LERNEN EINFACH GEMACHT

Kryptowährungen

für dummies®

Das macht Kryptowährungen aus

Die Technik hinter Kryptowährungen kennenlernen

So wird mit Kryptowährungen Geld verdient

Krijn Soeteman

die Deutsche Mark und der niederländische Gulden harte Währungen waren. Sie zeichneten sich durch eine geringe Inflation aus und besaßen daher im Vergleich zu anderen Währungen, bei denen mehr Münzen geprägt oder Geldscheine gedruckt wurden, einen höheren Wert. Beide Währungen waren daher gut geeignet, um für längere Zeit Geld zu sparen, falls Sie selbst in einem Land lebten, in dem der Wert der Währung schnell abnahm.

Der Wert, den etwas besitzt, hängt also von diesem Quotienten ab. Wenn mehr Menschen eine harte Währung wählen, um darin ihr Vermögen aufzubewahren, dann nimmt der Wert dieser Währung zu, da die Nachfrage nach dieser Währung steigt. Wenn Sie der Hersteller dieser Währung sind, dann ist die Verführung groß, mehr Münzen dieser Währung zu produzieren. Wenn dies jedoch technisch unmöglich ist, dann stellen Sie keine Bedrohung für den Wert der Währung dar, weil deren Wert nicht einfach dadurch abnimmt, dass Sie viel zu viel neues Geld drucken lassen. Sie wollen also etwas haben, was schwierig zu erstellen und schwer zu zerstören ist.

Jetzt höre ich mit der Lektion über die Geschichte des Geldes auf. Seit der letzten Finanzkrise sind viele dicke Bücher über Geld und darüber, wie es funktionieren soll oder nicht, erschienen. Einer meiner Favoriten in dieser Liste ist das Buch des Anthropologen David Graeber: *Schulden. Die ersten 5000 Jahre* (erschienen bei Goldmann). Aber natürlich gibt es viel interessanten Lesestoff zu diesem Thema.

Harte Währung in einer Welt ohne Knappheit

Sie haben gerade gelesen, dass der Wert des Geldes nichts mit emotionalen Werten zu tun hat, sondern mit Vereinbarungen. Diese Vereinbarungen sind: Es lässt sich nicht essen, ist nicht verderblich, ist nicht für etwas anderes geeignet, denn als System für den Werteaustausch, lässt sich in kleinere Einheiten aufteilen, ist schwer zu zerstören, leicht zu übertragen und nicht einfach zu vervielfältigen.

In der digitalen Welt ist das Merkmal »nicht einfach zu vervielfältigen« eines der schwierigsten Anforderungen. Man denke nur an die Musikindustrie, die wegen des Kopierverhaltens beinahe zugrunde ging.

In unserer digitalen Welt hat Gold keine große Bedeutung. Es passt nicht durch Kupferleitungen oder Glasfaserkabel. Wir müssen uns dann auf Dritte wie Banken und Staaten verlassen. Diese Parteien haben sich vor nicht allzu langer Zeit während der Kreditkrise nicht als unfehlbar für die Aufbewahrung von Werten erwiesen. Dass nun alle ihren eigenen Goldbarren kaufen und in den Tresor legen, ist auch keine Option. Gibt es einen besseren Weg, digitale Knappheit zu schaffen? Wie könnten wir das hinbekommen? Und noch stärker: Kann man besser sein als Gold?

Digital besser als Gold

Warum sollte und wie kann man im Hinblick auf die Knappheit besser sein als Gold? Gold ist zwar auf der Erde knapp, aber wir haben keine Ahnung, wie viel Gold tatsächlich noch im Boden lagert. Wir haben keine Ahnung, wie viel Gold wir finden werden, wenn wir mit dem Abbau von Rohstoffen auf Meteoren und anderen Planeten beginnen. Das Stock-to-Flow-Verhältnis von Gold wird sich nicht sehr schnell drastisch verschlechtern, aber wir können digitale Systeme erfinden, die wirklich endlich sind und bei denen man sich wirklich anstrengen muss, um das digitale Gut zu erhalten. Und da ist sie endlich: die Bitcoin.

Das System von Bitcoin ist so eingerichtet, dass maximal 21 Millionen Bitcoins von einem System von Computern erzeugt werden können, die hierfür Rechenleistung benötigen. Dieses System wird im Fachjargon *Mining* (Schürfen, Abbauen) genannt. Die Analogie zur Suche nach Rohstoffen ist klar: Es braucht Mühe, Bitcoins zu bekommen. Erst ging das Mining recht einfach. In dieser Zeit war die Bitcoin weit davon entfernt, eine harte Münze zu sein, einfach weil das Stock-to-Flow-Verhältnis sehr niedrig war. Das Mining dieser Bitcoins wird immer schwieriger und auch immer teurer. Rechnen Sie mit: Als es 1.000 Bitcoins gab, konnten noch 20.999.000 weitere Bitcoins gemint werden. Die Stock-to-Flow-Rate war also 1.000 geteilt durch 20.999.000 = 0,0047621. Während ich diese Zeilen schreibe, sind 17.282.713 Bitcoins im Umlauf und es können noch weitere 3.717.287 gemint werden. Das Stock-to-Flow-Verhältnis beträgt also 4,65.

Welche anderen Unterschiede existieren zwischen Bitcoin und Gold sowie Silber? Der Unterschied liegt im tatsächlichen Besitz. Gold und Silber werden gehandelt, aber es wird nicht wirklich etwas bewegt. Wenn man Gold kauft, kauft man einen Claim, ohne dass man wirklich weiß, ob man es besitzt. Wenn Sie das Gold tatsächlich besitzen wollen, müssen Sie ein paar Hürden bei Banken und Behörden überspringen, bevor Sie es zu Hause auf Ihren Kamin legen können. Wenn Sie Bitcoins erhalten, dann haben Sie die komplette Kontrolle über diese Bitcoins.

Der Beginn einer neuen Geschichte

Auf der Suche nach einer digitalen Währung, die als Bargeld fungiert, hat Bitcoin bereits Geschichte geschrieben. Dieses System wurde der Welt von einer immer noch unbekannten Person mit dem Pseudonym Satoshi Nakamoto in Form von Open-Source-Software gegeben. Er oder sie war (oder waren) in der Lage, in der digitalen Welt die Eigenschaften eines knappen Gutes zu simulieren. Damit hat Satoshi Nakamoto den Menschen die Möglichkeit gegeben, in der digitalen Welt praktisch ohne Verzögerung und ohne die Notwendigkeit, dass sich beide Seiten in räumlicher Nähe zueinander befinden, und ohne, dass sie einander kennen oder vertrauen, direkt und definitiv eine Werttransaktion durchzuführen. Eine Art Bargeld in der digitalen Welt ohne Grenzen. Unserer Welt.

Dieses System wurde mittlerweile in mehreren Tausend anderen Kryptowährungen

kopiert. Bitcoin hat im Vergleich zu all diesen Kopien einen besonderen Vorteil: Bitcoin hat keinen Inhaber oder Leiter. Außerdem besitzt niemand das Bitcoin-Netzwerk oder kann es beanspruchen oder kontrollieren. Das Bitcoin-Netzwerk ist ein verteiltes **Peer-to-Peer-Netzwerk** ohne einen einzigen Punkt, an dem es ausfallen kann. Jeder Computer im Netzwerk, auch Knotenpunkt oder **Node** genannt, hat Zugriff auf alle Transaktionen, die jemals in diesem System getätigt wurden. All diese Transaktionen wurden mit **digitalen Signaturen** verifiziert und durch digitale Schlüssel und einem System namens *Proof-of-Work* festgelegt.

Das Erzeugen neuer Münzen kostet Energie. Beim ersten Mal, als Bitcoin ein Wert zugewiesen wurde, wurden die Energiekosten pro Bitcoin zugrunde gelegt; damals waren dies 0,0008 Cent oder 1.309,03 Bitcoin pro Dollar. Manche finden, dass der Energiebedarf des Netzwerks groß ist, jedoch spielt auch die Sicherheit des Netzwerks eine Rolle. Die Frage ist, wofür Sie bereit sind, Energie zu verwenden, für Ihren Fernseher oder für ein supersicheres Netzwerk?

Das wichtigste nicht-technische Merkmal des Bitcoin-Netzwerks ist, dass es nicht politisch ist und keinen Eigentümer hat. Jeder kann mitmachen, keiner muss mitmachen. Das Schicksal des Netzwerks liegt in den Händen der Nutzer. Aufgrund der Funktionsweise des Systems kann der Zugang nicht von Regierungen oder anderen Behörden blockiert werden. Das Netzwerk schaut nicht darauf, wer oder was jemand ist und ist in diesem Sinne neutral. Das bedeutet, dass Bitcoin ein mächtiges Instrument ist, weil das Monopol der Geldschöpfung plötzlich nicht mehr bei Banken und Staaten liegt. Niemand verpflichtet Sie, Bitcoins zu verwenden.

Es würde zu weit gehen, diese Aspekte im Rahmen dieses Buchs noch weiter zu vertiefen. Ich hoffe, Sie verstehen nun besser, warum Bitcoin von vielen eher als interessantes Anlageobjekt denn als bequeme Online-Zahlungsmethode angesehen wird. Dafür ist das System zu umständlich, nicht zuletzt deswegen, weil es aufwendig ist, die Sicherheit des Systems zu gewährleisten. Wir werden später in diesem Buch sehen, dass es auch möglich ist, Systeme mit Bitcoin zu verknüpfen, sodass man Millionen von Zahlungen pro Sekunde verarbeiten kann, ohne dass dies direkt auf dem Bitcoin-Netzwerk geschehen muss.

Wenn Sie mehr über die Philosophie rund um Bitcoin und andere Online-Bezahlsysteme wissen wollen, lesen Sie dann das Buch *The Bitcoin Standard: The Decentralized Alternative to Central Banking* von Saifedean Ammous (erschienen bei Wiley) oder sehen Sie sich den Vortrag *The Streaming Money* von Andreas Antonopoulos an beziehungsweise lesen Sie das Transkript dieses Vortrags.

Kapitel 2

Kryptowährungen

IN DIESEM KAPITEL

Wie funktionieren Kryptowährungen?

Coins, Tokens, alles prima, aber wie viele gibt es?

Blasen

Der folgende Schritt besteht darin, die Frage zu beantworten, ob der Begriff »Kryptowährungen« die Bedeutung gut wiedergibt oder ob ein anderes Wort vielleicht geeigneter ist. Danach stelle ich Ihnen eine ganze Reihe von Kryptowährungen und Tokens vor und beleuchte dabei möglichen Nutzen sowie deren Gefahren.

Anschließend folgt ein Schnellkurs zum Thema Bitcoin, denn wenn Sie die Grundlagen verstehen, wird auch der ganze Rest deutlicher. Ethereum ist das nächste unverzichtbare Basiselement. Danach überfliegen wir einige verschiedene Ökosysteme, die alle ihre eigenen Erkenntnisse und Ziele aufweisen.

Vielleicht haben Sie bereits in verschiedene Kryptowährungen investiert, wissen aber nicht, was sie tun. Ja, der Kurs im Hinblick auf den Euro, den Dollar und andere (Krypto-)Währungen geht hoch und runter und das ist es, was viele Menschen beschäftigt. Jedoch sind Kryptowährungen mehr als nur eine Investitionsmöglichkeit. Start-ups entwickeln immer neue Anwendungen, die auf vorhandenen Blockchains basieren, oder sie erstellen eine eigene Blockchain. Es scheint derzeit noch immer kein Mangel an Mitteln zu bestehen, um diese Entwicklungen zu finanzieren (während Sie diese Zeilen lesen, kann dies jedoch anders sein). Handelt es sich also um ein aus dem Ruder gelaufenes Hobby von ein paar Nerds oder steckt mehr dahinter?

Kryptowährungen oder Kryptotokens?

Ich habe versprochen, mich noch ausführlich mit dem Begriff »Kryptowährung« zu beschäftigen. Bereits seit den Anfängen wird in englischen Fachartikeln von *cryptocurrency* gesprochen, was wörtlich übersetzt Kryptowährung bedeutet. Darum ist der Titel dieses Buchs auch nicht »Kryptotokens für Dummies« oder »Krypto-Assets für Dummies«, da dies keine Standardbegriffe sind, die für die verschiedenen auf Kryptografie basierenden Währungen verwendet werden.

Der Begriff »Kryptowährung« verweist auf ein digitales Gut, das entwickelt wurde, um als *medium of exchange* oder Tauschmittel zu funktionieren, und das aufgrund seiner starken Verschlüsselung (siehe Kapitel 3) sicher im Internet verwendet werden kann. Der Ursprung dieses Begriffs liegt bei Bitcoin, das im engeren Sinne des Wortes als digitale Form des Bargelds konzipiert wurde.

Sie merken es schon. Eigentlich passt der Begriff Kryptowährung nicht. Eine Währung verweist auf sich im Umlauf befindliches Geld, das verwendet wird, um Werte zu tauschen. Euro, Yen und Dollar sind Währungen und wenn Sie Währungen etwas weitfassender interpretieren, können Sie vielleicht noch Bitcoin an diese illustre Liste anfügen. Es gibt noch weitere Kryptowährungen, die das Ziel verfolgen, im engeren Sinne zur Gruppe der Währungen zu gehören. Der Großteil der Coins, die ich in diesem Buch behandle, sind jedoch keine Coins im Sinne von Währung oder Geld. Auch Bitcoin verfügt über bestimmte Aspekte, dies es möglich machen, dass Bitcoin anders als eine konventionelle Währungsart funktionieren kann. So besitzt Bitcoin ein eigenes Transaktionsprotokoll oder Hauptbuch (Ledger), das bei keiner anderen Währung der **Fiat**-Geldsysteme vorhanden sind.

Es läuft also darauf hinaus, dass wir es in den meisten Fällen mit Tokens zu tun haben, die unterschiedliche Eigenschaften aufweisen. In fast allen Fällen ist auch eine finanzielle Komponente anzutreffen, jedoch macht diese aus den Tokens noch keine Währung.

Warum, wie und was

Oft werden Dinge damit erklärt, *was* etwas ist, aber bei den Kryptowährungen ist das *Warum* vielleicht noch wichtiger. Erst dann, wenn die Frage nach dem Warum beantwortet ist, folgen die Fragen nach dem Wie und dem Was. Dann wird schnell ersichtlich, warum eine Blockchain, das System, das zuerst in Form der Bitcoin das Licht der Welt erblickte, mehr ist als nur eine Spielweise von ein paar obskuren *Cypherpunks*, deren Hobby es ist, sich mit Kryptografie zu beschäftigen.

Umrechnungskurse

Im Verlauf des Buchs verwende ich verschiedene Beispiele, in denen existierende Währungen vorkommen. In den meisten Fällen ist der exakte Wert einer bestimmten digitalen Münze im Vergleich zum Euro oder Dollar nicht wichtig. Daher verwende ich einfach zu verwendende ganze Zahlen, es sei denn, ein bestimmter Kurs aus der Vergangenheit ist relevant. So lässt sich beispielsweise mit einem Kurs von 10.000 Euro je Bitcoin einfach rechnen. Auch 1.000 je Bitcoin wäre möglich gewesen, jedoch ist dieser Wert zum Zeitpunkt, an dem ich diese Zeilen schreibe, weit vom tatsächlichen Kurs entfernt. Ob der Wert zu dem Zeitpunkt, an dem Sie das Buch lesen, (viel) zu hoch oder