BITCOIN

Funktionsweise, Chancen und Risiken der digitalen Währung

Daniel Kerscher

Bitcoin

Funktionsweise, Risiken und Chancen der digitalen Währung

Daniel Kerscher

Inhaltsverzeichnis

Vorwort

Geld ist eines der wichtigsten Instrumente für die Funktion jeder modernen Gesellschaft und gleichzeitig ist es ein Spiegel der Entwicklungen und Technologien der jeweiligen Zeit. Im digitalen Zeitalter der letzten Jahre kam es deshalb zur Entwicklung von digitalen Währungen, die rein virtuell im Internet existieren.

Eine dieser Währungen ist Bitcoin. Seit der Einführung im Jahr 2009 erregt die digitale Währung nicht nur die Aufmerksamkeit von erfahrenen Internetnutzern, die Bitcoin wegen seiner technischen Finesse mögen, sondern sie bekommt auch Zuspruch von Kritikern des bestehenden Banken- und Währungssystems, die nach besseren Alternativen suchen. Bitcoin findet auch Anklang unter normalen Nutzern, denen das System eine einfache, schnelle und kostenlose Bezahlmöglichkeit bietet, aber ebenso unter Kriminellen, die die Anonymität der Bitcoin-Transaktionen zu schätzen wissen.

Bitcoin existiert noch nicht sehr lange 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, die in seiner neuen und einzigartigen Struktur liegen. Obwohl die Software zur Verwaltung der Bitcoins 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 etwa eine Zentralbank. Dadurch kann die Geldmenge nicht angehoben werden, denn das Bitcoin-System sieht eine Maximalmenge von 21 Millionen Stück vor. Neben diesem im Vergleich zu bestehenden Währungen grundlegend anders gestalteten Konzept gibt es weitere Innovationen, z.B. die für Sender und Empfänger kostenfreie und anonyme Transaktion von Guthaben sowie die Möglichkeit, Bitcoins selbst zu erzeugen.

Die digitale Währung, die bei ihrer Einführung keinen Wert hatte und innerhalb von vier Jahren einen Kurssprung auf in der Spitze fast 200 Euro vollzog, hat viele interessante und neuartige Facetten. 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 eine digitale, dezentrale und weitgehend anonym handhabbare Online-Währung, die weder durch eine Regierung noch durch eine zentrale Organisation gesteuert wird und die auch nicht durch Gold oder andere werthaltige Gegenstände gedeckt ist. Der Begriff Bitcoin bezeichnet zwei unterschiedliche Dinge, einerseits das komplette Währungssystem, das aus einem globalen Netzwerk besteht und andererseits die einzelnen Währungseinheiten darin, die Bitcoins, die inoffiziell mit BTC abgekürzt werden. Während reguläres Geld in der Regel über Banken oder bei direkten Transaktionen in bar ausgetauscht wird, werden Bitcoins durch ein sogenanntes Peer-to-Peer-Computernetzwerk 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.

Bitcoins stellen eine elektronische Kette von Signaturen dar. Diese Signaturen sind mit elektronischen Informationen verknüpfte Daten, mit denen sich ein Signaturersteller bzw. Unterzeichner wie mit einer eigenhändig geleisteten Unterschrift identifizieren lässt und die Integrität der signierten elektronischen Informationen überprüft werden kann. Die Recheneinheiten, die Bitcoins, 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)

Bitcoins werden in einem dezentralen Computernetzwerk erschaffen und durch eine auf jedem Computer installierbare Software verwaltet. Mit dieser Software, dem sogenannten Client, lassen sich die Bitcoins von einem Nutzer auf den anderen übertragen. Die Übertragung erfolgt ähnlich wie beim Online-Banking durch Überweisungen, die von jedem Gerät vorgenommen werden können, das mit dem Internet verbunden ist, egal ob Computer, Smartphone oder Tablet. Obwohl der Namensbestandteil „Coin“ (eng. *coin* = Münze) die Vermutung nahelegt, dass es sich um einzelne virtuelle Geldstück handelt, sind Bitcoins doch nur Überweisungen von digitalen Informationen. 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 so einfach wie Bargeld zu handhaben sein und gleichzeitig die Flexibilität der elektronischen Überweisung garantieren.

Bitcoin ist ein Open-Source-Programm, d.h. der Quellcode ist für jeden zugänglich und einsehbar. Trotzdem soll die völlige Anonymität der jeweiligen Eigentümer der Bitcoins garantiert werden. Dies wird durch kryptografische Schlüssel ermöglicht, die den Besitz der Bitcoins belegen. Die Kryptografie, die Wissenschaft der Verschlüsselung von Informationen, liefert wichtige Grundlagen für die Sicherheit von Bitcoin. Jede Transaktion zwischen zwei Teilnehmern am Netzwerk wird

durch eine Datenbank aufgezeichnet und mit digitalen Signaturen versehen. Das garantiert eine hohe Fälschungssicherheit. Im Gegensatz zu normalen digitalen Dateien, die beliebig kopiert oder verändert werden können, verhindert die Verwendung kryptografischer Verfahren dies bei Bitcoins. Mithilfe einer asymmetrischen kryptografischen Methode sowie der digitalen Signaturen ist es praktisch unmöglich Bitcoins zu fälschen.

Der Besitz von Bitcoins wird durch eine elektronische Geldbörse ausgewiesen, die mit der Installation des Bitcoin-Clients eingerichtet wird. Ähnlich wie eine reale Geldbörse, so muss auch die elektronische Geldbörse gegen Verlust, etwa in Form eines Festplattendefekts, aber auch gegen Diebstahl und Ausspähen durch Schadsoftware 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 abgewickelt wurden. Dadurch ist sichergestellt, dass ein Bitcoin nicht zweimal ausgegeben werden kann, indem er an unterschiedliche Empfänger geschickt wird. In der Block Chain wird nur die erste Transaktion erfasst und die zweite verworfen. Damit wird das Problem des doppelten Ausgebens ein und desselben Betrages, das viele andere digitale Währungen aufgrund der Kopierbarkeit digitaler Informationen haben, 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. Das Fehlen einer zentralen Kontrollinstanz, z.B. einer Zentralbank, ist eine der wesentlichen Eigenschaften des Bitcoin-Systems.

Zahlungen werden mit Hilfe von Adressen abgewickelt, die die Bitcoin-Software für jeden Empfänger beliebig neu generiert. Genauso wie jedes normale Konto einen bestimmten Kontostand hat, so hat auch jede Adresse einen jeweils spezifischen Bestand an Bitcoins, der bei neu generierten Adressen „0“ beträgt. Da die Adresse nur aus einer Kombination von Zahlen und Buchstaben besteht, ist damit zwar keine Identifizierung der Handelspartner möglich, aber da in der Block Chain alle Transaktionen verzeichnet werden und eine Kopie dieser Datei auf jedem Computer des Bitcoin-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 Bitcoins mehr generiert werden, jedoch sind Bitcoins auch in kleinere Einheiten bis hin zu den sogenannten Satoshis teilbar. Im Gegensatz zu den real existierenden Währungen, die beliebig durch die Notenbanken vermehrt werden können und dadurch automatisch der Inflation unterliegen, ist Bitcoin eine deflationäre Währung. Aufgrund der Obergrenze von maximal 21 Millionen Stück kommt jedem Bitcoin ein immer höherer Wert zu.

Bitcoins werden durch das sogenannte Mining erzeugt. In diesem Prozess werden die Transaktionen der Bitcoins in Blöcken verarbeitet und verifiziert. Diese Blöcke werden dann einem öffentlichen Transaktionsprotokoll, der Block Chain, hinzugefügt, in der alle erfolgreichen Transaktionen verzeichnet sind. Die Mining-Tätigkeit ist aufgrund ansteigender Schwierigkeitsgrade sehr komplex und erfordert umfangreiche technische Kenntnisse, eine große Rechenleistung sowie einen erheblichen Stromverbrauch. Für diesen Einsatz erhalten die Miner, diejenigen, die Computer und Rechenleistung zur Verfügung stellen, eine Gegenleistung, denn jeder gelöste und zur Block Chain hinzugefügte Block enthält derzeit 25 neue Bitcoins.

Der Unterschied zwischen virtuellen Währungen und Bezahlsystemen

Bitcoin ist kein weiteres Online-Bezahlsystem, wie z.B. PayPal, sondern eine komplette digitale Währung. Zwischen Online-Bezahlsystemen und digitalen bzw. virtuellen Währungssystemen gibt es einige Unterschiede. Die offizielle Definition der elektronischen Bezahlsysteme (oder auch des sogenannten E-Geldes) in Europa sieht sie als

> […] einen monetären Wert in Form einer Forderung gegen die ausgebende Stelle, der
> i) auf einem Datenträger gespeichert ist,
> ii) gegen Entgegennahme eines Geldbetrags ausgegeben wird, dessen Wert nicht geringer ist als der ausgegebene monetäre Wert,
> iii) von anderen Unternehmen als der ausgebenden Stelle als Zahlungsmittel akzeptiert wird.
> (Richtlinie 2000/46/EG des Europäischen Parlamentes und Rates vom 18. September 2000 über die Aufnahme, Ausübung und Beaufsichtigung der Tätigkeit von E-Geld-Instituten, Artikel 1, Absatz 3 b).

Obwohl es Gemeinsamkeiten gibt, z.B. die Speicherung auf einem Datenträger, unterscheiden sich die Bezahl- von den Währungssystemen in einem wichtigen Punkt. Bei den Bezahlsystemen bleibt der Betrag in der Ursprungswährung, also z.B. Euro, erhalten, während er bei den Währungssystemen in die neue Währung, also z.B. Bitcoin, getauscht wird. Daraus ergibt sich ein Wechselkurs zwischen der Online-Währung und der „realen“ Währung. Es lassen sich aber noch weitere Unterschiede im Vergleich zu digitalen Bezahlsystemen feststellen.

Digitale Bezahlsysteme, wie PayPal oder Kreditkarten, sind weit verbreitet und werden von vielen Stellen akzeptiert. Bei digitalen Währungen ist dies nicht immer der Fall, da sie meist nur in einer kleinen, oft geschlossenen Gruppe akzeptiert werden. Digitale Bezahlsysteme unterliegen der gesetzlichen Regulierung und müssen entsprechende Auflagen einhalten. Digitale Währungen sind meist nicht reguliert, da sich der Gesetzgeber aufgrund ihrer erst sehr kurzen Existenz bisher noch nicht mit ihnen befasst hat. Für digitale Bezahlsysteme bestehen meist 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 System sehr 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 keine Wechsel in eine andere Währung statt, wenn nicht ausdrücklich eine entsprechende Überweisung vorgenommen wird. Da die europäische PayPal-Niederlassung in Luxemburg eine Bankenlizenz besitzt, unterliegt PayPal auch den europäischen Aufsichts- und Regulierungsbehörden. Aufgrund der Tatsache, dass 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.

Auch die BaFin, die Bundesanstalt für Finanzdienstleistungsaufsicht, die das Finanzwesen in Deutschland reguliert, sieht Bitcoin nicht als Form eines digitalen Bezahlsystems im Sinne von PayPal oder anderen E-Geld-Systemen. Für die BaFin scheiden als

> [...] Zahlungsmittel bestimmte Werteinheiten, die in Barter-Clubs, privaten Tauschringen oder anderen Zahlungssystemen gegen realwirtschaftliche Leistungen, Warenlieferungen oder Dienstleistungen geschöpft oder wie z.B. die Bitcoins gegenleistungslos in Computernetzwerken erschaffen werden, […] aus dem Tatbestand des E-Geldes aus, auch wenn sie wirtschaftlich die gleiche Funktion wie E-Geld haben und unter Geldschöpfungsgesichtspunkten das eigentliche Potential privat generierter Zahlungsmittel stellen. (Merkblatt der BaFin: Hinweise zu dem Gesetz über die Beaufsichtigung von Zahlungsdiensten (Zahlungsdiensteaufsichtsgesetz – ZAG)).

Bemerkenswert ist, dass die BaFin in ihren Ausführungen Bitcoins und andere private Zahlungsmittel nicht generell verbietet, sondern ihren Einsatz prinzipiell erlaubt. 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 Erlaubnis muss bei der BaFin jeweils individuell beantragt werden, denn eine generelle Einwilligung ist bei einem dezentralen System wie Bitcoin schwierig, da es keine zentrale Stelle gibt, die Bitcoins herausgibt und eine Banklizenz beantragen könnte.

Abgesehen von den Ausführungen der BaFin fehlt derzeit noch eine abschließende Erklärung der Finanzbehörden, wie Bitcoin und insbesondere die durch den Kauf und Verkauf erzielten Gewinne steuerlich zu behandeln sind. Lediglich die kanadische Steuerbehörde Canada Revenue Agency (CRA) hat bereits eine Stellungnahme zum Handel mit Bitcoin herausgegeben. Nach Ansicht der CRA sind Transaktionen mit der virtuellen Währung Bitcoin steuerpflichtig. Eine Bezahlung von Gütern mit Bitcoins entspreche einem Tauschhandel, der Ankauf der virtuellen Währung selbst aber einem Wertpapierhandel. Der Tauschhandel unterliegt der Einkommenssteuer, beim Wertpapierhandel muss der steuerpflichtige Bürger eventuell anfallende Gewinne und Verluste in der Steuererklärung angeben. Ob sich diese Ansicht weltweit durchsetzen wird und auch deutsche Steuerbehörden der Auffassung ihrer kanadischen Kollegen folgen, ist derzeit noch unklar.

Die Funktionsweise des Bitcoin-Systems ist einerseits 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, sollen hier zuerst zwei andere Konzepte erklärt werden, die die Basis für Bitcoin bilden: die Kryptografie und die Funktionsweise von Geldsystemen.

Die sichere Basis: Kryptografie

Eine der Grundlagen für die Sicherheit von Bitcoin ist der Einsatz von verschlüsselten 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. Die Kryptografie entstand ursprünglich als Wissenschaft der Verschlüsselung von Informationen. Schon im alten Ägypten wurden Geheimschriften benutzt, ebenso im Mittelalter. Auch die Enigma-Maschine, die während des Zweiten Weltkrieges die Nachrichten des deutschen Militärs verschlüsselte, war ein kryptografisches Instrument.

Lange Zeit waren für die Verschlüsselung von Nachrichten nur symmetrische Systeme im Einsatz, bei denen zur Ver- und Entschlüsselung identische Schlüssel zum Einsatz kamen. So nutzte bereits der römische Feldherr Gaius Julius Caesar ein einfaches System der geheimen Kommunikation für seine militärische Korrespondenz. Caesar benutzte bei seinen geheimen Botschaften eine Verschiebung des Alphabets um drei Buchstaben, aus A wurde D, aus B wurde E und so weiter. Dieses System wurde später vielfach abgewandelt und verfeinert. Bei einem symmetrischen System erlaubte der Besitz des Schlüssels – bei Caesars System die Information, dass alle Buchstaben der Nachricht um drei Stellen im Alphabet verschoben sind – sowohl das Verschlüsseln einer Nachricht als auch das Entschlüsseln. Dazu musste die Verschlüsselungsinformation aber zwischen zwei Kommunikationspartnern auf möglichst sicherem Weg ausgetauscht werden, was zusätzliche Probleme aufwarf. Zudem wurden bei mehreren Kommunikationspartnern auch mehrere Schlüssel benötigt, wenn nicht jeder alle Nachrichten entschlüsseln sollte.

Bis in die Neuzeit hinein wurde an immer ausgefeilteren symmetrischen Verfahren gearbeitet. So konnte beispielsweise die vom französischen König Ludwig XIV. um 1700 verwendete Codierung seiner Geheimnachrichten, die sogenannte „Große Chiffre“, erst zweihundert Jahre später geknackt werden. Die Grundproblematik, die Vorlage der gleichen Schlüssel bei Sender und Empfänger der Nachricht, blieb bei all diesen Systemen immer 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 vom Schlüsselinhaber geheim gehalten werden muss und zur Entschlüsselung eingesetzt wird. So nutzen beispielsweise die im Internet weit verbreiteten Protokolle SSH, SSL/TLS oder auch HTTPS asymmetrische Kryptoverfahren. Bitcoin nutzt ebenfalls ein asymmetrisches Kryptosystem bzw. ein Public-Key-Kryptosystem, da unterschiedliche Schlüssel für die Ver- und Entschlüsselung eingesetzt werden. Ein Nutzer erzeugt ein Schlüsselpaar, das aus einem geheimen Teil (privater Schlüssel) und einem nicht geheimen Teil (öffentlicher 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 bzw. 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 große Eingabemenge auf eine kleinere Zielmenge abbildet. So ergibt z.B. der Satz „Das ist ein Passwort.“ durch die Berechnung mit dem MD5-Algorithmus den Hashwert „b6ea69ae42b92b4201056aa3c09e4735a873f48d1be3f2d0b8e4a058d49ad7b5“. Der Satz „Das ist kein Passwort.“ ergibt den völlig anders lautenden Hashwert „e687b134da0dd208a9b52e88d42eda73f7d9fff517e46a98fd3633868714c70b“, obwohl bei der Eingabe nur ein Buchstabe hinzugefügt wurde.

Die wesentliche Eigenschaft eines aus Zahlen und Buchstaben bestehenden Hashwertes ist, dass durch ihn keine Rückschlüsse auf den ursprünglichen Eingabewert möglich sein dürfen. Aus einer bestimmten Zeichenfolge lässt sich zwar immer der gleiche Hashwert berechnen, aber umgekehrt kann aus dem Hashwert nicht wieder der ursprüngliche Eingabewert errechnen 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 für die Authentisierung abgespeichert. 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 der Bitcoin-Währung 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 TAN wirkt. Dadurch ist eine sichere Übertragung von Bitcoins möglich, wie der folgende Vorgang vereinfacht zeigt:

Nutzer A schickt Nutzer B seinen öffentlichen Schlüssel.

Nutzer B fügt den öffentlichen Schlüssel von Nutzer A mit dem Betrag, den er überweisen will, zu einer Transaktion zusammen.

Nutzer B unterschreibt diese Transaktion mit seinem privaten Schlüssel und bestätigt dadurch die Transaktion an Nutzer A.

Im Bitcoin-System kann jeder, der die öffentlichen Schlüssel von A und B kennt, sehen, dass B einverstanden war, einen bestimmten Betrag an A zu senden. Da kein anderer den privaten Schlüssel von B kennt, kann nur B diese Transaktion bestätigen. Wenn später A den Betrag weiterverwenden möchte, macht er dieselben Schritte wie zuvor B. Ein Großteil der Kryptografie bei diesem Prozess wird von der Bitcoin-Software erledigt. Die Nutzer müssen lediglich den öffentlichen Schlüssel im Hintergrund austauschen und die Transaktion initiieren.

Die Funktionsweise von Geldsystemen

Obwohl das Bitcoin-System als digitale Währung konzipiert ist, weist es doch Gemeinsamkeiten mit bereits bestehenden Währungssystemen auf und auch die grundlegende Funktion des Geldes will Bitcoin erfüllen. Geld wird seit jeher für den Austausch von Waren und Dienstleistungen benutzt. Das ist der Sinn jedes Geldsystems, unabhängig von der Bezeichnung. 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. So konnte zum Beispiel innerhalb einer Dorfgemeinschaft ein Bewohner bessere Waffen herstellen, während der andere ein guter Jäger war. Der Waffenschmied konnte seine Waffen nicht essen und der Jäger konnte ohne gute Jagdwaffen nur wenig Wild erlegen. Durch einen Tauschhandel erhielt der Schmied sein Wildbret vom Jäger und dieser wiederum konnte durch gute Waffen viel mehr Wild erlegen. Beide Seiten profitierten von diesem Geschäft mit Naturalgeld. Der einstufige Tausch, Ware gegen Ware, schränkte aber viele Geschäfte stark ein, da nicht immer passende Tauschgegenstände vorhanden waren. Im Laufe der Zeit wurde 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 auch nicht verderben.

Lange Zeit waren deshalb Münzen und später Scheine weit verbreitet. Nach dem Ende des Zweiten Weltkriegs wurden in Deutschland kurzzeitig auch Zigaretten als Geld akzeptiert. Auf einigen Inseln des Pazifiks wird beispielsweise 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 z.B. beim US-Dollar, der in vielen Ländern neben der nationalen Währung als Zahlungsmitteln akzeptiert wird; sie kann national sein, wie z.B. beim britischen Pfund, das nur in Großbritannien als Zahlungsmittel gilt; aber auch regional, wie z.B. beim Chiemgauer, einer Regionalwährung im Rosenheimer Raum.

Im Zuge des Internetbooms des vergangenen Jahrzehnts kam es zur Entstehung zahlreicher Online-Communitys und sozialer Netzwerke. Einige dieser Gruppen haben eigene Währungen entwickelt, um den Austausch der in der Gemeinschaft angebotenen Waren und Dienstleistungen zu ermöglichen. Als Beispiele sind hier die „Linden Dollars“ des Onlinespiels Second Life zu nennen, aber auch die „Nintendo Points“ oder die „Microsoft Points“ für die Communitys der jeweiligen Konsolen.

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 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 ausreichend akzeptiert werden. Außerdem muss Geld fungibel sein. Diese Eigenschaft beschreibt die leichte Aus- und Umtauschbarkeit des Geldes. 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 allgemeinen Bezugsgröße auszudrücken. Dadurch lassen sich unterschiedliche Güter vergleichen und ihr Wert abschätzen. Das Geld dient 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 Äpfel kennen und kann beide Güter durch Geld gegeneinander tauschen. Um diese Funktion erfüllen zu können, muss Geld in ausreichende und praktikable Einheiten teilbar sein.

3. Wertaufbewahrungsfunktion

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 Wertaufbewahrungsmittels zu erfüllen, 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 Metalle lange Zeit die Grundlage jeglicher Währung.

Über viele Jahrhunderte hindurch war es normal, dass jede Währung einen intrinsischen Wert hatte, d.h. 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 die Bedeutung und Verbreitung von Gold- und Silbermünzen. 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 realen 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 Herausgeber des Papiergeldes begründet. Mit der Zeit veränderte sich die Lagerhaltung und viele Länder setzten zur Deckung ihrer Währungen nur noch auf Gold. In Großbritannien, Deutschland, Frankreich und den Vereinigten Staaten existierte im 19. Jahrhundert der reine Goldstandard. Die im jeweiligen Land im Umlauf befindlichen Banknoten konnten ab einer bestimmten gesetzlich festgelegten Mindestsumme in Gold umgetauscht werden. Die Aufgabe der Zentralbanken 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-Regierung das Geldvolumen um 60 Prozent erhöhen, da ihr Goldvorrat nur noch 40 Prozent des Geldvolumens abdecken musste. Dies machte z.B. die Finanzierung des Ersten Weltkrieges 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 (eine Feinunze = 31,1 Gramm) von 20,67 Dollar auf 35 Dollar anhob. Dadurch stieg automatisch der Wert der amerikanischen Goldreserven um fast 70 Prozent, sodass die Goldvorräte wieder das komplette im Umlauf befindliche Bargeld abdeckten. Dadurch war der Dollar 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 festen 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 bis zum Zusammenbruch des Kommunismus 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 deshalb zunehmend in Schieflage. Insbesondere Frankreichs Präsident Charles de Gaulle war gegenüber dem US-Dollar sehr misstrauisch. Frankreich begann deshalb verstärkt Dollar aufzukaufen und bei der US-Notenbank gegen Gold zu tauschen. 1966 wurden durchschnittlich 10 Tonnen Gold pro Woche von New York nach Paris transportiert. Ob der Transport per Flugzeug, Schiff oder U-Boot abgewickelt wurde, ist nicht bekannt, aber der Transport an sich war bereits ein Novum. Die Zentralbanken der anderen europäischen 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. 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 jetzigen Form mit volatilen Wechselkursen zwischen den einzelnen Währungen. Durch die freien Wechselkurse stieg auch der Handel der Währungen untereinander sprunghaft an. Derzeit weist der weltweite Devisenmarkt ein tägliches Handelsvolumen von ca. 4 Billionen US-Dollar auf. 28 Prozent des Handelsvolumens machen Transaktionen zwischen US-Dollar und Euro aus.

Das Ende von Bretton Woods hatte also einerseits einen freien Goldpreis und andererseits frei schwankende Wechselkurse zur Folge. Die bis dahin existierende Verbindung zwischen dem Goldpreis und den Währungen, die durch den US-Dollar und den fixen Goldpreis von 35 Dollar je Unze bestanden hatte, existiert seitdem nicht mehr. Dies führte dazu, dass die Währungen nicht mehr durch Gold gedeckt werden mussten und die Zentralbanken aller Länder einfach Geld drucken konnten. Die Währungen wurden dadurch zu Fiat-Währungen (lat. *fiat* = es werde), die auf dem Vertrauen der Bürger in die Wirtschaftskraft und Leistungsfähigkeit des Staates beruhen.

Jede derzeit existierende Währung ist eine Fiat-Währung, d.h., eine Regierung oder eine Zentralbank hat beschlossen, dass eine Währung entstehen wird. Es handelt sich um Fiat-Geld, das auf dem Vertrauen in die Kreditwürdigkeit einer Regierung beruht. Die Regierungen wiederum finanzieren sich hauptsächlich über Steuereinnahmen ihrer Bürger. Die Bürger wiederum vertrauen darauf, dass das von der Regierung bzw. dem Staat ausgegebene Geld seine Funktionen erfüllen kann und vor allem dass es seinen Wert behält. Wie wenig Vertrauen in die frei schwankenden Währungen bestand, zeigt der Goldpreis, der 1980, neun Jahre nach dem Ende des Bretton-Woods-Abkommens, von 35 auf 850 Dollar je Feinunze gestiegen war.

In den letzten Jahren entwickelten sich die frei schwankenden Wechselkurse zunehmend zu einer politischen Waffe, nämlich dann, wenn einzelne Länder ihre Währungen abwerten, indem sie vermehrt Geld drucken. Schwache Währungen machen die eigenen Waren auf ausländischen Märkten günstiger und befeuern den Export. In einer zunehmend exportorientierten Weltwirtschaft löst dies einen „Währungskrieg“ zwischen wirtschaftlich starken Nationen aus, die sich darum bemühen, die

jeweils schwächste Währung zu haben, um den eigenen Export zu unterstützen. Gleichzeitig leidet darunter die einheimische Bevölkerung, die mit der schwachen Währung entlohnt wird und die sich dadurch immer weniger leisten kann. Die Abwertung der eigenen Währung lässt sich am besten über die Notenpresse und das größere Angebot der eigenen Währung erreichen. Wenn die neu geschaffene Geldmenge den freien Markt erreicht, führt dies zu einer zunehmenden Inflation.

Den Prozess der Inflation und Geldentwertung will das Bitcoin-System verhindern. Genau wie die Edelmetalle, die lange Zeit die Grundlage jeder Währung bildeten, sind auch Bitcoins limitiert. Durch die Begrenzung der Bitcoin-Menge auf 21 Millionen Stück, die in der Software festgeschrieben sind, kann es nicht zu einer ständigen Neuschaffung von Bitcoins kommen. Die Limitierung der Bitcoin-Menge kann aber einen deflationären Prozess entstehen lassen, d.h. aufgrund der Begrenztheit wird jeder Bitcoin immer wertvoller und kann gegen immer mehr Waren eingetauscht werden.

Im Gegensatz zu den bestehenden Fiat-Geldsystemen, die in ihrer Natur inflationär sind, setzt das Bitcoin-System auf Deflation. Neben dieser grundlegend anders ausgelegten Konzeption greift die digitale Währung auch einige Ideen der sogenannten Österreichischen Schule der Ökonomie auf. Dieser Zweig der Volkswirtschaftslehre wird durch österreichische Ökonomen wie Ludwig von Mises und Friedrich August von Hayek vertreten. Wesentliche Eckpunkte dieser Strömung der Volkswirtschaftslehre sind die Betrachtung der dynamischen Unsicherheit wirtschaftlicher Abläufe, die Bedeutung des einzelnen Menschen und seiner individuellen Vorlieben für die wirtschaftlichen Prozesse sowie eine gewisse Abneigung gegenüber der in vielen ökonomischen Theorien verbreiteten mathematischen Darstellungsform volkswirtschaftlicher Zusammenhänge.

Einer der bedeutendsten Vertreter der Österreichischen Schule war der Wirtschaftswissenschaftler Ludwig von Mises, der 1940 in die USA emigriert war und dort von 1945 bis 1969 an der New York University lehrte. Er entwickelte eine Konjunkturtheorie, gemäß der die Verantwortung für die sich abwechselnden Konjunkturzyklen – Aufschwung, Boom, Rezession und Depression – bei den Banken und Zentralbanken sowie der von ihnen betriebenen Geldschöpfung lag. Durch diese Institutionen werden Kredite aus dem Nichts geschaffen und unkontrolliertes Geldwachstum gefördert. Verstärkt durch künstlich niedrige Zinsraten, Inflation und Kreditexpansion wird dadurch das gesamte Preissystem verzerrt. Der Preis an sich kann seine Funktion der Information über Knappheit eines Gutes nicht mehr erfüllen. Außerdem werden durch ständig verfügbares günstiges Kapital ineffiziente Produktionsweisen künstlich am Leben gehalten. Da sich aber die Fehlinvestitionen irgendwann wieder an die Realität angleichen, sind Krisen und Rezessionen die Folge. Die Weltwirtschaftskrise der 1930er-Jahre war für von Mises das Ergebnis monetärer Fehlentscheidungen in den 1920er-Jahren, vor allem der Geldmengenausweitung durch Inflation. Nach von Mises Ansicht ist der moderne Stand der Produktion durch freies Wirtschaften entstanden und nur damit kann er auch erhalten werden. Staatliche Interventionen lehnte er ab, denn wenn der Staat einmal eingreift, würde er das immer wieder tun. Letztendlich führen für von Mises die wiederholten staatlichen Interventionen zum Sozialismus, der wiederum eine Senkung des allgemeinen Wohlstands zur Folge hätte.

Auch für den österreichischen Ökonom und Sozialphilosophen Friedrich August von Hayek entstand die Weltwirtschaftskrise zwischen 1928 und 1930 nicht als Folge zu geringer Nachfrage, sondern durch Fehlinvestitionen der Unternehmen und Banken. Diese Fehlinvestitionen beruhten in letzter Konsequenz auf der verfehlten Geld- und Wirtschaftspolitik der Staaten. Staatliche

Interventionen auf dem freien Markt, wie sie etwa vom britischen Ökonomen John Maynard Keynes gefordert wurden, waren für Hayek nicht die Lösung, sondern vielmehr die Ursache der Wirtschaftskrise, denn die staatliche Inflationspolitik vor 1929 hat den Zusammenbruch der Wirtschaft erst heraufbeschworen.

Nach Hayeks Theorie basieren die Konjunkturzyklen auf der Abweichung des Geldzinssatzes vom natürlichen Zinssatz, der bestehen würde, wenn die Geldmenge nicht durch exzessive Kreditvergabe ausgeweitet worden wäre. Die Differenz zwischen den beiden Zinssätzen muss durch zusätzliche Liquidität gedeckt werden. Dieses Überangebot an Fiat-Geld hat eine Ausweitung von Bankkrediten in Verbindung mit niedrigen Zinsen zur Folge. Die gesunkenen Kapitalkosten, das „billige“ Geld, veranlasst die Unternehmer zu immer riskanteren Investitionsprojekten, die nicht mehr an der Nachfrage der Konsumenten orientiert sind und die zuvor nicht rentabel gewesen wären. Die Wirtschaftsleistung weitet sich durch die gestiegene Investitionstätigkeit stärker aus, als es im natürlichen Fall möglich gewesen wäre. Da sich die Unternehmer nicht mehr an den Konsumenten orientieren, vernachlässigen sie die Produktion entsprechender Konsumgüter. Der verringerten Konsumgüterproduktion steht aber eine gleichbleibende Nachfrage der Verbraucher gegenüber. Dies führt zu steigenden Preisen. Dieses wachsende Ungleichgewicht, das sich durch Spekulationsblasen noch verstärkt, kann nur durch einen harten Anpassungsprozess wieder ausgeglichen werden, was letztendlich eine Rezession zur Folge hat. Die wegbrechende Nachfrage in der Rezession zwingt die Unternehmer dazu, ihre Produktionsmittel wieder an die Wünsche der Kunden anzupassen bevor der Zyklus von neuem beginnt und das reichlich verfügbare Fiat-Geld wieder riskantere Investitionen zulässt. Da ein Überangebot an jederzeit vermehrbarem Fiat-Geld die Grundlage dieser Entwicklung darstellt, sprechen sich die Vertreter der Österreichischen Schule für eine Begrenzung der Geldmenge und die Rückkehr zum Goldstandard aus.

Hayek lehnte eine Zentralverwaltungsgesellschaft und staatliche Eingriffe in den freien Markt im Allgemeinen ab. Jede noch so kleine Einmischung ziehe über kurz oder lang weitere staatliche Interventionen nach sich. Aus dieser Spirale von staatlichen Eingriffen folgen letztendlich Planwirtschaft und Diktatur. Hayek stellte in seinen Werken die Gefahren des Sozialismus dar, da jede Form von Kollektivismus und Sozialismus zum Abbau individueller Freiheit führt. Er sagte aber auch den Niedergang solcher totalitärer staatlicher Systeme voraus und der Zusammenbruch der kommunistischen Systeme um 1990 gab ihm Recht.

Hayek und die anderen Vertreter der Österreichischen Schule sehen in einem staatlichen Geldsystem, das sie auch als Papier-, Fiat- oder Schein-Geldsystem bezeichnen, die Ausweitung der Staatsaktivität als sehr kritisch an. Vor allem den Zentralbanken, die immer auch in Verbindung zur Politik stehen, kann es aus eben diesen politischen Verpflichtungen nicht gelingen, den Geldwert in einem Maß stabil zu halten, mit dem sich Krisen vermeiden lassen. Aus diesem Grund sprach sich Hayek dafür aus, die Produktion von Zahlungsmitteln in private Hände zu legen. In seinem Werk „Denationalisation of Money“ stellte er sich, getreu seiner Abneigung gegen jede Form der zentralen Planung und staatlichen Intervention, gegen das Monopol der Regierungen bzw. der Zentralbanken bei der Ausgabe von Geld. Dagegen sollten auch private Banken Zertifikate ausgeben können, die im freien Wettbewerb miteinander stehen.

Aus diesen nur sehr verkürzt dargestellten Ideen der Österreichischen Schule lassen sich einige Grundgedanken ableiten, die sich im Bitcoin-System wiederfinden:

Zentralbanken sollten kein Monopol auf die Geldschöpfung haben.

Die Geldmenge sollte nicht beliebig vermehrbar sein, sondern im Sinne eines Goldstandards begrenzt werden.

Die Entwicklung des Bitcoin-Systems

Das Konzept einer dezentralen Währung, die weder von Banken noch von Regierungen kontrolliert und mit der anonym umgegangen werden kann, ist schon länger bekannt. Bereits in den 1970ern wurde über verschlüsselte digitale Währungssysteme nachgedacht. 1990 gründete David Chaum das Unternehmen DigiCash, das ein elektronisches Zahlungssystem anbot. Mit dem System „eCash“ sollten vor allem kleinere Zahlungen abgewickelt werden. Innovativ war die Verwendung kryptografischer Protokolle, die die Anonymität der Benutzer garantieren sollten. Das System konnte sich jedoch nicht durchsetzen. Auch die digitalen Bezahlsysteme „b-money“ und „bit gold“, die zu dieser Zeit entstanden, fanden keine ausreichende Verbreitung, was wohl auch an der Frühzeit des Internet und den im Vergleich zur heutigen Zeit wesentlich geringeren Nutzerzahlen lag. Diese erfolglosen Versuche, eine digitale Währung zu schaffen, lieferten jedoch etliche Anregungen für Bitcoin.

Das Konzept der Bitcoin-Währung wurde erstmals am 31. Oktober 2008 von Satoshi Nakamoto in einem Aufsatz vorgestellt. Ob es sich bei Satoshi Nakamoto um eine reale Person oder das Pseudonym einer einzelnen Person oder einer Personengruppe handelt, ist bis heute unklar, denn er ist niemals öffentlich in Erscheinung getreten. Auf den ersten Blick erscheint Vertrauen in ein System, das von einer anonymen Person entwickelt wurde, nicht angebracht, denn niemand kennt die Interessen, die hinter dem Pseudonym Satoshi Nakamoto stehen. Dennoch ist Transparenz gegeben, denn die komplette Software ist nach dem Open-Source-Prinzip frei zugänglich, und auch die dahinter stehende Logik ist in Nakamotos Beitrag ausführlich dargestellt worden. In diesem Aufsatz beschreibt er das Grundproblem jeder modernen Währung und er versucht gleichzeitig eine Lösung dafür anzubieten:

> Das Kernproblem konventioneller Währungen ist das Ausmaß an Vertrauen, das nötig ist, damit sie funktionieren. Der Zentralbank muss vertraut werden, dass sie die Währung nicht entwertet, doch die Geschichte des Fiat-Geldes ist voll von Verrat an diesem Vertrauen. Banken muss vertraut werden, dass sie unser Geld aufbewahren und es elektronisch transferieren, doch sie verleihen es in Wellen von Kreditblasen mit einem kleinen Bruchteil an Deckung. Wir müssen den Banken unsere Privatsphäre anvertrauen, vertrauen dass sie Identitätsdieben nicht die Möglichkeit geben, unsere Konten leer zu räumen. Ihre massiven Zusatzkosten machen Micropayments unmöglich.
> Eine Generation früher hatten Nutzer von Time-Sharing Computersystemen ein ähnliches Problem. Vor dem Aufkommen von starker Verschlüsselung mussten die User sich auf Passwortschutz für ihre Daten verlassen und dem Systemadministrator vertrauen, dass dieser ihre Informationen vertraulich hielt. Diese Privatsphäre konnte jederzeit aufgehoben werden, wenn der Administrator zu dem Schluss kam, dass sie weniger wog als andere Belange, oder auf Anweisung seiner Vorgesetzten. Dann aber wurde starke Verschlüsselung für die Masse der Nutzer verfügbar, und Vertrauen war nicht länger nötig. Daten konnten auf eine Weise gesichert werden, die einen Zugriff durch Dritte – egal aus welchem Grund, egal mit wie guten Entschuldigungen, egal was sonst – unmöglich machten.
> Es ist Zeit, dass wir dieselbe Sache für Geld haben. Mit einer e-Currency basierend auf einem kryptografischen Beweis, ohne Notwendigkeit Mittelsmännern zu vertrauen, kann Geld sicher sein und mühelos transferiert werden. (Deutsche Übersetzung entnommen aus: *http://de.wikipedia.org/wiki/Bitcoin*).

Nakamoto beschreibt in seinen Ausführungen das Grundproblem jeder Transaktion zwischen unbekannten Partnern. Eine der beiden Seiten muss der anderen Seite Vertrauen entgegenbringen, um eine Transaktion in Gang zu setzen. In regulären Währungssystemen bringen die Menschen dieses „Grundvertrauen“ den Regierungen und Zentralbanken entgegen. Sie vertrauen darauf, dass die von diesen Institutionen herausgegebenen Papierscheine einen gewissen Wert haben und akzeptieren es als Geld. Das Bitcoin-Konzept ist entgegengesetzt ausgelegt, indem es keine zentrale Institution hat, der man vertrauen muss.

Basierend auf diesem Konzept, entstand das Bitcoin-Netzwerk mit der ersten Version des Bitcoin-Clients „bitcoind“, der die ersten Bitcoins auf einem normalen PC erzeugte. Der sogenannte „Genesis Block“ mit den ersten 50 Bitcoins wurde am 3. Januar 2009 von Satoshi Nakamoto generiert. Die ersten Bitcoins hatten noch keinen Bezugspunkt, deshalb wurde ihr Wert unter den ersten Teilnehmern des Netzwerks ausgehandelt. Sobald sich jemand fand, der den Preis eines Bitcoin in einer anderen Währung oder in Waren bzw. Dienstleistungen akzeptierte, war der Bitcoin-Markt entstanden. Dennoch war das Bitcoin-Projekt im Jahr 2009 nur einem kleinen Kreis von Internetnutzern bekannt. Dieser Kreis betrieb hauptsächlich Handel untereinander und befasste sich mit der Weiterentwicklung der Software. Bitcoin war ein Nischenprojekt, das Raum für Experimente bot. So wurden am 21. Mai 2010 in einem mittlerweile legendären Handel von einem Nutzer 10.000 Bitcoins für die Lieferung zweier Pizzas bezahlt. Damals entsprach dies einem Betrag von ca. 25 Dollar. Legt man dagegen den Höchstkurs vom April 2013 zugrunde, zahlte der Nutzer für seine zwei Pizzas über 2,6 Millionen Dollar.

Einen wesentlichen Schub erfuhr Bitcoin am 17. Juli 2010, als die Online-Plattform Mt.Gox eröffnet wurde. Damit war eine zentrale, leicht zugängliche Handelsplattform geschaffen worden, um Bitcoin in andere Währungen, wie Dollar und Euro, tauschen zu können. Einen Rückschlag gab es am 15. August 2010 als eine ernsthafte Sicherheitslücke im Bitcoin-System entdeckt wurde. Transaktionen wurden nicht ordnungsgemäß verifiziert, bevor sie in die öffentlich zugängliche Block Chain geschrieben wurden. Dadurch war es möglich, die Einschränkungen des Systems zu umgehen und beliebig viele Bitcoins zu generieren. Diese Lücke wurde ausgenutzt, als 184 Milliarden Bitcoins an zwei Adressen des Netzwerkes übertragen wurden. Das entsprach der 8762fachen Menge aller jemals im System existierenden Bitcoins. Die Transaktion wurde nur wenige Stunden danach im System bemerkt und die Sicherheitslücke sofort geschlossen. Die fälschlich erzeugten Bitcoins wurden gelöscht und bis heute blieb dies die einzige ernsthafte Sicherheitslücke im Bitcoin-System.

Am 6. November 2010 erreichte die Bitcoin-Notierung bei Mt.Gox den Wert von 0,50 US-Dollar, was den Wert der im Umlauf befindlichen Bitcoins auf 1 Million US-Dollar katapultierte. Im Februar 2011 lag der Kurs bereits bei 1 US-Dollar für einen Bitcoin. Der Kursanstieg setzte sich rasant fort und erreichte am 8. Juni den neuen Höchststand von 31,91 Dollar pro Bitcoin. Mittlerweile hatte auch die Zahl der Nutzer der Clientsoftware zugenommen, die Mitte 2011 bei ca. 60.000 lag. Im Juni 2011 kam es zu einem Hackerangriff auf die Handelsplattform Mt.Gox, was einen dramatischen Preiseinbruch zur Folge hatte. Der Kurs stürzte auf kurzzeitig auf 0,01 Dollar ab, da durch den Angriff sowohl Nutzerdaten und Bitcoins gestohlen worden waren als auch viel Vertrauen in die neue Währung verloren gegangen war. Danach wurde es ruhiger um Bitcoin und der Kurs stabilisierte sich auf niedrigem Niveau.

2012 kam es ab der zweiten Jahreshälfte zu einer Kurserholung, die sich auch 2013 fortsetzte.

Inzwischen berichteten auch die Medien verstärkt über das Thema Bitcoin. Ob die digitale Währung im Zusammenhang mit der Eurokrise und insbesondere mit der Zypernkrise als Fluchtmöglichkeit für Sparguthaben angesehen wurde, ist unklar. Jedenfalls erreichte der Kurs am 28. Februar 2013 sein altes Allzeithoch von 31,91 Dollar, um danach weiter anzusteigen, bis er am 10. April seinen bisherigen Höchststand von 266 US-Dollar erreichte. An diesem Tag brach die Handelsplattform Mt.Gox zusammen. Offiziell lautete die Begründung, dass sich zu viele neue Nutzer angemeldet hätten. Als der Handel wieder möglich war, brach der Kurs innerhalb weniger Tage auf 55 Dollar ein, um dann wieder auf 150 Dollar zu steigen. Derzeit hat sich der Kurs bei ca. 100 bis 120 Dollar stabilisiert (Stand: Juni 2013).

Eine elektronische Geldbörse für Bitcoin

Grundlage des Bitcoin-Systems und sämtlicher Transaktionen ist eine Client-Software, die auch als Wallet (eng. *wallet* = Brieftasche) bezeichnet wird. Die Software ist vergleichbar mit einer Geldbörse oder einem Bankkonto. Aber im Gegensatz zu einer Kontoeröffnung erfolgt die Nutzung der Software anonym. Für den Download und die Installation müssen keine persönlichen Angaben gemacht werden, auch die Erzeugung von Adressen funktioniert ohne das Einrichten eines Benutzerkontos. Es werden keine persönlichen Daten abgefragt und es ist auch keine Bonitätsprüfung erforderlich, um eine Bitcoin-Wallet eröffnen zu können.

Die Bitcoin-Software verfügt über eine grafische Benutzeroberfläche, „bitcoin“, und eine reine Kommandozeileneingabe, „bitcoind“. Für die meisten Zwecke ist die grafische Oberfläche einfacher und schneller zu bedienen. Jeder Bitcoin-Client stellt eine spezielle Implementierung des von Satoshi Nakamoto entwickelten Bitcoin-Protokolls dar. Ausgehend von der ursprünglichen Clientversion, gibt es mittlerweile mehrere Programme, die sich je nach Funktionsumfang und Bedienung unterscheiden.

bitcoin-qt: Bei dieser Software handelt es sich um die Weiterentwicklung des Originalclient mit der gesamten Basisfunktionalität. Nach der Installation wird die vollständige Block Chain heruntergeladen, deshalb kann es anfangs mehrere Stunden dauern, bis die Software einsatzbereit ist. Es gibt Versionen für Windows, Linux, Mac OS X unter *http://sourceforge.net/projects/bitcoin*.

Multibit: Dieser Client ist auf einfache Bedienung, hohe Geschwindigkeit und geringen Ressourcenbedarf ausgelegt. Es gibt Versionen für Windows, Linux, Mac OS X unter *https://multibit.org*.

Electrum: Ein Vorteil dieser Version ist die Nutzung von Guthaben auf mehreren Geräten. Neben den Versionen für Windows, Linux, Mac OS X gibt es auch eine Version für das Smartphone-Betriebssystem Android unter *http://electrum.org*.

Bitcoin Wallet: Die Software ist auf einfache Bedienung und hohe Sicherheit ausgerichtet, unabhängig von Servern und Web Services. Es gibt Versionen für Android (*https://play.google.com/store/apps/details?id=de.schildbach.wallet*) und Blackberry OS (*http://appworld.blackberry.com/webstore/content/23952882*).

Armory: Dabei handelt es sich um eine Erweiterung des Original-Client bitcoin-qt mit zusätzlichen Sicherheitsfunktionen für erfahrene Nutzer, einer Export/Import-Funktion für Schlüssel. Es gibt Versionen für Windows und Linux unter *https://bitcoinarmory.com*.

Auf der Website *http://de.wikipedia.org/wiki/Bitcoin#Bitcoin-Clients* finden sich noch weitere Informationen und technische Details zu den einzelnen Clients.

Es gibt zwei unterschiedliche Arten von Clients. Programme wie bitcoin-qt laden die vollständige Block Chain herunter. Die Datei hat eine Größe von ca. 7,5 Gigabyte (Stand: Juni 2013), deshalb kann der Download einige Zeit in Anspruch nehmen. Dadurch werden alle bis abgewickelten Transaktionen des Netzwerks auf dem Rechner gespeichert. Solche Clients unterstützen die Funktionsfähigkeit des gesamten Netzwerks und machen dadurch Angriffe oder Manipulationsversuche schwieriger. Die Speicherung der kompletten Block Chain dauert aber einige Stunden, nimmt mehrere Gigabyte Speicherplatz in Anspruch und muss zudem ständig aktualisiert

werden. Bereits nach wenigen Tagen ohne Aktualisierung dauert es wieder einzige Zeit, bis die Software die seitdem angefallenen Blöcke wieder heruntergeladen hat. Clients wie z.B. Multibit setzen auf ein anderes Konzept. Sie laden nicht die komplette Block Chain herunter, sondern gleichen nur zentrale Inhalte mit der kompletten Datei ab, die auf Remote Servern gespeichert ist. Sie sind deshalb schneller einsatzbereit und für den Einstieg ideal. Zudem sparen sie Speicherplatz und bieten sie einige Komfortfunktionen, die der Basisversion fehlen, z.B. die Anzeige des aktuellen Bitcoin-Kurses bei Mt.Gox.

Die grafischen Oberflächen der einzelnen Programme unterscheiden sich zwar, aber alle bieten zumindest die Anzeige des Guthabenstandes (Nr. 1 im Bild), die Möglichkeit, Bitcoins an andere Adressen zu senden (Nr. 2 im Bild), die Möglichkeit, eigene Adressen zu erzeugen (Nr. 3 im Bild) und diese mit bestimmten Bezeichnungen zu versehen, um eine leichtere Zuordnung der empfangenen Bitcoins vornehmen zu können. Zudem gibt es eine Transaktionsübersicht (Nr. 4 im Bild) und ein Adressbuch (Nr. 5 im Bild).

Oberfläche des Multibit-Client

Quelle: *https://multibit.org*

Bei der Installation der Software werden automatisch Adressen generiert, mit denen Bitcoins empfangen werden können. Alle Adressen mit ihren öffentlichen und privaten Schlüsseln werden in der Datei „wallets.dat“ gespeichert. Diese Datei ist das Herzstück der Software und gleichzeitig die tatsächliche Geldbörse. Wenn diese Datei gelöscht oder verloren wird, sind auch alle Bitcoins, die mit den darin gespeicherten Adressen verknüpft sind, verloren.

Neben den Clientversionen für den PC gibt es auch für die Android-Plattform mehrere Open-Source-Implementationen, wie etwa „Bitcoin Wallet“ (*https://github.com/schildbach/bitcoin-wallet*). Die Android-Versionen verfügen über Zusatzeigenschaften, die für den mobilen Betrieb nützlich sind. So kann eine Bitcoin-Adresse des Wallets auf dem Smartphone als QR-Code angezeigt werden, der einen speziellen Uniform Resource Identifier mit der benötigten Bitcoin-Adresse sowie dem Betrag enthält. Für Zahlungen können QR-Codes mit der Kamera eines anderen Smartphones gescannt werden. Es ist zudem bei nicht bestehender Internetverbindung möglich, Zahlungen später zu versenden.

Parallel zu den plattformbasierten Clients existiert eine Vielzahl von Webdiensten, die Online-Wallets anbieten. Das Bitcoin-Guthaben wird dabei vollständig an eine Adresse innerhalb des eigenen Kontos beim Anbieter der Plattform übertragen. Die Sicherheit der Guthaben hängt hier aber

vollständig von der serverseitigen Sicherheit und der nicht immer gegebenen Vertrauenswürdigkeit der Betreiber ab.

Die Speicherung von Bitcoins in Online-Wallets schützt vor dem Risiko eines Datenverlustes durch einen Hardwaredefekt des heimischen Computers und gleichzeitig sind die Bitcoins überall verfügbar, nicht nur auf dem Gerät, an das sie gesendet wurden. Aber der Betreiber des Online-Wallets erhält ebenfalls Zugriff auf die eigenen Bitcoins. Zudem besteht auch bei Online-Wallets die Gefahr eines Hackerangriffs und des Diebstahls der gespeicherten Bitcoins. Die Entwicklung der Online-Wallets schreitet aber rasch voran und auch die Sicherheit wird verbessert. Eine Übersicht der Online-Wallets findet sich unter: *https://en.bitcoin.it/wiki/Category:EWallets*.

Eine Alternative für mobile Plattformen, für die kein regulärer Client angeboten wird, sind hybride Wallets, wie z.B. die von blockchain.info angebotene My-Wallet-Websoftware (*https://blockchain.info/wallet*) Bei dieser wird der auszuführende Code vom Server des Anbieters geladen, die geheimen Schlüssel werden jedoch clientseitig verschlüsselt und übertragen. Eine Übersicht der Anbieter von Hybrid-Wallets ist zu finden unter: *https://en.bitcoin.it/wiki/Category:HybridEWallets*.

Die in der Wallet gespeicherten Bitcoin-Adressen beinhalten einen öffentlichen und einen privaten Schlüssel. Während der öffentliche Schlüssel zum Empfangen von Beträgen weitergegeben werden kann, muss der private Schlüssel streng vertraulich behandelt werden, denn er ermöglicht die Bestätigung sämtlicher Transaktionen innerhalb einer Wallet, also auch die Übertragung des gesamten Bitcoin-Guthabens an andere Adressen. Bei der Generierung neuer Adressen wird zuerst ein privater Schlüssel erzeugt, auf dessen Basis durch den ECDSA (Elliptic Curve Digital Signature Algorithm) ein öffentlicher Schlüssel erzeugt wird. Aufgrund der Komplexität des Algorithmus kann durch den öffentlichen Schlüssel kein Bezug auf den privaten Schlüssel genommen werden. Durch die Berechnung mit den Verschlüsselungsmethoden SHA256 und RIPEMD-160 wird aus dem öffentlichen Schlüssel die Adresse generiert, die beispielsweise folgendermaßen aussieht.

14tbYhU9Ca2ZABBcePCP8VjaRVASvsfi7c

Adressen sind zwischen 27 und 34 Zeichen lang und bestehen nur aus Buchstaben und Ziffern. Sie beginnen immer mit 1 oder 3. Die dazugehörigen öffentlichen und privaten Schlüssel werden in der wallet.dat-Datei der Clientsoftware gespeichert. Derartige Adressen können von der Software beliebig oft erzeugt werden. Die Adressen werden nicht zentral registriert oder gespeichert, sondern nur für die Transaktionen erzeugt und genutzt. Durch Verwendung jeweils spezifischer Adressen für unterschiedliche Bitcoin-Sender lässt sich eine leichte Zuordnung der Zahlungsströme vornehmen. Diese Zuordnung ist aber nur dem Empfänger der Bitcoins möglich, der dem Sender die entsprechende Adresse mitgeteilt hat. Allein durch die Adresse ist nicht feststellbar, wem sie gehört oder wo sie sich befindet. Nur derjenige, der die Adresse erzeugt hat, weiß, dass sie ihm gehört.

Zwar wird durch die Adressen weitgehende Anonymität gewährleistet, aber gleichzeitig liegt mit der Block Chain ein öffentliches Verzeichnis aller bisher abgewickelten Transaktionen vor. Durch eine Kombination mit weiteren Informationen wie z.B. IP-Adressen oder der Informationen aus Emails mit denen zuvor Adressen ausgetauscht wurden, wäre die Identifikation einzelner Nutzer denkbar. Dieses Verfahren ist allerdings extrem aufwändig und nur von staatlicher Seite legal durchführbar. Denkbar wäre dieses Vorgehen, um die Beteiligten an illegalen Geschäften zu identifizieren.

Die Adressen können nicht nur als Folge von Zahlen und Ziffern dargestellt werden, sondern auch als Barcode und in Form von QR-Codes. Dadurch eignen sie sich auch für den mobilen Einsatz mit Smartphones. Um eine Zahlung von einem Smartphone vorzunehmen, genügt es, den Betrag einzutippen und dem Empfänger den QR-Code, der von einer Client-App erzeugt wird, zu zeigen. Der Empfänger scannt den Code mit der Kamera seines Handys und wartet auf die Bestätigung der Transaktion durch das Netzwerk.

Bitcoin-Transaktionen haben eine andere Funktionsweise als Bargeldtransaktionen. Bargeld kennt nur den aktuellen Besitzer und weist keine Verlaufsgeschichte aller vorangegangenen Transaktionen auf. Eine Bitcoin-Transaktion ist hingegen eine Fortführung vorangegangener Transaktionen. Durch Transaktionen werden einer oder mehreren Adressen Bitcoins gutgeschrieben, die selbst wiederum von einer oder mehreren Adressen aus dem Netzwerk stammen. Die Bitcoins existieren nicht als eigenständige Objekte im Netzwerk. Stattdessen verwaltet das Netzwerk bzw. die allen zugängliche Block Chain die Transaktionen der Bitcoins, sowohl die der Nutzer untereinander als auch die Transaktionen bei der Entstehung neuer Bitcoins. Eine Transaktion besteht aus einem oder mehreren Inputs und zwei oder mehr Outputs. Die Inputs verweisen dabei auf die Outputs vergangener Transaktionen, die dem Aussteller der aktuellen Transaktion geschickt wurden. Sie werden zusammengerechnet und bilden Gesamtmenge an Bitcoins, die auf die Outputs verteilt werden kann. Bei einer Transaktion wird diese Menge durch mindestens einen Output an einen neuen Besitzer verschickt. Es ist zudem möglich, mit einer Transaktion Bitcoins an mehrere Empfänger zu versenden. Besteht eine Differenz zwischen der Summe an Bitcoins bei den Inputs und der Summe bei den Outputs, so wird sie als Transaktionsgebühr verstanden und geht an diejenigen, die die Transaktion bestätigen.

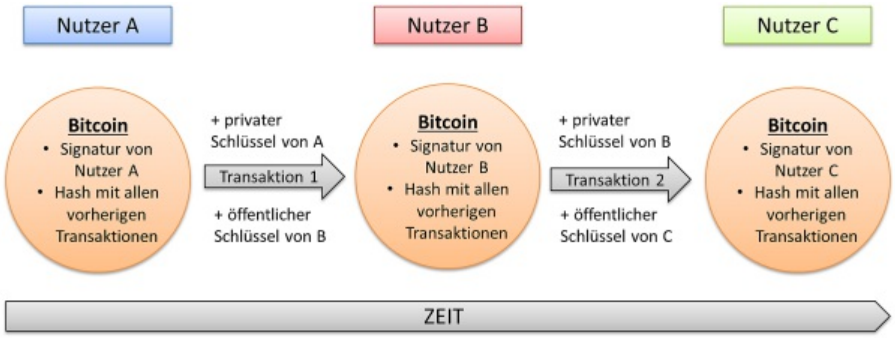
Um eine Transaktion zu starten, muss der Empfänger der Bitcoin-Transaktion dem Sender seinen öffentlichen Schlüssel mitteilen. Der Sender schickt daraufhin den Bitcoin-Betrag durch die digitale Signatur des Hashwertes der vorherigen Transaktion und des ihm zugesandten öffentlichen Schlüssels an den Empfänger. Transaktionen werden in Blöcken zusammengefasst, die beim Mining verarbeitet und dem öffentlichen Verzeichnis aller Transaktionen, der Block Chain, hinzugefügt werden. Sobald eine Transaktion der Block Chain hinzugefügt wurde, erhält sie eine Bestätigung. Das Bitcoin-Protokoll sieht vor, dass eine Transaktion mit sechs Bestätigungen, also sechs Blöcken in denen sie enthalten ist, als ausgeführt und nicht mehr umkehrbar gilt.

Ein Vorteil digitaler Informationen ist, dass sie auf einfache Weise kopiert werden können. Dieser Vorteil ist aber bei digitalen Währungen verheerend, denn dadurch können Beträge doppelt ausgegeben werden. Der Empfänger einer Zahlung erhält nur eine „Kopie“ des Betrages, während der ursprüngliche Besitzer das Original behält und es noch einmal ausgeben kann. Während bei traditionellen Fiat-Währungssystemen die physischen Scheine und Münzen doppeltes Ausgeben verhindern und die Banken den Kontostand kontrollieren, um mehrfaches Ausgeben des Guthabens zu verhindern, benötigen digitale Währungssysteme besondere Schutzmechanismen.

Um doppelte Ausgaben, d.h. das wiederholte Versenden derselben Bitcoins, zu verhindern, wird das Konzept des „Zeitstempels“ benutzt. Um sicherzustellen, dass die Daten der Bitcoins nicht manipuliert wurden und in unveränderter Form vorliegen, wird jeder Hashwert mit dem Zeitwert seines Vorgängers versehen. Dadurch werden mehrfache Ausgaben derselben Bitcoins verhindert. Wenn eine Adresse versucht, einen Bitcoinbetrag mehrfach zu versenden, wird im Netzwerk geprüft,

welche Transaktion die älteste ist. Diese Transaktion bleibt bestehen, während alle danach erfolgten für ungültig erklärt und verworfen werden. Jeder einzelne Bitcoin enthält die gesamte Verlaufsgeschichte seiner vorangegangenen Transaktionen und jede Transaktion wird dieser Verlaufsgeschichte hinzugefügt.

Die folgende Darstellung zeigt eine vereinfachte Transaktion eines Bitcoin mit fortlaufender Zeit. Um die Transaktion in Gang zu setzen, muss der Empfänger der Bitcoins, in diesem Fall Nutzer B, Nutzer A seinen öffentlichen Schlüssel zusenden. Nutzer A versendet den Bitcoin mit einer digitalen Signatur seines privaten Schlüssels. Später schickt Nutzer C Nutzer B seinen öffentlichen Schlüssel und eine weitere Transaktion kann von Nutzer B mithilfe seines privaten Schlüssels eingeleitet werden. Jeder Bitcoin beinhaltet die Transaktionen, die er bereits hinter sich hat und fügt dieser Historie aktuelle Transaktionen hinzu. Dabei wird der Bitcoin so gespeichert, dass nur der aktuelle Besitzer den Bitcoin mit seinem privaten Schlüssel erneut versenden kann.



Chronologischer Ablauf mehrerer Transaktionen eines Bitcoin

Quelle: Eigene Zusammenstellung.

Um einen Bezahlvorgang zu starten, wählt sich jeder Teilnehmer mit seiner jeweiligen Client-Software in das dezentrale Netzwerk ein. Dies erledigt die Software automatisch sobald sie eine Verbindung ins Internet hat. Der Bezahlvorgang läuft durch einen Dialog in der Client-Software ab. In diesen Dialog werden die Empfängeradresse sowie der Betrag eingegeben. Die Adresse muss zuvor vom Empfänger an den Sender der Bitcoins übermittelt worden sein. Mit dem privaten Teil seines Schlüssels signiert der Sender seine Zahlung an den Empfänger. Dies geschieht automatisch im Hintergrund durch das Programm. Außerdem kann eine freiwillige Gebühr eingestellt werden, um die Bestätigung der Transaktionen zu beschleunigen. Zur Sicherheit muss bei den meisten Clients noch ein Passwort eingegeben werden, um die Transaktion zu bestätigen. Die Transaktion wird daraufhin allen Teilnehmern des Netzwerkes bekannt gemacht. Dadurch sollen Störungen oder Manipulationen ausgeschlossen werden.

Eine Sammlung von Transaktionen im Bitcoin-Netzwerk wird als Block bezeichnet. In den Blöcken sind die Daten zu den Transaktionen zwischen Sendern und Empfängern von Bitcoins gespeichert. Jeder Block kann Transaktionen über eine kleine oder große Summe Bitcoins enthalten. Im Netzwerk werden die Blöcke verifiziert. Dies geschieht durch das sogenannte Mining. Blöcke werden in regelmäßigen Abständen generiert und durch das Bestätigen der Richtigkeit von Blöcken kann ein Miner Belohnungen in Form von Bitcoins erhalten.

Im Zuge einer Transaktion werden die Details darüber an so viele Computer wie möglich innerhalb des Bitcoin-Netzwerkes übermittelt. In der Block Chain werden zudem die Details über alle bisher abgewickelten Transaktionen gespeichert. Sollte ein Angreifer die Absicht haben, Transaktionen zu

löschen, um Bitcoins doppelt ausgeben zu können, muss er den Block, der seine Transaktion enthält, manipulieren oder löschen. Da die Blöcke durch die Hashwerte miteinander verknüpft sind, muss er auch alle nachfolgenden Blöcke entsprechend manipulieren. Dabei muss er aber schneller sein als das restliche Netzwerk, da seine Manipulationsversuche ansonsten durch die regulären Bestätigungen der übrigen Miner wirkungslos bleiben.

Die Übermittlung der Zahlung wird durch mehrere im Netzwerk generierte Bestätigungen festgestellt. Dabei gibt es kein grundsätzliches Vertrauen zwischen den Nutzern, jeder Teilnehmer „misstraut“ jedem Teilnehmer. Um zu verhindern, dass ein Teilnehmer seine Bitcoins mehrfach ausgibt, werden die Transaktionen im Netzwerk durch einen Flooding-Algorithmus verteilt. Mit Hilfe dieses Algorithmus gibt die Client-Software an jeden anderen erreichbaren Client, der noch nicht informiert wurde, Informationen weiter. Der auf diese Weise neu informierte Client schickt keine Antwort, sondern sendet die Information an alle ihm bekannten Teilnehmer außer dem Sender der Information weiter. Da informierte Teilnehmer keine weiteren Nachrichten aussenden, endet der Algorithmus automatisch, wenn alle erreichbaren Teilnehmer informiert wurden. Die erste Bestätigung der auf diesem Weg verbreiteten Transaktion dauert durchschnittlich zehn Minuten. Das Bitcoin-Protokoll sieht vor, dass Transaktionen nach sechs Bestätigungen als unumkehrbar gelten. Normalerweise geschieht dies sehr schnell, je nach Auslastung des Netzwerkes kann es bis zur Bestätigung aber auch mehrere Stunden dauern. Um den Vorgang zu beschleunigen, kann jeder Nutzer eine Gebühr entrichten, damit die Transaktion bevorzugt bestätigt wird. Die Entrichtung der Gebühren ist freiwillig, aber vor allem bei Transaktionen, die mehrere Adressen umfassen und deshalb auch eine größere Datenmenge produzieren, sinnvoll. Seit dem 10. Juni 2012 sind folgende minimale Gebühren vorgesehen:

Transaktion akzeptieren, um sie in einen neuen Block einzubetten: 0,0005 Bitcoin

Transaktion an andere Bitcoin-Clients weiterleiten: 0,0001 Bitcoin

Genauso wie Bargeld können auch Bitcoins gestohlen werden. Größere Summen Bitcoins auf einem Computer zu speichern, ohne diesen zu sichern, ist vergleichbar mit einer prall gefüllten Brieftasche, die man jederzeit mit sich herumträgt. Genau wie jede normale Geldbörse, so muss auch die Bitcoin-Wallet geschützt werden, denn es bestehen zwei Risiken für Bitcoin.

Ein Risiko ergibt sich aus der digitalen Natur des Systems. Da das Bitcoin-System auf Daten basiert und die Informationen in Dateien gespeichert werden, besteht das Risiko eines Datenverlustes. Außerdem besteht die Gefahr eines Diebstahls in Form von unberechtigtem Zugriff auf den Rechner und das dort gespeicherte Bitcoin-Guthaben durch Hacker. Es gibt jedoch Möglichkeiten, sich gegen beide Risiken abzusichern.

Wie bei allen wichtigen Dateien gilt auch für Bitcoin das Gebot der Datensicherung und der regelmäßigen Backups. Innerhalb der Bitcoin-Software muss vor allem die wallet.dat-Datei, die alle privaten und öffentlichen Adressen sowie deren Bitcoin-Guthaben enthält, vor Verlust oder Hardwaredefekten geschützt werden. Die Datei befindet sich standardmäßig in folgendem Verzeichnis:

Windows XP: C:\Dokumente und Einstellungen\Benutzername\Anwendungsdaten\BitCoin

Windows Vista und 7: C:\Users\Benutzername\Appdata\Roaming\BitCoin

Mac: ~/Library/Application Support/Bitcoin/

Gegen Hardwaredefekte helfen regelmäßige Sicherungen der Datei auf USB-Sticks und externen Festplatten. Um die Datei vor unberechtigten Zugriffen zu schützen, ist es empfehlenswert, sie durch eine Verschlüsselungssoftware vor fremden Zugriffen zu schützen; hierzu ist die Open-Source-Software Truecrypt (*http://www.truecrypt.org/downloads*) sehr gut geeignet. Mithilfe des Programms lassen sich einzelne Dateien oder ganze Laufwerke mit 128-, 256-, oder 448-Bit-Keys sichern und sind dann nur noch durch Eingabe des zugeteilten Passworts zugänglich. Die verschlüsselte wallet.dat-Datei kann dann als zusätzliches Backup als E-Mail-Anhang an die eigene Adresse eines Freemail-Anbieters gesendet werden.

Obwohl Bitcoins digital sind, lassen sie sich auch auf Papier sichern. Eine Möglichkeit für die Erstellung eine Papier-Wallet ist die Website bitaddress.org (*http://www.bitaddress.org*). Auf dieser Homepage können Adressen und die dazugehörigen privaten Schlüssel als ausdruckbare Datei erzeugt werden. Obwohl die Nutzung der Website sicher ist, empfiehlt es sich, die komplette Seite lokal auf dem Computer zu speichern und erst aufzurufen, wenn die Verbindung zum Internet getrennt ist. Da die Anwendung in JavaScript geschrieben wurde, ist auch eine Offline-Nutzung möglich. Für eine nahezu 100-prozentige Sicherheit ist es ratsam, mit einer Linux-Live-CD den Computer neu zu booten und dann die offline gespeicherte Website aufzurufen. Dadurch wird sichergestellt, dass keine Spyware aktiv ist. Die auf diese Weise erzeugte Datei sollte am besten ausgedruckt werden. Sie enthält sowohl den öffentlichen als auch den privaten Schlüssel. Ein Ausdruck kann mehrere Adressen und die dazugehörigen privaten Schlüssel enthalten.

Als nächster Schritt müssen Bitcoins aus der elektronischen Wallet an eine der Adressen auf dem Papierausdruck gesendet werden. Diese Bitcoins sind dann nicht mehr zugänglich, aber dafür auch vor fremden Zugriffen geschützt. Der Papierausdruck sollte gut verwahrt werden, denn er enthält jetzt das Bitcoin-Guthaben. Es mag zwar seltsam erscheinen, aber auf diese Weise lässt sich die digitale Währung in „reales“ Papier umwandeln.

Die Rückumwandlung der Papier-Bitcoin ist relativ einfach. Seit der Version 0.6.0 bietet die Kommandozeileneingabe der Bitcoin-Software die „importprivkey“-Funktion an, die den Import privater Schlüssel ermöglicht. Aber auch verschiedene Clients und Handelsbörsen wie etwa Mt.Gox bieten die Möglichkeit, private Schlüssel einzugeben und das eigene Konto mit den „Papier-Bitcoins“ aufzufüllen.

Die Quellen für Bitcoin

Es gibt zwei Möglichkeiten, um in den Besitz von Bitcoin zu gelangen. Man kann sie von anderen Nutzern gegen Geld, Waren oder Dienstleistungen erwerben oder durch das sogenannte Mining herstellen. Der leichtere Weg ist der Kauf von anderen Nutzern über eine Handelsplattform.

Kauf von Bitcoin

Bereits kurz nach dem Entstehen der ersten Bitcoins fand Handel zwischen den Mitgliedern des Netzwerkes statt. Dazu wurde der Internet-Relay-Chat-Kanal „#bitcoin-otc“ benutzt, wo Tauschangebote eingestellt wurden. Der breiten Masse blieb der Zutritt verwehrt, da der IRC-Kanal und das benutzte Bewertungssystem technisch eher anspruchsvoll sind. Um einerseits leichteren Handel von Bitcoin zu ermöglichen und andererseits auch neue Interessenten zu gewinnen, entstanden rasch einige Online-Plattformen, die Dienstleistungen im Bereich des Austauschs von Bitcoin anboten. Da Bitcoins nicht von einer zentralen Institution ausgegeben werden und auch nicht durch regionale oder nationale Grenzen eingeschränkt ist, richtet sich der Preis der Währung nach fünf Kriterien:

- Menge der angebotenen Bitcoin: Das System sieht eine Gesamtmenge von 21 Millionen Stück bis zum Jahr 2040 vor. Gleichzeitig ist aber jeder Bitcoin in 1/100.000.000 Einheiten teilbar, so dass insgesamt 2.100.000.000.000.000 Einheiten zur Verfügung stehen.
- Vertrauen in das System: Da Bitcoin nicht durch physische Werte abgesichert ist und auch nicht durch staatliche Garantien gedeckt wird, ist das Vertrauen der Nutzer in die Währung der entscheidende Punkt für deren zukünftige Wertenwicklung.
- Verbreitung: Je mehr Nutzer und auch Händler Bitcoin nutzen, desto stärker wird auch der Wert steigen.
- Sicherheitsaspekte des Systems: Je sicherer das System und die Transaktionen sind, desto mehr Nutzer werden sich für Bitcoin entscheiden.
- Liquidität: Für die Nutzung der Währung ist es entscheidend, wie liquide sie ist, d.h. wie leicht man sie kaufen kann, aber auch, wie leicht man sie wieder gegen andere Währungen eintauschen kann. Bei kleinen Märkten besteht immer das Risiko, dass nicht zu jedem Zeitpunkt ein Käufer oder Verkäufer zur Verfügung steht.

Derzeit existieren ca. 11,2 Millionen Bitcoins. Es werden zwar täglich mehr, aber dennoch ist momentan kaum mehr als die Hälfte aller jemals existierenden Bitcoin verfügbar. Da die Schaffung weiterer Bitcoin mit einem höheren Schwierigkeitsgrad verbunden ist und dadurch mit einer sinkenden Geschwindigkeit erfolgt, wird es noch bis 2040 dauern, bis die Gesamtmenge zur Verfügung steht. Bei einem Wert von 100 Euro pro Bitcoin (Stand: Juni 2013) ergibt sich eine Marktkapitalisierung von ca. 1,12 Milliarden Euro. Die Marktkapitalisierung errechnet sich aus der Multiplikation der im Umlauf befindlichen Stücke mit dem Wert pro Stück. Damit ist Bitcoin immer noch ein sehr kleiner Markt, denn selbst beim bisherigen Höchstkurs umfasste der gesamte Bitcoin-Markt gerade einmal zwei Milliarden Euro. Zum Vergleich: Die Aktien von BMW weisen eine Marktkapitalisierung von ca. 46 Milliarden Euro auf, die Anteilsscheine von Apple haben eine Marktkapitalisierung von ca. 330 Milliarden Euro. Gemessen daran ist die Kapitalisierung von Bitcoin immer noch relativ gering, obwohl die Entwicklung in den letzten Jahren stark zugelegt hat.

Der Kurs für die Bitcoins kommt wie jeder andere Kurs für ein Wirtschaftsgut zustande – durch Angebot und Nachfrage. Käufer und Verkäufer treffen sich auf verschiedenen Handelsplattformen im Internet. Es existieren mehrere Online-Börsen, mit deren Hilfe Bitcoin gegen andere Währungen ge- und verkauft werden kann. Dabei wird je nach Börse eine bestimmte Gebühr fällig. Die Konten bei den meisten Handelsplätzen können per Überweisung oder Lastschrift kapitalisiert werden. Eine

Zahlung mit Kreditkarten ist nicht möglich. Zum einen können diese Zahlungen zu leicht rückgängig gemacht werden und zum anderen kann mit einem groß angelegten Kreditkartenbetrug das gesamte Bitcoin-Netzwerk gefährdet werden.

Um Bitcoin kaufen zu können, ist zuerst die Kapitalisierung des eigenen Nutzerkontos notwendig. Dies geschieht meist durch eine (SEPA-)Überweisung auf das Konto des Börsenbetreibers, der den Betrag dann dem eigenen Kundenkonto gutschreibt. Für einen Verkauf ist es notwendig, die Bitcoins zuerst auf das eigene Nutzerkonto zu überweisen. Dazu wird für jedes Nutzerkonto eine individuelle Adresse generiert, an die Bitcoins gesendet werden können. Die Transferwege funktionieren auch umgekehrt, und so können vom eigenen Nutzerkonto Guthaben auf das eigene Bankkonto überwiesen bzw. Bitcoins an die eigene Wallet geschickt werden.

Im Gegensatz zu den Börsen und Handelsplätzen der klassischen Finanzwelt unterliegen die Bitcoin-Börsen keiner Regulierung durch die Finanzbehörden. Es gibt jedoch Maßnahmen zur Einschränkung der Geldwäsche, wie Auszahlungslimits, oder besondere Formen der Identifizierung, wie das Einreichen einer Ausweiskopie.

Da die Börsen nicht reguliert sind, unterliegen sie auch keiner Einlagensicherung. Für die Guthaben haftet allein der Betreiber der Börse. In der Vergangenheit kam es häufig zu Hackerangriffen auf Börsen, um die dort gespeicherten Bitcoins zu stehlen. Obwohl inzwischen die Sicherheitsmaßnahmen verstärkt wurden und einige Betreiber auch die Haftung für verlorene Einlagen übernehmen, stellt die Gefahr eines Hackerangriffs und des Verlustes der Einlagen immer noch eine ständige Bedrohung für die Bitcoin-Börsen dar.

Schon mehrfach wurde Mt.Gox (*https://www.mtgox.com*) Opfer eines Hackerangriffs. Dies ist nicht weiter verwunderlich, da Mt.Gox die größte Bitcoin-Börse ist, über die schätzungsweise zwei Drittel aller Transfers abgewickelt werden. Mt.Gox wurde 2010 gegründet und wird von der japanischen Tibanne Co. Ltd. betrieben. Der Name ist eine Abkürzung für „Magic: The Gathering Online Exchange“ und deutet auf die Ursprünge als Handelsplattform für Spielkarten des Fantasy-Spiels „Magic: The Gathering“ hin. Die komplette Website ist in englischer Sprache, ebenso der Anmeldeprozess. Es sind aber SEPA-Überweisungen in Euro möglich. Diese erfolgen auf ein polnisches Konto und werden nach ca. drei Tagen dem Nutzerkonto gutgeschrieben. Zudem bietet Mt.Gox die Möglichkeit, das Konto verifizieren zu lassen. Dazu müssen Legitimationsdokumente, wie etwa eine Kopie des Personalausweises sowie ein Nachweis über die aktuelle Wohnadresse, eingeschickt werden. Seit Ende Mai 2013 ist es nur noch mit einem verifizierten Account möglich, Bitcoin in andere Währungen zu tauschen und Geld von Mt.Gox abzuheben. Es gelten derzeit Abhebungsgrenzen von 10.000 US-Dollar oder dem Äquivalent in anderer Währung und 1.000 Bitcoins pro Tag. Darüber hinaus gibt es noch einen „Trusted-Status“ für besonders aktive Händler und Firmen mit zehnfach höheren Auszahlungslimits pro Tag.

Der Handel selbst gestaltet sich relativ unkompliziert. Es ist möglich, Kauf und Verkaufsorders zu platzieren. Diese können mit Limits versehen werden, d.h. der Kauf bzw. Verkauf wird erst ausgeführt, wenn ein bestimmter Kurs erreicht wurde. Alternativ kann auch sofort zum aktuellen Marktkurs gekauft werden. Eine Kauforder wird dann ganz oder teilweise ausgeführt, wenn im System von einem anderen Nutzer eine Verkaufsorder eingegeben wurde, die gleich oder kleiner als der Kaufpreis ist. Eine Verkaufsorder wird dann ganz oder teilweise ausgeführt, wenn im System von einem anderen Nutzer eine Kauforder eingegeben wurde, die gleich oder höher als der Verkaufspreis

ist. Nicht ausgeführte Aufträge bleiben im System bestehen, bis sie ausgeführt oder aber gelöscht werden. Pro Transaktion erhebt Mt.Gox eine Gebühr von maximal 0,6 Prozent. Diese Gebühr wird standardmäßig vom Kauf abgezogen. Bei einem Kauf von einem Bitcoin werden also dem Konto nur 0,994 Bitcoin gutgeschrieben.

Pro Monat wickelt Mt.Gox rund 420.000 Transaktionen mit einem Volumen von ca. 100 Millionen Euro ab. Obwohl Mt.Gox aufgrund dieses Handelsvolumens ein lukratives Ziel für Hackerangriffe darstellt, garantiert die Menge von ca. zwei Drittel aller gehandelten Bitcoins auch marktnahe Preise. Dadurch ist sichergestellt, dass immer ein Preis zustande kommt, da genügend Käufer und Verkäufer anwesend sind.

Wegen des schnellen und unkomplizierten Transfers erfreut sich auch der Handel zwischen Privatpersonen großer Beliebtheit. Erleichtert wird dies durch einige Online-Handelsplätze, die eine Plattform für Käufer und Verkäufer von Bitcoins darstellen. Die meisten Plattformen bieten auch Treuhänderdienste an, indem sie die zu verkaufenden Bitcoins auf einem Konto speichern und erst freigeben, wenn der Zahlungseingang vom Verkäufer bestätigt wurde. Dennoch setzt diese Art des Handels ein bestimmtes Maß an Vertrauen zwischen Käufer und Verkäufer voraus.

Die größte deutschsprachige Plattform für den Bitcoin-Handel direkt zwischen Privatpersonen ist bitcoin.de (*https://www.bitcoin.de*). Auf der Website sind Kauf- und Verkaufsangebote aus fast allen Ländern Europas gelistet, die sich auch filtern lassen. Als Zahlungsmethode steht die SEPA-Überweisung zur Verfügung.

Nach der Anmeldung erfolgt die Verifizierung des eigenen Bankkontos. Dies geschieht durch eine Testüberweisung von bitcoin.de, die im Verwendungszweck einen Bestätigungscode enthält, der wiederum im Nutzerkonto eingegeben werden muss. Dadurch ist das eigene Bankkonto verifiziert und kann für Überweisungen genutzt werden.

Anschließend kann mittels eines Filters im Marktplatz nach geeigneten Angeboten für den Kauf oder Verkauf von Bitcoins gesucht werden. Es können auch gezielt Limitaufträge für den Kauf oder Verkauf gesetzt werden. Sobald ein Verkäufer die Kaufanfrage bestätigt hat, sendet das System eine E-Mail mit den Kontoinformationen des Verkäufers. Nun muss vom Käufer schnellstmöglich die Bezahlung der Bitcoins erfolgen und durch das Klicken auf den Button „als bezahlt markieren“ der Zahlungsvorgang als abgeschlossen und bestätigt markiert werden. Geschieht dies nicht, wird der Kauf rückabgewickelt und eine negative Bewertung vergeben. Hat der Verkäufer den Zahlungseingang bestätigt, wird das gekaufte Bitcoin-Guthaben von bitcoin.de freigegeben. Dabei fallen Gebühren in Höhe von einem Prozent an, die sich Käufer und Verkäufer teilen.

Auch bei bitcoin.de finden sich zahlreiche Käufer und Verkäufer, dennoch weist die Preisbildung noch größere Lücken zwischen Angebot und Nachfrage auf als bei Mt.Gox. Da bitcoin.de ein strenges Bewertungssystem besitzt, können neu registrierte Benutzer zu Beginn nur kleine Mengen an Bitcoin handeln, da sie sich erst „Vertrauen“ erwerben müssen. Es gibt drei Stufen innerhalb des Bewertungssystems: „Bronze“ mit unter fünf Bewertungen, einem Umsatzvolumen aller Geschäfte von unter 25 Bitcoins und einem Anteil positiver Bewertungen von 0 bis 69 Prozent; „Silber“ mit 5 bis 15 Bewertungen, einem Umsatzvolumen aller abgeschlossenen Käufe und Verkäufe zwischen 25 bis 150 Bitcoins und einem Anteil positiver Bewertungen zwischen 70 und 89 Prozent; „Gold“ ab 16 Bewertungen, einem Umsatzvolumen aller Handelsgeschäfte über 150 Bitcoins und einem Anteil positiver Bewertungen von 90 bis 100 Prozent. Dementsprechend ergeben sich verschiedene

Handelsvolumina für die einzelnen Stufen: Der Bronze-Status ermöglicht Auszahlungen von maximal fünf Bitcoins pro Tag sowie einer Bitcoin-Menge pro Kauf und Verkauf von jeweils fünf Stück. Silber ermöglicht Auszahlungen von maximal 10 Bitcoins pro Tag sowie einer Bitcoin-Menge pro Kauf von 25 und pro Verkauf von 50 Stück. Der Gold-Status ermöglicht Auszahlungen von maximal 200 Bitcoins pro Tag sowie einer unbegrenzten Bitcoin-Menge pro Kauf und pro Verkauf.

Neben dem Online-Handel zwischen Privatpersonen haben sich in letzter Zeit auch regionale Marktplätze entwickelt. So bietet die Plattform Localbitcoins (*https://localbitcoins.com*) die Möglichkeit, Käufer und Verkäufer vor Ort zu finden und dann offline zu treffen, um Bitcoins zu handeln.

Natürlich können die aufgezeigten Möglichkeiten für den Erwerb von Bitcoins auch für den Verkauf von Bitcoins genutzt werden. Die Bitcoins werden über die jeweilige Plattform verkauft und das Guthaben wird auf das eigene Bankkonto übertragen.

Obwohl es sich bei Bitcoin um eine digitale Währung handelt, gibt es bereits physische Münzen. Der Hersteller Casascius (*https://www.casascius.com*) bietet derzeit 0,5-, 1- und 25-Bitcoin-Münzen und Barren mit 100 Bitcoins an. Die Münzen und Barren sind allerdings nur ein Transportmittel für einen privaten Schlüssel, der auf einem Stück Papier in einem Fach in jeder Münze verborgen ist und durch ein fälschungssicheres Hologramm geschützt ist. Bei Bedarf kann das Hologramm abgezogen und der dahinter liegende Code in eine Bitcoin-Clientsoftware eingegeben werden. Dadurch wird das Guthaben wieder digital verfügbar, aber die Münze verliert ihren Wert. Das Hologramm hinterlässt beim Abziehen eine wabenförmige Struktur, sodass jede Münze sofort auf Unversehrtheit überprüft werden kann. Auf der Website Casascius Bitcoin Analyzer (*http://casascius.uberbills.com*) kann der Status aller im Umlauf befindlichen Münzen und Barren überprüft werden.

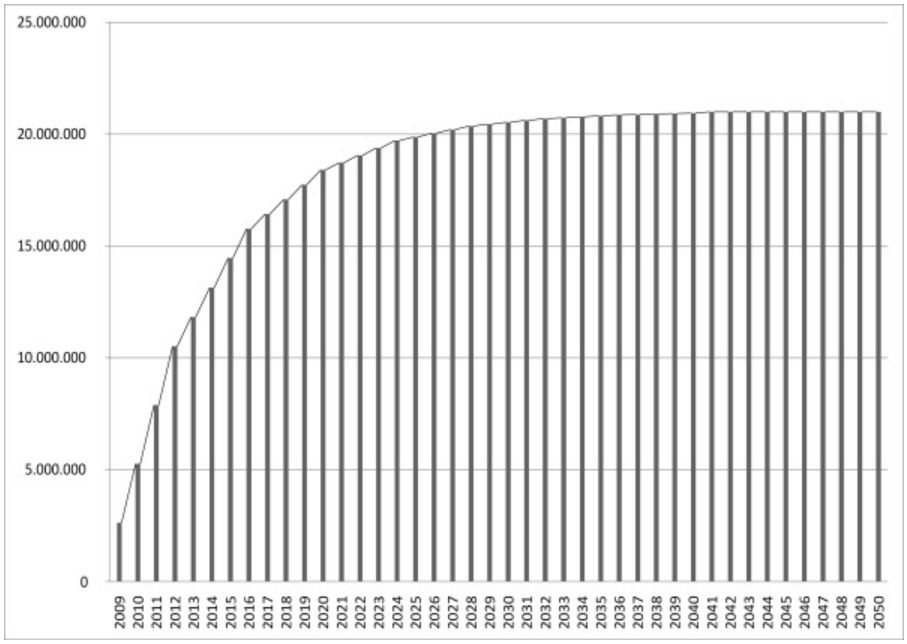
Herstellung von Bitcoin: Mining

Neben dem Kauf von Bitcoin stellt die Herstellung, das sogenannte Mining, den zweiten Weg dar, um an die digitale Währung zu gelangen. Eigentlich handelt es sich dabei um den ursprünglichen Weg, denn neue Bitcoins werden nur durch Mining erzeugt, da es keine zentrale Institution gibt, die Bitcoins ausgibt. Die Bezeichnung Mining entstand, weil das Errechnen der Bitcoins mit dem Schürfen von Rohstoffen wie beispielsweise Gold vergleichbar ist: Unter hohem Aufwand werden kleine Bitcoin-Mengen gewonnen. Der Vorteil des Bitcoin-Mining ist, dass die meiste Arbeit von Computer erledigt wird.

Beim Bitcoin-Mining werden keine Münzen ausgegraben, sondern die im Netzwerk anfallenden Transaktionen von Bitcoins an unterschiedliche Adressen verarbeitet. Während des Prozesses werden Transaktionen in Blöcke zusammengefasst, diese Blöcke werden durch Rechenoperationen bestätigt und an das Bitcoin-Netzwerk gesendet, wo sie in die Block Chain eingefügt werden. Die Block Chain ist die Aneinanderreihung aller Transaktionen im Bitcoin-Netzwerk. Etwa alle 10 Minuten wird die Block Chain durch Hinzufügen eines neuen Blocks mit den Daten der letzten angefallenen Transaktionen, wie z.B. Sender- und Empfängeradressen, Beträge und Gebühren, aktualisiert.

Während Client-Anwendungen die Block Chain nur lesen und Transaktionen an sie übermitteln, wird durch das Mining festgelegt, welche Transaktionen in die Block Chain übernommen werden. Ungültige oder manipulative Transaktionen werden ignoriert, während die Block Chain permanent fortgeschrieben wird.

Bitcoins werden im Bitcoin-Netzwerk in Blöcken erzeugt. Im Durchschnitt entsteht alle zehn Minuten ein Block. Um eine zu schnelle Ausschüttung aller Bitcoins zu verhindern, halbieren sich die in den Blöcken enthaltenen Einheiten alle 210.000 Blöcke, was einem Zeitraum von ungefähr vier Jahren entspricht (1 Block alle zehn Minuten = 144 Blöcke am Tag = 4.320 Blöcke im Monat = 52.560 Blöcke im Jahr). Die erste Reduzierung der ausgeschütteten Bitcoins von 50 auf 25 Stück fand am 28. November 2012 satt. Die letzten der 21 Millionen werden im Jahr 2140 erzeugt werden. Danach findet keine neue Generierung mehr statt, sondern nur noch ein Transfer der bestehenden Bitcoins.



Prognose der Bitcoin-Menge

Quelle: Eigene Darstellung, basierend auf Daten von *http://bitcoincharts.com/*.

Herzstück des Bitcoin-Systems ist die Block Chain, in der alle Transaktionen gespeichert werden. Um die Sicherheit dieser Datei zu garantieren, muss sie vor Manipulationen geschützt werden. Die Sicherung findet während des Mining statt. Ein beliebiger Rechner, der sich durch eine Software am Mining beteiligen kann, bekommt durch das Bitcoin-Netzwerk die Aufgabe zugewiesen, ein mathematisches Problem auf Basis der letzten verfügbaren Transaktionen zu lösen. Zur Lösung des Problems muss der Computer, unter Verwendung eines doppelten SHA256-Algorithmus, einen Schlüssel in Form eines Hashwertes finden, der mit der Liste der letzten Transaktionen und dem Hashwert des letzten abgeschlossenen Blocks in der Block Chain einen neuen Hashwert generiert. Da jeder neue Block auch den Hashwert des Vorgängerblocks enthält, ergibt sich eine fortlaufende Kette von Blöcken und Berechnungen, die aufeinander aufbauen. Die dadurch geschaffene Block Chain lässt sich bis zum sogenannten Genesis Block zurückverfolgen, der am 3. Januar 2009 als erster Block des Bitcoin-Netzwerkes geschaffen worden ist.

Jeder neue Hashwert muss eine vom Netzwerk geforderte Schwierigkeitsstufe, die als eine bestimmte Zahl von Nullen am Anfang des Hashwertes ausgedrückt wird, erfüllen. Der Computer kann den entsprechenden Wert nur durch die Versuch-und-Irrtum-Methode ermitteln. Je mehr Nullen am Anfang des Hashwertes stehen, desto schwieriger ist die Berechnung, denn der Computer muss so viele Werte berechnen, bis sich ein Hashwert mit den vielen Nullen ergibt.

Wird ein passender Wert gefunden und der Block gelöst, wird als Erstes eine Transaktion von derzeit 25 Bitcoins generiert, die an die Adresse des Rechners geschickt werden, der den richtigen Hashwert errechnet hat. Der Schwierigkeitsgrad für das Lösen der Blöcke wird alle 2.016 Blöcke, was einem Zeitraum von zwei Wochen entspricht, angepasst, um zu gewährleisten, dass durchschnittlich alle zehn Minuten ein Block gelöst und neue Bitcoins generiert werden.

Nachdem ein Block gelöst wurde, wird er in die Block Chain eingefügt. Die Block Chain ist eine Datenbank, die alle bisher im Bitcoin-Netzwerk abgewickelten Transaktionen enthält. Da jeder Block zum Zeitpunkt seiner Lösung in die Block Chain eingefügt wird und dieser Block die aktuellsten Transaktionen enthält, entsteht eine chronologische Abfolge aller Netzwerktransaktionen. Die jeweils aktuellen Blöcke, also die letzten, die der Block Chain hinzugefügt wurden, sind einsehbar unter *http://blockexplorer.com*. So hat z.B. Block Nr. 236.793, der am 18. Mai 2013 um 18:05 Uhr im Netzwerk generiert wurde, einen Hashwert von 000000000000000057339afe8c5b958e71fef62916e7fcb065e04aa4e1dbbcff3c. Er enthielt 378 Transaktionen mit einem Gesamtwert von 4.852,14664331 Bitcoins. Block Nr. 241.713, der am 15. Juni 2013 um 18:46 Uhr generiert wurde, hat den Hashwert 000000000000000916e3dfae22badced9eece31ed9afbce41abe8a61149e28a. Der Hashwert weist am Anfang zwei Nullen mehr auf, wodurch der Schwierigkeitsgrad bei der Berechnung höher ist. Der Block enthielt 95 Transaktionen mit einem Gesamtwert von 1.148,03068573 Bitcoins.

Auch wenn die einzelnen Rechenvorgänge beim Mining kompliziert sind, so wird die Detailarbeit doch von Software erledigt, die im Vergleich zu den im Hintergrund ablaufenden Rechenprozessen sehr einfach zu bedienen ist. Wichtiger als die Rechenoperationen an sich ist die zur Verfügung stehende Leistungsfähigkeit der Computer zur Berechnung der Aufgaben. Die Rechenkapazität des Netzwerkes wird in Hashes pro Sekunde gemessen. Ein Hashwert ist ein Wert fester Länge, typischerweise codiert als hexadezimale Zeichenkette, der aus beliebigen Eingabedaten gewonnen

wird. Da die Rechenleistung immer weiter ansteigt, ergeben sich auch ansteigende Messgrößen:

H/s = Hashes pro Sekunde = 1 Hash-Berechnung pro Sekunde

1.000 H/s = 1 KH/s (Kilohash pro Sekunde)

1.000 KH/s = 1 MH/s (Megahash pro Sekunde)

1.000 MH/s = 1 GH/s (Gigahash pro Sekunde)

1.000 GH/s = 1 TH/s (Terahash pro Sekunde)

1.000 TH/s = 1 PH/s (Petahash pro Sekunde)

Derzeit hat das Bitcoin-Netzwerk eine Rechenkapazität von ca. 110 bis 130 Terahashes in der Sekunde. Diese Leistung lässt sich nicht direkt mit der Rechenleistung von Supercomputern vergleichen, da diese eine andere Architektur aufweisen. Die Rechenkapazität entspricht aber ca. 300.000 Desktoprechnern mit jeweils einer Mittelklasse-Grafikkarte mit einer durchschnittlichen Leistung von 300 MH/s.

Die Block Chain und das Peer-to-Peer-Prinzip des Netzwerks ersetzen eine zentrale Institution, wie etwa eine Zentralbank. Gleichzeitig wird durch die Verwendung öffentlicher und privater Schlüssel die Anonymität aller Teilnehmer sichergestellt. Trotz aller Sicherheitseinstellungen bleibt das System transparent. Auf der Website Blockchain (*http://blockchain.info/*) werden die letzten Transaktionen und weitere Statistiken, wie etwa die Zeit seit der letzten Bestätigung eines Blocks, veröffentlicht.

Das Netzwerk besitzt einen variablen Schwierigkeitsgrad, der sich durch die Anzahl der Nullen am Beginn des Hashwertes regulieren lässt. Je mehr Rechenkapazität zur Verfügung steht, desto höher fällt der Schwierigkeitsgrad in Form zusätzlicher Nullen am Anfang der Blöcke aus. Der Schwierigkeitsgrad wird alle zwei Wochen bzw. alle 2.016 Blöcke angepasst. Zu Beginn der Erzeugung reichte ein normaler PC aus, um Bitcoins zu erzeugen. Mit zunehmender Nutzerzahl stieg auch der Schwierigkeitsgrad an und die Prozessoren normaler Computer reichten bald nicht mehr aus, um Mining betreiben zu können. Schon Mitte 2011 war der Schwierigkeitsgrad so hoch, dass ein einzelner Rechner mehrere Jahre gebraucht hätte, um einen einzelnen Bitcoin-Block zu lösen.

Der steigende Schwierigkeitsgrad ist ebenfalls mit dem Abbau einer Goldader vergleichbar, vor allem während eines Goldrausches. Die ersten Vorkommen sind noch relativ leicht abzubauen, aber je mehr Goldschürfer einen Teil des Vorkommens haben wollen, desto schneller ist das Vorkommen ausgebeutet und ein immer höherer Aufwand muss betrieben werden, um auch die letzten Goldreste abbauen zu können. Genauso verhält es sich mit dem Mining von Bitcoin, nur dass die Arbeit rein virtuell von Computern geleistet wird.

Um dem steigenden Schwierigkeitsgrad zu begegnen, fanden zwei parallele Entwicklungen statt. Das Mining, die reinen Rechenoperationen, verlagerte sich vom Hauptprozessor des Computers hin zu den Grafikkarten und deren Prozessoren. In den letzten Jahren hatten Grafikkarten, die hauptsächlich in Spiele-PCs eingesetzt werden, enorme Entwicklungsschübe erfahren. Die auf den Karten eingesetzten Prozessoren sind zwar spezialisiert für bestimmte Rechenanwendungen, erledigen diese aber effizienter als Computerprozessoren, die als Allrounder eine Vielzahl unterschiedlicher Rechenoperationen erledigen müssen. So werden beispielsweise auch bei der Videobearbeitung und Berechnung der dazugehörigen Effekte immer häufiger Grafikkarten eingesetzt. Auch für die Bitcoin-Rechenoperationen sind Grafikkarten besser geeignet als PC-Prozessoren.

Jedoch gibt es auch bei den Grafikkarten Unterschiede. Je leistungsfähiger und teurer eine Grafikkarte ist, desto besser ist sie in der Regel auch für das Mining geeignet. Jedoch zeichnen sich besonders leistungsfähige Grafikkarten auch durch einen erhöhten Stromverbrauch aus.

Eine Auswahl unterschiedlicher Leistungs- und Preisklassen zeigt diese Tabelle:

Grafikkarte	Leistung (MH/s)	Stromverbrauch (W)	Kosten (€)
ATI 6670	ca. 110	ca. 66	ca. 55
ATI 7750	ca. 130	ca. 50	ca. 75
ATI 7950	ca. 500	ca. 200	ca. 250
ATI 7970	ca. 650	ca. 250	ca. 325
NVIDIA GTX680	ca. 120	ca. 100	ca. 350

Quelle: Eigene Zusammenstellung mit Daten aus: *https://en.bitcoin.it/wiki/Mining_hardware_comparison* (Stand: Juni 2013).

Auf der Website *https://en.bitcoin.it/wiki/Mining_hardware_comparison* finden sich umfangreiche Vergleichstabellen mit Daten zu fast allen erhältlichen Grafikkarten sowie Vergleichsdaten aller gängigen Prozessoren. Aufgrund zahlreicher Erfahrungsberichte von Anwendern scheinen Grafikkarten der Firma AMD/ATI für das Mining besonders effizient zu sein.

Die Website Bitcoinx (*http://www.bitcoinx.com/profit*) bietet einen sehr guten Vergleichsrechner, der die Eingabe mehrerer Variablen ermöglicht. Basierend auf dem aktuellen Schwierigkeitsgrad des Netzwerkes und dem aktuellen Bitcoin/Dollar-Kurs, lässt sich berechnen, ab wann sich das Mining mit vorhandener oder neu anzuschaffender Hardware amortisiert.

Inzwischen werden PCs speziell für das Mining zusammengestellt. Sie können mehrere Grafikkarten aufnehmen und werden besonders gekühlt, um die durch die Karten erzeugte Hitze besser abzuführen. Ein speziell für das Mining gebauter PC wird als Mining Rig bezeichnet.

Da der Schwierigkeitsgrad bei der Lösung der Blocks aufgrund der wachsenden Anzahl an Minern immer weiter anstieg, benötigten selbst die besten Mining Rigs bald Jahre, um einen einzelnen Block zu lösen. Das sogenannte Solo Mining, das Suchen nach den richtigen Lösungen für die Blöcke auf eigene Rechnung, wurde bald völlig unrentabel. Aus diesem Grund entstanden Mining-Pools. Dabei handelt es sich um den Zusammenschluss mehrerer Rechner zur Bündelung ihrer Rechenkapazität. Gemeinsam werden die Bitcoin-Rechenoperationen schneller gelöst und die dabei erzeugten Bitcoins werden je nach Beitrag des Einzelnen zur Lösung eines Blocks, der aktuell 25 Bitcoins enthält, auf die beteiligten Rechner verteilt. Mittlerweile gibt es viele verschiedene Mining Pools, die sich je nach regionalem Schwerpunkt und Gebühren unterscheiden. Die Anmeldung erfolgt meist unkompliziert über eine entsprechende Webseite des Pools.

Generell unterscheiden sich die Mining Pools durch ihre Abrechnungsmethoden. Eine Variante ist die sogenannte Pay-per-Share-Methode. Ein Share besteht aus einer bestimmten Menge an Hashes, also Versuchen einen Blockwert richtig zu berechnen, die von einem Miner an den Pool geliefert werden. Die Auszahlung erfolgt dann je nach Anzahl der eingelieferten Shares aus dem Guthaben des Mining Pools. Dadurch lassen sich sofort Einnahmen erzielen, weshalb diese Methode ideal für Einsteiger ist. Da die Auszahlungen vom Betreiber des Mining Pools getragen werden, trägt er das

Risiko, dass ein Block nicht gelöst wird. Dieses höhere Risiko lässt sich der Pool-Betreiber durch höhere Gebühren bezahlen, die bis zu 10 Prozent betragen können. Dafür erhalten die Miner fortlaufende kleinere Zahlungen.

Viele Pools bieten auch die proportionale Methode an. Dabei wird jeder Miner gemäß seines Beitrags an Rechenleistung zur Lösung eines Blocks bezahlt. Die Auszahlung erfolgt aber nur, wenn tatsächlich ein Block gelöst wird. Werden keine Blöcke gelöst, gibt es auch keine Auszahlung. Da das Risiko bei den Minern liegt, sind die Gebühren in der Regel niedriger als bei der Pay-per-Share-Methode, meist bei drei bis fünf Prozent.

Eine aktuelle Übersicht der gegenwärtig 25 Mining Pools mit Angaben zum Standort, den eingesetzten Abrechnungsmethoden, den aktuellen Leistungsdaten sowie vielen weiteren Informationen findet sich unter *https://en.bitcoin.it/wiki/Comparison_of_mining_pools*.

Folgende grundlegenden Fragen sollten bei der Auswahl eines Mining Pools beachtet werden:

Wie hoch ist die Pool-Gebühr?

Wo ist der Standort des nächsten Poolservers?

Fließen die in den Blöcken enthaltenen Transaktionsgebühren an den Pool oder werden sie an die Miner ausgeschüttet?

Ist eine sofortige Auszahlung des Guthabens möglich oder gibt es Auszahlungslimits und Wartefristen?

Unabhängig von der Methode, wird für das Mining eine bestimmte Software benötigt, die die Hardware steuert und die Kommunikation mit dem Netzwerk bzw. den Pool-Servern übernimmt. Einige Mining Pools bieten auch speziell vorkonfigurierte Programme an, die an die jeweiligen Pool-Schnittstellen angepasst sind und nur noch installiert werden müssen. Eine Übersicht der Programme findet sich unter *https://en.bitcoin.it/wiki/Software#Mining_apps*.

Als Universallösung für das Mining bei mehreren Pools bietet sich die Software Guiminer an (*http://guiminer.org/*). Die Software muss nach dem Download nur entpackt und durch einen Klick auf „guiminer.exe“ gestartet werden. Sie erkennt die installierten Grafikkarten automatisch, ebenso sind Profile für die bekanntesten Mining Pools bereits vordefiniert. Es fehlen nur noch die individuellen Zugangsdaten. Diese Zugangsdaten werden nach der Anmeldung bei einem Pool von diesem zur Verfügung gestellt.

Obwohl die Software relativ leicht zugänglich ist, erfordert der gesamte Mining-Prozess ein gewisses technisches Verständnis. Die Auswahl der richtigen Komponenten für einen Mining-PC, der Zusammenbau und die Installation der Treiber sowie die Konfiguration der Software nehmen Zeit in Anspruch. Zudem ist die Leistung einzelner Grafikkarten durch die Eingabe zusätzlicher Befehlsparameter beeinflussbar. Dies ist jedoch mit Risiken verbunden, da falsche Eingaben oder auch eine falsche Konfiguration die Grafikkarten überlasten oder beschädigen können.

Um den zahlreichen technischen Fragen und Schwierigkeiten begegnen zu können, hat sich im Internet eine aktive Community gebildet, die sich mit den vielfältigen Problemen des Mining beschäftigt. Die wichtigste Anlaufstelle ist das Bitcoin-Forum (*https://bitcointalk.org*). In diesem Forum werden alle Themen des Mining, sowohl die Software als auch die Hardware, diskutiert und vielfältige Problemlösungen angeboten. Speziell für die Guiminer-Software gibt es einen eigenen

(englischsprachigen) Bereich: https://bitcointalk.org/?topic=3878.0. Darüber hinaus werden in dem Forum auch viele andere Aspekte des Bitcoin diskutiert. Das Forum ist überwiegend auf Englisch, es gibt aber auch eine deutsche Sektion.

Mit dem steigenden Energieverbrauch regulärer Grafikkarten beim Mining begann bald die Suche nach Alternativen. Eine Alternative besteht im Einsatz von FPGAs (Field Programmable Gate Arrays). Dabei handelt es sich um stark spezialisierte Schaltkreisplatinen, die hauptsächlich in Forschung und Industrie eingesetzt werden. Sie bieten zwar eine besonders hohe Rechenleistung bei sehr niedrigem Energieverbrauch, kosten dafür aber ein Vielfaches im Vergleich zu normalen Grafikkarten.

Eine weitere Möglichkeit, dem steigenden Schwierigkeitsgrad und dem enormen Energieverbrauch zu begegnen, stellt die Entwicklung von ASIC (Application Software in an Integrated Circuit) dar. Dabei handelt es sich um speziell für das Bitcoin-Mining entwickelte Prozessoren, die sich durch eine enorm hohe Rechenleistung bei sehr geringem Stromverbrauch auszeichnen. Einige amerikanische Unternehmen, z.B. Butterfly Labs (http://www.butterflylabs.com/de), haben die Auslieferung von ASIC bereits Mitte 2012 angekündigt und Vorbestellungen für die Auslieferung im Oktober 2012 entgegengenommen. Die ASIC-Modelle sollten bis zu 100-mal schneller rechnen als durchschnittliche Grafikkarten und dabei nur ca. 60 bis 100 Watt Strom verbrauchen. Die von Butterfly Labs für Oktober 2012 angekündigte Lieferung wurde immer wieder verschoben, ebenso wurden die Spezifikationen der Geräte geändert und die Leistungsdaten nach unten korrigiert. Dennoch nimmt die Firma weiterhin Vorbestellungen an, was zu einer permanenten Diskussion unter den Bitcoin-Nutzern führt, ob es sich bei dem Geschäftsmodell nicht doch um einen Betrugsversuch handelt. Eine weitere Firma, Avalon (http://launch.avalon-asics.com), brachte mittlerweile 1.500 Stück eigener ASICs auf den Markt, die aber mehr Energie verbrauchen als die Geräte von Butterfly Labs. Inzwischen haben auch andere Firmen angekündigt, ASICs in unterschiedlichen Konfigurationen ausliefern zu wollen.

Sobald ASICs in größeren Stückzahlen auf den Markt kommen, werden sie zweifellos das Mining verändern. Das Mining mit Grafikkarten und FPGAs wird unrentabel werden, da durch die Leistung der ASICs der Schwierigkeitsgrad so stark ansteigen wird, dass mit der bisher eingesetzten regulären Hardware keine nennenswerten Bitcoin-Beträge mehr verdient werden können. Wie dramatisch der Leistungsunterschied zwischen ASICs und der übrigen Mining-Hardware ist, zeigt diese Tabelle:

Hardware	Rechenleistung (MH/s)	Stromverbrauch (W)	Kosten (€)
CPU/Prozessor	ca. 1–10	ca. 40–150	ca. 50–350
Grafikkarte	ca. 200–800	ca. 50–250	ca. 100–350
FPGA	ca. 860	ca. 60	ca. 670
ASIC (Avalon)	ca. 65.000	ca. 620	ca. 1.200
ASIC (Butterfly)	ca. 50.000	unbekannt	ca. 2.000

Quelle: Eigene Zusammenstellung, basierend auf https://en.bitcoin.it/wiki/Mining_hardware_comparison (Stand: Juni 2013).

Mining erscheint verlockend. Der Computer rechnet und verdient dabei stetig Geld. Da normale Computer für das Mining aber inzwischen völlig ungeeignet sind und selbst gut ausgestattete Rechner

mit Hochleistungsgrafikkarten im Vergleich zu den ASICs bald nicht mehr konkurrenzfähig sein werden, ist der Einstieg in das Mining, sofern die Hardware noch nicht vorhanden ist, mittlerweile nur noch mit erhöhtem Kapitalaufwand möglich. Zudem kommen vor allem in Deutschland die hohen Energiekosten hinzu, die das Mining mit stromhungrigen Grafikkarten zusätzlich belasten. Oftmals ist es sinnvoller, einen Betrag statt in Hardware besser direkt in Bitcoin zu investieren und von den zukünftigen Wertsteigerungen zu profitieren.

Die Risiken des Bitcoin-Systems

Das Bitcoin-System wirft viele Fragen auf, die vom Haftungsrisiko bis ins Vertrags- und Privatrecht reichen. Weder die Bitcoin-Website noch die Softwarelizenz nehmen zu juristischen Problemen Stellung. In der Textdatei, die mit der Installation des Bitcoin-Clients aufgerufen wird, wird jegliche Haftung für die Software ausgeschlossen. Neben den rein rechtlichen Fragen ergeben sich noch weitere Risiken, die mit Bitcoin einhergehen.

Verlustrisiko

Im Gegensatz zu Kreditkarten und anderen Zahlungsmöglichkeit sind Bitcoin nicht gegen Manipulationen und Diebstahl geschützt. Werden Kreditkartendaten missbraucht, bekommt der Eigentümer den Schaden erstattet, bei Bitcoin ist dies nicht der Fall. Im Gegensatz zu normalen Sparguthaben gibt es keine Einlagensicherung, die Bitcoin schützen würde. Für reguläre Guthaben bei Banken und Sparkassen existieren in Deutschland mehrere unterschiedliche Einlagensicherungsfonds, die im Falle der Insolvenz einer Bank die Guthaben der Sparer schützen. Seit dem 1. Januar 2011 greift außerdem eine Verordnung der EU-Kommission, wodurch Mitgliedsländer der EU zu einer gesetzlichen Entschädigung von 100.000 Euro verpflichtet sind. All diese Sicherungsinstrumente gibt es für Bitcoin nicht.

So ist schon die Möglichkeit, Bitcoin zu speichern, mit vielen Risiken verbunden. Bei der lokalen Speicherung auf der Festplatte eines Computers kann ein Hardwaredefekt auftreten, der die Festplatte und damit das gesamte Bitcoin-Guthaben zerstört. Zudem ist Bitcoin durch Hackerangriffe und Malware gefährdet. Ohne Verschlüsselung und Absicherung gegen fremde Zugriffe besteht immer ein Risiko bei der lokalen Speicherung auf einem Computer. Maßnahmen zur Verschlüsselung sind jedoch für Privatanwender relativ komplex, und schon kleine Fehler können Sicherheitslücken verursachen. Auch die Online-Speicherung der Bitcoins bei entsprechenden Dienstleistern ist nicht sicher. Die sogenannten Online-Wallets stellen ein beliebtes Ziel für Hackerangriffe dar und bei einem erfolgreichen Angriff ist das Guthaben ebenfalls weg.

Auch die Bitcoin-Börsen sind ein beliebtes Ziel für Hackerangriffe. So wurde am 20. Juni 2011 bei einem Hackerangriff auf Mt.Gox eine Datenbank mit Nutzernamen, E-Mail-Adressen und Zugangsdaten von über 61.000 Kunden gestohlen. Zudem wurden 25.000 Bitcoins, die damals einen Marktwert von ca. 500.000 US-Dollar hatten, an den Angreifer ausgezahlt. Einige Tage später kam es zu einem zweiten Hackerangriff, wobei 400.000 Bitcoins erbeutet wurden. Die Bitcoins wurden sofort auf dem Markt zum Verkauf angeboten, was den Kurs innerhalb einer halben Stunde von 17,50 auf 0,01 Dollar sinken ließ. Mt.Gox setzte daraufhin den Handel aus und fror alle Konten ein. Die Transaktionen wurden von Mt.Gox wieder rückgängig gemacht, was den Preis wieder auf dem alten Niveau stabilisierte und die Nutzer beruhigte. Trotz der Rückabwicklung und des dadurch begrenzten Schadens stellen die Sicherheitsmechanismen der Handelsplattformen eine Schwachstelle dar. Zudem verwenden viele Nutzer bei mehreren Handelsplattformen identische Zugangsdaten, sodass bei einem erfolgreichen Angriff oft der Zugang zu mehreren Websites erbeutet wird. Inzwischen verstärken aber auch die Bitcoin-Handelsplätze ihre Sicherheits- und Abwehrmaßnahmen und bieten doppelte Authentifizierungen an, etwa durch Google Authenticator.

Verbotsrisiko

Noch gibt es für Bitcoin keinerlei staatliche Regulierungsmaßnahmen, es besteht aber das Risiko staatlicher Eingriffe bis hin zum Verbot. Der dezentrale Charakter des Netzwerkes macht einen Zugriff für jede staatliche Institution sehr schwer, da es keinen zentralen Server gibt, den man überwachen und bei Verstößen abschalten kann. Eigentlich ist dies ein Vorteil der digitalen Währung, aber ein Zahlungssystem ohne staatliche Regulierung lockt auch Kriminelle an, die mithilfe von Bitcoin illegale Geschäfte abwickeln. Mit der zunehmenden Verbreitung von Bitcoin nimmt auch die Zahl der illegalen Geschäfte zu. Da keine Regierung Bitcoin regulieren kann und die komplette Abschaltung eines dezentralen Netzwerkes nicht möglich ist, besteht die Gefahr, dass Bitcoin in einigen Ländern schlicht für illegal erklärt wird. Bei einem Verbot der Bitcoin-Währung würden zwar weiterhin Handel und Transaktionen damit im Internet stattfinden, jedoch wäre Bitcoin als Zahlungsmittel für legale Geschäfte nicht mehr einsetzbar. Dies würde wahrscheinlich einen enormen Preisverfall und das Ende von Bitcoin als Alternative zu regulären Währungen bedeuten.

Einer der Vorteile von Bitcoin, die Anonymität bei den Transaktionen, könnte sich in diesem Zusammenhang zu einem Nachteil entwickeln. Bereits jetzt werden Bitcoins für Geschäfte in grauen und schwarzen Märkten eingesetzt und allerlei dubiose Angebote kursieren im Netz. Beliebt ist Bitcoin vor allem auf dem virtuellen Handelsplatz „Silk Road“. Silk Road existiert seit Februar 2011 in Form von Hidden Services im Tor-Netzwerk. Dies ist ein spezielles Netzwerk, das weitgehende Anonymität garantiert. Auf dem Markplatz werden hauptsächlich illegale Waren, wie Drogen, Waffen und Arzneimittel, gehandelt. Der Großteil der Anbieter stammt aus den USA, aber der Versand der Waren findet weltweit statt. Allein im ersten Halbjahr 2012 wurden durchschnittlich monatliche Umsätze von umgerechnet 1,2 Millionen US-Dollar erzielt und der Handel über Silk Road machte ca. 4,5 bis 9 Prozent aller Bitcoin-Transaktionen aus.

Für die Käufer hat Silk Road den Vorteil, nicht mit dem Verkäufer physisch in Kontakt treten zu müssen. Allerdings besteht beim Versand von Drogen oder anderen illegalen Waren für die Polizeibehörden eine Chance, die Güter zu entdecken und den Empfänger zu überführen. Da die meisten Sendungen als normale Briefe verschickt werden und diese aufgrund der schieren Masse nur stichprobenartig kontrolliert werden, ist die Entdeckungswahrscheinlichkeit aber sehr gering. Auch der Standort der Silk-Road-Server ist unbekannt, sodass es kaum möglich ist, den Handelsplatz durch Abschalten der Server zu schließen. Selbst wenn die Server ausgeschaltet werden könnten, würde wahrscheinlich bald eine Kopie von Silk Road entstehen.

Derzeit wächst der Handel auf Silk Road um durchschnittlich 6 Prozent pro Monat. Immer mehr Verkäufer kommen auf die Plattform, um die Wünsche von immer mehr Käufern nach illegalen Waren zu befriedigen und der gesamte Handel wird mit Bitcoin abgewickelt. Die einzige Möglichkeit, den Handel einzudämmen, besteht darin, die Handelswährung komplett zu verbieten, um die Nutzung der Profite außerhalb von Silk Road zu erschweren. Da Bitcoin momentan nur von einer kleinen Gruppe von Teilnehmern genutzt wird, die Akzeptanz gering ist und die Nutzung hauptsächlich über das Internet stattfindet, hätte ein Verbot keine großen Auswirkungen auf die bestehende Wirtschaft.

Die Anzeichen, dass die Regierungen gegen Bitcoin bzw. dessen Handelsplattformen vorgehen, mehren sich. Ende April 2013 stellte die amerikanische Bitcoin-Börse Bitcoin24 den Betrieb ein, da die US-Bankkonten des Unternehmens gesperrt worden waren. Da es dadurch nicht mehr möglich war, Ein- und Auszahlungen in US-Dollar auf dem bisherigen Niveau vorzunehmen, wurde der

Betrieb eingestellt. Kurz zuvor war eine der größten europäischen Handelsbörsen, Bitcoin24, abgeschaltet worden. Polnische Behörden hatten die Konten der Betreiber wegen Geldwäscheverdachts gesperrt.

Noch werden nur einzelne Handelsplätze geschlossen, die zudem eher kleine Umschlagplätze sind. Wenn das Bitcoin-System jedoch in einigen der großen Industrienationen verboten würde, könnte es nicht mehr im Alltag eingesetzt werden. Auch sämtliche Tausch- und Handelsbörsen würden in diesen Ländern illegal werden. Die Verbreitung und Akzeptanz von Bitcoin wäre somit schlagartig beendet. Da Akzeptanz aber eine Grundeigenschaft jeder Währung ist, hätte Bitcoin bei einem internationalen Verbot keine Chance mehr, sich als alternative Währung zu etablieren.

Zwar kann ein Verbot von Bitcoin leicht ausgesprochen werden, es ist allerdings sehr schwierig umsetzbar. Das Bitcoin-Netzwerk ist dezentral und die verwendeten kryptografischen Verfahren sind auch bei anderen, regulären Geschäftsvorgängen im Einsatz. Würde man diese Verschlüsselungsverfahren verbieten, wären keine sicheren Kreditkartentransaktionen, kein Online-Banking und kein Online-Handel mehr möglich.

Staaten sind aber durchaus bereit, auch etablierte Zahlungsmittel zu verbieten, wenn es ihren Interessen dient. Selbst Gold, das seit Jahrtausenden zur Speicherung von Werten dient, wurde immer wieder verboten, wie etwa in den USA, wo für mehrere Jahrzehnte ein Goldverbot bestand. Am 5. April 1933 unterzeichnete Präsident Franklin D. Roosevelt die Executive Order 6102, wonach der private Goldbesitz ab dem 1. Mai 1933 in den USA verboten wurde. Roosevelt wollte damit den Abfluss des amerikanischen Goldes in Folge der Weltwirtschaftskrise verhindern, denn zuvor hatten zahlreiche Kunden ihre Bankschließfächer geleert und das Gold ins eigene Heim oder ins Ausland geschafft.

Aufgrund des Erlasses musste das gesamte private Gold bei staatlichen Annahmestellen innerhalb von 14 Tagen zum festen Goldpreis von 20,67 US-Dollar pro Feinunze umgetauscht werden. Lediglich Goldmünzen und -zertifikate, die den Wert von 100 US-Dollar nicht überschritten, durften behalten werden. Entdeckten die Behörden danach bei einer angeordneten Durchsuchung von Tresoren und Schließfächern in Banken noch Gold, enteigneten sie dieses entschädigungslos.

Bei einem Verstoß gegen das Goldverbot konnte eine Geldstrafe von bis 10.000 US-Dollar oder eine Gefängnisstrafe von bis zu zehn Jahren oder beides in Kombination verhängt werden. Dennoch wurde der private Goldhandel auch in den folgenden Jahren fortgesetzt und auch die Preise für Goldmünzen stiegen. Letztlich erzielte die Verbotsverordnung nicht den gewünschten Effekt, sondern erreichte genau das Gegenteil. Sie ließ die Schmugglertätigkeit an der kanadischen und mexikanischen Grenze sowie den Lufttransport von Gold zu einem neuen lukrativen Geschäft werden und führte gleichzeitig zu einer Kapitalflucht durch unkonzessionierten Kauf von Goldmünzen und -barren im Ausland. Das Goldverbot von 1933 hatte dennoch 41 Jahre lang Bestand, bis es am 31. Dezember 1974 von Präsident Gerald Ford aufgehoben wurde.

Das Goldverbot in den USA zeigt, dass staatliche Eingriffe bei Wertgegenständen nicht immer erfolgreich sind und sogar preissteigernd wirken können. Nun ist der Goldbesitz nicht mit dem Besitz von Bitcoin vergleichbar, dennoch könnte bei ihrem Verbot eine ähnliche Entwicklung einsetzen und die Währung könnte weiterhin in der Illegalität existieren.

Auch digitale Bezahlsysteme können sehr schnell von der Justiz geschlossen werden, wie Liberty

Reserve erfahren musste. Das Unternehmen Liberty Reserve betrieb von Costa Rica aus ein kontobasiertes Internet-Bezahlsystem. Auf den Konten wurden die Einzahlungen realer Währungen in die Liberty-Währung „LR“ umgetauscht. Diese digitale Währung konnte dann an andere Kontoinhaber bei Liberty Reserve gesendet werden. Liberty Reserve kassierte bei jeder Transaktion ein Prozent an Gebühren, maximal 2,99 Dollar. Für zusätzliche 75 US-Cent wurde die Kontonummer des Überweisenden im System anonymisiert. Genauso wie im Bitcoin-System waren einmal abgeschlossene Zahlungen unwiderruflich. Da Liberty Reserve keinerlei Ausweis oder Identifizierung bei der Eröffnung eines Kontos verlangte, war de facto die anonyme Nutzung bei Angabe falscher Daten möglich. Aufgrund der Anonymität wurden kriminelle Aktivitäten gefördert. Liberty Reserve wurde aber nicht nur von Kriminellen genutzt, sondern auch von Menschen in Regionen, in denen Firmen wie PayPal oder Western Union nicht verfügbar sind. Es stellte eine Alternative zu den anderen Bezahlsystemen dar.

Im Gegensatz zu anderen Online-Bezahldiensten fanden bei Liberty Reserve keine direkten Zahlungen der Kunden an den Betreiber der Plattform statt. Ein- und Auszahlungen erfolgten über Drittanbieter, die dafür einen prozentualen Anteil der Summe als Gebühren behielten. Diese Drittanbieter, die hauptsächlich in Ländern mit sehr oberflächlichen Finanzkontrollen, wie Malaysia, Russland, Nigeria oder Vietnam, ihren Sitz hatten, kauften große Kontingente der virtuellen Währung LR bei Liberty Reserve und verkauften sie gegen eine Kommission von fünf oder mehr Prozent an die Nutzer weiter. Die Käufe und Verkäufe der Währung konnten mittels PayPal, Visa, MasterCard, American Express, Western Union, Banküberweisung, Paysafecard, MoneyGram oder Ukash vorgenommen werden. Einige Anbieter boten auch die Einzahlung von Bitcoin an.

Sobald ein Kunde ein Konto eröffnet hatte, konnte er sein Bargeld in Liberty-Reserve-Währungen bei den Händlern tauschen. Anschließend konnte er mit der digitalen Währung handeln und sie bei einem weiteren Händler wieder in Bargeld umtauschen - an einem völlig anderen Ort der Welt. Dadurch konnte Geld über Landesgrenzen hinweg auf andere Konten transferiert werden ohne dass die Behörden davon Kenntnis nehmen konnten.

Aufgrund der sehr laschen Identifizierungsvorschriften, die eine Kontoeröffnung nur mit Angabe eines Namens, einer Adresse und eines Geburtsdatums ohne jegliche Überprüfung ermöglichten, geriet Liberty Reserve schnell ins Visier zahlreicher Strafermittlungsbehörden und wurde verdächtigt, Geldwäsche, sowie illegalen Drogen- und Arzneimittelhandel zu unterstützen. Bei einer internationalen Aktion am 24. Mai 2013, die von der US-Justiz koordiniert wurde, verhafteten die Behörden den Betreiber von Liberty Reserve. Gleichzeitig wurden das gesamte System sowie die Internetpräsenz des Unternehmens vom FBI abgeschaltet. Der US-Staatsanwaltschaft zufolge soll das Unternehmen mindestens 55 Millionen illegale Transaktionen für mehr als eine Million Nutzer vorgenommen haben und dabei Geldwäsche im Volumen von insgesamt sechs Milliarden Dollar unterstützt haben.

Das Beispiel von Liberty Reserve zeigt, dass ein komplettes und durchaus auch umfangreiches Bezahlsystem von heute auf morgen abgeschaltet werden kann, wenn sich die Behörden zum Handeln entschließen. Dennoch ist dieses Vorgehen, selbst in einer koordinierten internationalen Aktion, nicht auf das Bitcoin-System übertragbar. Zwar war Liberty Reserve auch eine digitale Währung, die gegen andere Währungen eingetauscht werden konnte, aber sie war in der Menge nicht limitiert. Solange es genügend Kunden gab, die LR kaufen wollten, konnte die LR-Menge in inflationärer Weise immer

weiter aufgebläht werden. Das Bitcoin-System ist auf insgesamt 21 Millionen Stück begrenzt. Sie werden auch nicht von einer Firma mit einem bestimmten Geschäftsmodell herausgegeben, sondern in einem Peer-to-Peer-Computernetzwerk erzeugt. Der große Unterschied zu Liberty Reserve besteht aber darin, dass das Bitcoin-Netzwerk dezentral ausgelegt ist. Dadurch gibt es keinen zentralen Server, der einfach abgeschaltet werden kann. Wenn das Bitcoin-System durch einen staatlichen Eingriff ausgeschaltet werden soll, müsste jeder Rechner auf dem eine Version der Client-Software läuft, abgeschaltet werden. Das ist aber schon aufgrund der globalen Verteilung der zahlreichen Rechner unmöglich.

Die Schließung von Liberty Reserve könnte die Nutzerzahl des Bitcoin-Systems sogar weiter ansteigen lassen. Leider ist damit zu rechnen, dass sich auch ein Teil der illegalen Transaktionen, die bisher bei Liberty Reserve abgewickelt wurden, in das Bitcoin-Netzwerk verlagert. Dadurch kann Bitcoin verstärkt ins Visier der Ermittlungsbehörden rücken. Da es aber keinen zentralen Server gibt, der abgeschaltet werden kann und es auch keinen Verantwortlichen gibt, der festgenommen werden kann, geraten die Handelsplattformen in den Fokus der Behörden. So ist es wenig überraschend, dass die größte Handelsbörse für Bitcoin, Mt.Gox, bereits zwei Tage nach dem Schlag gegen Liberty Reserve Maßnahmen ergriffen hat. Kunden müssen ihr Konto zukünftig durch Einreichen einer Ausweiskopie sowie eines Adressnachweises verifizieren, wenn sie Bitcoin in andere Währungen tauschen oder Geld abheben möchten. Nur die Einzahlung und Abhebung von Bitcoin ist weiterhin anonym möglich.

Neben dem Einsatz von Bitcoin für illegale Geschäfte gibt es noch einen weiteren Aspekt, der das System für staatliche Institutionen problematisch erscheinen lässt. Alle etablierten Währungen werden durch Banken erschaffen. Zentralbanken schöpfen neues Geld und geben dieses an die Geschäftsbanken weiter. Diese geben wiederum Kredite aus und schaffen dadurch neues Geld. Durch die Schöpfung neuen Geldes ist die Geldmenge durch die Banken jederzeit vergrößerbar. Die Warenmenge ist jedoch nicht beliebig vermehrbar, sodass es bei einer immer stärker wachsenden Geldmenge und gleich bleibendem Warenbestand zur Inflation kommt. Der dadurch erzeugte Kaufkraftverlust würde den Vermögenstransfer an die ausgebenden Zentral- und Geschäftsbanken begünstigen. Um dieses staatlich kontrollierte Monopol der Geldschöpfung zu beschützen, könnten einzelne Regierungen Bitcoin verbieten.

Überlastungsrisiko

Bitcoin könnte auch am eigenen Erfolg scheitern. Viele Versionen der Client-Software, die am Bitcoin-Netzwerk teilnehmen, müssen zu Beginn die Datei mit allen bisher abgewickelten Transaktionen aus dem Internet laden. Dies kann je nach Internetverbindung bereits jetzt einige Stunden dauern. Noch läuft das gesamte Bitcoin-System weiter unter seiner Kapazitätsgrenze. Wenn jedoch zukünftig immer mehr Teilnehmer immer mehr Zahlung abwickeln, kann die Bestätigung dieser Transaktionen länger dauern. Das ist an sich kein großes Problem, da durch die freiwilligen Gebühren wichtige Zahlungen bevorzugt behandelt und bestätigt werden. Für eine allgemeine und schnelle Zahlungsmethode, wie z.B. Kredit- oder EC-Karten, stellt das Bitcoin-System aufgrund des Kapazitätslimits jedoch dann keine Alternative dar.

Auch die Block Chain, in der alle Transaktionen gespeichert werden, wird immer größer. Derzeit umfasst sie ca. 7,5 Gigabyte (Stand: Juni 2013). Nutzer mit einer langsamen Internetverbindung benötigen für den Download der gesamten Datei etliche Stunden. Wenn zukünftig mehr Transaktionen abgewickelt werden, nimmt die Größe der Datei immer weiter zu, sodass auch Aktualisierungen der Datei immer größer werden und länger dauern.

Es gibt bereits Überlegungen, wie die zukünftige Überlastung des Systems verhindert werden kann. Eine bereits praktizierte Lösung besteht darin, dass nicht alle Clients die vollständige Transaktionshistorie in der Block Chain speichern. Einige Clients gleichen Teilstücke der Block Chain mit der vollständigen Datei ab, die auf Remote Servern liegt. Eine Ausweitung dieses Vorgehens würde zwar das gesamte Netzwerk entlasten. Gleichzeitig wird dadurch aber die Dezentralität des Netzwerkes gefährdet, wenn einige zentrale Knoten geschaffen werden, die die gesamte Historie speichern. Diese Knoten stellen dann primäre Angriffspunkte für Hacker aber auch für ein mögliches Verbot des gesamten Netzwerkes dar.

Nischenrisiko

Ein Risiko liegt in der Entstehung weiterer digitaler Währungen. Bitcoin ist ein Open-Source-Projekt, die Software ist für jeden zugänglich und veränderbar und es gibt bereits einige andere digitale Währung, die auf dem Bitcoin-Protokoll basieren, wie z.B. Litecoin, PPCoin, Terracoin, Feathercoin und andere. Diese Währungen sind zwar noch weniger verbreitet als Bitcoin, aber es gibt auch für sie bereits erste Wechselkurse und Tauschbörsen. Eine dieser Währungen könnte Bitcoin in Akzeptanz und Verbreitung sogar übertreffen. Diese Entwicklung wäre nicht weiter tragisch, wenn die neue Währung eine breitere Akzeptanz unter den Nutzern findet. Eine Möglichkeit besteht in der Existenz mehrerer paralleler digitaler Währungen, die ihre jeweilige Nische besetzen und ihren speziellen Nutzerkreis haben. Diese Entwicklung wäre fatal, denn eine derartige Aufsplitterung würde die Durchsetzung des Konzeptes einer digitalen Währung verhindern. Keine dieser „Nischenwährungen“ wäre verbreitet und akzeptiert genug, um genügend Nutzer an sich zu binden.

Bitcoin hat zumindest den Startvorteil, sodass die Nachahmer zunächst einmal die Startschwierigkeiten überwinden müssen. Jede neue Währung, die auf der Bitcoin-Software basiert, hat zunächst keinen direkten Vorteil im Vergleich zu Bitcoin und kann auch nicht auf die Infrastruktur zugreifen, die sich mittlerweile um Bitcoin entwickelt hat. Erst wenn eine Währung auftritt, die all die Vorteile bietet, die auch Bitcoin hat und zusätzliche nützliche Eigenschaften aufweist, könnte Bitcoin rasch an Akzeptanz und Wert verlieren.

Selbst wenn Bitcoin die einzige Währung bleibt, die auf dem ursprünglichen Konzept basiert, so liegen Risiken in der mangelnden Akzeptanz bei der Wirtschaft und den fehlenden Anwendungen. Obwohl die Zahl der Nutzer und auch der Wert von Bitcoin in den letzten Monaten rasant gestiegen sind, so gibt es immer noch relativ wenige Anwendungen und Stellen, die Bitcoin akzeptieren. Wenn Bitcoin weiterhin eine Nischenexistenz fristet, könnte sich die derzeitige Bewertung als zu hoch erweisen und der Kurs entsprechend fallen.

Kontrollrisiko

Die Dezentralität und das Fehlen einer steuernden Institution, wie etwa einer Zentralbank, ist ein großer Vorteil des Bitcoin-Netzwerkes. Das Bitcoin-Protokoll wurde zwar von einer Person, Satoshi Nakamoto, erfunden, aber die Entwicklung blieb danach nicht stehen. Da Nakamoto öffentlich nie in Erscheinung getreten ist, übernahm ab 2011 ein fünfköpfiges Entwicklerteam die Betreuung der Software. Wenn es im gesamten Bitcoin-Netzwerk so etwas wie eine zentrale Autorität gibt, dann ist es wohl dieses Entwicklerteam, das versucht, die Software zu verbessern und Sicherheitslücken zu schließen.

Das Entwicklerteam besteht aus einer kleinen Gruppe von Programmierern um Gavin Andresen, die im Rahmen der „Bitcoin Foundation“ die Software betreuen und auf Sicherheitslücken oder Angriffe reagieren. Die meisten Nutzer vertrauen diesen Entwicklern und würden wohl auch Änderungen im Protokoll oder im Gesamtablauf des Bitcoin-Netzwerkes akzeptieren, da diese Änderungen bisher immer im Interesse des Gesamtsystems erfolgten. Dennoch ist nicht auszuschließen, dass das Entwicklerteam eigene Interessen verfolgt oder interessierte Kreise versuchen, Einfluss auf das Team zu nehmen, um die Entwicklung von Bitcoin in eine bestimmte Richtung zu lenken.

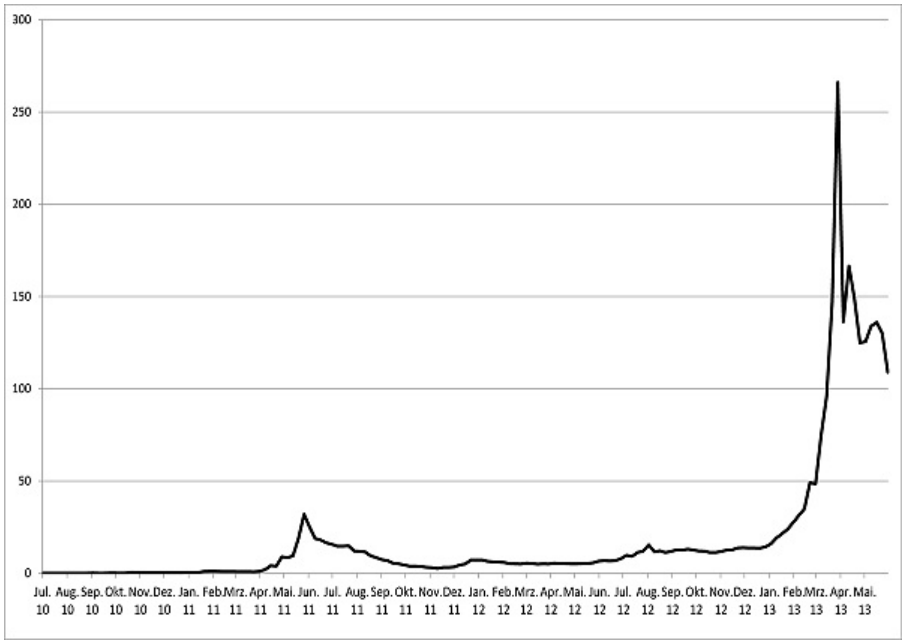
Ein weiteres Risiko besteht in der Übernahme der Kontrolle des Netzwerkes durch 51 Prozent der Rechenkapazität. Wenn sich 51 Prozent der Kapazität des Bitcoin-Netzwerkes in einer Hand befinden, sind alle Transaktionsbestätigungen von dieser Person oder Institution abhängig. Die Dezentralität des Netzwerkes, eines der Kernprinzipien für die Funktionsweise von Bitcoin, wäre damit nicht mehr gegeben. Zwar könnten selbst durch die Kontrolle von mehr als 51 Prozent des Netzwerkes keine neuen Bitcoins außerhalb der vorgesehenen Protokolle erzeugt werden, aber zumindest die Möglichkeit einer Blockade wäre gegeben. Im März 2011 umfasste die Rechenkapazität des gesamten Bitcoin-Netzwerkes ca. 500 Gigahashes pro Sekunde. Eine Grafikkarte mit einer Kapazität von 500 Megahashes kostete damals ca. 500 Euro. Das gesamte Netzwerk hatte also eine Kapazität von 1.000 dieser Grafikkarten. Mit 500 Grafikkarten, die einer Investition von ca. 250.000 Euro entsprechen, wäre es möglich gewesen, die Kontrolle über das Netzwerk zu übernehmen. Aufgrund der stark gestiegenen Nutzerzahlen und der umfangreicheren Rechenkapazität des Netzwerkes seit 2011 wird eine 51-Prozent-Attacke aber immer schwieriger und kostspieliger. Mit einer Gesamtrechenleistung des Netzwerkes von ca. 130 Terahashes, wie sie im Juni 2013 vorlag, müssten bereits 130.000 Grafikkarten zu je 500 Megahashes zur Verfügung stehen, um die Kontrolle über das Netzwerk übernehmen zu können. Mittlerweile kosten Grafikkarten dieser Leistungsklasse zwar nur noch ca. 250 Euro, aber es wäre immer noch eine Gesamtinvestition von 32.500.000 Euro sowie ein enormer Energieaufwand nötig.

Es gibt durchaus Personen oder Gruppen, die eine 51-Prozent-Attacke durchführen, allerdings nicht auf Bitcoin. Im Juni 2013 wurde aber eine auf dem Bitcoin-Protokoll basierende Alternativwährung, Feathercoin, Opfer eines 51-Prozent-Angriffs. Die Marktkapitalisierung der Währung betrug zu dem Zeitpunkt aber nur ca. 700.000 US-Dollar und dementsprechend gering war auch der notwendige Rechenaufwand. Die Gelegenheit für eine 51-Prozent-Attacke auf Bitcoin bot sich zu Beginn des Systems, als die Rechenleistung noch gering war. Mittlerweile ist eine derartige Attacke aber schwieriger und nur mit großem Ressourceneinsatz durchführbar.

Spekulationsrisiko

Bei dem kleinen Bitcoin-Markt mit noch wenigen Marktteilnehmern ist Liquidität ein Problem. Nicht immer gibt es genügend Käufer und Verkäufer von Bitcoins, um einen Austausch zu ermöglichen. Dies erschwert den Transfer von Guthaben in andere Währungen und umgekehrt. Gleichzeitig ist die Gefahr von heftigen Kursschlägen nach oben und unten gegeben. Der Bitcoin-Kurs ist sehr volatil und Schwankungen von 10 Prozent und mehr am Tag sind durchaus normal. Auch Spekulationsblasen können sich bilden. 2011 gab es die erste Spekulationsblase, als der Kurs Mitte des Jahres auf fast 32 Dollar hochschnellte, um dann im November wieder auf 2 Dollar zu fallen.

Von September 2012 bis April 2013 gab es eine ähnliche Entwicklung. Ein langsamer Anstieg des Kurses setzte ein, der sich zu Beginn des Jahrs 2013 beschleunigte. In zahlreichen Medienberichten wurde verstärkt über Bitcoin berichtet, nicht zuletzt auch im Zusammenhang mit der Bankenkrise in Zypern. Bitcoin wurde als Alternative angesehen, um Guthaben auch während einer Krise mit erzwungenen Bankenschließungen retten zu können. Infolge des gestiegenen öffentlichen Interesses setzte sich der Anstieg beinahe ohne Kursrückschläge fort und erreichte am 28. Februar 2013 wieder seinen alten Höchststand vom Juni 2011. Am 6. März stand der Kurs bereits bei 48 Dollar und Ende des Monats, am 28. März, hatte der Kurs 94 Dollar erreicht. Am 10. April erreichte er schließlich sein bisheriges Hoch bei 266 Dollar, um sich dann, nach einer kurzzeitigen Schließung der Handelsbörse Mt.Gox, im Bereich von 100 bis 120 Dollar zu stabilisieren.



Bitcoin-Kurs in Dollar seit 2010

Quelle: Eigene Darstellung, mit Daten von *http://bitcoincharts.com*.

Die Kursentwicklung zeigt deutlich, dass Bitcoin sehr starken Schwankungen unterliegt und eine Investition sehr spekulativ ist. Für diejenigen, die früh in Bitcoin investiert haben, hat sich das Risiko bereits gelohnt. Für alle, die erst in der Nähe des Höchstkurses eingestiegen sind, erweist sich das Investment momentan als Fehlschlag. Die hohe Volatilität der Währung steht der Funktion als Zahlungsmittel entgegen. Wenn sich ein Bitcoin über Nacht im Wert verdoppeln oder aber halbieren kann, ist dies für Käufer und Verkäufer keine solide Kalkulationsgrundlage.

Interessanterweise erreichte der Bitcoin-Kurs parallel zur Zypernkrise seinen Höchststand. Die Inselrepublik war aufgrund der engen Verflechtungen mit dem griechischen Bankensystem in eine

finanzielle Schieflage geraten und benötigte Anfang 2013 dringend Hilfsgelder der EU, um einen Staatsbankrott abzuwenden. Da Zypern aber durch seine niedrigen Kapitalsteuern auch für ausländisches Kapital, vor allem aus Russland, beliebt war und sich hauptsächlich auf dieses Geschäftsmodell verlassen hatte, wollte die EU Hilfsgelder nicht ohne zyprische Beteiligung auszahlen. Die im März 2013 erzielte Einigung zwischen Zypern und der EU sah vor, die angeschlagene Cyprus Popular Bank aufzulösen und dortige Einlagen mit einem Volumen von mehr als 100.000 Euro – insgesamt 4,2 Milliarden Euro – vollständig in eine abzuwickelnde „Bad Bank“ auszulagern, sodass auch die Möglichkeit eines Komplettverlustes für diese Einleger nicht ausgeschlossen ist. Einlagen von unter 100.000 Euro wurden der Bank of Cyprus übertragen, die verkleinert und restrukturiert werden soll. Einlagen in der Bank of Cyprus von über 100.000 Euro wurden eingefroren und sollen später vermutlich an den Kosten beteiligt werden. Dadurch wurden erstmals in der Geschichte des Euro Spareinlagen direkt zur Beseitigung der Folgen der Finanzkrise herangezogen. Aufgrund tagelanger Bankenschließungen und beschränkter Auszahlungsmöglichkeiten konnten die Menschen nicht an ihre Einlagen auf den Konten herankommen.

In einer derartigen Notsituation ist ein Bezahlsystem, das unabhängig von Banken funktioniert, eine willkommene Alternative. Die während der Zypernkrise im Februar und März 2013 geschürte Hoffnung, Bitcoin-Guthaben seien eine sichere Alternative zu Bankguthaben, erfüllte sich angesichts des Kursverlaufs bisher aber nicht.

Deflationsrisiko

Ein Risiko besteht in der Begrenzung des Bitcoin-Systems auf insgesamt 21 Millionen Stück, die 2040 komplett errechnet sein werden. Danach können keine neuen Bitcoins mehr erzeugt werden und es gibt auch keine Zentralbank, die sie erschaffen könnte. Wenn jedoch immer mehr Teilnehmer das Bitcoin-System nutzen, die Menge an Bitcoin aber gleich bleibt, steigt deren Wert. Dies kann zu einer Deflation führen, denn die Bitcoin-Besitzer werden nicht bereit sein, ihre Bitcoins gegen andere Währungen oder Waren einzutauschen, da sie auf einen steigenden Wert in der Zukunft und damit auf sinkende Preise der anderen Waten hoffen. Dadurch würde eine deflationäre Spirale in Gang gesetzt werden.

Bei einer Deflation sinkt das allgemeine Preisniveau über einen längeren Zeitraum. Verbraucher und Unternehmen halten sich mit ihren Anschaffungen zurück, da sie damit rechnen, dass die Preise in Zukunft weiter zurückgehen werden und sie die Waren später noch preiswerter erwerben zu können. Unternehmen reagieren auf die sinkende Nachfrage mit Preissenkungen und Produktionseinschränkungen. Diese Einschränkungen führen wiederum zu Entlassungen, was die Nachfrage der Verbraucher weiter zurückgehen lässt. Die Spirale von Produktions- und Nachfragerückgängen wird durch die abwartende Haltung der Verbraucher in der Hoffnung auf niedrigere Preise in der Zukunft erneut verstärkt.

Letztendlich endet die Deflationsspirale in einer wirtschaftlichen Depression, deshalb ist nach Ansicht vieler Ökonomen eine Deflation für eine Volkswirtschaft gefährlicher als eine Inflation. Während die Inflation mit höheren Leitzinsen bekämpft werden kann, sind bei der Deflation Zinssenkungen angebracht, um mit dem „billigen“ Geld die Nachfrage anzukurbeln. Der Leitzins kann jedoch minimal auf 0 Prozent gesenkt werden. Wenn diese Grenze erreicht ist, muss die Zentralbank andere geldpolitische Maßnahmen ergreifen, um Liquidität in die Wirtschaft zu pumpen. Eine dieser Maßnahmen ist die „quantitative Lockerung“. Dabei kauft die Zentralbank eines Landes die eigenen Staatsanleihen auf, um die Wirtschaft mit Geld zu versorgen.

Nachdem die amerikanische Notenbank Fed im Zuge der Finanzkrise von 2008 den Leitzins auf 0–0,25 Prozent gesenkt hatte, griff sie ebenfalls zur quantitativen Lockerung und kauft seitdem in größerem Umfang Staatsanleihen auf, um den Markt mit Liquidität zu versorgen. Mittlerweile läuft das dritte Programm dieser Art und pro Monat werden 85 Milliarden Dollar in den Markt gepumpt. In Japan, das sich seit den frühen 1990ern in einer deflationären Phase befindet, läuft derzeit das achte Programm zur quantitativen Lockerung. Die Dauer und die Maßnahmen zur Bekämpfung einer Deflation zeigen, dass sie hartnäckiger und schwieriger zu beseitigen ist als eine Inflation.

Da Bitcoin nicht auf ein Land beschränkt ist, sondern global gehandelt werden kann, ist noch nicht klar, ob das deflationäre Szenario im Bitcoin-System vergleichbar ist mit der Deflation einer nationalen Währung und deren negativen Auswirkungen auf die Ökonomie eines einzelnen Landes. Es gibt schlicht keine Bitcoin-Zentralbank, die geldpolitische Maßnahmen zur Stabilisierung des Systems ergreifen kann. Außerdem sind Bitcoins auf die achte Nachkommastelle teilbar. Jeder Bitcoin besteht aus 100.000.000 Satoshis, der kleinsten Recheneinheit im Bitcoin-System. Bei 21 Millionen Bitcoin stehen insgesamt 2.100.000.000.000.000 Einheiten zur Verfügung. Bei einer geschätzten Weltbevölkerung von ca. 7 Milliarden kann jeder Mensch über 300.000 Satoshis bzw. 0,003 Bitcoin verfügen. Sollte diese Menge nicht mehr ausreichen, kann die Kommastelle im System von den Entwicklern weiter versetzt werden, um eine noch kleinere Stückelung zu ermöglichen.

Die Chancen des Bitcoin-Systems

Ein Grund, warum sich Bitcoin trotz der zahlreichen Risiken und Rückschläge so rasch verbreiten konnte, ist das Misstrauen vieler Menschen gegenüber dem bestehenden Finanzsystem. Die völlige Freiheit von staatlicher Kontrolle und die Unabhängigkeit von Banken lässt Bitcoin als attraktive Alternative zu den existierenden Banken- und Währungssystemen erscheinen. Dabei handelt es sich nicht um ein lokal begrenztes Phänomen. Das Misstrauen und die Unzufriedenheit mit den bestehenden Finanzsystemen finden sich weltweit. Auch das ist ein Grund, warum sich ein dezentrales Geldsystem, das nur über das Internet funktioniert, so schnell ausbreiten kann.

Wertsteigerungschance

Als Anlage- und Investitionsmedium gewinnt Bitcoin an Bedeutung, vor allem in Zeiten der Eurokrise. Kürzlich wurde das Britische Pfund vom Euro als zweithäufigste Bitcoin-Tauschwährung abgelöst. Mittlerweile werden ca. 10 Prozent aller Bitcoins in Euro getauscht, vor allem angetrieben durch die Nachfrage aus Griechenland, Spanien, Italien und Zypern. Ähnlich wie Gold werden Bitcoins derzeit als Wertspeicher und nicht für den Handel genutzt. Vermögen wird in Form von Bitcoin gespeichert, um gegen staatliche Zugriffe, wie bei der Zwangsbeteiligung der Sparer während der Zypernkrise, geschützt zu sein.

In der Studie „Quantitative Analysis of the Full Bitcoin Transaction Graph“ fanden Dorit Ron und Adi Shami heraus, dass ca. 78 Prozent aller bisher erzeugten Bitcoins nicht für den Handel genutzt werden (Vgl. *http://eprint.iacr.org/2012/584.pdf*). Die beiden Forscher analysierten die Block Chain und stellten fest, dass viele Adressen zwar Bitcoins empfangen, aber von diesen Adressen dann keine Bitcoins mehr gesendet werden. Von den derzeit ca. 11,2 Million Bitcoins werden also über 8 Millionen als Sparguthaben gespeichert. Da die digitale Währung, genauso wie Gold, keine Zinsen abwirft, kann dies nur bedeuten, dass die Bitcoins in der Hoffnung auf eine zukünftige Wertsteigerung gespeichert werden oder als Schutz gegen den drohenden Wertverlust der bestehenden Fiat-Währungen durch Inflation.

Angesichts der Wertentwicklung in den letzten beiden Jahren hätte sich bei einem Bitcoin-Sparguthaben eine jährliche Verzinsung von ca. 400 Prozent ergeben. Damit wird die Inflationsrate locker geschlagen. Wenn sich die hohe Volatilität im Bitcoin-Kurs legt und Käufer und Verkäufer mit stabilen Kursen kalkulieren können, ohne befürchten zu müssen, über Nacht die Hälfte ihres Guthabens zu verlieren, bestehen gute Chancen, dass sich die Währung als Zahlungsmittel im Internet etablieren kann.

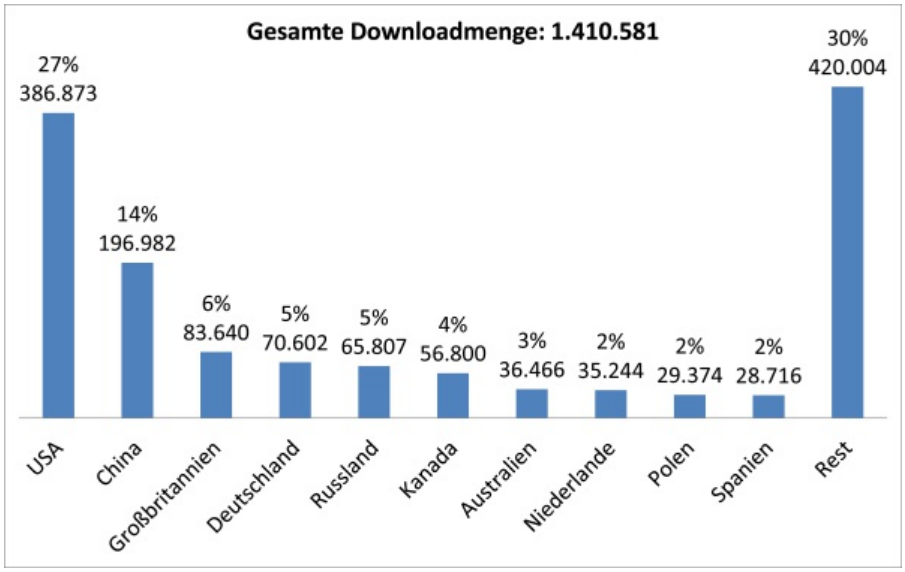
Gab es zu Beginn der Bitcoin-Währung nur den US-Dollar als Referenzkurs, so ist bei vielen Börsen eine Ausweitung der Wechselkurse festzustellen. Mittlerweile gibt es Kurse für US-Dollar, Britisches Pfund, Euro, Polnische Zloty, Tschechische Kronen, Australische Dollar, Chinesische Renminbi, Indische Rupien, Saudische Rial, Chilenische Pesos, Japanische Yen, Schweizer Franken, Dänische Kronen, Russische Rubel, Schwedische Kronen, Kanadische Dollar, Brasilianische Real, Hongkong-Dollar, Neuseeland-Dollar, Singapur-Dollar und Thailändische Baht. Bitcoin ist also in fast alle gängigen Währungen wechselbar und kann auch als „Speicher“ benutzt werden, wenn der direkte Wechselkurs zwischen zwei Währungen momentan ungünstig erscheint.

Dezentralitätschance

Im Gegensatz zu allen existierenden Fiat-Währungen gibt es keine Bitcoin-Zentralbank. Dies ist ein Vorteil, denn alle Zentralbanken verfolgen neben der reinen Geldverwaltung auch andere Ziele. So hat die amerikanische Zentralbank, die Federal Reserve, einen hohen Beschäftigungsstand, Preisniveaustabilität und moderate langfristige Zinsen zum Ziel. Die Europäische Zentralbank hat die allgemeine Preisstabilität und die Unterstützung der Wirtschaftspolitik der Europäischen Gemeinschaft als Zielvorgaben. Die Verfolgung dieser Ziele schließt nicht aus, dass die ursprünglichen Aufgaben der Zentralbanken, das Halten der Währungsreserve und die Funktion als Bank der Banken und der öffentlichen Hand sowie die Herausgabe von Scheinen und Münzen, vernachlässigt oder der Erreichung der Ziele untergeordnet werden. Ohne zentrale Institution kann Bitcoin den reinen Zwecken des Geldes als Tausch- und Zahlungsmittel, als Recheneinheit sowie als Wertspeicher dienen.

Durch die Dezentralität ist das Bitcoin-Netzwerk auch besser gegen Angriffe geschützt. Es gibt zwar immer wieder Attacken gegen einzelne Handelsplätze und Börsen, aber das Bitcoin-Netzwerk an sich und seine grundlegende Funktionalität können durch einen Hackerangriff nicht außer Funktion gesetzt werden, da es keinen zentralen Server gibt, der die Transaktionen verwaltet und der attackiert werden kann. Da sich das Netzwerk aus mehreren zehntausend Rechnern der Nutzer zusammensetzt, die weltweit verteilt sind, ist ein koordinierter Angriff sehr schwierig; mit der wachsenden Zahl der Nutzer würde er außerdem immer schwieriger werden.

Die Zahl der Bitcoin-Nutzer und damit auch die Dezentralität wächst ohnehin stetig. Allein vom Client bitcoin-qt wurden von Januar bis Mai 2013 über 1,4 Millionen Stück heruntergeladen, wobei sich in einigen Ländern besondere Schwerpunkte herausbilden:



Downloads von bitcoin-qt im Zeitraum von 1. Januar bis 31. Mai 2013

Quelle: Eigene Darstellung basierend auf Daten von *http://sourceforge.net/projects/bitcoin/*.

Neben dem „Ursprungsland“ von Bitcoin, den USA, holt China mittlerweile stark auf. Im Mai 2013 haben die Downloadzahlen aus China mit 84.538 die amerikanischen Downloads von 63.844 bereits überholt. Nachdem Bitcoin in China noch kaum verbreitet ist, werden die Download-Zahlen in den nächsten Monaten wahrscheinlich weiter ansteigen. Die hier genannten Zahlen beziehen sich nur auf den Client bitcoin-qt. Insgesamt liegt die Nutzerzahl wesentlich höher, da es noch weitere Client-

Programme gibt, die ebenfalls weltweit genutzt werden.

Das Bitcoin-System existiert seit 2009 und bisher konnte es noch nicht gehackt werden. Die einzige bekannte Sicherheitslücke im System wurde im August 2010 sehr schnell erkannt und geschlossen. Alle weiteren Angriffe fanden nicht mehr gegen das System selbst statt. Dafür gerieten die Tauschbörsen ins Visier der Angreifer. Attacken auf Mt.Gox verursachen immer wieder Handelsausfälle und beeinträchtigen die Möglichkeit, Bitcoins zu kaufen und zu verkaufen. Gleichzeitig zeigt der Fokus der Hackerangriffe, wo das schwächste Glied der Bitcoin-Kette ist. Es wird nicht das System angegriffen, sondern die Handelsplattformen. Hier besteht vonseiten der Plattformbetreiber noch Handlungsbedarf zur Verbesserung der Sicherheit.

Darüber hinaus kommt den großen Handelsbörsen aber auch eine stabilisierende Funktion zu. Im Augst 2011 hatte die polnische Website bitomat.pl, die damals drittgrößte Plattform für den Bitcoin-Handel, aufgrund eigener technischer Fehlkonfigurationen den Zugang zu einer Wallet-Datei mit über 17.000 Bitcoin an Kundeneinlagen verloren. Mt.Gox kaufte daraufhin bitomat.pl, stellte die Guthaben wieder her und integrierte den polnischen Złoty in die eigene Wechselkursliste. Der Kauf wurde von Mt.Gox mit der Wiederherstellung des Vertrauens in das Bitcoin-System begründet.

In Zeiten des „gläsernen Bürgers“ und der zunehmenden Überwachung sämtlicher Aktivitäten stellt die Anonymität einer dezentralen Bitcoin-Transaktion einen Vorteil dar, der die zukünftige Verbreitung fördern kann. Im Gegensatz zu Bankkonten, die weder anonym noch vor dem Zugriff der staatlichen Behörden geschützt sind, sind die Wallets der Bitcoin-Clients nur dem jeweiligen Besitzer zugänglich.

Auch der anonyme Transfer größerer Summen über Ländergrenzen hinweg ist denkbar. Dies ist in Zeiten zunehmender grenzübergreifender Kontrollen der Staaten zur Aufdeckung von Kapitalströmen eine interessante Option. Derzeit plant z.B. die EU-Kommission in einer Richtlinie die Ausweitung des Austauschs von Steuerinformationen innerhalb der 27 Mitgliedsstaaten auf alle Kapitaleinkünfte. Bisher wurden nur Zinserträge gemeldet, aber zukünftig sollen auch Dividenden, Kapitalerträge, anderweitige Finanzeinkommen und Kontenguthaben ausgetauscht werden. Damit wäre das Bankgeheimnis so gut wie aufgehoben. Die EU-Kommission folgt dem Beispiel der US-Behörden. Die US-Finanzbehörden haben bereits die Herausgabe der Kontodaten von US-Bürgern bei ausländischen Banken durchgesetzt.

Mit Bitcoin steht ein Transfermittel zur Verfügung, das es ermöglicht, anonym größere Summen ins Ausland zu transferieren. Ohne größere Probleme gelangen Bitcoin-Guthaben auf einem Smartphone oder USB-Stick durch jede Zoll- oder Devisenkontrolle und können an einem anderen Ort wieder in reale Währungen zurückgetauscht werden. Bei besonders strengen Kontrollen ist noch nicht einmal ein elektronisches Gerät für den Transfer notwendig. Der private Schlüssel einer Bitcoin-Adresse lässt sich – ein gutes Gedächtnis vorausgesetzt – auch auswendig lernen und an jedem Computer mit Internetzugang wieder in die digitale Währung umwandeln.

Marktchance

Niemand war am Anfang bereit, etwas gegen Bitcoin einzutauschen oder etwas für Bitcoin zu tun. Nachdem ihr Erfinder, Satoshi Nakamoto, seinen ersten Tauschpartner gefunden hatte, entstand ein Markt, und seitdem wächst dieser Markt mit jeder Transaktion und jedem Nutzer. Die Gefahr der zu geringen Akzeptanz und des Nischenprojektes ist noch lange nicht eingedämmt, aber das wachsende Interesse am Bitcoin und die steigende Anzahl an Transaktionen lassen diese Gefahr täglich kleiner werden. Einen großen Sprung bei der Verbreitung machte die Währung am 15. November 2012, als die Website Wordpress.com ankündigte, zukünftig auch Bitcoin als Zahlungsmittel zu akzeptieren. Wordpress.com ist mit rund 60 Million Websites eine der größten Hostingseiten für Blogs. Dies ist ein Zeichen dafür, dass sich die Akzeptanz und der Markt für den Bitcoin vergrößert.

Mittlerweile gibt es eine breite Palette an Geschäften, die Bitcoin akzeptieren. Viele Waren und Dienstleistungen können bereits mit Bitcoin bezahlt werden. Hauptsächlich werden Online-Dienste angeboten, wie Webdesign, Grafikgestaltung und Webhosting. Aber auch Software, Bücher, Blumen, Kleidung, Spielzeug, Handwerks- und Beratungsdienstleistungen lassen sich mit Bitcoin kaufen. Auch Finanzdienstleistungen finden sich bereits im Angebot. So ist es inzwischen möglich, sich Bitcoin zu leihen bzw. diese zu verleihen. Der Bitcoin-Markt ist dennoch sehr jung und dynamisch. Zahlreiche Händler verschwinden bald wieder von der Bildfläche oder akzeptieren keine Bitcoin mehr. Trotz diverser Rückschläge kann mit der Zeit ein belastbares Wirtschaftssystem um Bitcoin entstehen.

Eine detaillierte Liste mit Anbietern verschiedenster Waren und Dienstleistungen sowie Akzeptanzstellen vor allem im deutschsprachigen Raum findet sich unter *https://de.bitcoin.it/wiki/Handel*. Im internationalen Bereich gibt es bereits wesentlich mehr Händler und Shops, die Bitcoin akzeptieren. Eine ausführliche Liste findet sich unter *https://en.bitcoin.it/wiki/Trade*. Einige Organisationen nehmen mittlerweile auch Spenden in Bitcoin entgegen: *https://de.bitcoin.it/wiki/Spenden*. Gerade im Bereich der Mikrospenden zeigt sich der Vorteil der kostenlosen Übertragung der Bitcoins. Eine Spende von 10 Cent macht bei den traditionellen Bezahlsystemen, wie einer Überweisung, keinen Sinn, da die Gebühren viel zu hoch wären. Im Bitcoin-System ist die Transaktion kostenlos und selbst Spenden von nur 0,00000001 BTC kommen ohne Abzug beim Empfänger an.

Trotz der vielfältigen Shops und Händler, die Bitcoin annehmen, ist die Währung noch weit davon entfernt, breit akzeptierte zu sein. Die meisten Geschäfte mit Bitcoin werden online abgewickelt, der Handel in der realen Welt ist noch selten. Dennoch gibt es in Berlin bereits erste Bars und Kneipen, die Bitcoin als Zahlungsmittel akzeptieren; hierfür ist natürlich ein Smartphone Voraussetzung.

Bitcoin gewinnt zunehmend auch das Interesse von Investoren auf der Suche nach neuen Geschäftsideen. So konnte die Online-Wallet-Website Coinbase (*https://coinbase.com*) im Mai 2013 fünf Millionen Dollar Investitionskapital einsammeln, um die eigenen Services auszuweiten. Auch andere Startup-Unternehmen aus dem Bitcoin-Sektor werden momentan von Investoren mit Risikokapital verstärkt nachgefragt. Dies sind Anzeichen, dass der neuen Technologie ernsthafte Chancen auf eine weitere Ausbreitung eingeräumt werden.

Im Gegensatz zu regulären Zahlungsmitteln, wie etwa Lastschriften oder anderen besonders im Onlinebereich verbreiteten Zahlungsmethoden, können Bitcoin-Zahlungen nicht rückgängig gemacht werden. Wenn das Bitcoin-Netzwerk den Transfer bestätigt hat, gibt es keine Möglichkeit der

Rückabwicklung mehr, es sei denn, der Empfänger sendet die Bitcoin in einer neuen Transaktion wieder zurück. Für Verkäufer im Onlinehandel stellt dies einen großen Vorteil dar, denn neben den nicht vorhandenen bzw. sehr geringen Transaktionskosten besteht für Verkäufer ein sehr geringes Ausfallrisiko. Das Risiko verlagert sich hin zum Käufer. Für ihn besteht ein höheres Ausfallrisiko, da er bei Vorauszahlung der Ware und anschließender Nichtlieferung keine unmittelbare Möglichkeit hat, sein Geld zurückzubekommen. Bewertungssystemen kommt dadurch eine stärkere Bedeutung zu, da sie Rückschlüsse auf die Vertrauenswürdigkeit eines Verkäufers zulassen. Da das Ausfallrisiko bei vielen Anbietern bereits im Angebotspreis einkalkuliert ist, können die verbreitete Zahlung mit Bitcoin und der damit verbundene Wegfall dieses Risikos für den Käufer zu sinkenden Preisen führen. Unterstützt wird diese Tendenz durch die generell kostenlosen Transaktionen von Bitcoin.

Kostenchance

Grundsätzlich sind die Transaktionen von Bitcoin kostenlos; es gibt nur freiwillige Gebühren, um die Bestätigung der Transaktion im Netzwerk zu beschleunigen. Durch die Geschwindigkeit und die geringen Kosten tritt Bitcoin dadurch in Konkurrenz zu etablierten Bezahlsystemen, vor allem im internationalen Zahlungsverkehr. Aufgrund der Geschwindigkeit bei der Übertragung ist die digitale Währung Systemen, wie SWIFT- oder SEPA-Überweisungen, überlegen, und wegen der nicht oder kaum vorhandenen Transaktionskosten tritt sie in Konkurrenz zu PayPal- und Kreditkartenzahlungen.

Allein MasterCard macht pro Jahr ca. 7,5 Milliarden Dollar Umsatz. Nimmt man die Umsätze der anderen Kreditkartengesellschaften und Bezahlsysteme hinzu, so ergeben sich riesige Summen, die jährlich eingespart werden könnten, wenn für den Transfer Bitcoins eingesetzt würden. Außerdem sind die Bitcoin-Transaktionen sehr schnell, denn in der Regel sind die Bitcoin innerhalb von wenigen Minuten beim Empfänger. Dies kann die Zahlung mit Bitcoin zukünftig zu einer Alternative werden lassen, vor allem im Internet und vor allem bei kleineren Beträgen, bei denen sonst zu hohe Gebühren entstehen würden.

Die kostenlosen Transaktionen wirken sich bereits in der realen Wirtschaft aus. So bietet beispielsweise der amerikanische Webshop bitcoinstore (*https://www.bitcoinstore.com*) gegen Bitcoin elektronische Geräte, wie Laptops, Digitalkameras, MP3-Player usw., günstiger als die Konkurrenz an. Das ist möglich, weil die Zahlung mit Bitcoin keine zusätzlichen Gebühren für den Verkäufer verursacht – im Gegensatz zu Kreditkarten oder PayPal. Auch das Ausfallrisiko muss der Händler nicht mehr einpreisen und kann diesen Vorteil an seine Kunden weitergeben. Der Shop verzichtet momentan aber auch auf seine eigene Gewinnmarge, da der Besitzer mit weiter steigenden Kursen rechnet und er momentan versucht, so viele Bitcoin wie möglich anzusammeln.

Damit die günstigen Transaktionsgebühren funktionieren können, muss das System allgemein akzeptiert werden, nicht nur beim Sender und Empfänger einer Transaktion, sondern auch im Alltag. Wenn jemand, der keine Bitcoins hat, einem Empfänger Bitcoins schicken will, muss er sie erst gegen eine andere Währung eintauschen. Wenn der Empfänger der Bitcoins dann etwas anderes kaufen möchte und Bitcoins bei seinem Händler nicht akzeptiert werden, muss er sie zuerst wieder in eine andere Währung zurücktauschen. Die Transaktion der Bitcoins ist zwar immer noch kostenlos oder nur mit freiwilligen Gebühren möglich, allerdings entstehen durch den Tausch in eine andere Währung aufseiten des Senders und des Empfängers Kosten, die sich durchaus mit denen anderer Bezahlsysteme vergleichen lassen.

Im Bereich des Mikropayment ergeben sich durch Bitcoin völlig neue Geschäftsmodelle, nicht nur im Spendensegment. Denkbar ist eine Kombination mit dem aktuell boomenden Crowdfunding. Dabei handelt es sich um eine Methode der Geldbeschaffung, die Produkte und Dienstleistungen durch Eigenkapital, zumeist in Form von stillen Beteiligungen, ermöglicht. Die Kapitalgeber setzen sich aus einer Vielzahl von Personen zusammen, die sich über eine Plattform im Internet zur Finanzierung eines gemeinsamen Projektes koordinieren. Dank der Bitcoin-Währung und ihrer geringen Kosten wird der Einstieg in das Crowdfunding bereits mit sehr geringen Beträgen möglich. Da es für das Versenden von Bitcoins keine Beschränkungen gibt, erweitert sich der Kreis potentieller Kapitalgeber auf die gesamte Welt.

Ende März 2013 hat eine Unterbehörde des US-Finanzministeriums erstmals Richtlinien für

Bitcoin-Wechselstuben herausgegeben und klargestellt, dass sie ebenso wie die Händler herkömmlicher Währungen Buchhaltungs- und Prüfstandards einhalten müssen. Dies mag auf den ersten Blick wie eine Einschränkung der bis dahin herrschenden Freiheit im Bitcoin-Handel wirken. Gleichzeitig ist es aber auch ein Beweis dafür, dass Bitcoin mittlerweile verstärkt von den Behörden, zumindest den amerikanischen, wahrgenommen und sogar anderen Währungen gleichgesetzt wird, da für die Handelsplätze dieselben Regeln gelten sollen wie für andere Währungsbörsen.

Fazit

Das Bitcoin-System ist zweifellos komplex und nicht für jeden auf den ersten Blick zu verstehen. Die technischen Feinheiten des Bitcoin-Systems sind kompliziert, aber auch die Details etablierter Währungen, wie des Euro oder Dollar, sind nicht auf den ersten Blick erfassbar und trotzdem werden sie täglich milliardenfach benutzt. Im Gegensatz zu vielen Währungen ist Bitcoin frei zugänglich und die Software ist leicht zu bedienen, auch wenn man die dahinter stehenden Vorgänge nicht im Detail versteht.

Bitcoin steht in Konkurrenz zu traditionellen Fiat-Währungen, aber ebenso zu Wertspeichern wie etwa Gold. Ein Vergleich der gängigsten Eigenschaften mit den bereits erwähnten Fiat-Währungen sowie Gold zeigt, dass Bitcoin relativ gut abschneidet.

	Gold	Fiat-Währung	Bitcoin
Tausch- und Zahlungsmittel	0	+	-
Recheneinheit	0	+	+
Wertaufbewahrung	+	0	0
Sicherheit	+	+	0
Übertragbarkeit	0	+	+
Kontrolle/Überwachung	+	-	+
Kosten/Gebühren	-	-	+

Als Tausch- und Zahlungsmittel ist Bitcoin noch sehr begrenzt einsetzbar. Die digitale Währung wird nicht, wie reguläre Währungen, überall akzeptiert. Auch Gold, das zwar keine offizielle Währung ist, findet wesentlich mehr Akzeptanz als Bitcoin. Gängige Währungen sind weit verbreitet und werden, wie der US-Dollar, weltweit akzeptiert.

Als Recheneinheit ist Bitcoin gut verwendbar, da er bis auf die achte Nachkommastelle in kleinere Einheiten teilbar ist. Somit ist es möglich noch mit 0,00000001 Bitcoin zu bezahlen. Auch die regulären Währungen sind mit ihren zwei üblicherweise genutzten Nachkommastellen als Recheneinheit gut geeignet. Gold ist dagegen weniger gut geeignet, da es zwar in Feinunzen (31,1 Gramm) gemessen wird und auch diese teilbar sind, aber nicht in ausreichender Feinheit. Kleinere gängige Stückelungen sind z.B.1/20 Feinunze, was aber immer noch 1,555 Gramm Gold oder ca. 50 Euro entspricht. Kleinere Zahlungen sind mit Gold nur schwer zu bewerkstelligen.

Zur Wertaufbewahrung in Krisenzeiten eignet sich Gold allerdings hervorragend, denn egal ob in der Antike, im Mittelalter oder in der Neuzeit, das Edelmetall besaß stets einen gewissen Wert. Fiat-Währungen eignen sich dagegen weniger zur Wertaufbewahrung. Da sie durch die Zentralbanken beliebig vermehrt werden können, schwindet ihr Wert permanent, was durch die jährliche Inflationsrate belegt wird. Bitcoin existiert erst seit vier Jahren. In diesem Zeitraum hat die digitale Währung die Funktion als Wertspeicher aber nicht ausreichend erfüllt, da ihr Kurs zu stark schwankt. Eine Anlage zu Beginn der Entwicklung von Bitcoin hätte sich zwar vervielfacht, aber momentan mangelt es noch an ausreichenden Beweisen, dass sich eine Investition in Bitcoin auch in Zukunft als beständiger Wertspeicher erweisen wird. Genauso wie Gold und Fiat-Währungen müssen auch

Bitcoins nicht sofort wieder ausgegeben werden, sie können im Sinne eines Wertspeichers auch für später aufbewahrt werden.

Die Sicherheit von Bitcoin ist ambivalent. Das System an sich ist zwar sehr gut gegen Angriffe und Fälschungen abgesichert, da es auf kryptografischen Verfahren beruht, aber viele Tauschbörsen sind Hackerangriffen ausgesetzt. Zudem besteht die Gefahr des Datenverlustes, da Bitcoin eine rein digitale Währung ist. Fiat-Währungen sind weitgehend sicher. Es gibt Einlagensicherungsfonds zum Schutz der Guthaben und zahlreiche Regulierungsvorschriften, die den Schutz der Besitzer garantieren. Auch Gold ist sicher, da es im Gegensatz zu den Fiat-Währungen und Bitcoin einen intrinsischen Wert besitzt und folglich niemals völlig wertlos sein wird.

Für eine leichte Übertragbarkeit ist Gold weniger gut geeignet. Physisches Gold lässt sich nur schwer übertragen, da der Transfer meist persönlich erfolgen muss. Fiat-Währungen hingegen lassen sich problemlos via Überweisung oder digitale Bezahlsysteme übertragen. Das gleiche gilt für Bitcoins, die sich ebenfalls schnell und problemlos online übertragen lassen.

Da es keine zentrale Kontrollinstanz für Bitcoin gibt, wird das System auch nicht überwacht. Transaktionen finden anonym ohne staatliche Einsicht statt. Das ist vergleichbar mit physischem Gold, das ebenfalls ohne staatliche Einsicht zu Hause gelagert werden kann und bei Goldhändlern anonym ge- und verkauft werden kann, solange die Bestimmungen des Geldwäschegesetzes eingehalten werden. Bei Fiat-Währungen existiert eine starke staatliche Kontrolle. Mittlerweile kann das Finanzamt Kontoabfragen durchführen, und auch international tauschen die Staaten immer mehr Vermögensdaten ihrer Bürger aus, um Steuerflucht und andere illegale Aktivitäten zu verhindern.

Die Transaktionskosten von Gold sind relativ hoch. Ein Kauf oder Verkauf ist bei Händlern meist nur mit hohen Aufschlägen möglich. Auch die Lagerung verursacht Kosten, da entweder Gebühren für den Unterhalt eines Bankschließfachs anfallen oder zu Hause entsprechende Sicherheitsvorkehrungen getroffen werden müssen. Auch die Transaktionskosten bei Fiat-Währungen sind beachtlich. Angefangen bei den Gebühren für Überweisungen bis hin zu den Transaktionskosten von Kreditkartenzahlungen fallen etliche Kosten für den Geldverkehr an. Bitcoins hingegen können völlig kostenfrei übertragen werden. Auch die Bitcoin-Konten sind kostenlos, und es können beliebig viele angelegt werden.

Für eine Währung, die erst vier Jahre existiert, schneidet Bitcoin im Vergleich mit den traditionellen Fiat-Währungen und alternativen Wertspeichern, wie Gold, gut ab und weist vor allem bei den Transaktionskosten und Anonymität Vorteile auf. Momentan halten viele Nutzer Bitcoin als Investition und spekulieren auf eine Wertsteigerung in der Zukunft. Bitcoins können zwar zukünftig noch stark im Wert steigen, aber dies kann unter großen Kursschwankungen nach oben oder unten passieren. Derzeit spielt der Ein- und Ausstieg eine wichtige Rolle, wodurch Bitcoin stark spekulativ ist.

Die langfristigen Aussichten für Bitcoin sind durchaus positiv zu bewerten. Die digitale Währung existiert seit vier Jahren und hat seitdem eine gewaltige Wertsteigerung erfahren. Vor allem der hohe Grad an Anonymität und die nicht vorhandenen bzw. freiwillig zu zahlenden Transaktionsgebühren machen Bitcoin als Zahlungsmittel im Internet attraktiv. Wenn das Bitcoin-System die Schwierigkeiten meistert, die sich aus der Nutzung für illegale Geschäfte und der mangelnden Sicherheit einiger Handelsplattformen ergeben und sich der Kurs ohne große Schwankungen stabilisiert, kann die Akzeptanz der digitalen Währung auf breiter Basis steigen.

Dennoch ist Bitcoin momentan eine Nischenentwicklung, die weltweit nur in einem kleinen Netzwerk verbreitet ist. Viele juristische, steuerliche und wirtschaftliche Fragen sind noch nicht beantwortet und auch die Gesetzgeber haben sich noch nicht eingehend mit dem Bitcoin-System beschäftigt. Ohne eine breite öffentliche Diskussion über das Bitcoin-System wird es ein Nischenprojekt bleiben. Das Bitcoin-Netzwerk und die Community könnten viel zu einer breiteren Akzeptanz beitragen, wenn rechtliche Fragen offen diskutiert und entsprechende Stellungnahmen abgegeben würden. Gleichwohl ist dies bei einem dezentralen Netzwerk schwierig, da niemand die Legitimation besitzt, um für die Gesamtheit der Bitcoin-Nutzer zu sprechen.

Im Moment ist Bitcoin aufgrund fehlender rechtlicher Rahmenbedingungen und Sicherheitslücken bei den großen Plattformen noch nicht konkurrenzfähig, aber vor allem für kleinere Transaktionen bereits gut geeignet, wenn die Gegenseite ebenfalls Bitcoin akzeptiert. Ob sich Bitcoin darüber hinaus entwickeln kann, wird sich zeigen. Bis dahin gilt, was der Bitcoin-Entwickler Gavin Andresen in seinem Blog schreibt:

> Bitcoin ist ein Experiment. Behandeln sie es wie ein vielversprechendes Internet-Startup-Unternehmen: Vielleicht wird es die Welt verändern, aber bedenken Sie, dass es immer riskant ist, Zeit und Geld in neue Ideen zu investieren.

Anhang: Die Geschichte des Bitcoin-Systems

Eine kurze Zusammenfassung der Bitcoin-Geschichte zeigt die rasante Entwicklung der Währung seit ihrer Einführung (ausführlicher unter *https://en.bitcoin.it/wiki/History*):

2008

18. August: Registrierung der Domain bitcoin.org.
31. Oktober: Veröffentlichung des Bitcoin-Aufsatzes von Satoshi Nakamoto.

2009

03. Januar: Erste Bitcoins werden im sog. „Genesis Block“ erzeugt.
11. Januar: Version 0.1 der Bitcoin-Software wird veröffentlicht.
12. Januar: Erste Bitcoin-Transaktion von Satoshi Nakamoto an Hal Finney.
05. Oktober: Erster Wechselkurs wird veröffentlicht: 1 Dollar = 1.309,03 Bitcoin.

2010

06. Februar: Erste Handelsplattform für Bitcoin wird eröffnet.
21. Mai: Kauf zweier Pizzas für 10.000 Bitcoin durch den User „laszlo“.
17. Juli: Eröffnung der Handelsplattform Mt.Gox.
15. August: Erste Sicherheitslücke im System wird entdeckt und geschlossen.
06. November: Der Wechselkurs erreicht 0,5 Dollar für 1 Bitcoin.
16. Dezember: Der erste Mining Pool wird eröffnet.

2011

28. Januar: 5,25 Million Bitcoin wurden bisher erzeugt, d.h. ein Viertel der Gesamtmenge.
09. Februar: Der Dollar-Bitcoin-Wechselkurs erreicht Parität, 1 Dollar = 1 Bitcoin.
23. April: Der Euro-Bitcoin-Wechselkurs erreicht Parität, 1 Euro = 1 Bitcoin.
02. Juni: Der Preis für einen Bitcoin bei Mt.Gox erreicht 10 Dollar.
08. Juni: Der Bitcoin-Kurs erreicht einen neuen Höchststand, 1 Bitcoin = 31,91 Dollar.
19. Juni: Nach einem Hackerangriff auf Mt.Gox sinkt der Kurs kurzzeitig auf 0,01 Dollar.
22. Juli: Mit „BitCoins Mobile“ wird die erste Bitcoin-App für das iPad veröffentlicht.
20. August: Erste Bitcoin-Konferenz in New York.
25. November: Erste europäische Bitcoin-Konferenz in Prag.

2012

01. März: Diebstahl von 50.000 Bitcoins beim Webhoster Linode.
15.–16. September: Bitcoin-Konferenz in London.
15. November: Die Website Wordpress.com akzeptiert Bitcoin als Zahlungsmittel.
28. November: Die generierten Bitcoins pro Block werden von 50 auf 25 reduziert.

2013

01. April: Der Kurs erreicht 100 Dollar pro Bitcoin.
10. April: Der Kurs erreicht mit 266 Dollar seinen bisherigen Höchststand.
17.–19. Mai: Bitcoin-Konferenz in San Jose, Kalifornien.
2. Juli: Europäische Bitcoin-Konferenz in London.

Anhang: Nützliche Links

http://www.bitcoin.org
Website des Bitcoin-Projekts mit grundlegenden Erklärungen und Downloadmöglichkeiten für unterschiedliche Versionen der Client-Software. Auf Englisch.

https://www.bitcoin.de
Größte deutschsprachige Handelsplattform für Bitcoin.

http://bitcoincharts.com
Website mit aktuellen Bitcoin-Wechselkursen und Charts. Auf Englisch.

http://www.bitcoinmonitor.com
Echtzeit-Übersicht aller Aktivitäten im Bitcoin-Netzwerk. Auf Englisch.

https://bitcointalk.org
Zentrales Forum der Bitcoin-Community, das alle Aspekte des Bitcoin-Systems behandelt. Hauptsächlich auf Englisch, mit deutscher Untersektion.

http://www.bitcoinx.com/profit
Umfangreicher Rechner, mit dessen Hilfe die Rentabilität von Bitcoin-Mining berechnet werden kann. Auf Englisch.

https://www.bitaddress.org
Möglichkeit, Bitcoin-Adressen zu generieren, auch als ausdruckbare „Speicheradressen“. Auf Englisch.

http://www.bitmit.net/de/recent
Auktionsplattform für Artikel aller Art mit Bitcoin als Zahlungsmittel.

http://blockchain.info
Echtzeit-Übersicht über die abgewickelten Transaktionen im Bitcoin-Netzwerk. Auf Englisch.

http://blockexplorer.com
Aktuelle Übersicht über die gelösten Blöcke des Bitcoin-Systems. Auf Englisch.

https://www.casascius.com
Anbieter physischer Bitcoin-Münzen und Barren. Auf Englisch.

https://en.bitcoin.it
Umfangreiches Wiki über das Bitcoin-System. Enthält viele weitere Links in die Welt des Bitcoin-Netzwerkes. Auf Englisch. Unter *https://de.bitcoin.it/wiki/Hauptseite* findet sich eine deutsche Übersetzung mit etwas weniger Inhalten.

https://de.bitcoin.it/wiki/Handel
Liste hauptsächlich deutschsprachiger Händler und Shops, die Bitcoin akzeptieren. Unter *https://en.bitcoin.it/wiki/Trade* existiert ein internationales Verzeichnis.

http://guiminer.org
Software für das Bitcoin-Mining mit grafischer Benutzeroberfläche. Auf Englisch. Die Software kann auf Deutsch umgestellt werden.

https://localbitcoins.com
Plattform für den Tausch von Bitcoin zwischen Privatpersonen vor Ort.

https://www.mtgox.com

Größte Handelsbörse für Bitcoin und Referenz für die Bitcoin-Wechselkurse. Auf Englisch.

http://www.truecrypt.org/downloads

Software zur Verschlüsselung von Dateien und Festplatten.

Literaturverzeichnis

ANDRESEN, Gavin (2011): That which does not kill us makes us stronger. Abrufbar unter: *http://gavinthink.blogspot.de/2011/06/that-which-does-not-kill-us-makes-us.html*.

BATTERSON, Travis (2013): Bitcoin. A Basic Explanation of Everything. (E-book).

BUNDESANSTALT FÜR FINANZDIENSTLEISTUNGSAUFSICHT (2011): Merkblatt – Hinweise zu dem Gesetz über die Beaufsichtigung von Zahlungsdiensten (Zahlungsdiensteaufsichtsgesetz – ZAG). Abrufbar unter: *http://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Merkblatt/mb_111222_zag.html*.

CAUGHEY, Michael (2013): Bitcoin Step by Step. (E-book).

CAUGHEY, Michael (2013): Bitcoin Mining Step by Step. (E-book).

CHAPMAN, Stephen (2011): Bitcoin: A Guide to the Future of Currency. Abrufbar unter: *http://www.zdnet.com/blog/btl/bitcoin-a-guide-to-the-future-of-currency/50601*.

CHRISTIN, Nicolas (2012): Traveling the Silk Road. A Measurement Analysis of a Large Anonymous Online Marketplace. Abrufbar unter: *http://arxiv.org/abs/1207.7139v2*.

DALE, James (2013): Profiting With Bitcoin. (E-book).

DENNIS, Jarrod; WRIGHT, Max (2013): Bitcoin Revolution. Ending Tyranny for Fun and Profit. (E-book).

DORIT, Ron; SHAMIR, Adi (2012): Quantitative Analysis of the Full Bitcoin Transaction Graph. Abrufbar unter: *http://eprint.iacr.org/2012/584.pdf*.

EUROPÄISCHES PARLAMENT (2000): Richtlinie 2000/46/EG des Europäischen Parlamentes und Rates vom 18. September 2000 über die Aufnahme, Ausübung und Beaufsichtigung der Tätigkeit von E-Geld-Instituten. Abrufbar unter: *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:275:0039:0043:DE:PDF*.

EUROPÄISCHE ZENTRALBANK (2012): Virtual Currency Schemes. Frankfurt am Main.

GISCHER, Horst; HERZ, Bernhard; MENKHOFF, Lukas (2012): Geld, Kredit und Banken. Eine Einführung. Heidelberg.

GREENWOOD, John (2013): Canada Revenue Agency Zeroes in on Bitcoin. Abrufbar unter: *http://business.financialpost.com/2013/04/29/canada-revenue-agency-zeroes-in-on-bitcoin/*.

GRINBERG, Reuben (2011): Bitcoin. An Innovative Alternative Digital Currency. In: Hastings Science & Technology Law Journal, Ausgabe 4, S. 159–207. Abrufbar unter: *http://ssrn.com/abstract=1817857*.

HAYEK, Friedrich A. (1976): Denationalisation of Money: The Argument Refined. An Analysis of the Theory and Practice of Concurrent Currencies Series. London.

JACOBS, Edwin (2011): Bitcoin. A bit too far? Abrufbar unter: *http://www.timelex.eu/nl/blog/detail/bitcoin-a-bit-too-far*.

LEE, Timothy B. (2013): Four Reasons You Shouldn't Buy Bitcoins. Abrufbar unter: *http://www.forbes.com/sites/timothylee/2013/04/03/four-reason-you-shouldnt-buy-bitcoins*.

MÖLLEKEN, Dirk (2012): Bitcoin. Geld ohne Banken. Ist das möglich? Hamburg.

NAKAMOTO, Satoshi (2009): Bitcoin. A Peer-to-Peer Electronic Cash System. Abrufbar unter: *http://bitcoin.org/bitcoin.pdf*.

NEUMANN, Heike B.; SCHWARZPAUL, Thomas (2010): Kryptografie in Theorie und Praxis. Wiesbaden.

PALLAS, Carsten (2005): Ludwig von Mises als Pionier der modernen Geld- und Konjunkturlehre. Eine Studie zu den monetären Grundlagen der Austrian Economics. Marburg.

POLLEIT, Thorsten; PROLLIUS, Michael von (2011): Geldreform. Vom schlechten Staatsgeld zum guten Marktgeld. Grevenbroich.

SAUERBREY, Anna (2013): 130 Dollar für ein paar Bits. Abrufbar unter: *http://www.tagesspiegel.de/medien/digitale-waehrungen-130-dollar-fuer-ein-paar-bits/8026408.html*.

SORGE, Christoph; KROHN-GRIMBERGHE, Artus (2012): Bitcoin: Eine erste Einordnung. In: Datenschutz und Datensicherheit Nr. 7, S. 479–484. Abrufbar unter: *http://www.ismll.uni-hildesheim.de/pub/pdfs/sorge-krohn-grimberghe-bitcoin.pdf*.

STÖCKER, Christian (2011): Geld aus der Steckdose. In: Der Spiegel, 31. Mai.

WIKIPEDIA (2013): Bitcoin. Abrufbar unter: *http://de.wikipedia.org/wiki/Bitcoin*.

Rechtliche Hinweise und Impressum

Wir sind um die Richtigkeit und Aktualität der in diesem E-Book dargestellten Informationen bemüht. Trotzdem können Fehler und Unklarheiten nicht vollständig ausgeschlossen werden. Aus diesem Grund übernehmen wir keine Gewähr für die Aktualität, Richtigkeit, Vollständigkeit und Qualität der bereitgestellten Informationen. Weder Autor noch Verlag können für Schäden haftbar gemacht werden, die in Zusammenhang mit der Verwendung dieses Buches stehen. Für Hinweise auf Fehler oder Unklarheiten sind wir dankbar. Schreiben Sie uns dazu bitte an *info@kemacon.de*.

Die Inhalte dieses E-Books dienen ausschließlich der Information der Leser und stellen keine Anlageberatung und keine Empfehlung im Sinne des Wertpapierhandelsgesetzes (WpHG) dar.

Für Inhalte der in diesem Buch abgedruckten Internetseiten sind ausschließlich die Betreiber der jeweiligen Internetseiten verantwortlich. Verlag und Autor haben keinen Einfluss auf die Gestaltung und Inhalte fremder Internetseiten. Verlag und Autor distanzieren sich daher von allen fremden Inhalten.

Impressum

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

ISBN: 978-3-9816017-2-5

1. Auflage 2013

Coverbild: © Nmedia / www.fotolia.de

E-Book Distribution: XinXii
http://www.xinxii.com

Herausgeber:

Kemacon UG (haftungsbeschränkt)
Sossauer Str. 30
84130 Dingolfing

Email: *info@kemacon.de*

Über den Autor:

Dr. Daniel Kerscher absolvierte eine Ausbildung zum Bankkaufmann und ein Studium der Politik- und Informationswissenschaft mit Promotion. Er beschäftigt sich seit vielen Jahren mit dem Finanzsystem

und den digitalen Informationstechnologien.