, ob sie erfolgreich waren, ist die Ressource Blockchain Explorer (blockchain.com/explorer).

Geben Sie einfach Ihre Adresse in die Suchleiste ein, um den Status aller ein- und ausgehenden Transaktionen anzuzeigen. Denken Sie daran, dass alle Transaktionen im Zusammenhang mit ERC-20-Tokens oder anderen verwandten Standards auf der Ethereum-Blockchain verfolgt werden müssen.

Kapitel 18

Kauf, Verkauf und Besitz von Kryptowährungen

Als Bitcoin im Jahr 2009 auf den Markt kam, gab es keine praktische Möglichkeit, den Kurs zu verfolgen. Meistens fand der Tausch zwischen Einzelpersonen statt, die sich auf den Wert eines BTC einigten. Nicht selten fanden die Treffen persönlich statt, und die Fiat-Währung wurde in bar übergeben. Eine der beliebtesten Seiten, um andere Menschen zu treffen, die am Kauf und Verkauf von Kryptowährungen interessiert sind, war LocalBitcoins (localbitcoins.com). Die Website ist auch heute noch in Betrieb, obwohl sich das öffentliche Interesse auf die großen Börsen verlagert hat.

Die Entwicklung und Reifung des Marktes hat eindeutig dazu geführt, dass immer ausgeklügeltere Einrichtungen entstanden sind, die den einfachen Kauf und Verkauf von Kryptowährungen ermöglichen. Die Einrichtungen, die den Umtausch von Fiat-Währungen in Kryptowährungen ermöglichen, werden Exchange (Börsen) genannt

(im Englischen bedeutet es „Geldwechsel“). Es gibt unzählige Börsen, von denen einige empfehlenswerter sind als andere. Wenn Sie ein Neuling in der Welt der Kryptowährungen sind, ist es ratsam, eine Börse mit Sitz in Ihrem Wohnsitzland zu nutzen. Der Handel über eine Börse in Ihrem eigenen Land bietet mehr Sicherheit und erleichtert die steuerliche Deklaration von Kryptowährungen.

Aus Gründen der Vollständigkeit müssen auch zwei andere international wichtige Börsen erwähnt werden.

Die erste ist Coinbase (www.coinbase.com), die auch das erste Unternehmen war, das in der Welt der Kryptowährungen an die Börse ging. Die Notierung an der Nasdaq erfolgte am 14. April 2021 (Ticker: COIN).

Die zweitbeliebteste internationale Börse ist Binance (binance.com), die dafür bekannt ist, ihren Nutzern die größte Auswahl an Kryptowährungen und Token zu bieten.

Unabhängig davon, welche Börse Sie für den Kauf von Kryptowährungen nutzen, sollten Sie Ihre Token niemals auf diesen Plattformen aufbewahren. Schon bei der ersten Annäherung an diese Welt ist es wichtig, dass Sie das Sprichwort „not your keys, not your coins“ (wenn Sie die privaten Schlüssel nicht haben, gehören die Coins nicht Ihnen) befolgen und die Gelder auf Ihr persönliches Wallet

übertragen. Halten Sie sich von Börsen fern, die das Abheben von Kryptowährungen an eine externe Adresse nicht zulassen.
In dem Moment, in dem Sie sich entscheiden, Ihre Kryptowährungen zu verkaufen, können Sie Ihr Geld einfach an Ihre Kontoadresse bei der Börse Ihrer Wahl senden und den Verkauf durchführen. Zu diesem Zeitpunkt können Sie bei fast allen Börsen eine Auszahlung auf Ihr Bankkonto vornehmen.

Der Proof of Keys-Day

Der Proof of Keys-Day wurde ins Leben gerufen, um darauf hinzuweisen, wie wichtig es ist, Kryptowährungen in der eigenen Wallet zu halten.

Die Idee stammt von Trace Mayer, einem Kryptowährungsinvestor und Podcaster. Er hat diese Veranstaltung als jährliche Feier ins Leben gerufen, die Kryptowährungsinvestoren dazu ermutigen soll, ihre monetäre Autonomie zurückzufordern. In diesem Zusammenhang zielt der Proof of Keys-Day darauf ab, die Abhängigkeit der Investoren von Börsen zu verhindern, indem sie zumindest für einen Tag Anreize erhalten, Token an eine Wallet zu senden, deren private Schlüssel sie kontrollieren.

Der erste Proof of Keys-Day fand am 3. Januar 2019 statt, dem 10. Jahrestag der Entstehung der Bitcoin-Blockchain. Es handelt sich um eine Veranstaltung, deren Philosophie das ganze Jahr über befolgt werden sollte.

Nachwort

Nun sind wir am Ende unserer Reise in die Welt der Kryptowährungen angelangt. Wie Sie vielleicht schon erraten haben, handelt es sich um eine sich ständig weiterentwickelnde Branche mit sehr guten Zukunftsaussichten, aber ebenso vielen kritischen Problemen, die es zu bewältigen gilt. Sicherlich war 2021 ein Schlüsseljahr für diese Branche, dank des institutionellen Interesses, das um Bitcoin und andere Kryptowährungen entstand. Die nächsten Jahre werden entscheidend sein, um zu verstehen, ob Kryptowährungen tatsächlich Bestand haben werden oder ob sie durch übermäßig strenge Vorschriften oder einen starken Rückgang des Interesses in die Enge getrieben werden.

Liste der nützlichen Ressourcen

Bitcoin und andere Kryptowährungen kaufen und verkaufen:

- coinbase.com
- binance.com

Finden Sie die richtige Hardware-Wallet für sich:

- ledger.com
- trezor.io

Überwachen Sie die Performance Ihrer bevorzugten Kryptowährungen:

- coinmarketcap.com
- coingecko.com

Überwachen Sie Ihre Transaktionen auf der Blockchain:

- blockchain.com/explorer