Daniel Kerscher

BITCOIN

Funktionsweise, Risiken und Chancen der digitalen Währung

Über den Autor:

Dr. Daniel Kerscher absolvierte eine Ausbildung zum Bankkaufmann und ein Studium der Politikwissenschaft und Informationswissenschaft mit Promotion. Er beschäftigt sich seit vielen Jahren mit dem Finanzsystem und den digitalen Informationstechnologien und ist Autor des Buches „Handbuch der digitalen Währungen. Bitcoin, Litecoin und 150 weitere Kryptowährungen im Überblick“.

Daniel Kerscher

Bitcoin

Funktionsweise, Risiken und Chancen der digitalen Währung

Impressum

Daniel Kerscher: Bitcoin. Funktionsweise, Risiken und Chancen der digitalen Währung

ISBN: 978-3-9816017-1-8
2. überarbeitete und erweiterte Auflage 2014
Coverbild: © Nmedia – www.fotolia.de
Herstellung und Druck: Siehe Eindruck auf der letzten Seite

Kemacon UG (haftungsbeschr.)
Sossauer Str. 30
84130 Dingolfing
info@kemacon.de

1. Auflage 2013

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

Inhalt

Einleitung

Geld ist ein wichtiges Instrument jeder modernen Gesellschaft und gleichzeitig ist es ein Spiegel der Entwicklungen und Technologien der jeweiligen Epoche. Im digitalen Zeitalter der letzten Jahre kam es deshalb zur Entwicklung von Währungen, die rein digital im Internet existieren.

Eine dieser digitalen Währungen ist Bitcoin. Seit der Einführung im Jahr 2009 erregt die Währung nicht nur die Aufmerksamkeit von erfahrenen Internetnutzern, die Bitcoin wegen der technischen Finesse mögen, sondern sie bekommt auch Zuspruch von Kritikern des bestehenden Banken- und Währungssystems, die nach besseren Alternativen suchen. Bitcoin findet auch zunehmend Verbreitung unter normalen Anwendern, denen das System eine einfache, schnelle und kostenlose Bezahlmöglichkeit bietet.

Obwohl die Software zur Verwaltung von Bitcoin sehr einfach zu bedienen ist, steckt hinter dem gesamten Bitcoin-Konzept eine komplizierte Logik, die nicht nur die rein technischen Aspekte umfasst, sondern auch die grundlegende Funktionsweise eines Geldsystems. Was Bitcoin von vielen anderen Währungen unterscheidet, ist die fehlende Kontrolle durch eine Institution, wie zum Beispiel eine Zentralbank. Dadurch kann die Geldmenge nicht einfach angehoben werden, denn das Bitcoin-System sieht eine Menge von maximal 21 Millionen Stück vor. Neben diesem im Vergleich zu den

derzeit existierenden Währungen grundlegend anders gestalteten Konzept gibt es weitere Innovationen, beispielsweise die für Sender und Empfänger kostenfreie und anonyme Transaktion von Guthaben sowie die Möglichkeit, Bitcoin selbst zu generieren.

Die digitale Währung, die bei ihrer Einführung keinen Wert hatte und seit dem Jahr 2009 einen Kurssprung auf in der Spitze fast 900 Euro vollzog, hat viele interessante und neuartige Facetten. Bitcoin existiert erst seit wenigen Jahren und gerade zu Beginn eines neuen Systems gibt es zahlreiche Risiken, die sich aus der Natur der digitalen Währung ergeben, angefangen von Sicherheitsbedenken und Spekulationsblasen bis hin zu Verbotsszenarien. Das Bitcoin-System bietet aber auch zahlreiche Chancen, wie die langfristige Wertsteigerung und die Entstehung neuer Märkte. Dieses Buch will deshalb die technische Funktionsweise, die denkbaren Risiken und die möglichen Chancen der neuen digitalen Währung Bitcoin aufzeigen.

Die Grundlagen des Bitcoin-Systems

Bitcoin ist ein Kunstwort, das sich aus den englischen Bezeichnungen Bit, der kleinsten Maßeinheit für eine Daten- oder Informationsmenge, und Coin (eng. *coin* = Münze) zusammensetzt. Vereinfacht ausgedrückt definiert Bitcoin ein Set von Regeln in Form einer Software, die zur Erzeugung und Verwaltung von Geldeinheiten und zur Abwicklung von Zahlungen zwischen den Nutzern dient. Die Regeln schaffen ein Zahlungssystem in einem Netzwerk mit virtuellem Geld und kryptografischen Funktionen.

Der Begriff Bitcoin bezeichnet zwei unterschiedliche Dinge, einerseits das komplette Währungssystem, das aus einem globalen Netzwerk mit vielen Teilnehmern besteht und andererseits die einzelnen Währungseinheiten darin, die Bitcoin, die inoffiziell mit BTC abgekürzt und manchmal auch als „bitcoins“ bezeichnet werden. Inzwischen wird gelegentlich auch die Abkürzung XBT verwendet. Gemäß der SO4217, der von der Internationalen Organisation für Normung publizierten Norm für Währungsabkürzungen, sollen Währungen, die nicht von einem Einzelstaat herausgegeben werden, als ersten Buchstaben ein X führen, während die beiden folgenden Buchstaben den Namen der Währung angeben, der im internationalen Zahlungsverkehr zur eindeutigen Identifizierung benutzt werden soll. Damit wird der rechtliche Status von Bitcoin deutlich, denn es ist eine Währung, die in keinem Land der Erde von staatlicher Seite anerkannt ist.

Während reguläres Geld in der Regel über Banken oder bei direkten Transaktionen in bar ausgetauscht wird, werden Bitcoin durch ein sogenanntes Peer-to-Peer-Computernetzwerk (P2P) transferiert. Das Netzwerk wird durch alle Teilnehmer gebildet, die eine bestimmte Software, den Bitcoin-Client, ausführen. Es gibt keinen zentralen Server zur Verwaltung und dadurch unterliegt Bitcoin nicht der Kontrolle durch eine Behörde oder Regierung. Ebenso wenig existiert eine Firma, die Bitcoin herausgibt oder betreut.

Bitcoin stellen eine elektronische Kette von Signaturen dar. Diese Signaturen sind mit elektronischen Informationen verknüpfte Daten, mit denen sich ein Signaturersteller wie mit einer eigenhändig geleisteten Unterschrift identifizieren lässt und die Integrität der signierten elektronischen Informationen überprüft werden kann. Bitcoin lassen sich in kleinere Einheiten unterteilen. Die gängigsten Einteilungen sind:

1 Bitcoin =	1 BTC
0,01 BTC =	1 cBTC (1 Centbitcoin oder bitcent)
0,001 BTC =	1 mBTC (1 Millibitcoin oder mbit)
0,000001 BTC =	1 µBTC (1 Mikrobitcoin oder µbit)
0,00000001 BTC =	1 Satoshi (kleinste teilbare Menge eines BTC, benannt nach dem Bitcoin-Erfinder Satoshi Nakamoto)

Bitcoin werden in einem dezentralen Computernetzwerk generiert und durch eine auf jedem Computer installierbare Software verwaltet. Damit lassen sich Bitcoin von einem Anwender auf den anderen übertragen. Die Übertragung erfolgt, wie beim Online-Banking, durch Überweisungen, die von jedem internetfähigen Gerät vorgenommen werden können, egal ob Computer, Smartphone oder Tablet.

Im Gegensatz zu Überweisungen im normalen Bankensystem, bei denen Name und Kontonummer des Empfängers bekannt sind, finden die Bitcoin-Überweisungen weitgehend anonym für alle Beteiligten statt, da Sender und Empfänger nur durch einen mathematisch generierten Schlüssel aus Zahlen und Buchstaben miteinander in Verbindung treten. Auch für Dritte sind nur die Adressen einsehbar und es ist nicht nachvollziehbar, wer dahinter steht. Bitcoin soll dadurch so einfach wie Bargeld zu handhaben sein und gleichzeitig die Flexibilität einer elektronischen Überweisung ermöglichen.

Bitcoin ist ein Open-Source-Programm, denn der Quellcode ist für jeden frei zugänglich und einsehbar. Trotzdem soll die Sicherheit der Transaktionen garantiert werden. Dies wird durch kryptografische Schlüssel ermöglicht, die den Besitz der Bitcoin belegen. Die Kryptografie, die Wissenschaft der Verschlüsselung von Informationen, liefert wichtige Grundlagen für die Sicherheit von Bitcoin. Die Kryptografie ist von so fundamentaler Bedeutung für die digitale Währung, dass sie häufig auch als Kryptowährung bezeichnet wird. Die Be-

zeichnung Kryptowährung ist nicht ganz korrekt, denn eigentlich bezeichnet der Begriff Währung die Systematik und Ordnung des gesamten Geldwesens eines Staates. Bei Bitcoin handelt es sich aber um privat geschöpftes Geld ohne jegliche staatliche Garantien oder Regulierungen. In den USA hat sich jedoch der Begriff „cryptocurrency“ durchgesetzt, sodass auch im Folgenden der Begriff Kryptowährung synonym mit digitaler Währung verwendet wird. Entsprechend der Gepflogenheit im deutschen Sprachraum, bei Geldmengen auf den Plural zu verzichten (beispielsweise 4,99 Euro), soll auch im Folgenden bei Bitcoin der Singular verwendet werden.

Der Besitz von Bitcoin wird durch eine elektronische Geldbörse ausgewiesen, die mit der Installation der Bitcoin-Software eingerichtet wird. Ähnlich wie eine reale Geldbörse, so muss auch die elektronische Geldbörse gegen Verlust, etwa in Form eines Festplattendefekts, aber auch gegen Diebstahl gesichert werden. In einer zentralen Verzeichnisdatei, der sogenannten Block Chain, erfolgt die Speicherung jeder Transaktion. Die Block Chain enthält sämtliche Transaktionen, die bisher im Netzwerk zwischen den Nutzern abgewickelt wurden. Das garantiert eine hohe Fälschungssicherheit, denn dadurch ist sichergestellt, dass ein Bitcoin-Betrag nicht zweimal ausgegeben werden kann, indem er an unterschiedliche Empfänger geschickt wird. Im Gegensatz zu normalen digitalen Dateien, die beliebig kopiert oder verändert werden können, verhindert die Verwendung kryptografischer Verfah-

ren dies bei Bitcoin. Mithilfe einer asymmetrischen kryptografischen Methode sowie der digitalen Signaturen ist es praktisch unmöglich Bitcoin zu fälschen, denn in der Block Chain wird nur die erste Transaktion erfasst und die zweite verworfen. Damit wird das Problem des doppelten Ausgebens desselben Betrages, das aufgrund der Kopierbarkeit digitaler Informationen grundsätzlich besteht, auf einfache Weise gelöst. Gleichzeitig wird durch die Block Chain sichergestellt, dass es keine zentrale Institution zur Verwaltung geben kann, denn die Block Chain wird vom gesamten Netzwerk aktualisiert und ist jederzeit von allen Teilnehmern einsehbar. Sie wird auf jeden Computer heruntergeladen, der die Grundversion der Bitcoin-Software nutzt. Dadurch entsteht ein dezentrales Netzwerk. Das Fehlen einer zentralen Kontrollinstanz, zum Beispiel einer Zentralbank, ist eine der wesentlichen Eigenschaften des Bitcoin-Systems.

Zahlungen werden mit Hilfe von Adressen abgewickelt, die die Bitcoin-Software für jeden Empfänger neu generieren kann. So wie jedes normale Konto einen bestimmten Kontostand hat, so hat auch jede Adresse einen jeweils spezifischen Bestand an Bitcoin. Da die Adresse nur aus einer Kombination von Zahlen und Buchstaben besteht, ist damit keine Identifizierung der Handelspartner möglich, aber da in der Block Chain alle Transaktionen verzeichnet werden und eine Kopie dieser Datei auf jedem Computer des Netzwerkes gespeichert werden kann, liegt ein für alle einsehbares Verzeichnis vor.

Die Bitcoin-Menge ist begrenzt. Insgesamt sind im Bitcoin-Protokoll 21 Millionen Stück vorgesehen. Sobald diese erzeugt sind, können keine weiteren Bitcoin mehr generiert werden, jedoch sind Bitcoin auch in kleinere Einheiten bis hin zu den sogenannten Satoshi teilbar. Da jeder Bitcoin aus 100.000.000 Satoshi besteht, ergeben sich 2,1 Billiarden Recheneinheiten. Im Gegensatz zu den regulären Währungen, die beliebig durch die Notenbanken vermehrt werden können und dadurch automatisch der Inflation unterliegen, ist Bitcoin eine deflationäre Währung mit einer limitierten Menge. Neue Bitcoin werden beim Prozess des sogenannten Mining ausgeschüttet. In diesem äußerst komplexen Rechenverfahren werden die Bitcoin-Transaktionen zu Blöcken zusammengefasst und verifiziert. Blöcke werden in Abständen von durchschnittlich zehn Minuten generiert und auf Richtigkeit geprüft. Die Blöcke werden dann der öffentlichen Datei, der Block Chain, hinzugefügt. Mining ist sehr komplex und erfordert umfangreiche technische Kenntnisse und große Rechenkapazitäten. Für diesen Einsatz erhalten die Miner, diejenigen, die Rechenleistung zur Verfügung stellen, eine Gegenleistung, denn jeder gelöste und zur Block Chain hinzugefügte Block enthält derzeit 25 neue Bitcoin.

Bitcoin ist eine digitale, dezentrale und anonym handhabbare Online-Währung, die weder durch eine Regierung noch durch eine zentrale Organisation gesteuert wird und die nicht durch Gold oder andere werthaltige Gegenstände gedeckt ist.

Der Unterschied zwischen digitalen Währungen und Bezahlsystemen

Obwohl Bitcoin als Zahlungssystem konzipiert ist, handelt es sich um kein weiteres Online-Bezahlsystem, wie etwa PayPal. Wenngleich es Gemeinsamkeiten gibt, beispielweise die digitale Speicherung der Daten, unterscheiden sich die Bezahl- von den Währungssystemen in wichtigen Punkten. Während bei Bezahlsystemen eine zentrale Betreiberfirma existiert, gibt es diese bei digitalen Währungen nicht. Bei Bezahlsystemen bleibt der Betrag in der Ursprungswährung, beispielsweise Euro, erhalten, während er bei einer digitalen Währung umgetauscht wird, zum Beispiel in Bitcoin. Daraus ergibt sich ein Wechselkurs zwischen der digitalen und der realen Währung.

Es lassen sich aber noch weitere Unterschiede im Vergleich zu digitalen Bezahlsystemen feststellen. Digitale Bezahlsysteme, wie zum Beispiel PayPal oder Kreditkarten, sind weit verbreitet und werden von vielen Stellen akzeptiert. Bei einer digitalen Währung ist dies nicht immer der Fall, da sie meist nur in kleinen Gruppen akzeptiert werden. Digitale Bezahlsysteme unterliegen gesetzlichen Regulierungen und müssen entsprechende Auflagen einhalten. Digitale Währungen sind meist unreguliert. Für digitale Bezahlsysteme bestehen Rückgaberegelungen und Garantien durch den Systembetreiber, während bei digitalen Währungen häufig keinerlei Garantien oder Schutzmechanismen existieren.

Am Beispiel von PayPal wird der Unterschied zwischen den beiden Systemen deutlich. Ein PayPal-Konto wird durch Geldzahlungen von einem Bankkonto oder einer Kreditkarte mit Geldmitteln versehen. Das Guthaben auf dem PayPal-Konto bleibt aber in der Ursprungswährung. Es findet kein Wechsel in eine andere Währung statt, wenn nicht ausdrücklich eine entsprechende Überweisung vorgenommen wird. Da die europäische PayPal-Niederlassung in Luxemburg eine Bankenlizenz besitzt, untersteht PayPal auch den europäischen Aufsichts- und Regulierungsrichtlinien. Da es sich um ein reines Online-Bezahlmedium handelt, wird durch das System keine neue Währung generiert, sondern es werden lediglich bestehende Währungen digital transferiert. Im Gegensatz dazu findet bei einem Online-Währungssystem vorab der Tausch eines Guthabens in eine neue Währung statt.

Virtuelle Bezahlsysteme stellen kein neues Phänomen dar, da lediglich vorhandenes Geld in das System transferiert wird. Eine digitale Währung, wie Bitcoin, ist jedoch ein Novum, das viele Fragen aufwirft und das von staatlicher Seite erst ansatzweise behandelt und reguliert wird. Auch die BaFin, die Bundesanstalt für Finanzdienstleistungsaufsicht, die das Finanzwesen in Deutschland reguliert, sieht Bitcoin nicht als digitales Bezahlsystem. Die BaFin definiert Bitcoin als

> eine virtuelle Währung, deren Transaktionen und Guthaben in einem dezentralen Netzwerk verwaltet werden. Durch kryptografische Berechnungen kann prinzipiell jeder Netzwerk-Nutzer an der Geldschöpfung teilnehmen.

> Eine Zentralbank, die diese Aufgabe bei realen Währungen wahrnimmt, existiert daher nicht. (Jens Münzer: Bitcoins. Aufsichtliche Bewertung und Risiken für Nutzer. In: BaFin Journal Januar 2014, S. 26)

Da es keinen Emittenten gibt, stuft die BaFin Bitcoin als sogenannte virtuelle Währung ohne den Status eines gesetzlichen Zahlungsmittels ein. Es handelt sich vielmehr um ein Finanzinstrument in der Form von Rechnungseinheiten gemäß § 1 Absatz 11 Satz 1 Kreditwesengesetz (KWG). Die BaFin verbietet Bitcoin und andere private Zahlungsmittel nicht generell. Nur wenn mit diesen Zahlungsmitteln selbst Handel getrieben wird, muss dies von der BaFin genehmigt werden. Demzufolge muss jeder, der gewerbsmäßig Dienstleistungen im Zusammenhang mit Bitcoin, wie etwa den Betrieb eines Handelssystems, erbringen möchte, zunächst die Erlaubnis der BaFin einholen. Die bloße Nutzung von Bitcoin als Ersatzwährung zur Teilnahme am Wirtschaftskreislauf ist allerdings keine erlaubnispflichtige Tätigkeit. Auch das nicht geschäftsmäßige Mining sowie der Verkauf der dafür erhaltenen Bitcoin ist grundsätzlich keine erlaubnispflichtige Tätigkeit.

Das Bitcoin-System ist sehr einfach, da die Software leicht zu verstehen und einfach zu bedienen ist. Die dahinter stehende Logik ist allerdings sehr kompliziert. Um das Bitcoin-System besser verstehen zu können, ist zunächst die Betrachtung zweier Konzepte notwendig, die die Basis für Bitcoin bilden: die Kryptografie und die Funktionsweise von Geld.

Die sichere Basis: Kryptografie

Eine der Grundlagen für die Sicherheit von Bitcoin ist der Einsatz verschlüsselter Informationen bei der Übertragung. Die bei Bitcoin verwendeten Verschlüsselungstechnologien sind nicht völlig neu, denn das grundlegende Prinzip der Codierung von Nachrichten ist wesentlich älter als das digitale Zeitalter. Der Wunsch, dass Nachrichten nur vom Sender und vom Empfänger gelesen werden können, besteht seit Beginn der menschlichen Kommunikation über weite Entfernungen hinweg. Aus diesem Wunsch entstand die Kryptografie als Wissenschaft der Verschlüsselung von Informationen. Schon im alten Ägypten wurden Geheimschriften benutzt, ebenso im Mittelalter und der Neuzeit.

Lange Zeit waren für die Verschlüsselung von Nachrichten nur symmetrische Systeme im Einsatz, bei denen zur Ver- und Entschlüsselung identische Schlüssel zum Einsatz kamen. Bei symmetrischen Systemen erlaubt der Besitz des Schlüssels sowohl das Verschlüsseln einer Nachricht als auch das Entschlüsseln. Dazu muss die Verschlüsselungsinformation zwischen zwei Kommunikationspartnern auf möglichst sicherem Weg ausgetauscht werden, was zusätzliche Probleme aufwirft. Zudem werden bei mehreren Kommunikationspartnern auch mehrere Schlüssel benötigt, wenn nicht jeder alle Nachrichten entschlüsseln können soll. Die Grundproblematik, die Vorlage der gleichen Schlüssel bei Sender und Empfänger der Nach-

richt, blieb bei allen symmetrischen Systemen, die im Laufe der Jahrhunderte immer weiter verfeinert wurden, bestehen. Im Informationszeitalter nahm allerdings sowohl der Bedarf an sicherer Nachrichtenübermittlung als auch die Komplexität der Verschlüsselung zu. Aus der Kryptografie entwickelte sich deshalb der Forschungszweig der Informationssicherheit, deren Ziel die Schaffung von Informationssystemen ist, die gegen unberechtigtes Lesen und Verändern geschützt sind. Ein Durchbruch im Rahmen der Informationssicherheit war die Entwicklung asymmetrischer Verschlüsselungssysteme in den 1970ern.

Bei einem asymmetrischen Kryptosystem wird ein Paar zusammenpassender Schlüssel eingesetzt. Ein öffentlicher Schlüssel, der zum Verschlüsseln von Nachrichten für den Schlüsselinhaber benutzt wird, und ein privater Schlüssel, der geheim gehalten werden muss und zur Entschlüsselung eingesetzt wird. So nutzen beispielsweise die im Internet weit verbreiteten Protokolle SSH, SSL/TLS und HTTPS asymmetrische Kryptoverfahren.

Bitcoin nutzt ebenfalls ein asymmetrisches Kryptosystem in Form eines Public-Key-Kryptosystems, da unterschiedliche Schlüssel für die Ver- und Entschlüsselung eingesetzt werden. Ein Nutzer erzeugt ein Schlüsselpaar, das aus einem geheimen Teil, dem privaten Schlüssel, und einem nicht geheimen Teil, dem öffentlichen Schlüssel, besteht. Der öffentliche Schlüssel ermöglicht es jedem, Daten, die für den Inhaber des privaten

Schlüssels bestimmt sind, zu verschlüsseln oder dessen digitale Signaturen zu prüfen. Der private Schlüssel ermöglicht seinem Inhaber, mit dem öffentlichen Schlüssel verschlüsselte Daten zu entschlüsseln, digitale Signaturen zu erzeugen oder sich zu authentifizieren. Der private Schlüssel ist deshalb vergleichbar mit der persönlichen Unterschrift zur Freigabe von Dokumenten. Die digitale Signatur wird aus dem privaten Schlüssel und den zu signierenden Daten beziehungsweise ihrem Hashwert berechnet. Ein Hashwert ist ein Wert fester Länge der typischerweise als hexadezimale Zeichenkette codiert ist und der aus beliebigen Eingabedaten gewonnen werden kann. Er wird durch einen Algorithmus berechnet, der eine beliebig große Eingabemenge auf eine kleinere Zielmenge abbildet. So ergibt beispielsweise der Satz „Das ist ein Passwort.“ durch die Berechnung mit dem MD5-Algorithmus den Hashwert „b6ea69ae42b92b4201056aa3c09e4735a873f4 8d1be3f2d0b8-e4a058d49ad7b5“. Der Satz „Das ist kein Passwort.“ ergibt den völlig anders lautenden Hashwert „e687b134da0dd208a9b52e88d42eda73f7d9fff517e46a98fd3 633868714c70b“, obwohl bei der Eingabe nur ein Buchstabe hinzugefügt worden ist.

Die wesentliche Eigenschaft eines aus Zahlen und Buchstaben bestehenden Hashwertes ist, dass durch ihn keine Rückschlüsse auf den ursprünglichen Eingabewert möglich sind. Aus einer bestimmten Zeichenfolge lässt sich zwar immer der gleiche Hashwert berechnen, aber umgekehrt kann aus dem

Hashwert nicht wieder der ursprüngliche Eingabewert errechnet werden. Der Hashwert hat Einwegcharakter. Diese Eigenschaft macht Hashwerte für die Speicherung von Passwörtern und anderen sensiblen Daten interessant. Statt des Passwortes wird oft nur der Hashwert eines Passwortes gespeichert. Wird das Passwort bei der Anmeldung an das System eingegeben, wird daraus der Hashwert errechnet und dieser mit dem abgespeicherten Hashwert verglichen. Sollten die Anmeldedaten in die Hände unberechtigter Dritter gelangen, ist es aufgrund des Einwegcharakters der Hashfunktion für den Angreifer schwieriger das ursprüngliche Passwort zu ermitteln. Hashwerte werden auch zur Überprüfung der Datenintegrität genutzt. Da eine Hashfunktionen mit gleicher Dateneingabe auch stets gleiche Hashwerte liefert, kann auf diese Weise überprüft werden, ob Daten bei einer Übertragung über ein unsicheres Netz verfälscht wurden. Dieses Prinzip wird auch bei digitalen Signaturen genutzt.

Die digitalen Signaturen von Bitcoin sind Teil des asymmetrischen Kryptosystems, das öffentliche und private Schlüssel einsetzt. Der öffentliche Schlüssel ist mit einer Kontonummer vergleichbar, während der private Schlüssel wie eine Unterschrift oder TAN wirkt. Dadurch ist eine sichere Übertragung von Bitcoin möglich. Ein Großteil der kryptografischen Prozesse wird von der Bitcoin-Software im Hintergrund erledigt. Die Nutzer müssen lediglich den öffentlichen Schlüssel austauschen und die Transaktion initiieren.

Die Funktionsweise von Geld

Obwohl das Bitcoin-System eine digitale Währung ist, weist es doch Gemeinsamkeiten mit bereits bestehenden Währungssystemen auf und auch die grundlegenden Funktionen des Geldes will Bitcoin erfüllen. Geld wird seit jeher für den Austausch von Waren und Dienstleistungen benutzt. In der heutigen Zeit findet ein Großteil der Geldtransaktionen bereits auf elektronischem Weg statt, aber vor der Digitalisierung waren Münzen und Scheine das gängigste Zahlungsmittel. Davor war es lange Zeit üblich, mit Waren- oder Naturalgeld im Tauschhandel zu bezahlen.

Der Tauschhandel war praktisch, wenn beide Parteien jeweils das haben wollten, was die andere Partei anzubieten hatte. Der einstufige Tausch, Ware gegen Ware, schränkte aber viele Geschäfte stark ein, da nicht immer passende Tauschgegenstände vorhanden waren, die beide Tauschpartner haben wollten. Oftmals mussten mehrere Tauschvorgänge zwischen unterschiedlichen Personen vorgenommen werden, um letztendlich das gewünschte Gut zu erhalten. Das erhöhte nicht nur die Kosten, sondern dauerte auch länger. Im Laufe der Zeit wurde deshalb das Naturalgeld durch Edelmetalle, allen voran Gold und Silber, aber auch Bronze und Kupfer, ersetzt. Diese Metalle haben den Vorteil, dass sie schwer zu bekommen sind und deswegen nur in begrenzter Menge zur Verfügung stehen, wenig Lagerfläche benötigen, leicht teilbar sind und im Gegensatz zu Tieren oder Nahrungsmitteln nicht verderben.

Lange Zeit waren deshalb Münzen und später Scheine weit verbreitet. Die Form des Geldes kann sich jedoch immer wieder ändern und den aktuellen Verhältnissen anpassen, denn nach dem Ende des Zweiten Weltkriegs wurden in Deutschland kurzzeitig auch Zigaretten als Geld akzeptiert. Auf einigen Inseln des Pazifiks wird heute noch mit Muscheln oder auch mit Steinscheiben, die ein Loch in der Mitte haben, bezahlt. Mittlerweile ist ein Großteil des Geldes aber nicht einmal mehr in Form von Münzen oder Scheinen vorhanden, sondern nur noch elektronisch als Guthaben auf Konten. Unabhängig von der Form ist im Allgemeinen also Geld, was als Geld gilt und als solches akzeptiert wird. Die Akzeptanz kann global sein, wie beim US-Dollar, der in vielen Ländern neben der nationalen Währung als Zahlungsmittel akzeptiert wird; sie kann national sein, wie zum Bespiel beim britischen Pfund, das nur in Großbritannien als Zahlungsmittel gilt; aber auch regional, wie beispielsweise beim Chiemgauer, einer privaten Regionalwährung im Rosenheimer Raum.

Unabhängig davon, ob Geld in Form von Muscheln, Edelmetallen oder digitalen Ziffern akzeptiert wird, weist es stets drei wichtige Funktionen auf:

1. Tausch- und Zahlungsmittel

Geld wird als Tauschmittel benutzt, um den Austausch von Gütern und Dienstleistungen zu vereinfachen. Geld ersetzt die zahlreichen Wechselbeziehungen zwischen einzelnen Gütern, die im reinen Tauschhandel notwendig sind. Dadurch wird der

Warenaustausch erleichtert. Geld kann aber auch als Kredit vergeben und zur Begleichung von Schulden benutzt werden. Bei derartigen Transaktionen wird Geld dann als Zahlungsmittel benutzt. Um diese Funktion zu erfüllen, muss Geld bei allen Teilnehmern am Warenverkehr akzeptiert werden. Überdies muss Geld fungibel sein. Diese Eigenschaft beschreibt die leichte Aus- und Umtauschbarkeit. Fungible Werte werden nicht individuell, sondern der Gattung nach bestimmt und können durch andere Stücke gleicher Menge ersetzt werden. So sind beispielsweise zwei 100-Euro-Scheine beliebig austauschbar, da sie keine besonderen individuellen Merkmale besitzen, die einen Schein wertvoller machen als den anderen.

2. Recheneinheit

Die Einteilung von Geld in bestimmte Einheiten erlaubt es, Waren und Vermögenswerte in einer generellen Bezugsgröße zueinander auszudrücken. Dadurch lassen sich verschiedene Güter vergleichen und ihr Wert abschätzen. Das Geld dient dabei als Recheneinheit und als Maßstab zur Bewertung. Statt beispielsweise das Tauschverhältnis von Kartoffeln gegen Äpfel zu kennen, muss der Käufer nur noch den Preis von Kartoffeln und Äpfeln wissen. Er kann dadurch den Wert beider Güter abwägen und durch Geld gegeneinander tauschen. Um diese Funktion erfüllen zu können, muss Geld in ausreichende und praktikabel teilbare Einheiten untergliedert sein.

3. Wertspeicher

Beim direkten Tausch zweier Güter werden diese meist sofort gegeneinander ausgetauscht. Durch den Einsatz von Geld kann der Austausch von Waren auch zu unterschiedlichen Zeitpunkten erfolgen. Wenn etwas heute verkauft wird und mit dem Geld erst später wieder etwas gekauft wird, dann speichert das Geld den Wert der verkauften Güter und gibt diesen später wieder frei. Dieses Prinzip wird auch beim Sparen verfolgt. Der Sparer bewahrt den Wert seiner geleisteten Arbeit oder seines verkauften Gutes, indem er das Geld nicht sofort ausgibt, sondern es später bei Bedarf wieder abruft. Um die Funktion des Wertspeichers erfüllen zu können, müssen Material und Wert des Geldes beständig sein. Damit ist neben der Wertstabilität auch die physische Stabilität des Geldes gegen jede Form der Zerstörung gemeint. Gutes Geld sollte widerstandsfähig und robust gegen Natureinwirkungen sein. Aus diesem Grund waren lange Zeit Edelmetalle die Grundlage jeglicher Währung.

Über viele Jahrhunderte hindurch war es üblich, dass jede Währung einen intrinsischen Wert hatte. Das Geldstück an sich hatte einen Wert, weil es aus Gold und Silber hergestellt war. Gold und die anderen Edelmetalle waren selten und deshalb entsprechend begehrt. Egal, ob in der Antike, im Mittelalter oder in der frühen Neuzeit, immer gab es Gold- und Silbermünzen, die einen bestimmten Wert hatten. So war es meist auch nebensächlich, woher diese Münzen kamen oder

wer sie geprägt hatte. Allein die Tatsache, dass die Münzen aus Gold oder Silber bestanden, machte sie als Zahlungsmittel wertvoll. So war beispielsweise der spanische Peso im 17. und 18. Jahrhundert eine der wichtigsten Handelsmünzen der Welt. Er wurde in Spanien und den amerikanischen Kolonien in riesigen Mengen geprägt und war weltweit akzeptiert. Noch heute heißen die Währungen vieler lateinamerikanischer Länder Peso und selbst das Dollarsymbol $ stand ursprünglich für den spanisch-mexikanischen Peso und wurde später auch für den US-Dollar verwendet.

Mit dem Aufkommen von Papiergeld änderte sich jedoch die Bedeutung und Verbreitung von Gold- und Silbermünzen. In China war das Papiergeld schon länger bekannt, aber in Europa wurde es erstmals 1483 in Spanien als Ersatz für fehlende Münzen eingesetzt. Ab 1609 gab die Bank von Amsterdam Papierscheine aus, achtete dabei aber immer auf ausreichende Deckung durch Münzen. In Deutschland wurden erstmals 1705 in Köln Papierzettel als Banknoten herausgegeben. Die ersten Papierscheine stellten noch eine Art Schuldschein dar. Die Unterzeichner, meist die ersten Banken, garantierten, eine entsprechende Menge Gold zu besitzen und auf Verlangen gegen den Papierschein einzutauschen. Somit war es nicht mehr notwendig, einen Beutel Goldmünzen mit sich herumzutragen, denn es gab ein entsprechendes Papier, das den Besitz bewies, und dieses konnte jederzeit gegen die real existierenden Münzen eingetauscht werden.

Das Vertrauen in Papiergeld beruhte lange Zeit darauf, dass das Papier nur ein Wechsel war, der jederzeit in Münzgeld umgetauscht werden konnte. Dieses Vertrauen war durch ausreichende Bestände an Gold- und Silbermünzen in den Tresoren der Banken begründet. Mit der Zeit veränderte sich die Lagerhaltung weg vom Silber, das in größeren Mengen vorkam und mehr Lagerplatz benötigte. Viele Länder setzten zur Deckung ihrer Währungen nur noch auf Gold. In Großbritannien, Deutschland, Frankreich und den USA existierte seit dem 19. Jahrhundert der reine Goldstandard. Die im jeweiligen Land im Umlauf befindlichen Banknoten konnten ab einer bestimmten gesetzlich festgelegten Mindestsumme bei der Zentralbank in Gold umgetauscht werden. Die Aufgabe der Notenbanken bestand darin, die Höhe der Goldreserven des Landes durch Käufe und Verkäufe an die Zentralbanken anderer Länder in dem Umfang zu halten, dass die Bindung der Währung an den Goldstandard gesichert war. Dadurch sollte stets eine ausreichende Menge an Gold vorhanden sein, um die Deckung des zirkulierenden Papiergeldes gewährleisten zu können.

Mit Gründung der amerikanischen Notenbank, des Federal Reserve System oder kurz Fed, durch den Federal Reserve Act im Jahr 1913 wurde das Einlöseversprechen des Papiergeldes in den USA gelockert. Es konnten nur noch 40 Prozent des aufgedruckten Wertes eines Geldscheins gegen Gold eingetauscht werden. Im Umkehrschluss konnte die US-Regier-

ung das Geldvolumen um 60 Prozent erhöhen, da der Goldvorrat nur noch 40 Prozent des Geldvolumens abdecken musste. Dies machte die Finanzierung des Ersten Weltkrieges für die USA wesentlich leichter. Die Kosten des Ersten Weltkrieges zwangen auch viele andere Länder den Goldstandard aufzugeben und mehr Papiergeld zu drucken als durch die eigenen Goldreserven gedeckt waren. Eine Rückkehr zu dem alten System goldgedeckter Währungen wurde durch die Weltwirtschaftskrise am Ende der 1920er Jahre verhindert.

Im Zuge der Weltwirtschaftskrise war die US-Regierung 1934 gezwungen, den Dollar um 41 Prozent abzuwerten, indem sie den Preis einer Feinunze Gold (= 31,1 Gramm) von 20,67 Dollar auf 35 Dollar anhob. Dadurch stieg der Wert der amerikanischen Goldreserven schlagartig um fast 70 Prozent. Der Dollar war wieder vollständig durch Gold abgesichert, obwohl der Goldvorrat der USA nicht zugenommen hatte.

1944 wurde mit dem Abkommen von Bretton Woods, an dem 44 Staaten teilnahmen, darunter alle großen Industrienationen, der Goldstandard international festgeschrieben. Der Goldpreis wurde bei 35 Dollar je Feinunze fixiert und die Währungen aller Unterzeichnerstaaten wurden an den Dollar gekoppelt. Die Notenbanken verpflichteten sich zu einem System fester Wechselkurse mit engen Schwankungsbreiten, das sie durch Währungskäufe und -verkäufe unterstützen wollten. Alle Zentralbanken der teilnehmenden Länder waren anderen Zentralbanken gegenüber verpflichtet, Devisen gegen Gold zu

einem festen Kurs von 35 Dollar pro Feinunze einzutauschen. Zur Überwachung und Kontrolle dieses Systems wurde der Internationale Währungsfonds (IWF) geschaffen.

Das Bretton-Woods-Abkommen garantierte für mehrere Jahrzehnte einen fixen Goldpreis und feste Wechselkurse. Die wirtschaftlichen Verflechtungen zwischen den Ländern wurden jedoch immer enger und im Rahmen des Kalten Krieges mussten die USA nicht nur für viele Länder Wirtschafts- und Aufbauhilfe leisten, sondern auch die Kriege in Korea und Vietnam finanzieren. Die amerikanische Außenpolitik, die vielfältige Zahlungen an befreundete Staaten leistete, um diese für sich und gegen die Sowjetunion einzunehmen, hatte einen beständigen Dollarstrom aus den USA in andere Länder zur Folge.

Das System von Bretton Woods geriet zunehmend in Schieflage. Vor allem Frankreichs Präsident Charles de Gaulle war gegenüber dem US-Dollar sehr misstrauisch. Frankreich begann deshalb verstärkt Dollar bei der US-Notenbank gegen Gold zu tauschen. 1966 wurden durchschnittlich zehn Tonnen Gold pro Woche von New York nach Paris transportiert. Ob der Transport per Flugzeug, Schiff oder U-Boot abgewickelt wurde, ist unklar, aber der Transport an sich war bereits ein Novum. Die Zentralbanken der anderen Länder begnügten sich damit, das durch Umtausch von Dollar erworbene Gold einfach in ihre bei der New Yorker Filiale der Fed reservierten Tresorräume schaffen zu lassen. Nur Frankreich bestand

auf der Auslieferung realen Goldes. So ist es nicht verwunderlich, dass der Goldvorrat der USA in den 1960er-Jahren kontinuierlich dahinschmolz und historische Tiefstände erreichte.

Anfang der 1970er-Jahre konnten die USA ihre Verpflichtung, den Goldpreis bei 35 Dollar pro Unze zu halten, nicht mehr erfüllen. Das Land hatte nicht mehr genügend Gold, um all die weltweit zirkulierenden Dollar zu decken. Im Jahr 1971 kündigte Präsident Richard Nixon das Bretton-Woods-Abkommen, die Goldpreisbindung und das System fester Wechselkurse auf. Zukünftig sollten frei schwankende Wechselkurse den Wert der Währungen zueinander bestimmen. Dies führte in den folgenden Jahrzehnten zu größeren Schwankungen zwischen den Währungen und schuf den Devisenmarkt in seiner heutigen Form mit volatilen Wechselkursen zwischen den einzelnen Währungen. Durch die freien Wechselkurse stieg der Handel der Währungen untereinander sprunghaft an. Derzeit weist der weltweite Devisenmarkt ein tägliches Handelsvolumen von etwa fünf Billionen US-Dollar auf. Mehr als ein Viertel des Handelsvolumens entfallen auf Transaktionen zwischen Euro und US-Dollar.