IN DIESEM KAPITEL

- Digitale Währungen
- Die Blockchain nutzen
- Blöcke hashen
- Public-Key-Verschlüsselung
- Nachrichten mit dem privaten Schlüssel signieren

Kapitel 1
Kryptowährungen kurz erklärt

Sie können es vielleicht kaum erwarten, Ihren Mining-Betrieb aufzunehmen, aber bevor Sie Kryptowährungen schürfen können, müssen Sie verstehen, was Kryptowährungen eigentlich sind.

Die Sache mit den Kryptowährungen ist so neu – oder zumindest ist das allgemeine Interesse erst in jüngster Zeit entstanden, obwohl es seit den 1980er Jahren Kryptowährungen unterschiedlicher Ausprägungen gibt – dass die meisten Beteiligten eher nur ein vages Verständnis davon haben, was Kryptowährungen sind und wie sie funktionieren. Die meisten Halter von Kryptowährungen wissen vielleicht gar nicht, was sie da überhaupt besitzen.

In diesem Kapitel betrachten wir die Geschichte der Kryptowährungen und das Zusammenspiel der einzelnen Komponenten. Wenn Sie die Grundlagen von Kryptowährungen kennen, dann werden Sie auch die Abläufe beim Krypto-Mining besser verstehen.

Eine kurze Historie des digitalen Dollars

Kryptowährung ist nur eine Form von digitaler Währung … eine besondere Form. Letztlich kann man sich Kryptowährung als eine Form des digitalen Geldes vorstellen.

Was ist also *digitales Geld*? Nun, das ist ein sehr weit gefasster Begriff, der viele verschiedene Dinge umfasst. Im weitesten Sinne ist es aber Geld, das nur in digitaler und nicht in greifbarer Form (wie etwa Münzen und Banknoten) existiert. Sie können digitales Geld über ein elektronisches Netzwerk übertragen, sei es über das Internet oder ein privates Bankennetzwerk.



Auch Kredit- und Geldkartentransaktionen können als digitale Währungstransaktionen betrachtet werden. Schließlich wird das Geld elektronisch überwiesen, wenn Sie Ihre Kredit- oder EC-Karte bei einem Einkauf (online oder offline) verwenden; das Netzwerk bündelt ja keine Euro- oder Dollarscheine und verschickt sie an den Händler.

Zuerst kam das Internet

Die Geschichte der Kryptowährungen beginnt mit dem Internet. Digitale Währungen existierten bereits, bevor das Internet in großem Umfang genutzt wurde, aber damit eine digitale Währung von Nutzen ist, brauchen Sie eben auch eine Art digitales Transportmittel für diese Währung. Wenn kaum jemand ein digitales Kommunikationsnetzwerk einsetzt – und bis 1994 taten dies nur sehr wenige Menschen –, worin liegt dann der Nutzen einer digitalen Währung?

Aber nach 1994 verwendeten Millionen von Menschen ein globales, digitales Kommunikationsnetzwerk – das Internet – und ein Problem tauchte auf: Wie lässt sich Geld online ausgeben? Okay, heute ist die Antwort ziemlich einfach: Sie verwenden dazu Ihre Kredit- oder Debitkarte oder Ihr PayPal-Konto. Aber Mitte der 1990er Jahre war das noch etwas komplizierter.

Verwirrung mit Kreditkarten

Falls Sie sich daran erinnern – vielen von Ihnen werden dazu natürlich zu jung sein –: Mitte der 90er Jahre hatten viele Menschen Vorbehalte, Kreditkarten im Internet zu verwenden. Als ich meinen eigenen Verlag hatte und im Jahr 1997 Bücher über meine Website verkaufte, erhielt ich (Peter, Tyler ist zu jung, um sich an 1997 zu erinnern) häufig ausgedruckte Produktseiten meiner Website per Post. Der Sendung lag dann außerdem noch ein Scheck zur Bezahlung des gekauften Buchs bei. Ich akzeptierte auf meiner Website auch Kreditkarten, aber viele Leute wollten sie einfach nicht einsetzen; sie wollten ihre Kartendaten nicht dem Internet anvertrauen.

Außerdem war die Einrichtung eines Zahlungsportals für Kreditkarten für den Verkäufer schwierig und teuer. Heutzutage ist es ziemlich einfach, Kreditkartenzahlungen auf Ihrer Website zu akzeptieren – die Funktion ist praktisch in jede E-Commerce-Software integriert und Dienste wie Stripe und Square senken die Einstiegsbarrieren, sodass ein *Händlerkonto* längst nicht mehr so aufwendig und teuer ist wie früher.

Natürlich sprechen wir hier von geschäftlichen Zahlungen, aber was ist mit privaten Buchungen? Wie konnte man die Schulden bei einem Freund übers Netz begleichen oder wie konnten Eltern ihren studierenden Sprösslingen Geld für Bier schicken? (Ich rede hier von den Zeiten vor PayPal und Online-Banking.) In der entstehenden digitalen Welt würden wir mit Sicherheit auch digitale Zahlungsmittel benötigen.



Ein wichtiges Merkmal von Bargeld ist, dass die Transaktionen im Wesentlichen anonym sind – es gibt keine schriftlichen oder elektronischen Aufzeichnungen darüber. Viele Menschen erwarteten von einer gleichwertigen anonymen oder pseudonymen digitalen Währung eine enorme Verbesserung gegenüber den traditionellen Abwicklungsmethoden.

Viele Leute waren also der Ansicht, dass es einen besseren Weg geben müsse. Für die digitale Welt brauchten wir eine digitale Währung. Heutzutage erscheint diese Sichtweise vielleicht naiv. Rückblickend war es doch offensichtlich, dass die Kreditinstitute nicht zusehen würden, wie sich Transaktionen im Wert von Billionen ins Netz verlagerten und sie sich klaglos davon verabschieden würden! Sie wollten ein Stück vom Kuchen und waren nicht bereit, ihr Monopol aufzugeben. Deshalb stützen sich die wichtigsten Transaktionsmethoden in den Vereinigten Staaten und im größten Teil von Europa heute auf die unterschiedlichsten Bankkarten.

Und noch ein wenig David Chaum

Mitte der 1990er Jahre strömten die Leute ins Internet und wollten oder konnten aus verschiedenen Gründen (siehe vorheriger Abschnitt) keine Kreditkarten verwenden. Schecks waren noch schwieriger (es sei denn, Sie steckten sie in einen Briefumschlag) und Bargeld kam nicht in Frage. (Obwohl – und das ist ein Witz für die älteren Geeks unter Ihnen – ich erinnere mich an einen Freund, der mir sagte, ich solle die $10, die ich ihm schuldete, per UUENCODE und E-Mail an ihn schicken. Hier spricht wiederum Peter; ich wette, Tyler ist zu jung, um UUENCODE zu kennen.)

Aber 1983 hatte ein Mann namens David Chaum ein Paper mit dem Titel »Blind Signatures for Untraceable Transactions« geschrieben. Chaum war Kryptograph und Informatikprofessor. In seiner Arbeit beschrieb er eine Möglichkeit, mit kryptographischen Mitteln ein digitales Zahlungssystem zu schaffen, das, genau wie Bargeld, anonyme Transaktionen ermöglichen könnte. (Die moderne Kryptografie ist die Wissenschaft der Absicherung von Online-Kommunikation; darauf kommen wir später noch zurück). Tatsächlich wird Chaum oft als Vater der digitalen Währung und der Anonymität im Netz bezeichnet.

Ergebnis? DigiCash, E-Gold, Millicent, Cybercash und weitere

Wenn wir jetzt Internet, komplizierte Online-Transaktionen, Angst vor dem Einsatz von Kreditkarten im Internet, den Wunsch nach bargeldähnlichen, anonymen Online-Transaktionen und die Forschung von David Chaum in den 1980er Jahren (siehe vorhergehender Abschnitt) zusammenbringen, was ergibt sich dann daraus?

Zunächst einmal erhalten Sie DigiCash, das digitale Bargeldsystem von David Chaum von 1990. Leider war Herr Chaum mit seinen Innovationen wohl oft etwas zu früh dran, und DigiCash war 1998 wieder aus dem Rennen. Es gab auch E-Gold, ein digitales Zahlungssystem, das angeblich durch Gold gestützt wurde, Millicent von DEC (ja, ja, die meisten von Ihnen sind auch zu jung, um sich an DEC zu erinnern … Ich fühle mich langsam ganz schön alt beim Verfassen dieses »geschichtlichen« Teils), First Virtual, Cybercash, b-money, Hashcash, eCash, BitGold, Cybercoin und viele mehr. Es gab auch Beenz mit 100 Millionen Dollar Investment-Kapital; das von Whoopi Goldberg unterstützte Flooz (ja, wirklich!); die Liberty Reserve (die nach Geldwäschevorwürfen geschlossen wurde) und die chinesischen QQ Coins.

Mit Ausnahme der QQ Coins, die noch immer beim QQ Messaging Service von Tencent im Einsatz sind, sind all diese digitalen Währungen wieder von der Bildfläche verschwunden. Auffallend ist, dass viele der frühen digitalen Währungen auf die eine oder andere Weise zentralisiert waren.

Das war aber noch nicht das Ende des digitalen Geldes. Es gab erhebliche Startschwierigkeiten mit viel Herumprobieren und etlichen Fehlschlägen, aber viele Menschen waren immer noch der Meinung, dass die Welt bargeldähnliche (mit anderen Worten, anonyme) Online-Transaktionen brauchte. Damit sollte ein neues Zeitalter beginnen: das Zeitalter der Kryptowährungen.

Auch die frühen digitalen Währungen basierten zwar auf Kryptografie aber sie wurden nie als Kryptowährungen bezeichnet. Erst durch die Kombination von digitalem Geld mit einer Blockchain im Jahr 2008 begann der Begriff Kryptowährung an Bedeutung zu gewinnen, und erst um 2012 fand der Begriff wirklich eine weite Verbreitung (Blockchain? Das ist eine spezielle Datenbankform, auf die wir später in diesem Kapitel näher eingehen werden.)

Das Bitcoin-Whitepaper

Im Jahr 2008 veröffentlichte Satoshi Nakamoto in einem als »Cypherpunk Mailing List« bekannten Kryptografieforum ein Dokument mit dem Titel »Bitcoin: A Peer-to-Peer Electronic Cash System«. Dazu schrieb er: »Ich habe an einem neuartigen elektronischen Zahlungssystem gearbeitet, das komplett auf Peer-to-Peer-Basis funktioniert und ohne vertrauenswürdige Dritte auskommt«.

Die nachfolgende Liste enthält laut Nakamoto die wichtigsten Eigenschaften von Bitcoin:

- ✔ Mehrfaches Ausgeben von Geld (double spending) wird durch ein Peer-to-Peer-Netzwerk verhindert.
- ✔ Es gibt keine zentrale Ausgabestelle oder andere notwendig vertrauenswürdige Parteien.
- ✔ Die Teilnehmer können anonym sein.
- ✔ Neue Coins entstehen durch den Nachweis von erbrachter Rechenarbeit (Proof-of-Work), so wie bei Hashcash.
- ✔ Bei der neuen Coin-Generation stärkt das Proof-of-Work zugleich das Netzwerk, um doppelte Ausgaben zu vermeiden.

Das Dokument liest sich recht trocken, aber es lohnt sich, es für einige Minuten zu überfliegen. Sie können es problemlos unter `https://bitcoin.org/bitcoin.pdf` finden. Seine Zusammenfassung des *Bitcoin Whitepaper* beginnt Nakamoto mit folgender Feststellung: »Eine rein auf Peer-to-Peer basierende Version elektronischen Geldes würde Online-Zahlungen direkt von einer Partei zur anderen ermöglichen, ohne dabei über ein Finanzinstitut zu gehen.« Er erklärt, dass diese Methode das Problem des »double spending« löst, mit dem frühere digitale Währungen zu kämpfen hatten: zu verhindern, dass digitales Geld mehrfach ausgegeben werden kann.

Nakamoto beschreibt außerdem den Einsatz von Blockchain-Technologie, obwohl der Begriff Blockchain nirgendwo im Whitepaper auftaucht:

> *Wir schlagen vor, … ein Peer-to-Peer-Netzwerk zu verwenden. Das Netzwerk versieht Transaktionen mit einem Zeitstempel, indem es sie zu einer fortlaufenden Kette von hash-basiertem Proof-of-Work zusammenfügt. So entsteht eine Aufzeichnung, die ohne Wiederholung des Proof-of-Work nicht mehr verändert werden kann.*

Bitcoin: Die erste Blockchain-Anwendung

Anfang Januar 2009 nahm Nakamoto das Blockchain-basierte Bitcoin-Netzwerk in Betrieb (das Blockchain-Konzept gab es seit Anfang der 1990er Jahre, jedoch wurde es hier zum ersten Mal korrekt implementiert. Er erzeugte den ersten Block in der Blockchain, den sogenannten *Genesis-Block*.

Neben 50 Bitcoins enthielt dieser Block auch den Text *»The Times 03/Jan/2009 Chancellor on brink of second bailout for banks«* als Rechtfertigung und Erklärung dafür, warum ein System wie Bitcoin so wichtig war. Nakamoto programmierte weitere Aktualisierungen für das Protokoll, betrieb einen Netzwerkknoten und schürfte dabei bis zu rund einer Million Bitcoins, eine Summe, die ihn Ende 2017 zu einem der reichsten Menschen der Welt gemacht hätte (zumindest »auf dem Papier«).

Ende 2010 postete Satoshi Nakamoto seinen letzten Forumsbeitrag und meldete sich offiziell vom Projekt ab. Zu diesem Zeitpunkt hatten sich aber schon viele andere Krypto-Enthusiasten angeschlossen, die selbst zu schürfen begannen und die Entwicklung des quelloffenen Codes unterstützten. Der Rest ist Geschichte.

Wer (oder was) ist Satoshi Nakamoto?

Wer war also dieser Satoshi Nakamoto … ein Mann, eine Frau oder eine Gruppe? Das weiß niemand. Satoshi Nakamoto scheint kein echter Name zu sein; sehr wahrscheinlich handelt es sich dabei um ein Pseudonym. Und falls es Menschen gibt, die die wahre Identität von Nakamoto kennen, dann sagen sie es nicht. Dies ist das große Geheimnis der Kryptowährungen.

Es gibt einen japanischstämmigen Amerikaner namens Dorian Prentice Satoshi Nakamoto, offenbar geborener Satoshi Nakamoto. Dieser Mann ist ausgebildeter Physiker, Systementwickler und Programmierer für Finanzunternehmen – vielleicht war er der Satoshi Nakamoto. Er hat es jedoch mehrfach abgestritten.

Wie wäre es mit Hal Finney, der nur ein paar Straßen weiter von Dorian Prentice Satoshi Nakamoto entfernt lebte? Er beschäftigte sich schon vor Bitcoin mit Kryptografie und gehörte zu den ersten Nutzern von Bitcoin. Er behauptet auch, per E-Mail mit dem Bitcoin-Gründer kommuniziert zu haben. Einige Leute haben vermutet, er hätte sich Satoshi Nakamotos Namen »geliehen« und als Pseudonym verwendet.

Dann ist da Nick Szabo, der sich schon lange mit digitalen Währungen beschäftigte und sogar vor Nakamotos Bitcoin-Whitepaper ein Whitepaper über Bitgold veröffentlichte. Oder

was ist mit Craig Wright, der bereits behauptete, Nakamoto zu sein, später aber des Betrugs beschuldigt wurde? Oder Dr. Vili Lehdonvirta, ein finnischer Wirtschaftssoziologe, oder Michael Clear, ein irischer Kryptografie-Doktorand – oder die drei Kerle, die in ihrer Patentschrift dieselbe obskure Phrase (»computationally impractical to reverse«) wie Nakamoto im Bitcoin-Whitepaper verwenden, oder der japanische Mathematiker Shinichi Mochizuki oder Jed McCaleb oder irgend eine Regierungsbehörde oder irgend eine andere Personengruppe oder Elon Musk oder … nun, niemand weiß es, aber Theorien gibt es gewiss genug.

Und das zweitgrößte Geheimnis von Bitcoin? Nakamoto besaß rund eine Million Bitcoin, die im Deczmber 2017 rund 19 oder 20 Milliarden Dollar wert waren. Nichts von Nakamotos wahrscheinlichem Bitcoin-Vermögen wurde bisher verschoben oder ausgegeben; warum hat er oder sie (oder die Gruppe) das Geld noch nicht angefasst? Auch dies ist nicht bekannt.

Was ist die Blockchain?

Um Kryptowährungen zu verstehen, müssen Sie ein wenig über Blockchains wissen. Die Blockchain-Technologie ist komplex, aber das ist in Ordnung – Sie brauchen nicht alles zu verstehen. Es genügt, wenn Sie die Grundlagen kennen.

Blockchains sind spezielle Datenbanken. Eine *Datenbank* ist einfach eine Ansammlung strukturierter Daten. Sagen wir, Sie stellen eine Reihe von Namen, Anschriften, E-Mail-Adressen und Telefonnummern zusammen und geben sie in eine Textverarbeitung ein. Das ist dann keine Datenbank, sondern nur ein Haufen Text.

Sagen wir jetzt aber, Sie geben diese Daten in eine Tabellenkalkulation ein. Die erste Spalte ist der Vorname, die zweite der Nachname der Person, und es gibt weitere Spalten für die E-Mail-Adresse, die Telefonnummer, die Straße und Hausnummer, den Ortsnamen, die Postleitzahl, das Land und so weiter – das sind strukturierte Daten. Das ist eine Datenbank.

Die meisten Leute verwenden ständig Datenbanken. Wenn Sie ein Buchhaltungsprogramm wie Quickbooks, Quicken oder Mint verwenden, werden Ihre Daten in einer Datenbank gespeichert. Wenn Sie Kontaktinformationen in einem Programm zur Kontaktverwaltung, einem »Adressbuch« speichern, werden sie in einer Datenbank abgelegt. Datenbanken bilden hinter den Kulissen einen festen Bestandteil des modernen digitalen Lebens.

Eine Kette rund um die Welt – das Blockchain-Netzwerk

Die Blockchain ist eine Datenbank; sie speichert Informationen in strukturierter Form. Blockchains können für viele verschiedene Zwecke eingesetzt werden: zum Beispiel zur *Registrierung von Eigentumsrechten* (wem gehört ein Stück Land, und wie wurde es erworben?), oder zur *Überwachung einer Lieferkette* (woher stammt der Wein oder der Fisch und wie ist er zu Ihnen gekommen?) Blockchains können alle Arten von Daten speichern. Im Falle von Kryptowährungen speichern Blockchains jedoch Transaktionsdaten: Wer besitzt wieviel Kryptowährung, wer hat sie ihm gegeben und an wen hat er sie weitergegeben (wie wurde sie ausgegeben)?

Natürlich haben Blockchains mehrere besondere Eigenschaften. Erstens sind sie netzwerkbasiert. Es gibt ein Bitcoin-Netzwerk, ein Litecoin-Netzwerk, ein Ethereum-Netzwerk, genau wie es ein E-Mail-Netzwerk oder ein World-Wide-Web-Netzwerk gibt.

Bitcoin ist zum Beispiel ein Netzwerk aus Tausenden von Knotenpunkten beziehungsweise Nodes genannten Servern, die über den ganzen Planeten verteilt sind.

Diese *Nodes* verfügen jeweils über eine Kopie der Bitcoin-Blockchain, und sie stehen miteinander in Kontakt und synchronisieren sich gegenseitig. Mithilfe eines *Konsensverfahrens* einigen Sie sich darauf, wie die aktuelle, gültige Blockchain-Datenbank aussieht. Das heißt, sie nutzen alle die gleiche, passende Kopie der Blockchain.

Hashing: »Fingerabdrücke« von Blöcken nehmen

Die Blockchain auf viele verschiedene Computer zu kopieren, ist sehr wirkungsvoll – dadurch wird es viel schwieriger, sie zu hacken oder zu manipulieren. Aber etwas anderes ist auch noch sehr wirkungsvoll: das *Hashing*. Ein *Hash* ist eine lange Zahl, die eine Art Fingerabdruck für Daten darstellt. Die Blockchain nutzt Hash-Werte folgendermaßen:

1. **Ein Node, also ein Computer, auf dem ein Netzwerkknoten läuft, sammelt und validiert Bitcoin-Transaktionen (Aufzeichnungen von Bitcoin-Beträgen, die zwischen Adressen innerhalb der Blockchain hin- und hergesendet werden), die zur Blockchain hinzugefügt werden sollen.**

2. **Wenn der Computer genügend Transaktionen gesammelt hat, erstellt er einen Datenblock und *hasht* die Daten, das heißt, er wendet eine spezielle Hash-Funktion auf die Daten an, die den Hash zurückgibt.**

   Hier ist ein Beispiel für einen echten Hash eines Blocks aus der Bitcoin-Blockchain:

   ```
   00000000000000000297f87446dc8b8855ae4ee2b35260dc4af61e1f5eec579Th
   ```

   Ein *Hash* ist ein Fingerabdruck der Daten, der dank der komplexen Mathematik dahinter auf keinen anderen Datensatz passen kann. Wenn die gehashten Daten auch nur minimal verändert werden – aus einer 0 wird eine 5, oder aus einem A wird ein B – passt dieser Fingerabdruck nicht mehr zu den ursprünglichen Daten.

3. **Der Hash wird dem Transaktionsblock hinzugefügt.**

4. **Der Block wird an die Blockchain angehängt.**

5. **Es werden weitere Transaktionen für den nächsten Block gesammelt.**

6. **Wenn ein vollständiger Transaktionsblock fertig ist, wird der Hash des vorherigen Blocks zum aktuellen Block hinzugefügt.**

7. **Der neue Block – mit den Transaktionen und dem Hash des vorherigen Blocks – wird ebenfalls gehasht.**

8. **Dieser Vorgang wiederholt sich und es entsteht eine Kette aus Blöcken, die mit einem Zeitstempel versehen sind.**

Jeder Block enthält also zwei Hashes: den Hash des vorherigen Blocks und den Hash des aktuellen Blocks, der durch Hashing aller darin enthaltenen Bitcoin-Transaktionen und des Hashs des vorherigen Blocks erzeugt wird.

So werden die Blöcke in der Blockchain miteinander verknüpft (siehe Abbildung 1.1). Jeder Block enthält den Hash des vorherigen Blocks – also eine Kopie des eindeutigen Fingerabdrucks des vorherigen Blocks. Jeder Block kennzeichnet auch seine Position in der Blockchain; der Hash des vorherigen Blocks kennzeichnet die Reihenfolge, in der sich der aktuelle Block befindet.

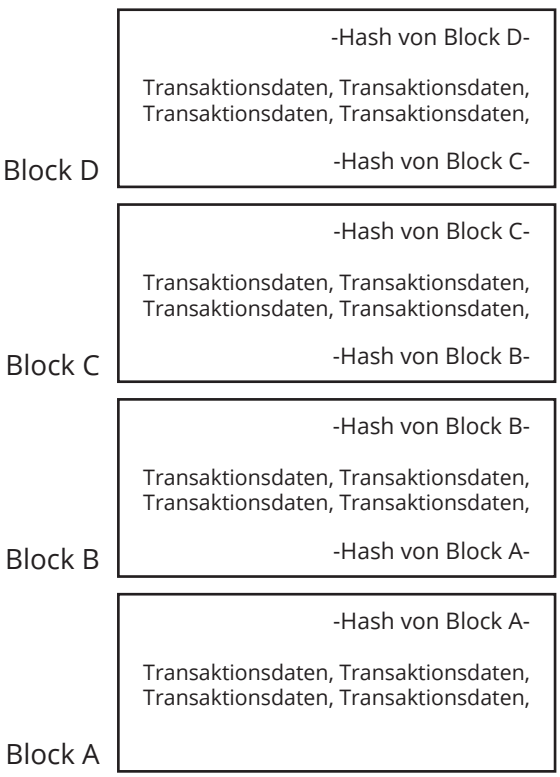


Abbildung 1.1: Der Hash jedes Blocks wird in diesem sowie in den Daten des darauf folgenden Blocks gespeichert.

Die Blockchain ist »unveränderbar«

Vielleicht haben Sie schon einmal gehört, dass die Blockchain praktisch *unveränderbar* ist. Wenn die Bitcoin-Blockchain aussagt, dass Sie x Bitcoin besitzen, dann besitzen Sie x Bitcoin, es kann darüber keine Uneinigkeit entstehen. Und niemand kann in die Blockchain eindringen und sie hacken oder irgendwie verändern oder verfälschen.

Stellen Sie sich vor, was passieren würde, wenn jemand in einem Block (nennen wir ihn Block A) einige Daten ändern würde –wenn er zum Beispiel dafür sorgte, dass Sie, statt jemandem 1 Bitcoin geschickt zu haben, 9 Bitcoins geschickt hätten.

Nun, der Hash von Block A würde nicht mehr mit den darin enthaltenen Daten übereinstimmen. Denken Sie daran, dass ein Hash ein Fingerabdruck ist, der die Daten identifiziert. Wenn Sie also die Daten ändern, dann passt der Hash nicht mehr dazu.

Okay, also könnte der Hacker die Daten von Block A erneut durch die Hashfunktion laufen lassen und dann den »korrigierten« Hash speichern. Aber Moment, jetzt würde der nächste Block (Block B) nicht mehr passen, weil Block B den Hash von Block A enthält. Sagen wir also, der Hacker verändert den Hash von Block A, der in Block B gespeichert ist.

Aber jetzt stimmt der Hash von Block B nicht mehr mit den Daten in Block B überein, denn dieser Hash wurde aus einer Kombination der Transaktionsdaten in Block B mit dem Hash von Block A erstellt!

Also müsste auch Block B neu gehasht und der Hash aktualisiert werden. Aber Moment! Das heißt, dass der in Block C gespeicherte Hash von Block B jetzt nicht mehr passt!

Sehen Sie, wo das hinführt? Dies würde sich durch die komplette Blockchain ziehen. Die Veränderung eines einzigen Zeichens in einem vorhergehenden Block zerstört die gesamte Blocksequenz. Um das Problem zu beheben, muss die gesamte Blockchain neu berechnet werden. Ab dem gehackten Block muss sie »neu gemined« werden. Ein scheinbar einfacher Hack zur Änderung einer Datenbank wird nun zu einem gewaltigen Rechenproblem, das sich nicht einfach mal eben so lösen lässt.

Diese Hash-Funktion plus die Tatsache, dass Tausende anderer Netzwerkknoten mit identischen Kopien der Blockchain synchronisiert sein müssen, macht die Blockchain praktisch unveränderbar; sie kann nicht mit einem praktisch leistbaren Aufwand gehackt werden.

Niemand kann sie verändern oder zerstören. Hacker können nicht in das Peer-to-Peer-Netzwerk eindringen und Transaktionen erstellen, um Coins zu stehlen, Regierungen können sie nicht abschalten (China könnte zum Beispiel versuchen, Bitcoin auf nationaler Ebene auszuschalten, aber die Blockchain würde in vielen anderen Ländern weiter existieren), eine terroristische Gruppe kann sie nicht zerstören, ein Land kann kein anderes Land angreifen und dessen Blockchain vernichten und so weiter. Da es so viele Kopien der Blockchain gibt, ist sie nach menschlichem Ermessen unveränderbar und unverwüstlich, so lange es weiterhin genug Menschen gibt, die sie verwenden wollen.

Wo ist das Geld?

Sie fragen sich vielleicht: »Und wo ist jetzt die Kryptowährung? Wo ist das Geld?« Oder vielleicht haben Sie von Kryptowährungs-Wallets gehört und glauben, dass das Geld darin aufbewahrt wird? Falsch. In einer Krypto-Wallet liegt kein Geld. Es gibt eigentlich überhaupt keine Kryptowährung.

Kryptowährungs-Blockchains werden oft mit Kontobüchern (Ledgers) verglichen. Kontobücher gibt es schon seit Hunderten von Jahren, um Transaktionen von Einzelpersonen, Unternehmen, Regierungsbehörden und so weiter aufzuzeichnen. Der Kontoauszug von Ihrer Bank oder Ihrem Kreditkartenanbieter ist auch eine Art von Kontobuch, dem Sie Ihre einzelnen Transaktionen entnehmen können – Geld, das Sie anderen überwiesen, und Geld, das Sie selbst von anderen erhalten haben.

Im Zusammenhang mit Kryptowährungen stellt die Blockchain ein digitales Kontobuch dar, das die Kryptowährungsbeträge, die Sie an andere senden und die Sie von anderen erhalten, erfasst.

Stellen Sie sich die Sache so vor: Sagen wir, Sie sind etwas zwanghaft und wollen eine Aufzeichnung über den Bargeldbestand in Ihrer Tasche führen. Sie haben immer einen Notizblock dabei, und notieren sich darin jedes Mal, wenn Sie Geld in Ihre Tasche stecken und wenn Sie etwas davon ausgeben, und Sie berechnen Ihren aktuellen Saldo. Dieser Notizblock ist eine Art Buch über Ihre Transaktionen, richtig?

Kryptowährungen funktionieren ganz ähnlich wie diese gedachte Buchführung über Bargeldtransaktionen … nur, dass es hier keine Tasche gibt. Die Blockchain ist das Kontobuch; sie speichert jede Transaktion ab (wann Sie die Kryptowährung zum ersten Mal gekauft oder erhalten haben, wann Sie sie ausgegeben oder verkauft haben und welches Guthaben Sie besitzen).



Den Saldo in der Blockchain finden

Nun ja, die Blockchain speichert nicht wirklich für jede Adresse einen Kontostand. In der Blockchain steht nirgends, wie viel Kryptowährung ein bestimmter Teilnehmer besitzt oder wie viele Coins einer bestimmten Adresse zugeordnet sind. Sie können aber einen Blockchain-Explorer verwenden, um all Ihre Transaktionen nachzuverfolgen, eingehende wie ausgehende, und der Blockchain-Explorer kann dann Ihren Saldo anhand dieser Transaktionen bestimmen.

Es gibt keine Tasche und keine Kryptowährung, die irgendwo aufbewahrt wird. Die Blockchain ist einfach eine Aneinanderreihung »mythischer« (oder virtueller) Transaktionen, die im Kontobuch aufgezeichnet sind. Es wird keine Währung physisch übertragen; wir aktualisieren einfach nur die Aufzeichnungen, um anzuzeigen, dass die Währung transferiert wurde.

Das Kontobuch sagt aus, dass Sie Kryptowährung besitzen, und damit kann jeder überprüfen und nachvollziehen, dass Sie sie tatsächlich besitzen. Und denken Sie daran, dass das Kontobuch nach der Verankerung in der Chain nicht mehr bearbeitet werden kann – es lässt sich nicht hacken. (Im vorhergehenden Abschnitt finden Sie weitere Informationen zu diesem Thema.) Wenn das Kontobuch also sagt, dass Sie zum Beispiel einen halben Bitcoin besitzen, dann ist das auch so, und Sie können diesen halben Bitcoin an jemand anderen verkaufen, indem Sie im Kontobuch einen neuen Eintrag vornehmen, der besagt, dass er nun ihm gehört!

Aber was ist mit der Wallet? Darin muss doch das Geld aufbewahrt werden, oder? Nein, Kryptowährungs-Wallets speichern keine Kryptowährung. Sie speichern private Schlüssel, öffentliche Schlüssel und Adressen. Private Schlüssel sind am wichtigsten, weil sie Zugriff auf die Adressen bieten, mit denen Ihr Kryptoguthaben in der Blockchain verknüpft ist.

Was bedeutet das »Krypto« in Kryptowährung?

Das *Krypto* in Kryptowährung steht für Kryptografie. Aber was genau ist Kryptografie?

Laut Wikipedia ist Kryptografie »ursprünglich die Wissenschaft der Verschlüsselung von Informationen. Heute befasst sie sich auch allgemein mit dem Thema Informationssicherheit, also der Konzeption, Definition und Konstruktion von Informationssystemen, die widerstandsfähig gegen Manipulation und unbefugtes Lesen sind.«

Die Geschichte der Kryptografie reicht mindestens 4000 Jahre zurück. Schon immer mussten Menschen gelegentlich geheime Nachrichten übermitteln. Und genau darum geht es in der Kryptografie.

Die heutige computergestützte Kryptografie ist viel komplizierter als die alten Chiffren der klassischen Welt und sie wird auch wesentlich umfangreicher genutzt. Tatsächlich ist Kryptografie ein integraler Bestandteil des Internets; ohne sie könnte das Internet unsere heutigen Ansprüche einfach nicht erfüllen.

Fast immer, wenn Sie Ihren Webbrowser verwenden, nutzen Sie Kryptografie. Kennen Sie das kleine Schlosssymbol in Abbildung 1.2, das in der Adressleiste Ihres Browsers erscheint?

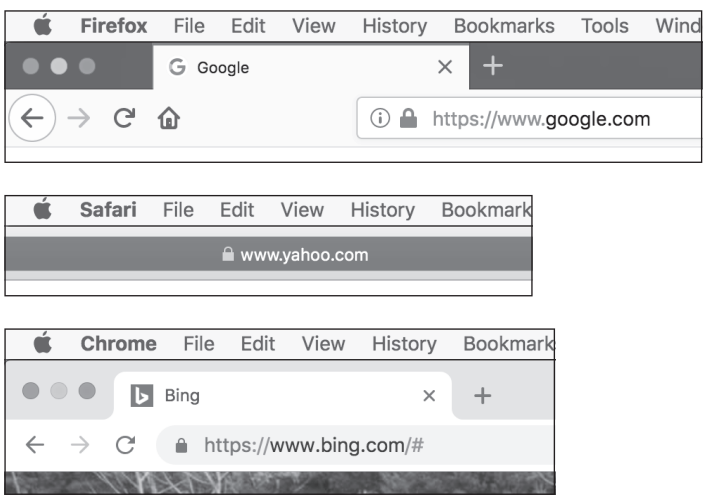


Abbildung 1.2: Das Schlosssymbol im Browser zeigt an, dass die Datenübertragung zum Webserver verschlüsselt wird.

Das Schlosssymbol bedeutet, dass die Seite gesichert ist. Wenn Informationen in beiden Richtungen zwischen Ihrem Browser und dem Webserver ausgetauscht werden, dann erfolgt das *verschlüsselt*. Sollten die Daten also auf dem hunderte oder tausende Kilometer langen Übertragungsweg im Internet zwischen den beiden Endpunkten abgefangen werden, können sie nicht gelesen werden. Wenn Ihre Kreditkartennummer beispielsweise an einen Online-Händler übertragen wird, sendet Ihr Browser diese verschlüsselt an den Webserver und sie wird dann erst vom Empfangsserver wieder entschlüsselt.

Ah, die Blockchain ist also verschlüsselt, stimmts? Nein. Kryptowährungen nutzen Kryptografie, aber nicht, um die Daten in der Blockchain zu verschlüsseln. Die Blockchain ist offen, frei zugänglich und überprüfbar. Abbildung 1.3 zeigt ein Beispiel für einen Blockchain-Explorer für Bitcoin. Mit einem Blockchain-Explorer kann jeder die Blockchain erkunden und jede Transaktion einsehen, die seit dem Genesis-Block (dem ersten erzeugten Bitcoin-Block) durchgeführt wurde.

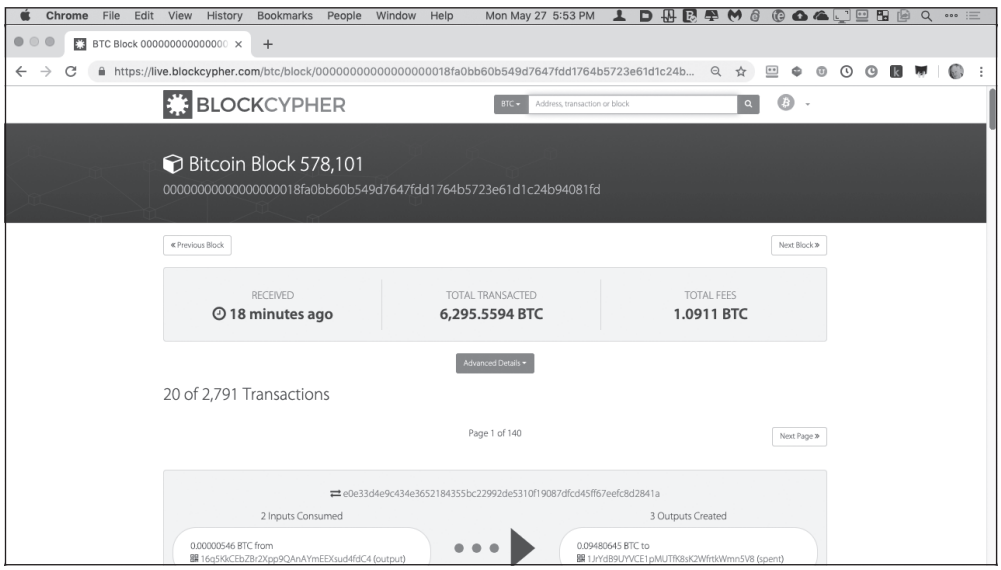


Abbildung 1.3: Beispiel für einen Blockchain-Explorer, zu finden unter `https://live.blockcypher.com/btc/`



Verschlüsselte Blockchains

Es können auch verschlüsselte Blockchains erstellt und die Daten innerhalb einer Blockchain verschlüsselt werden. Während etwa die Bitcoin-Blockchain unverschlüsselt und für jedermann einsehbar ist (siehe Blockchain-Explorer in Abbildung 1.3), gibt es auch verschlüsselte Blockchain-Implementierungen, die die Transaktionsdaten verschleiern, wie beispielsweise bei Zcash. Im Allgemeinen sind Kryptowährungs-Blockchains aber nicht verschlüsselt, sodass jeder die darin gespeicherten Transaktionen einsehen kann.

Nein, Kryptografie dient nicht dazu, die Daten in der Blockchain zu verschlüsseln. Sie dient dazu, Nachrichten zu signieren, die Sie an die Blockchain senden. Diese Nachrichten lösen Transaktionen aus und sorgen für Aktualisierungen des Blockchain-Kontobuchs.

Public-Key-Verschlüsselung

Die Public-Key-Verschlüsselung ist ein raffinierter kleiner Trick der digitalen Kryptografie. Dahinter steckt übrigens sehr komplizierte Mathematik, die selbst die meisten Matheabsolventen nicht verstehen, mit Bezeichnungen wie *Carmichael-Zahlen* und *Goppa-Codes* – wir verstehen sie jedenfalls definitiv nicht, und Sie, liebe Leser, wohl auch nicht (das dürfte jedenfalls auf die meisten von Ihnen zutreffen). Aber das macht nichts: Die Schwerkraft wurde auch noch nicht hinreichend erklärt, und doch machen wir jeden Tag davon Gebrauch.

Vergessen Sie also, was hinter dieser erstaunlichen Sache steckt, und überlegen Sie sich stattdessen, was sie eigentlich bewirkt. Stellen Sie sich dazu einen Tresor mit zwei Schlüssellöchern und zwei entsprechenden Schlüsseln vor. Einer davon ist ein öffentlicher Schlüssel (»Public Key«) und einer ein privater (»Private Key«). Stellen Sie sich nun vor, Sie legen etwas in den Tresor und schließen ihn mit dem öffentlichen Schlüssel ab. Sobald die Tür geschlossen und verriegelt ist, lässt sich der Tresor nicht mehr mit dem öffentlichen Schlüssel aufschließen. Er kann nicht mehr verwendet werden, um den Tresor zu öffnen und den Inhalt zu entnehmen. Der private Schlüssel funktioniert allerdings. Der einzige Weg, den Tresor zu öffnen, ist der Einsatz des privaten Schlüssels.

Tatsächlich funktioniert dieser magische mathematische Tresor in beide Richtungen. Sie können ihn mit dem privaten Schlüssel verriegeln, aber nachdem Sie ihn abgeschlossen haben, können Sie den Tresor nicht mehr mit dem privaten Schlüssel öffnen. Nur der öffentliche Schlüssel öffnet einen mit einem privaten Schlüssel verschlossenen Tresor.

Ach ja, und es gibt eine magische Verbindung zwischen diesen beiden Schlüsseln. Sie funktionieren nur untereinander und nicht in Kombination mit anderen Schlüsseln. Der private Schlüssel X funktioniert nur mit dem öffentlichen Schlüssel X und umgekehrt. Sie können den Tresor nicht mit dem öffentlichen Schlüssel X abschließen und ihn dann zum Beispiel mit dem privaten Schlüssel W oder dem privaten Schlüssel K entsperren.

Okay, nehmen wir dasselbe Prinzip, wenden es aber jetzt auf elektronische Nachrichten an. Sie können eine elektronische Nachricht mit einem öffentlichen Schlüssel schützen, die Nachricht damit also verschlüsseln beziehungsweise chiffrieren. Bei dieser Nachricht kann es sich etwa um eine E-Mail oder um Informationen handeln, die von Ihrem Browser an einen Webserver gesendet werden.

Nachdem diese gesicherte (verschlüsselte) Nachricht von der Gegenseite (dem E-Mail-Empfänger oder dem Webserver) empfangen wurde, lässt sie sich nur mit dem privaten Schlüssel wieder öffnen; der öffentliche Schlüssel ist an dieser Stelle nutzlos. Und es muss der magisch (na gut, mathematisch) zugeordnete Schlüssel sein und kein anderer.

Verschlüsselung ist etwas sehr Nützliches. Ich kann Ihnen einen öffentlichen Schlüssel geben, und Sie können mir dann eine Nachricht schreiben, die Sie mit dem öffentlichen Schlüssel verschlüsseln. Einmal verschlüsselt, kann niemand auf der Welt sie lesen, es sei denn, er ist im Besitz des privaten Schlüssels. Wenn ich also meine Schlüssel sorgfältig verwahre, bin ich der einzige Mensch auf der Welt, die die Nachricht lesen kann.

Die Namen dieser Schlüssel sind nicht zufällig gewählt. Der private Schlüssel muss wirklich privat sein – nur Sie und niemand sonst auf der Welt sollte Zugang dazu haben. Der

öffentliche Schlüssel darf auch wirklich öffentlich sein. Sie können ihn weitergeben. Wenn Sie zum Beispiel möchten, dass Leute E-Mails an Sie senden, können Sie Ihren Public Key veröffentlichen – auf Ihrer Website, in Ihrer Email-Signatur, auf Ihrer Visitenkarte oder wo auch immer – dann kann jeder, der eine Nachricht an Sie senden möchte, diese mit Ihrem Public Key verschlüsseln, in der Gewissheit, dass Sie die einzige Person auf der Welt sind, die das dann lesen kann (weil Sie den privaten Schlüssel geheim halten).



Wie verschlüsselt man E-Mails? E-Mail-Verschlüsselung gibt es seit Jahrzehnten, aber sie hat sich in der breiten Öffentlichkeit einfach nie durchgesetzt. Dennoch können Sie E-Mails in den meisten E-Mail-Systemen wie Outlook, Google Mail und Yahoo! verschlüsseln, und es gibt Systeme wie ProtonMail, die standardmäßig eine Verschlüsselung einsetzen.

Dieser Vorgang läuft im Grunde genommen auch dann ab, wenn Sie mit Ihrem Webbrowser Kreditkarteninformationen online versenden; der Browser nutzt den Public Key des Webservers, um die Daten zu verschlüsseln, sodass nur der Webserver mit dem zugehörigen Private Key die Kreditkarteninformationen entschlüsseln und lesen kann. (Zugegeben, das ist eine Vereinfachung. Die Kommunikation zwischen Browser und Server ist komplizierter als hier beschrieben, etwa mit temporären Session Keys und so weiter, aber das Grundprinzip stimmt trotzdem.)

Nachrichten an die Blockchain

Bei der Übertragung von Transaktionen an die Blockchain nutzen Sie die Public-Key-Verschlüsselung. Wenn Sie zum Beispiel Bitcoins an jemand anderen senden wollen, senden Sie eine verschlüsselte Nachricht mit dem Inhalt »x.xx Bitcoins von mir an diese Adresse senden« an die Blockchain.

Aber Moment. Ich habe Ihnen gerade erklärt, dass die Blockchain nicht verschlüsselt ist, und jetzt behaupte ich, dass die Nachrichten an die Blockchain verschlüsselt sind! Was kümmert es Sie also, ob die Nachricht an die Blockchain verschlüsselt ist, wenn Sie dann doch sowieso entschlüsselt werden soll?

Erinnern Sie sich, dass ich Ihnen erzählt hatte, dass dieses Verschließen und Entriegeln in beiden Richtungen funktioniert. Sie können mit dem Public Key verschlüsseln und mit dem Private Key entschlüsseln oder mit dem Private Key verschlüsseln und mit dem Public Key entschlüsseln. In beiden Fällen werden die Daten verschlüsselt. Der Unterschied besteht darin, wer in der Lage ist, sie wieder zu entschlüsseln. Wenn Sie etwas mit dem öffentlichen Schlüssel verschlüsseln, kann es nur der Inhaber des privaten Schlüssels wieder entschlüsseln. Aber wenn Sie etwas mit dem privaten Schlüssel verschlüsseln, ist der einzige Mensch auf der Welt, der es wieder entschlüsseln kann … jeder! Absolut jeder kann auf den öffentlichen Schlüssel zugreifen. Deshalb heißt er ja schließlich auch so!

Was ist also der Zweck davon, eine Nachricht mit dem privaten Schlüssel zu verschlüsseln? Natürlich nicht, sie abzusichern, da sie ja jeder wieder entschlüsseln kann. Nein, der Zweck ist es, die Nachricht (Transaktion) zu signieren und damit nachzuweisen, dass man sich im Besitz des entsprechenden Private Keys befindet.

Nachrichten mit dem Private Key signieren

Sagen wir, ich veröffentliche meinen Public Key auf meiner Website, in meinen E-Mails und auf meinen Visitenkarten. Eines Tages erhalten Sie eine Nachricht, die von mir zu kommen scheint. Aber wie können Sie sicher sein, dass ich der Absender bin? Tja, ich habe die Nachricht mit meinem privaten Schlüssel verschlüsselt. Also nehmen Sie meinen öffentlichen Schlüssel (der ja frei zugänglich ist) und benutzen ihn zur Entschlüsselung der Nachricht. Wenn die Nachricht wirklich von mir stammt, kann mein Public Key sie entschlüsseln und Sie können sie lesen. Wenn nicht, wird die Entschlüsselung nicht funktionieren, weil die Nachricht von jemand anderem stammt.

Indem ich also die Nachricht mit dem privaten Schlüssel verschlüsselt habe, habe ich die Nachricht de facto signiert und damit bewiesen, dass sie von mir stammt. Der Empfänger weiß, dass die Nachricht von der Person erstellt wurde, die den privaten Schlüssel besitzt, der zu dem öffentlichen Schlüssel gehört, mit dem die Nachricht geöffnet und lesbar gemacht wurde.

Die Blockchain-Adresse – hier liegt Ihr Geld

Die gesamte Kryptowährung in der Blockchain ist auf Adressen verteilt. Diese hier habe ich gerade beispielhaft mit dem Blockchain-Explorer aus der Bitcoin-Blockchain herausgepickt:

```
1L7hHWfJL1dd7ZhQFgRv8ke1PTKAHoc9Tq
```

Es gibt unzählige Möglichkeiten für verschiedene Adresskombinationen, sodass diese Adresse tatsächlich einzigartig ist. Nun, woher kommt diese Adresse? Sie entstammt einer Wallet, die sie aus dem privaten Schlüssel generiert hat. Diese Wallet enthält einen öffentlichen und einen privaten Schlüssel.



Der öffentliche Schlüssel gehört fest zum privaten Schlüssel, er wird sogar aus dem privaten Schlüssel erzeugt. Die Adresse ist dem öffentlichen Schlüssel zugeordnet, sie wird sogar aus dem öffentlichen Schlüssel erzeugt. Alle drei sind also mathematisch eindeutig und exklusiv miteinander verbunden.

Eine Transaktionsnachricht senden

Und wie wird nun die Kryptografie eingesetzt, wenn Sie eine Transaktion an die Blockchain übermitteln wollen, um einen Krypto-Betrag an eine andere Person zu senden? Angenommen, es gibt eine Adresse in der Blockchain mit einem Bitcoin-Guthaben. Als ich zuletzt nachgesehen habe, wies die Adresse

```
1L7hHWfJL1dd7ZhQFgRv8ke1PTKAHoc9Tq
```

ein Guthaben von 0,10701382 Bitcoin auf. Sagen wir, dies sind Ihre Bitcoins und Sie möchten vielleicht 0,05 Bitcoin an einen Freund, eine Börse oder an einen Online-Händler senden, von dem Sie eine Ware oder Dienstleistung erwerben.



Ich nutze für dieses Beispiel eine echte Adresse, die Sie sich in einem Blockchain-Explorer selbst ansehen können. (Rufen Sie ihn über diesen Link auf: `https://blockstream.info/address/1L7hHWfJL1dd7ZhQFgRv8ke1PTKAHoc9Tq`.) Während ich dies schreibe, verfügt diese Adresse über 0,107.013.82 Bitcoin. Wenn Sie nachsehen, kann der Betrag natürlich auch abweichen.

Sie senden eine Nachricht an die Blockchain, die im Grunde Folgendes besagt: »Als Inhaber der Adresse

```
1L7hHWfJL1dd7ZhQFgRv8ke1PTKAHoc9Tq
```

möchte ich 0,05 Bitcoin an die Adresse

```
1NdaT7URGyG67L9nkP2TuBZjYV6yL7XepS
```

schicken.«

Wenn ich nur eine unverschlüsselte Textnachricht an die Blockchain senden würde, wäre es sehr schwierig, die Gültigkeit zu überprüfen. Woher weiß der Bitcoin-Node, der die Nachricht empfängt, dass ich wirklich der Inhaber dieser Adresse und damit der Besitzer des entsprechenden Bitcoin-Guthabens bin? Ich könnte mir das ja auch einfach ausdenken und diese Informationen fälschen, oder?



Nachricht an die Blockchain

Wie schicken Sie eine Nachricht an die Blockchain? Das erledigt Ihre Wallet-Software. Tatsächlich hat die Wallet-Software weniger mit einer Brieftasche gemein – die Wallet enthält keine Kryptowährung – als vielmehr mit einem E-Mail-Programm. Ihr E-Mail-Programm verschickt Nachrichten über das E-Mail-Netzwerk. Ihre Wallet verschickt Nachrichten (über Transaktionen) über das Kryptowährungsnetzwerk.

Wir selbst verwenden die Wallet, um die Nachricht mit dem zur Adresse gehörenden privaten Schlüssel zu signieren. Mit anderen Worten verschlüsseln wir die Nachricht mit unserem Private Key. Dann fügen wir den Public Key an die verschlüsselte Nachricht an und versenden sie an das gesamte Kryptowährungsnetzwerk.

Die Nachricht entziffern

Der Node – ein Computer, der eine Kopie der Kryptowährungs-Blockchain enthält – empfängt also die Nachricht. Mit dem angehängten öffentlichen Schlüssel liest er die Nachricht aus. Der Node erfährt dabei: »Diese Nachricht muss mit dem privaten Schlüssel, der dem öffentlichen Schlüssel zugeordnet ist, verschlüsselt – also signiert – worden sein.« Natürlich sagt das nicht allzu viel aus. Es ist eine Tautologie! Wenn der öffentliche Schlüssel eine

Nachricht entschlüsseln kann, muss die Nachricht per Definition mit dem passenden privaten Schlüssel verschlüsselt worden sein. Ta-daa.

Aber denken Sie daran, dass der öffentliche Schlüssel mathematisch mit der Adresse

`1L7hHWfJL1dd7ZhQFgRv8ke1PTKAHoc9Tq`

verknüpft ist. Der Node kann die beiden nun also betrachten und sich fragen: »Ist der öffentliche Schlüssel mit der Adresse verknüpft?« Wenn die Antwort ja ist, dann weiß der Netzwerkknoten, dass auch der private Schlüssel der Adresse zugeordnet ist (alle drei sind eindeutig miteinander verbunden). Was sagt sich der Node also nun?

»Diese Nachricht, mit der Geld von der Adresse

`1L7hHWfJL1dd7ZhQFgRv8ke1PTKAHoc9Tq`

gesendet wird, wurde mit dem Private Key verschickt, der zur Erstellung dieser Adresse verwendet wurde … also muss die Nachricht vom Inhaber dieser Adresse und damit auch dem Besitzer des damit verknüpften Guthabens stammen.«



Ich weiß, dass dieses Konzept verwirrend wirken kann; es ist schwer, sich das vorzustellen. Hier ist also noch eine weitere Betrachtungsweise: Der einzige Mensch, der eine verschlüsselte Nachricht mit Transaktionsanweisungen für diese Adresse, plus den öffentlichen Schlüssel, der ursprünglich zur Erstellung dieser Adresse gedient hatte, hätte versenden können, ist die Person, die den zugehörigen privaten Schlüssel besitzt – also der Eigentümer der Adresse und des damit verknüpften Guthabens. Damit ist der Besitzanspruch bewiesen und die Transaktion zulässig.



Wer die Private Keys besitzt, besitzt das Geld

Na gut, aber vielleicht haben ja auch mehrere Leute Zugriff auf den Schlüssel. Aus technischer Sicht ist das aber völlig unerheblich. Wer auf den privaten Schlüssel zugreifen kann, hat das kryptographische Recht, das Geld zu verwalten, das mit der diesem Schlüssel zugeordneten Blockchain-Adresse verknüpft ist. Vielleicht haben Sie schon einmal den Satz »nicht Ihr Private Key, nicht Ihre Bitcoins« gehört. Egal, ob jemand rechtmäßig oder unrechtmäßig an die Schlüssel gelangt ist, er hat damit in jedem Fall Zugriff auf die Blockchain-Adresse und auf das Guthaben. Schützen Sie deshalb Ihre privaten Schlüssel wie Ihren Augapfel!

Das bedeutet also das »Krypto« in Kryptowährung: Sie können Geld in der Blockchain mithilfe von Kryptografie anonym verwalten, indem Sie öffentlich-private Schlüsselpaare und die dazugehörigen Adressen verwenden und Nachrichten kryptographisch signieren.



Pseudonyme Kryptowährungen

Einige Kryptowährungen sind anonymer als andere. Der Bitcoin wird beispielsweise oft als *pseudonym* bezeichnet, weil er nur teilweise anonym ist. Stellen Sie sich vor, dass jemand Transaktionsaufzeichnungen von einer Handelsplattform ausliest und dabei herausfindet, dass Sie dort einige Bitcoins gekauft haben. Ihre Identität wurde aufgrund der Anti-Geldwäsche-Bestimmungen (AML) und der in vielen Ländern verpflichtenden Datenerhebung (Know you Customer, KYC) mit diesen Transaktionen verknüpft. Die interessierte Stelle kennt dann auch die Adresse, unter der die Exchange die Coins verwahrt hatte, oder? Nun, jetzt lassen sich die Transaktionen von dieser Adresse mithilfe eines Blockchain-Explorers durch die Blockchain weiterverfolgen. Und verschiedene Adressen können auf bestimmte Weise miteinander in Zusammenhang gebracht werden, sodass es für jemanden mit diesen Informationen – zum Beispiel eine Steuer- oder Polizeibehörde – von einem einzigen Ausgangspunkt aus möglich wäre, ein Bild aller weiteren Bitcoin-Transaktionen eines Menschen zu erstellen. Also ist Bitcoin in der heute üblichen Verwendungsform nicht komplett anonym. Andere Währungen, wie Monero oder Zcash, erheben den Anspruch, einer echten Anonymität viel näher zu kommen. Allerdings werden Verbesserungen an Bitcoin, wie etwa Conjoin und Layer 2, auch Bitcoin in Zukunft wahrscheinlich anonymer machen.

Die wesentlichen Elemente von Kryptowährungen

Die folgenden Abschnitte beschäftigen sich mit dem Zusammenspiel der Grundkomponenten von Kryptowährungen.

Was befindet sich in einer Wallet?

In der *Wallet* nimmt alles, was Ihr Krypto-Guthaben betrifft, seinen Ursprung. Wenn Sie eine Wallet-Datei erzeugen, erstellt die Wallet-Software einen privaten Schlüssel. Dieser private Schlüssel dient zum Erstellen eines öffentlichen Schlüssels, und der öffentliche Schlüssel zum Erstellen einer Adresse. Die Adresse hat noch nie zuvor in der Blockchain existiert und sie wurde in der Blockchain bisher auch noch nicht angelegt.

Sobald Sie eine Adresse haben, können Sie die Kryptowährung verwahren. Sie können die Adresse beispielsweise an eine Börse oder an jemanden weitergeben, von dem Sie Kryptowährung kaufen, und er kann die Kryptowährung dann an diese Adresse senden – mit

anderen Worten sendet er eine Nachricht an die Blockchain, die die Anweisung »Schicke Betrag *x* der Kryptowährung an Adresse *x*.« Ab diesem Zeitpunkt existiert die Adresse in der Blockchain und ihr ist ein Kryptowährungsguthaben zugeordnet.

Eine *Wallet-Software* ist ein Messaging-Programm, das Ihre Schlüssel und Adressen in einer Wallet-Datei speichert. Die Wallet-Software übernimmt folgende Hauptaufgaben:

- ✔ Sie ruft aus der Blockchain Daten über Ihre Transaktionen und Ihren Saldo ab.
- ✔ Sie sendet Nachrichten an die Blockchain und überträgt Ihre Coins von Ihren Adressen an andere Adressen, etwa wenn Sie einen Kauf mit Kryptowährung tätigen.
- ✔ Sie erzeugt Adressen, die Sie an andere Personen weitergeben können, damit diese Ihnen Kryptowährung schicken können.

Private Schlüssel erzeugen öffentliche Schlüssel

Der Private Key in Ihrer Wallet dient dazu, den Public Key zu erzeugen, mit dem Ihre an die Blockchain gesendeten Nachrichten entschlüsselt werden können. Private Keys müssen geheim gehalten werden; jeder, der Zugriff auf den privaten Schlüssel hat, hat Zugriff auf Ihr Geld in der Blockchain!

Öffentliche Schlüssel erzeugen Blockchain-Adressen

Public Keys werden auch zum Erstellen von Adressen verwendet. Wenn eine Adresse zum ersten Mal verwendet wird, sendet die Wallet-Software eine Nachricht mit dem Inhalt »Schicke Betrag *x* der Kryptowährung von Adresse *y* an Adresse *x*« an das Blockchain-Netzwerk. Bis zu diesem Zeitpunkt gab es diese Adresse in der Blockchain noch gar nicht. Nachdem die Wallet-Software die Nachricht jedoch verschickt hat, befindet sich die Adresse in der Blockchain und es ist ein Geldbetrag mit ihr verknüpft.

Der private Schlüssel gibt Zugriff auf die Adresse

Die Regelung des Zugriffs auf die Adresse über den Private Key ist ein ganz entscheidendes Konzept von Kryptowährungen, das Menschen, die den Zugriff auf ihre Kryptowährung verlieren oder deren Kryptowährung gestohlen wird, oftmals nicht verstehen (siehe Abbildung 1.4). Die Kryptowährung ist einer Blockchain-Adresse zugeordnet; die Adresse wird vom öffentlichen Schlüssel abgeleitet, der zu einem privaten Schlüssel gehört, der in einer Wallet sicher verwahrt wird. In diesem Buch werden wir nicht im Detail auf die Absicherung von privaten Schlüsseln eingehen. Aber Sie sollten sicherstellen, dass Sie Ihre privaten Schlüssel schützen! Verlieren Sie sie nicht und achten Sie darauf, dass andere Menschen sie niemals erfahren!



Abbildung 1.4: Ohne privaten Schlüssel kommen Sie an Ihre Kryptowährung nicht mehr heran!



»Forks« von Kryptowährungen

Eine *Fork* tritt auf, wenn eine Kryptowährung in zwei Teile aufgespalten wird. Das heißt, die Netzwerkknoten verlieren ihren Konsens und es wird eine veränderte Kopie der Kryptowährungssoftware erstellt. Die beiden verschiedenen Softwareversionen erzeugen dann separate Blockchains. So wurde zum Beispiel im Januar 2015 eine Kopie des DASH-Codes mit der Bezeichnung DNET (DarkNet) erstellt. Sowohl DASH als auch DNET entwickelten sich dann als separate Kryptowährungen weiter, wobei DNET später in PIVX (Private Instant Verified Transaction) umbenannt wurde.

Woher kommt die Kryptowährung? Aus Kryptominen (manchmal)

Woher kommt eigentlich eine Kryptowährung? Kryptowährung kann *gemined* werden – die am wenigsten verbreitete Form, obwohl Sie als Leser oder Leserin dieses Buches gerade daran offensichtlich am meisten interessiert sind – oder sie entsteht durch sogenanntes *Premining*.

Premining bedeutet nichts weiter, als dass die Kryptowährung bereits vorhanden ist. Die Blockchain ist ein Kontobuch mit Informationen über Transaktionen. Bei der Erstellung der Blockchain enthielt das Kontobuch bereits einen Datensatz mit der gesamten Krypto-Geldmenge, die die Gründer vorgesehen hatten. Es kommen keine neuen Coins oder Token hinzu; alles ist bereits in der Blockchain vorhanden.

Es wird zwar viel über Krypto-Mining gesprochen, aber die Mehrzahl der Kryptowährungen (zum Zeitpunkt, an dem dieses Buch geschrieben wurde, waren es über 2000 verschiedene Varianten) sind »premined«: Etwa 74 der 100 wichtigsten Kryptowährungen lassen sich nicht durch Mining gewinnen und auch insgesamt liegt diese Quote bei etwa 70 Prozent aller Kryptowährungen.

Ein Beispiel für eine vorab erstellte Kryptowährung ist XRP, auch bekannt als Ripple, die derzeit die zweitgrößte Kryptowährung ist (gemessen an der *Marktkapitalisierung* – also dem Wert aller im Umlauf befindlichen Kryptowährungen). XRP wird in der RippleNet-Blockchain gespeichert.

Als die Ripple-Blockchain erstellt wurde, waren bereits 100 Milliarden XRP in der Blockchain gespeichert, obwohl die meisten nicht verteilt wurden. Die Gründer von Ripple hielten 20 Prozent, und selbst heute wurden nahezu 60 Prozent der Währung noch gar nicht in Umlauf gebracht.

Ein weiteres Beispiel ist Stellar, ein Zahlungsnetzwerk, das ursprünglich vom Zahlungsdienstleister Stripe finanziert wurde und das zum Zeitpunkt des Schreibens in Punkto Marktkapitalisierung an Platz 4 rangierte. Stellar verfügt über eine Geldmenge von über als 100 Milliarden Lumen, 2 % davon wurden Stripe für seine Investition zugeschrieben.

Also, nein, nicht alle Kryptowährungen können durch Mining abgebaut werden (bei den meisten ist das nicht möglich). Aber das ist nicht der Grund, weshalb Sie dieses Buch lesen, nicht wahr?

Die gute Nachricht ist aber, dass Sie rund 600 Kryptowährungen minen können (obwohl Sie von der überwiegenden Mehrheit die Finger lassen sollten). Um zu entscheiden, welche Sie schürfen wollen, lesen Sie bitte Kapitel 8.

Kent716630_c01.indd 50 2/14/2020 2:37:27 PM