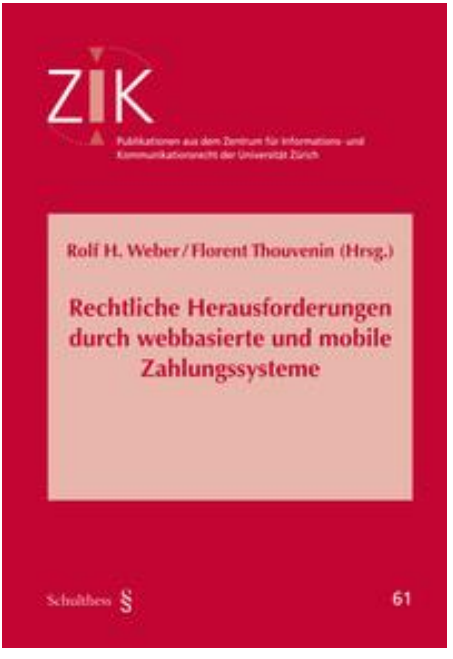
Luzius Meisser *

Kryptowährungen: Geschichte, Funktionsweise, Potential



Beitrag zum Tagungsband «**Rechtliche Herausforderungen durch webbasierte und mobile Zahlungssysteme**»

Rolf H. Weber / Florent Thouvenin (Hrsg.), Schulthess 2015, 217 Seiten, broschiert, ISBN 978-3-7255-7217-5, CHF 82.00

Bestellen Sie Ihr Exemplar bei Schulthess

---

* MSc Computer Science ETH, Präsident der Bitcoin Association Switzerland

Inhaltsverzeichnis

Abbildungsverzeichnis

I. Einführung

Bitcoin und verwandte Kryptowährungen stellen eine technologische Innovation dar, welche diverse rechtliche Fragen aufwirft.[1] Kryptowährungen sind virtuelle Währungen, die durch Verschlüsselungstechnologie gesichert und üblicherweise dezentral organisiert sind.[2] In diesem Beitrag werden Entstehungsgeschichte, Funktionsweise, und zukünftiges Potential von Kryptowährungen erläutert, wobei Bitcoin als prominenteste Variante die wichtigste Rolle spielt. Damit soll die Grundlage geschaffen werden, Kryptowährungen besser einordnen und verstehen zu können.

Der folgende Teil enthält die Entstehungsgeschichte und begründet die Bezeichnung „digitales Bargeld“ für Kryptowährungen. Im dritten Teil wird die Funktionsweise erklärt. Der wichtigste technologische Baustein sind dabei elektronische Unterschriften, während die sogenannte Blockchain – ein dezentrales Transaktionsarchiv – die grösste Innovation darstellt. Zuletzt werden Zukunftsszenarien skizziert, die prinzipiell von dieser Technologie ermöglicht werden. Dazu gehört das Emittieren klassischer Währungen und Wertschriften ins Bitcoinsystem, aber auch völlig neuartige, universelle Systeme, die darauf abzielen, ganze virtuelle Organisationen und Gesellschaften zu ermöglichen.

---

[1] Vgl. die Beiträge von Prof. Dr. Seraina Grünewald, Dr. Harald Bärtschi und Christian Meisser über virtuelle Währungen in diesem Band

[2] Vgl. auch die Definition im Glossar des “Bericht des Bundesrates zu virtuellen Währungen in Beantwortung der Postulate Schwaab (13.3687) und Weibel (13.4070)”, 25.6.2014, www.news.admin.ch/NSBSubscriber/message/attachments/35361.pdf

II. Geschichte

1. Cypherpunks

„We the Cypherpunks are dedicated to building anonymous systems. We are defending our privacy with cryptography, with anonymous mail forwarding systems, with digital signatures, and with electronic money."
- Eric Hughes, 1993, A Cypherpunk's Manifesto[3]

Anfang der 90ern begann eine Gruppe von Programmierern und Kryptographen, die sich selbst in Anlehnung an den Begriff Cyberpunk „Cypherpunks" nannte, sich über eine Mailingliste auszutauschen, in der sowohl technisch als auch politisch diskutiert wurde. Cypherpunks sehen Verschlüsselung (cipher) und verwandte Technologien als Weg, die eigene Privatsphäre vor Firmen und Regierungen zu schützen. Sie stellen sich dabei auf den Standpunkt, dass der Bürger den Schutz der Privatsphäre in die eigene Hand nehmen muss und sich nicht auf das Wohlwollen dieser Institutionen verlassen kann. Das Mittel dazu ist Technologie, deren Sicherheit mathematisch beweisbar ist und universal gilt, im Gegensatz zu lokal begrenzten und umgehbaren Gesetzen.

Zentrales Thema unter den Cypherpunks ist daher die Verschlüsselung persönlicher Nachrichten zum Schutz vor Überwachung. Man will sich nicht auf rechtlichen Schutz - etwa durch das Fernmeldegeheimnis - verlassen. Dieses Misstrauen ist, wie sich inzwischen verschiedentlich bestätigt hat, durchaus gerechtfertigt. In diesem Geist ist Anfang der 90er Jahre zum Beispiel PGP (Pretty Good Privacy)[4], ein bekanntes Email-Verschlüsselungsprogramm entstanden. In der Tradition der Cypherpunks stehen auch Systeme wie Tor[5], eine Software zum anonymen Surfen im Internet oder Julien Assanges Wikileaks[6]. Das grundsätzliche Misstrauen gegenüber zentralisierten Systemen ist in dieser Philosophie tief verankert. Im Allgemeinen gelten in der Informatik dezentrale, redundante Systeme mit klarer Aufgabenteilung[7] gegenüber zentralisierten Alternativen als überlegen, da letztere stets mindestens einen „single

---

[3] Eric Hughes, A Cypherpunk's Manifesto, 9.3.1993, www.activism.net/cypherpunk/manifesto.html

[4] Wikipedia über PGP, en.wikipedia.org/wiki/Pretty_Good_Privacy

[5] Tor, Anonymity Online, www.torproject.org

[6] WikiLeaks, wikileaks.org

[7] Separation of Concerns, en.wikipedia.org/wiki/Separation_of_concerns

point of failure“[8] aufweisen und weniger skalierbar[9] sind. Die Übertragung solcher Design-Prinzipien von IT-Systemen auf politische Systeme ist nicht ganz unproblematisch, findet aber existierende Parallelen vor, etwa im Prinzip der Gewaltenteilung, der Subsidiarität, oder der Demokratie im Allgemeinen.

Ein aktiver Cypherpunk ist der Brite Adam Back,[10] welcher 1997 Hashcash[11] zur Bekämpfung von Spam vorgeschlagen hat und bis heute eine wichtige Rolle in der Entwicklung von Bitcoin spielt. Hashcash verwendete erstmals Proof-of-Work zum Beweis geleisteter Arbeit, ein Grundbaustain von Bitcoin und den meisten anderen Kryptowährungen. Bei Hashcash investiert ein Computer Rechenleistung in schwer zu lösende, aber einfach zu überprüfende Rechnungen, die vom exakten Inhalt und Empfänger eines Emails abhängen. Damit kann der Absender eines Emails beweisen, dass er zum Beispiel mindestens 10 Minuten Rechenleistung zum Versand dieses Emails investiert hat, und es sich damit mit sehr grosser Wahrscheinlichkeit nicht um Spam handelt, denn Spam ist nur effektiv, wenn man Hunderte von Emails pro Sekunde verschicken kann. Aufgrund der Erfindung von Hashcash wird manchmal gemutmasst, Adam Back sei Satoshi Nakamoto, der unbekannte Erfinder von Bitcoin.

2. Entwicklung von Bitcoin

Satoshi Nakamoto ist das Pseudonym des unbekannten Erfinders von Bitcoin. Dieser hat am 1. November 2008 in „The Crypography Mailing List“ Bitcoin vorgestellt[12] und in einem Whitepaper mit dem Titel „Bitcoin: A Peer-to-Peer Electronic Cash System“[13] beschrieben. Bis heute ist die reale Identität von Satoshi Nakamoto unbekannt. Der Name „Satoshi Nakamoto“ ist das japanische Äquivalent von „Hans Muster“. Mit wenigen Ausnahmen ist er seit 2011

---

8 Single Point of Failure, en.wikipedia.org/wiki/Single_point_of_failure

9 Skalierbarkeit, de.wikipedia.org/wiki/Skalierbarkeit

10 Adam Back, persönliche Webseite, www.cypherspace.org/adam/

11 Hashcash, hashcash.org

12 Satoshi Nakamoto, „Bitcoin P2P e-cash paper“, The Cryptography Mailing List, 1.11.2008, www.mail-archive.com/cryptography%40metzdowd.com/msg09959.html

13 Satoshi Nakamoto, “Bitcoin: A Peer-toPeer Electronic Cash System”, 1.11.2008, bitcoin.org/bitcoin.pdf

nicht mehr aktiv in Erscheinung getreten und hat die Weiterentwicklung von Bitcoin anderen überlassen.

Nakamoto hat die wichtigsten technischen Grundlagen von Bitcoin gelegt und die erste Implementierung des Systems veröffentlicht. Heute gibt es mehrere Implementierungen in verschiedenen Programmiersprachen und von verschiedenen Autoren.[14] [15] Auch wurde die Originalversion von Nakamoto inzwischen fast vollständig überarbeitet.[16] Die meiste Arbeit wird wie bei anderen open-source Projekten von freiwilligen Programmierern erbracht. Einer der Kernentwickler, Gavin Andressen, wird von der amerikanischen Bitcoin Foundation[17] bezahlt, welche sich über Mitgliederbeiträge finanziert. Mit der zunehmenden Professionalisierung wird nun aber auch öfters Entwicklungsleistung von Startups erbracht, welche durch Risikokapital finanziert sind. Ein Beispiel dafür ist die von Adam Back mitgegründete Blockstream,[18] welche 21 Millionen USD an Risikokapital erhalten hat und das Ziel verfolgt, die Bitcoin-Infrastruktur weiterzuentwickeln.[19] Insgesamt ist 2014 schätzungsweise 400 Millionen USD an Risikokapital in Bitcoin-Startups geflossen. [20]

Es entstehen Firmen aller Art rund um Bitcoin: Zahlungsdienste wie BitPay oder Coinbase, Börsen wie Bitstamp.de oder Bitfinex, Broker wie SBEX oder Bitcoin Suisse in der Schweiz, Kontoführungsdienste wie Blockchain.info oder Bitcoin Armory, Hersteller von Bankomaten wie Robocoin oder Lamassu, Hersteller spezialisierter Hardware zum Schürfen von Bitcoins wie Butterfly Labs oder KNX, Newsportale wie Coindesk, Anlagefonds wie der von Exante oder SecondMarket, diverse Konferenzen, lokale Unterstützungsorganisationen wie die Bitcoin Association Switzerland, und viele weitere mehr. Im Gegensatz zu zentralisierten Zahlungssystemen entsteht so ein symbiotisches

---

[14] BitcoinJ, Java Library für Bitcoin, bitcoinj.github.io

[15] Gocoin, Go Library für Bitcoin, github.com/piotrnar/gocoin

[16] Bitcoin Quellcode und Versionshistorie: github.com/bitcoin/bitcoin

[17] Bitcoin Foundation: bitcoinfoundation.org

[18] Blockstream, Founders, blockstream.com/founders

[19] Coindesk, "Blockstream: $21 Million Funding Will Drive Bitcoin Development", 18.11.2014, coindesk.com/blockstream-21-million-funding-will-drive-bitcoin-development

[20] CB Insights, "Despite Falling Price, Bitcoin Startup Investment Continues to Hit New Records", 21.11.2014, cbinsights.com/blog/bitcoin-startup-funding-2014

Ökosystem das aus vielen kleineren Teilnehmern besteht und robust ist gegenüber dem Ausfall einzelner – zum Beispiel dem spektakulären Kollaps der Börse MtGox anfang 2014. Wichtigste Foren sind Bitcointalk[21] und das Bitcoinforum auf Reddit.[22] In der Schweiz setzt sich die Digital Finance Compliance Association mit Rechts- und buchhalterischen Fragen von Kryptowährungen auseinander.[23]

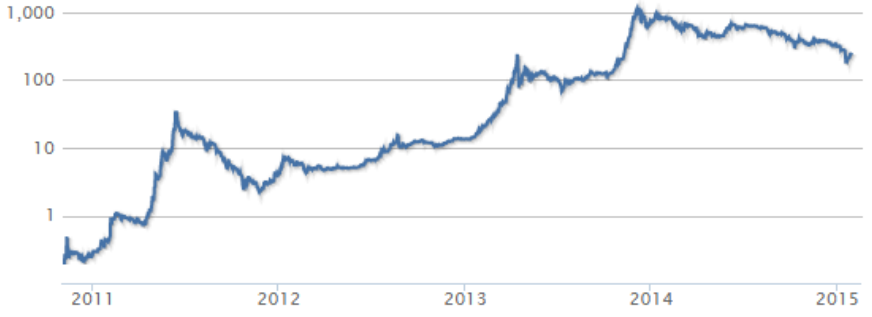


Abbildung 1: Preis eines Bitcoins in USD seit 2011, logarithmisch

Im Sommer 2011 hat Bitcoin erstmals breite mediale Aufmerksamkeit und einen grossen Kurssprung erfahren. Im Gleichschritt mit der zunehmenden Aufmerksamkeit ist auch der Kurs von Bitcoin gestiegen. Während sich die Anzahl Transaktionen pro Tag in den letzten zwei Jahren auf gegen 100‘000 etwa verdoppelt hat,[24] hat sich der Preis eines Bitcoins in der gleichen Zeitspanne verzwanzigfacht und steht nun um 300 USD. [25] Der Gesamtwert aller sich im Umlauf befindlicher Bitcoins beträgt heute rund 4 Milliarden, was vergleichbar ist mit der Geldmenge M1 von Ländern wie Libanon oder Island.[26] Gemessen an der Geldmenge ist Bitcoin mit Abstand die wichtigste Kryptowährung, gefolgt von Ripple mit etwa 700 Millionen.

3. Digitales Bargeld

---

[21] Bitcointalk.org, enthält bereits über eine Million Diskussionsbeiträge.

[22] Bitcoin Reddit, reddit.com/r/bitcoin

[23] Digital Finance Compliance Association, dfca.ch

[24] Blockchain.info, “Number of transactions per day”, blockchain.info/charts/n-transactions?timespan=2year&daysAverageString=10

[25] Blockchain.info, “Bitcoin Market Cap”, blockchain.info/charts/market-cap

[26] Coinometrics, “Narrow Money Stock (M1)”, coinometrics.com/bitcoin/bmix

Da die Transaktionen direkt von Person zu Person stattfinden, wird Bitcoin oft als digitales Bargeld bezeichnet. So wurde es schon vom Erfinder als solches unter dem Titel “Bitcoin: A Peer-to-Peer Electronic Cash System” vorgestellt.[27] Diese Bezeichnung darf einem nicht dazu verleiten, Bitcoin als E-Geld zu bezeichnen, denn Bitcoin stellt weder eine Forderung dar, noch gibt es einen identifizierbaren Emittenten, so dass Bitcoin nicht unter diesen Rechtsbegriff fällt. [28] Bitcoin gleicht damit klassischen Fiat-Währungen wie dem Schweizer Franken oder dem Euro, da diese Währungseinheiten seit der Aufgabe des Goldstandards auch keine Forderung mehr darstellen. Vor diesem Hintergrund hat die parlamentarische Gruppe für digitale Nachhaltigkeit in ihrem Postulat[29] auch nahegelegt, Bitcoin rechtlich wie Fremdwährungen zu behandeln, worauf in der Antwort des Bundesrats aber nicht gross eingegangen wurde.[30] Der technisch spannende Punkt ist die direkte Übertragung von Person zu Person, welche bislang nur mit physischem Bargeld möglich war, und viele neue Möglichkeiten eröffnet.

[27] FN 13

[28] EU-Richtlinie 2000/46/EG http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:275:0039:0043:DE:PDF

[29] Nationalrat, Postulat 13.4070 „Rechtssicherheit für Bitcoin schaffen“, 5.12.2013, parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20134070

[30] Bundesrat, „Bericht des Bundesrates zu virtuellen Währungen in Beantwortung der Postulate Schwaab (13.3687) und Weibel (13.4070)“, 25.6.2014, news.admin.ch/message/index.html?lang=de&msg-id=53513

III. Funktionsweise

Ausgehend von einer einfachen Analogie wird in diesem Kapitel die Funktionsweise von Kryptowährungen Schritt um Schritt erklärt.

1. Einfaches, öffentliches Zahlungssystem

Nehmen wir an, eine Gruppe von Leuten, die sich gemeinsam in einem Raum befindet, einigt sich auf folgende Regeln:

1. Zu Beginn hat jeder im Raum 100 Coins. Diese Coins sind frei erfunden und an keinerlei realen Wert gebunden.

2. Die Coins sind durch öffentliche Erklärung frei übertragbar.

3. Jeder führt Buch über alle geschehenen Transaktionen. Ungültige Transaktionen werden ignoriert.

Wenn zum Beispiel Alice 30 Coins an Bob übertragen möchte, erklärt sie deutlich hörbar „Hiermit schicke ich 30 Coins and Bob“. Jeder im Raum notiert sich diese Transaktion und weiss nun, dass Alice nur noch 70 Coins hat, während Bob 130 besitzt. Wenn nun Alice weiter ankündigt, „Hiermit schicke ich 80 Coins an Charles“, wird diese Transaktion von allen ignoriert, da Alice nicht mehr über das erforderliche Guthaben verfügt.

Damit haben wir ein System geschaffen, das dem von Bitcoin sehr ähnlich ist. Es gibt eine abstrakte Währung ohne Emittenten und für die niemand einen Wert garantiert. Man kann sie aber trotzdem als Zahlungsmittel einsetzen, solange man jemanden findet, der dieses akzeptiert. Ähnlich wie bei Bitcoin ist die Geldmenge auch von Anfang an begrenzt. Zudem gibt es gleich wie bei Bitcoin keinen identifizierbaren Finanzintermediär, der die Zahlungen abwickelt. Stattdessen finden die Transaktionen direkt von Person zu Person statt, mit den restlichen Personen im Raum als Zeugen und Archivare.

Das grösste Problem dieses Systems besteht in der Frage, was jemand tun soll, der eine oder mehrere Transaktionen verpasst hat und den anderen Personen im Raum nicht vertraut. Ein Spezialfall dieses Problems ist die Frage, wie zusätzliche Personen dazukommen können. Diese haben nämlich sämtliche Transaktionen bis zum Betreten des Raums verpasst. Ein weiterer Spezialfall dieses Problems ist der Fall, dass die Erklärung nicht genug laut war, so dass

die Leute am anderen Ende des Raums sie nicht hören konnten. Die Lösung dieser Probleme ist die Kerninnovation von Bitcoin.

2. Elektronische Signaturen

Ein zwar nicht besonders neuartiger, aber essentieller technologischer Baustein von Bitcoin und verwandten Systemen sind elektronische Signaturen. Für elektronische Signaturen benötigt man eine Identifikationsnummer und einen zugehörigen geheimen Schlüssel. Mit dem geheimen Schlüssel können beliebige Transaktionen fälschungssicher signiert werden. Man sieht jeder Signatur an, zu welcher Identifikationsnummer und Transaktion sie gehört. Damit ist es unmöglich, die Signatur einer Transaktion einfach zu kopieren und in ein anderes Dokument einzufügen, wie das mit papierernen Unterschriften technisch möglich wäre.

Es gibt Dienste, die solche Identifikationsnummern mit realen Identitäten in Verbindung bringen und diese Verbindung mit einer eigenen Signatur zertifizieren. Handelt es sich bei diesem Dienst um einen regulierten Zertifizierungsdienst, sind die resultierenden Signaturen qualifizierte elektronische Signaturen. [31] Im Bitcoin-System ist eine solche Zuordnung von Identifikationsnummern zu realen Personen aber irrelevant, da Empfänger und Absender stets nur über die Identifikationsnummern identifiziert werden und eine allfällige Verknüpfung mit realen Personen den Vertragsparteien überlassen wird.[32]

Genau genommen sind die Benutzer von Bitcoin nicht anonym, sondern pseudonym, wobei jede Identifikationsnummer ein Pseudonym darstellt. Diese

---

[31] ZertES, Bundesgesetz über die elektronische Signatur, admin.ch/opc/de/classified-compilation/20011277/200808010000/943.03.pdf

[32] In der Schweiz gilt die Schriftform beim Unterschreiben mit elektronischer Signatur nur dann als erfüllt, wenn eine von einer regulierten Zertifizierungsstelle zertifizierte Identifikationsnummer verwendet wird. Jede andere Form von Nachweis, dass eine Identifikationsnummer zu einer bestimmten Person gehört, gilt nicht.

Identifikationsnummern können im Allgemeinen als Kontonummern betrachtet werden, werden aber als Adressen bezeichnet.[33] Manche Dienste verwenden für alle Transaktionen die gleiche Adresse, welche dadurch früher oder später allgemein bekannt wird. Das Spendenkonto von Wikileaks ist zum Beispiel allgemein bekannt und hat die Adresse 1HB5XMLmzFVj8ALj6mfBsbifRoD4miY36v. Da alle Transaktionen öffentlich sind, kann man auch jederzeit den Kontostand berechnen. Im Moment beträgt er 3.9 Bitcoins. Es wurden im Verlauf der Zeit bereits 3‘885 Bitcoins empfangen, was zum heutigen Kurs einem Wert von etwas über einer Million Franken entspricht.[34] Andere Services verwenden standardmässig für jede Transaktion eine neue Empfangsadresse, so dass die einzelnen Zahlungen nicht so leicht miteinander in Verbindung gebracht werden können. Da die Adressen lang genug sind, ist die Gefahr, dass zwei verschiedene Personen zufälligerweise die gleiche Adresse generieren, vernachlässigbar klein[35], selbst wenn jeder Benutzer Abertausende verschiedene Adressen verwendet. Einen zentralen Dienst, der Adressen vergibt und so Adresskollisionen verhindert, braucht es damit nicht.

Mit der Technologie digitaler Signaturen kann man bereits die allermeisten Funktionen unseres öffentlichen Zahlungssystems realisieren. Sie ermöglicht Identitäten und fälschungssichere Transaktionen. Man könnte ein System bauen, in dem der Absender einer Zahlung stets die vollständige Kette aller vorangegangen Transaktionen beilegt – also sozusagen den Stammbaum der Coins mitschickt. Damit kann der Absender beweisen, dass er die Coins besitzt bzw. irgendwann besessen haben muss. Dieses System könnte alle wesentlichen Funktionen einer Kryptowährung bieten, bis auf eine: das Vermeiden sogenannter Double-Spends. Der Absender kann mit der beigelegten Transaktionskette nämlich nicht beweisen, dass er die gleichen Coins nicht bereits schon jemand anderem geschickt hat.

---

[33] Eine Adresse kann auch zu mehreren Identifikationsnummern gehören, so dass für ausgehende Transaktionen mehrere Signaturen nötig sind (zum Beispiel drei von fünf).

[34] Blockchain.info, Transaktionen der Wikileaks Spendenadresse: blockchain.info/address/1HB5XMLmzFVj8ALj6mfBsbifRoD4miY36v

[35] Die Adressen sind 160 Bits lang. Selbst wenn eine Million Jahre lang täglich eine Milliarde neue Adressen generiert würden, wäre die Wahrscheinlichkeit, dass es je zu einer Kollision kommt, noch um Grössenordnungen kleiner als eins zu einer Milliarde.

Der Absender müsste also beweisen, dass er etwas Bestimmtes nicht gemacht hat (nämlich die Coins jemand anderem verschickt). Bei herkömmlichen Banknoten nimmt einem die materielle Realität diese Arbeit ab: Wenn man eine Banknote in der Hand hält, beweist man damit hinreichend, dass man sie noch nicht anderswo ausgegeben hat. In der digitalen Welt, wo Daten beliebig kopiert werden können, funktioniert diese Art von Beweis nicht. Stattdessen ist Bitcoin darauf angewiesen, dass es ein verlässliches Archiv aller vergangenen Transaktionen gibt, so dass man nachprüfen kann, ob der Absender die versprochenen Bitcoins nicht bereits früher ausgegeben hat. Diese Archivfunktion könnte relativ einfach von einer einzelnen, zentralen Instanz, der jeder vertraut, übernommen werden. Eine solche Lösung würde aber der dezentralen Philosophie des Systems zuwiderlaufen. Stattdessen übernimmt bei Bitcoin die dezentral organisierte Blockchain diese Archivfunktion. Sie stellt die grosse Innovation von Bitcoin dar.

3. Distributed Ledger (Dezentrales Register)

Wenn allgemein auf die Technologie hinter Bitcoin Bezug genommen wird, wird oft von Distributed Ledger Technology gesprochen.[36] Damit wird hervorgehoben, dass solche Systeme prinzipiell als Eigentumsregister für beliebige übertragbare Werte dienen können. Ein Distributed Ledger besteht aus einer Datenstruktur, in der die relevanten Daten festgehalten werden, sowie einem Protokoll, das spezifiziert, wie diese Daten ausgetauscht und abgeglichen werden. Bei den meisten Kryptowährungen nennt man die Datenstruktur Blockchain.

3.1 Distributed Consensus

[36] Bank of England, Quarterly Bulletin 2014 Q3, “Innovations in payment technologies and the emergence of digital currencies”, www.bankofengland.co.uk/publications/Documents/quarterlybulletin/2014/qb14q3digitalcurrenciesbitcoin1.pdf

Distributed Ledger Technology löst das sogenannte Problem des Distributed Consensus, nämlich die Frage, wie sich eine dynamische Gruppe weltweit verteilter Computer auf eine einzige Wahrheit einigen können. Im Fall von Bitcoin besteht diese Wahrheit darin, welche Transaktionen in welcher Reihenfolge stattgefunden haben. Das ist schon so nicht trivial, doch kommt erschwerend hinzu, dass keiner dieser Computer zuverlässig ist, sie sich gegenseitig nicht vertrauen, und dass starke finanzielle Anreize bestehen, das System zu manipulieren. In der Informatik spricht man von byzantinischer Fehlertoleranz, wenn ein verteiltes System nicht nur Fehlern, sondern auch bösartigen Angriffen in ausreichendem Mass standhält. Diese zu erreichen ist oft sehr aufwändig, so auch bei Bitcoin. Bei Bitcoin fliesst derzeit täglich Rechenleistung mit Wert in Millionenhöhe in die Sicherung des Systems, das sogenannte Mining, welches durch neu geschöpfte Bitcoins und Transaktionsgebühren[37] belohnt wird.

Abbildung 2: Bitcoin-Mining in einer Lagerhalle

[37] Es hat sich zwar der Begriff Transaktionsgebühr etabliert, doch genau genommen handelt es sich eher um eine Belohnung, die vom Absender der Transaktion für die Aufnahme ins Transaktionsarchiv (der Blockchain) ausgesetzt wird. Bei Transaktionen ohne Trinkgeld dauert es oft etwas länger, bis sie in die Blockchain aufgenommen werden, doch meistens findet sich früher oder später ein Miner, der so freundlich ist.

Eine ganz passable Interpretation von dem, was in Kryptowährungen beim Finden des Distributed Consensus geschieht, ist die der Abstimmung nach Rechenleistung. Man kann Distributed Consensus dadurch erreichen, dass man Abstimmungen durchführt und der Mehrheit glaubt.[38] Bei Bitcoin besteht nun aber das Problem, dass weder Anzahl noch Identität der teilnehmenden Benutzer oder Computer bekannt sind. Man kann also nicht einfach jedem Teilnehmer eine Stimme geben. Es wäre viel zu einfach, mehrere Identitäten vorzutäuschen und so das eigene Stimmengewicht zu manipulieren. Stattdessen wird das Stimmengewicht an etwas gemessen, das man im Internet nicht vortäuschen kann, nämlich Rechenleistung.[39] Doch der einzige Weg, fortlaufend zu beweisen, dass man Rechenleistung besitzt, ist es, permanent zu rechnen. Deshalb rechnen die Miner ohne Unterlass. Über den Beweis der Rechenleistung hinaus sind diese Rechnungen völlig nutzlos. Um Abstimmungen in einem solchen System manipulieren zu können, muss man die Mehrheit der Rechenleistung im Netzwerk kontrollieren. Damit steigen die Kosten eines solchen Angriffs proportional mit der sich bereits im Netzwerk befindlichen Rechenleistung. Um diese sicherzustellen existieren finanzielle Anreize. So werden die Miner mit frisch geschöpfter Kryptowährung und Transaktionsgebühren entlöhnt. Und zwar wird diese Belohnung etwa alle zehn Minuten unter den richtigen Stimmen verlost, wobei „richtig“ als „so wie die Mehrheit“ definiert ist. Damit besteht ein starker Anreiz, so wie die Mehrheit abzustimmen und damit auch sinnvoll abzustimmen, solange man davon ausgehen kann, dass die Mehrheit sinnvoll stimmt. Diese Art der Abstimmungen nennt sich „Proof-of-Work“, da auf Arbeit bzw. Rechenleistung abgestellt wird. Eine umstrittene Alternative dazu ist „Proof-of-Stake“. Hier wird die Stimmkraft nicht an der Rechenleistung, sondern am Reichtum gemessen. Die Idee dahinter ist, dass die Reichsten Teilnehmer des Systems das grösste Interesse an einem korrekten Funktionieren haben. Manche Kryptowährungen mischen die beiden Ansätze auch. Bitcoin setzt aber vollständig auf Proof-of-Work.

Wem die Analogie der Abstimmungen genügt, kann die folgenden Abschnitte getrost überspringen. Sie genügt aber nicht, um Schlüsse über Details wie dem genauen Zeitpunkt einer Transaktion zu ziehen.

---

[38] So funktioniert zum Beispiel der oft verwendete Paxos-Algorithmus. en.wikipedia.org/wiki/Paxos_%28computer_science%29

[39] Diese Analogie wird bereits von Nakamoto selbst in seinem Whitepaper benutzt. Siehe FN 13.

3.2 Die Blockchain

Die Datenstruktur, in der alle Transaktionen archiviert werden, heisst Blockchain. Sie ist das Archiv aller Transaktionen und besteht aus einer Kette von Transaktionsblöcken. Jeder Benutzer, der die Bitcoin-Software auf seinem Computer laufen hat, führt eine vollständige Kopie dieses Transaktionsarchives mit. Das bedeutet, dass es weltweit abertausende von Kopien der Blockchain gibt. Neue Transaktionen werden etwa alle 10 Minuten zu einem Block zusammengefasst und an die Kette angefügt.

Die Teilnehmer im Bitcoin-Netzwerk stellen die Informationen, die sie haben, gegenseitig zur Verfügung. Ich kann also als Netzwerkteilnehmer jederzeit jeden anderen Teilnehmer danach fragen, aus welchen Blöcken die Blockchain seiner Ansicht nach besteht und diese von ihm beziehen. Solange ich von allen die gleichen, plausiblen Daten erhalte, besteht kein Problem. Doch für den Fall, dass die empfangenen Informationen inkonsistent sind, muss ich mich für eine Variante entscheiden. Dafür gibt es klare Regeln. Zunächst kann ich alle offensichtlich falschen Blöcke verwerfen, nämlich solche, die ungültige Transaktionen enthalten.[40] Bleiben mehrere mögliche Varianten von gültigen Blockchains, entscheide ich mich für die längste. Gibt es mehrere gleich lange, entscheide ich mich für diejenige, von der ich zuerst gehört habe. Bei diesem letzten Kriterium wird es offensichtlich, dass ich meine Meinung möglicherweise revidieren muss. Dann nämlich, wenn ich erfahre, dass die verworfene Variante länger geworden ist. Das Kriterium der Länge hat Vorrang.

Theoretisch ist es möglich, dass man sehr viele Blöcke wieder verwerfen muss. Ein solches Szenario wäre eine längere Trennung sämtlicher Internetverbindungen zwischen Europa und Amerika. Damit würde auch das Bitcoinnetzwerk getrennt. Die europäischen und die amerikanischen Teilnehmer begännen, die Blockchain unabhängig voneinander fortzusetzen. Sobald es wieder eine funktionierende Transatlantikverbindung gäbe, fügte sich das Netzwerk wieder zusammen und die kürzere der beiden Blockchains würde verworfen. In einem solchen Extremszenario verschwänden auf einem der beiden Kontinente Transaktionen aus der Blockchain und müssten erneut eingebaut werden. Ein bösartiger Netzwerkteilnehmer könnte eine solche Situation

---

[40] Typischste Ursache für ungültige Blöcke sind Datenübertragungsfehler. Im offenen Internet kommt je nach Verbindungsqualität etwa ein Bit pro Gigabyte falsch an. Solche Fehler können dank der Prüfsummen der Blöcke einfach erkannt und der Block neu übermittelt werden.

ausnutzen, indem er während der Trennung des Netzwerks die gleichen Bitcoins für Einkäufe in den USA und in Deutschland verwendet. Bei der Wiedervereinigung der Blockchain würde dann eine der beiden Transaktionen verworfen und der betroffene Händler verlöre die empfangenen Bitcoins.

Je länger die Blockchain wird und desto tiefer in der Blockchain eine bestimmte Transaktion damit liegt, desto kleiner ist die Wahrscheinlichkeit, dass sie von einer Revision der Blockchain betroffen ist und nochmals neu eingebaut werden muss. Das erneute Einbauen dürfte aber nur dann fehlschlagen, wenn der Absender der Transaktion dies durch konkurrierende Transaktionen mit den gleichen Bitcoins forciert, und erfordert demnach einen bösartigen Eingriff von Seiten des Absenders.[41]

3.3 Zeitpunkt einer Transaktion

In der Praxis werden Transaktionen je nach Wichtigkeit zu unterschiedlichen Zeitpunkten akzeptiert. Je länger man wartet, desto sicherer ist man, dass die Transaktion nicht mehr vereitelt werden kann. Vollständige Sicherheit gibt es nie, doch die Unsicherheit wird rasch vernachlässigbar klein.

Der erste Zeitpunkt, zu dem der Empfänger über die zu transferierenden Bitcoins verfügen kann, ist das Empfangen der signierten Transaktion vom Absender. Zu diesem Zeitpunkt ist die Transaktion noch nicht im Netzwerk bekannt. Es besteht eine Situation, in der sowohl der Absender als auch der Empfänger über die Bitcoins verfügen könnten. Der Absender hat das Geld sozusagen auf den Tresen gelegt, der Empfänger aber noch nicht an sich genommen. Dies kann innert Millisekunden geschehen.

---

[41] Eine Transaktion kann auch aufgrund von fehlender Transaktionsgebühren fehlschlagen. Dem kann der Empfänger aber begegnen, indem er nur Transaktionen mit angemessenen Gebühren akzeptiert. Zudem gehen wir in diesem Szenario ja davon aus, dass die Transaktion schon einmal in eine andere Variante der Blockchain aufgenommen wurde, womit es sehr wahrscheinlich ist, dass die Gebühr hoch genug gewählt wurde.

Eine weitere Form der Transaktion ist die Übergabe des Schlüssels zu einem Bitcoin-Konto, zum Beispiel in Form einer physischen Münze, die den Schlüssel hinter einem holographischen Siegel enthält. Hier besteht die Möglichkeit, dass der Absender heimlich eine Kopie des Schlüssels zurückbehalten hat und somit weiterhin über die Bitcoins verfügen kann. Dieses Risiko wird bei Münzen und Noten üblicherweise durch geeignete Sicherheitsmerkmale reduziert.

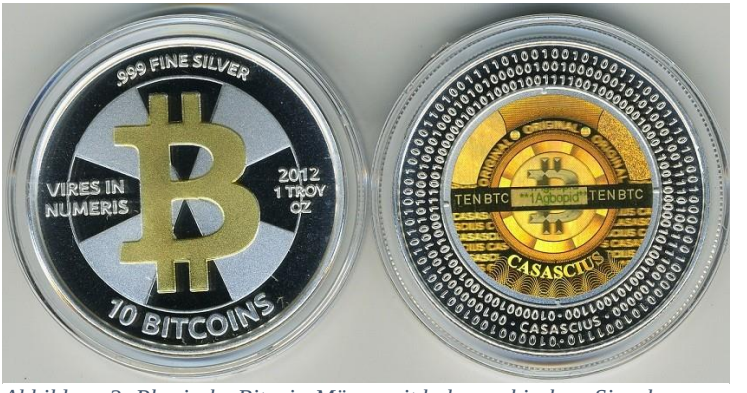


Abbildung 3: Physische Bitcoin-Münze mit holographischem Siegel

Der üblichste Zeitpunkt, zu der eine Zahlung akzeptiert wird, ist der der Veröffentlichung der Transaktion. Zu diesem Zeitpunkt hat eine Mehrheit der Netzwerkteilnehmer von der Transaktion erfahren. Auf diesen Zeitpunkt stützt sich zum Beispiel der Zahlungsdienstleister BitPay. Transaktionen können so innert Sekunden akzeptiert werden.

Grössere Zahlungen werden oft erst akzeptiert, nachdem diese eine bestimmte Anzahl Blöcke tief in der Blockchain eingebaut ist. Pro Block spricht man von einer Bestätigung. Die Börse Bitstamp verlangt zum Beispiel sechs Bestätigungen, [42] bevor man mit den eingezahlten Bitcoins handeln darf. So dauert es bis zum Akzeptieren einer Zahlung etwa 10 Minuten pro Bestätigung, im Fall von Bitstamp also etwa eine Stunde.

4. Mining und Geldmenge

4.1 Mining

In Abschnitt 3.2 wurde dargelegt, dass die Länge der Blockchain das wichtigste Entscheidungskriterium für deren Akzeptanz ist. Dies kann nur dann

[42] Bitstamp FAQ, www.bitstamp.net/faq

funktionieren, wenn nicht jeder einfach Block-Ketten beliebiger Länge generieren und so die Blockchain manipulieren kann. Aus diesem Grund wird das Erzeugen eines Blocks künstlich erschwert. Ein Block wird nur dann akzeptiert, wenn sein digitaler Fingerabdruck[43] bestimmte Kriterien erfüllt. Die einzige Möglichkeit, einen solchen Block zu finden, besteht darin, Milliarden von Varianten des Blocks durchzuprobieren und deren Fingerabdrücke zu berechnen, bis man schliesslich einen findet, der die Kriterien erfüllt.[44] Hat man aber einmal einen solchen Block gefunden, ist es für jeden sehr leicht verifizierbar, dass er tatsächlich einen solch seltenen Fingerabdruck hat. So kann der Erzeuger eines Blocks sehr einfach beweisen, dass er sehr viel Rechenleistung ins Erzeugen des Blocks investiert hat.

Aufgrund dieser nötigen Rechenleistung ist es einem Angreifer auch nicht möglich, beliebig viele Blöcke zu erzeugen und so das Netzwerk zu manipulieren. Um eine manipulierte, längere Blockchain zu erzeugen als alle anderen müsste ein Angreifer die Mehrheit der Rechenleistung im Netzwerk haben. Allerdings sind die ökonomischen Anreize so gesetzt, dass ein Angreifer mit sehr viel Rechenleistung langfristig mehr Geld durch korrektes Mitrechnen als durch Angriffe verdienen kann. Der Erzeuger eines Blocks erhält die Transaktionsgebühren aller Transaktionen im Block sowie eine vorbestimmte Menge neu geschöpfter Bitcoins. Zurzeit sind dies 25 Bitcoins. Diese schreibt er sich selbst in der ersten Transaktion gut, die er in den Block einbaut. So wird das Finden von Blöcken belohnt. Würde er sich zu viel oder zu wenig gutschreiben, würde der Block vom Rest des Netzwerks nicht akzeptiert.

4.2 Geldmenge

Die maximale Anzahl Bitcoins ist auf 21 Millionen begrenzt. Die Tatsache, dass die Geldmenge bei Bitcoin endlich ist, wird von Anhängern der österreichischen Schule der Wirtschaftstheorie oft als Garant für langfristige Stabilität gepriesen. Daher wird gemutmasst, Satoshi Nakamoto hätte diese Entscheidung aus wirtschaftlichen Überlegungen getroffen. Der wahre Grund dürfte

---

[43] Ein sogenannter Hash, konzeptionell vergleichbar mit einer Quersumme.

[44] Die Kriterien selbst sind künstlich gewählt und in der Art von „der Fingerabdruck muss in Binärdarstellung mit 40 Nullen beginnen“. Für die Transaktionen selbst sind diese Kriterien aber völlig irrelevant. Sie dienen nur dazu, den Schwierigkeitsgrad zum Erzeugen eines Blocks zu steuern.

aber profaner sein. So sind 21 Millionen Bitcoins in vielen Programmiersprachen die höchste Zahl, die sich ohne Rundungsverlust abspeichern lässt.[45]

Nun hätte Nakamoto beim Design des Systems die gesamte Geldmenge sich selbst gutschreiben können, doch wäre er damit wohl auf nur wenig Akzeptanz gestossen. Da ist es naheliegend, die Bitcoins über einen längeren Zeitraum verteilt nach Regeln in Umlauf zu bringen, die jedem Teilnehmer eine Chance lässt, ein paar zu erhaschen. Da die Gesamtmenge begrenzt ist, muss die Rate der neu geschöpften Bitcoins aber zwangsläufig abnehmen. Ein üblicher Weg, dies zu tun, ist eine Halbierung der Rate nach Ablauf bestimmter Zeitintervalle.[46] Bei Bitcoin ist dieses Intervall vier Jahre. Zu Beginn kamen 50 neue Bitcoins pro 10 Minuten in Umlauf, nun sind es 25, und ab Mitte 2016 werden es noch 12.5 sein. So kommt man den 21 Millionen beliebig nahe, ohne sie jemals zu erreichen.[47]

Ein grosser Vorteil der Reduktion der Schöpfungsrate liegt darin, dass die Miner immer stärker von den Transaktionsgebühren abhängig werden und damit auch einen zunehmenden Anreiz haben, an der Attraktivität des Gesamtsystems mitzuwirken, so dass es viele Nutzer anzieht, die viele Transaktionen ausführen. Eine begrenzte Geldmenge führt aber auch zu mehr Spekulation und dem Horten von Bitcoins. Andere Kryptowährungen haben aus solchen Überlegungen andere Begrenzungen und Ausschüttungskriterien. Allen gemeinsam ist aber, dass diese Kriterien von vornherein feststehen und die Geldmenge somit kaum dynamisch an die Wirtschaft angepasst werden kann, wie das Nationalbanken bei Landeswährungen machen. Diese Schwäche wird oft von Ökonomen kritisiert und als eine der Ursachen für die hohe Volatilität gesehen.

4.3 Mining Pools

---

[45] Die weitverbreiteten „double precision“ Gleitkommazahlen verwenden 52 Bits für die Mantisse. Berücksichtigt man die Aufteilbarkeit eines Bitcoins in 100 Millionen Satoshis, kann man nicht viel mehr als 21 Millionen Bitcoins ohne Präzisionsverlust als solche Zahl abspeichern. Grössere Zahlen zu unterstützen wäre möglich, aber mühsam für den Programmierer.

[46] Sogenanntes Exponential Backoff. en.wikipedia.org/wiki/Exponential_backoff

[47] Mathematisch gesehen handelt es sich um eine geometrische Reihe mit einem Grenzwert von etwa 21 Millionen.

Mit der zunehmenden Professionalisierung des Bitcoin-Netzwerks sind Mining-Pools entstanden. Die meisten Miner schliessen sich heute einem Pool an. In der Analogie der Abstimmung nach Rechenleistung wäre ein Mining-Pool eine Partei, welche von der Parteileitung (der Pool-Betreiber) koordiniert wird. Diese Entwicklung hat Nakamoto nicht vorhergesehen und sie stellt insofern eine Bedrohung dar, als starke Parteien in Versuchung geraten könnten, das Netzwerk zu ihren Gunsten zu manipulieren.[48]

Der Zweck der Mining-Pools ist ein ähnlicher wie bei Lotterie-Gemeinschaften. Das Einkommen eines einzelnen Miners hängt sehr stark vom Glück ab, Blöcke zu finden und ist damit sehr unregelmässig. Die Miner in einem Mining-Pool teilen die verdienten Bitcoins im Pool auf, so dass Glücks- oder Pechssträhnen weniger starke Einkommensschwankungen zur Folge haben. Ebenfalls einen leicht positiven Effekt hat die Koordination, indem sichergestellt wird, dass alle Pool-Teilnehmer im Zweifelsfall stets an der gleichen Variante der Blockchain weiterrechnen. Oft verlangt der Betreiber eines Pools für seine Leistung eine geringe Gebühr. De facto bietet ein teilnehmender Miner also Rechenleistung an den Poolbetreiber an, und wird dafür in Bitcoins bezahlt, was die rechtliche Betrachtung der so arbeitenden Miner deutlich vereinfachen dürfte, da ein Vertragsverhältnis zwischen zwei identifizierbaren Parteien besteht. Die etwas schwierigeren Fragen verschieben sich so auf den Pool-Betreiber, welcher die frisch geschöpften Bitcoins und die Transaktionsgebühren vom Netzwerk entgegennimmt und danach an die angeschlossenen Miner weiterleitet.

[48] Ein sogenannter 51%-Attack.

IV. Ausblick

„Bitcoin is like technology that's arrived from Mars, and so regulators don't know what to do with it. That's a good thing. What a lot of financial technology entrepreneurs will tell you is that if you are going to innovate in financial services, you want to do something so new and so different that the existing regulatory system doesn't know how to react to you. That is your window of opportunity."
– Marc Andreessen, founder of Netscape and Bitcoin-Investor[49]

Distributed Ledger Technology ist noch jung, und es bestehen diverse Möglichkeiten, diese auf weitere Anwendungszwecke auszudehnen. Es sind bereits Hunderte von Konkurrenzwährungen zu Bitcoin entstanden, allerdings sind dies meist simple Kopien des Systems mit einem neuen Namen und ein paar leicht angepassten Parametern. Bitcoin ist noch immer mit Abstand die bedeutendste Kryptowährung und dürfte es auf absehbare Zeit auch bleiben. Aufgrund des starken Netzwerkeffekts[50] kann Bitcoin nur von einem fundamental besseren System vom Thron gestossen werden. Ein Kandidat für ein solches System ist Ethereum, welches in Abschnitt 4.3 vorgestellt wird. Besser Chancen haben aber vermutlich Innovationen, die sich die existierende Infrastruktur von Bitcoin zunutze machen, so zum Beispiel das Konzept der Colored Coins, welches in Abschnitt 4.2 beschrieben wird.

1. Die Stärke offener Systeme

Die Stärke von Kryptowährungen liegt nicht in ihrer technischen Effizienz. Im Gegenteil: im Vergleich zu zentralisierten Lösungen sind Kryptowährungen auf ungleich mehr Rechenleistung angewiesen, um korrekt zu funktionieren, da jede Transaktion tausendfach nachvollzogen und archiviert wird. Die Stärke von Kryptowährungen liegt in ihrer dezentralen Natur und Unabhängigkeit. Dies ist für Technologien, die als Plattform dienen, essentiell. Dank seiner dezentralen Natur hat sich zum Beispiel das Internet als weltweites Informationsnetzwerk durchgesetzt, und nicht etwa das französische Minitel.

---

[49] Bloomberg, „Marc Andreessen on Finance: 'We Can Reinvent the Entire Thing'", 7.10.2014, bloomberg.com/news/2014-10-07/andreessen-on-finance-we-can-reinvent-the-entire-thing-.html

[50] Metcalfe's Law besagt, dass der Wert einer Netzwerktechnologie überproportional mit der Anzahl der Benutzer ansteigt.
Siehe auch en.wikipedia.org/wiki/Metcalfe%27s_law .

Ebenso läuft heute die grosse Mehrheit aller Server im Internet mit dem offenen Betriebssystem Linux. Und zwar nicht, weil es das beste System wäre, sondern weil eine Firma wie Google darauf setzen kann, ohne sich in die Abhängigkeit eines potentiellen Konkurrenten wie Microsoft zu begeben. Im Zahlungsverkehr setzen sich tendenziell ebenfalls gemeinsame Standards durch, so zum Beispiel Swift, welches den teilnehmenden Banken gehört, denn Banken möchten im Allgemeinen nicht ein Zahlungssystem verwenden, das von einer Konkurrenzbank kontrolliert wird. Bitcoin geht hier einen grossen Schritt weiter, indem es ein Zahlungssystem schafft, dass nicht von Banken, sondern von den Benutzern selbst kontrolliert wird und keine Eintrittsbarrieren kennt. So wie das Internet ein offenes System für den Austausch von Informationen ist, sind Kryptowährungen offene Systeme für den Zahlungsverkehr. Dies eröffnet eine noch schwer abzuschätzende, aber grosse Anzahl neuer Möglichkeiten zur Innovation der Finanzwelt.

2. Colored Coins

Im Vergleich zu anderen Kryptowährungen fliesst mit Abstand am meisten Rechenleistung ins Bitcoin-Netzwerk. Und je mehr Rechenleistung ins System fliesst, desto sicherer wird es. Zudem ist Bitcoin das älteste solche System, so dass das Risiko unbekannter Schwachstellen kleiner ist als bei neuen Konkurrenzsystemen. Deshalb liegt es nahe, für neue Ideen soweit möglich die existierende Infrastruktur von Bitcoin wiederzuverwenden. Ein Ansatz, dies zu tun, ist der der Colored Coins. Diese erlauben es, beliebige Werte im Bitcoin-Netzwerk zu emittieren. So wäre es zum Beispiel denkbar, dass ein Emittent Frankencoins ins Bitcoin-Netzwerk emittiert, welche dann frei zwischen den Benutzern übertragen werden könnten und am Ende bei Bedarf beim Emittenten wieder in herkömmliche Zahlungsmittel zurückgetauscht werden könnten.

Die Funktionsweise von Colored Coins ist denkbar einfach: der Emittent ordnet einem bestimmten Bitcoin (oder Bruchteil davon)[51] einen bestimmten Wert zu und garantiert diesen. Da alle Transaktionen öffentlich bekannt sind, sind sämtliche Bitcoins exakt nachverfolgbar und es kann damit auch leicht bewiesen werden, dass es sich bei einem Bitcoin (oder Bruchteil davon) um einen Teil dieses vom Emittenten bezeichneten Bitcoins handelt. Um zum Beispiel des Frankencoins zurückzukommen, könnte der Emittent zum Beispiel erklären, dass ein bestimmter Bitcoin 1 Million Franken wert ist und dann

[51] Bitcoins sind maximal auf Hundertmillionstel aufteilbar.

Bruchteile davon zum entsprechenden Preis verkaufen. Retourniert ein Benutzer einen Zehntausendstel dieses Bitcoins an den Emittenten, erhält er dafür 100 Franken. Colored Coins könnten somit als das digitale Äquivalent klassischer Banknoten angesehen werden, wie sie vor dem Bargeldmonopol der Zentralbank existierten.[52] Der Wert der zugrundeliegenden Bitcoins ist dabei vernachlässigbar, so wie der Wert des Metalls beim Einfränkler im Alltag vernachlässigt wird.

Das Emittieren klassischer Währungen ist aber nur ein mögliches Anwendungsszenario von vielen. Colored Coins könnten zum Beispiel auch mit Gold oder Gütern wie einem Auto hinterlegt werden. Im Fall des Autos könnte der bezeichnete Bitcoin als Schlüssel dienen, um das Auto aufzuschliessen und anzulassen, sofern das Auto ans Internet angeschlossen ist und das entsprechende Protokoll versteht. Colored Coins könnten aber auch verwendet werden, um Aktien oder Anleihen abzubilden. Da jederzeit bekannt ist, auf welcher Adresse sich diese befinden, könnten mit minimalem Aufwand Dividenden- bzw. Zinszahlungen ausgeführt werden. Technisch gesehen könnten auch jederzeit kryptographisch sichere Aktionärsabstimmungen durchgeführt werden, wobei sich die Aktionäre nur als Inhaber der Aktien identifizieren müssten, und nicht als reale Personen.

Ob diese Anwendungsszenarien nicht nur technisch möglich, sondern auch sinnvoll sind und sich bewähren, muss sich aber erst noch zeigen. Zurzeit werden Colored Coins und verwandte Ansätze (etwa Mastercoin oder Counterparty.io) noch nicht in nennenswertem Umfang verwendet.

3. Ethereum

Kryptosysteme der nächsten Generation zielen oft darauf ab, flexibler und universeller zu sein als die der ersten Generation, welche sich mit der Funktion als Zahlungssystem begnügen. Eines der weltweit ambitioniertesten Projekte dieser Art ist Ethereum mit Sitz in Zug. Genau wie Bitcoin ist Ethereum dezentral organisiert und verwendet eine eigene Währung, den Ether. Die Firma Ethereum treibt die Entwicklung der Ethereum-Software voran, übt aber keine direkte Kontrolle über das laufende System aus.

---

[52] Die Nationalbank könnte theoretisch auch selbst digitales Bargeld in Form von Colored Coins oder anderen Kryptowährungen ausgeben. Dies wäre ein eleganter Weg, die Vollgeldinitative (vollgeld-initiative.ch) umzusetzen, sollte der unwahrscheinliche Fall einer Annahme eintreten.

Ethereum ist, was Informatiker als Turing-vollständig bezeichnen. Das bedeutet, dass im Prinzip jeder Algorithmus, der auf einem Computer in endlicher Zeit ausgeführt werden kann, auch in Ethereum in endlicher Zeit ausgeführt werden kann. Man könnte zum Beispiel Verträge in einer von Ethereum unterstützten Programmiersprache formulieren, die dann automatisch vom System ausgeführt werden. Ein einfaches Beispiel für einen solchen Vertrag wäre eine Wette: Alice wettet mit Bob um 100 Ether, dass Deutschland die Fussball-WM gewinnt. Dazu wird ein Algorithmus spezifiziert, der am Tag nach dem Final auf der FIFA-Webseite nachschaut, wer die WM gewonnen hat und dann je nach dem Alice oder Bob die Wetteinsätze auszahlt. Diese Einsätze werden bereits bei Abschluss der Wette ans System bezahlt werden und bleiben bis zur Ausführung des Algorithmus blockiert.

Von diesem Konzept ausgehend kann man theoretisch beliebig komplizierte Algorithmen erstellen, die nicht auf eine einmalige Ausführung einer Zahlung beschränkt sind. So kann man in Ethereum eigene Währungen spezifizieren, Abstimmungen mit vorprogrammierten Konsequenzen durchführen, Finanzinstrumente implementieren, oder gar dezentrale, computergesteuerte Organisationen erstellen. Zum Beispiel wäre ein Programm denkbar, das ohne menschliches Zutun selbständig mit Kryptowährungen handelt und allfällige Gewinne dazu verwendet, für die im Ethereum-System verbrauchte Rechenleistung zu bezahlen. Ein solches Programm könnte seinen Schöpfer ohne weiteres überleben und selbständig wirtschaften, falls es clever genug gemacht ist. Auch liesse es sich aufgrund Ethereums dezentraler Natur kaum aufhalten.

Ob und für welche dieser Anwendungen es einen tatsächlichen Bedarf gibt, muss sich ebenfalls erst noch zeigen. Zurzeit ist Ethereum in der Entwicklungsphase und noch nicht funktionstüchtig.