Virtuelle Währungen – Das Zahlungsmittel der Zukunft? Vergleich zwischen der rechtlichen Regulierung ausgewählter Staaten

Felix Schmid

Band 19

Analysen und Berichte zum Wirtschafts- und Steuerrecht
Herausgegeben von Prof. Dr. iur. Heribert M. Anzinger

Felix Schmid

Virtuelle Währungen – Das Zahlungsmittel der Zukunft? Vergleich zwischen der rechtlichen Regulierung ausgewählter Staaten

Schriftenreihe
Analysen und Berichte zum Wirtschafts- und Steuerrecht

Herausgeber:
Prof. Dr. iur. Heribert M. Anzinger

Band 19

Felix Schmid

Virtuelle Währungen – Das Zahlungsmittel der Zukunft? Vergleich zwischen der rechtlichen Regulierung ausgewählter Staaten

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.dnb.de abrufbar.

Dissertation/Magisterarbeit, Universität Ulm,
Fakultät für Mathematik und Wirtschaftswissenschaften,
Jahr

Impressum

Universität Ulm
Institut für Rechnungswesen und Wirtschaftsprüfung
Prof. Dr. iur. Heribert M. Anzinger
Helmholtzstraße 22
89081 Ulm
http://www.uni-ulm.de/index.php?id=43569

Eine Übersicht über alle Bände der Schriftenreihe finden Sie unter
http://www.uni-ulm.de/index.php?id=44832

Diese Veröffentlichung ist im Internet auf dem institutionellen Repositorium der Universität Ulm (https://oparu.uni-ulm.de) verfügbar und dort unter der Lizenz CC BY-NC-ND 4.0 publiziert.
Details zur Lizenz sind unter
https://creativecommons.org/licenses/by-nc-nd/4.0/ zu finden.

ISSN: 1868 – 0518

Zu dieser Reihe

In der Reihe Analysen und Berichte zum Wirtschafts- und Steuerrecht werden herausragende Studien- und Diplomarbeiten veröffentlicht, die einen Beitrag zum Erkenntnisgewinn insbesondere im Steuerrecht, im Bilanzrecht, im Unternehmensrecht, im Finanz-, Bank- und Kapitalmarktrecht und in angrenzenden Rechtsgebieten liefern wollen.

Anlass zur Begründung dieser Reihe war der Umstand, dass mir als Hochschullehrer immer wieder gute Arbeiten vorgelegt wurden, deren Gedanken und Erkenntnisse ich gerne einer breiteren Fach-öffentlichkeit zugänglich gemacht hätte. Doch zu oft ließen vereinzelte methodologische Zweifel, kleinere formale Mängel oder schlicht der Umfang der Arbeiten den Weg zu einer wissenschaftlichen Zeitschriftenveröffentlichung als weit erscheinen. Und die studentischen Verfasser hatten zwar regelmäßig großes Interesse an einer Veröffentlichung, oft aber bereits bei Abgabe ihrer Arbeiten mit dem ersten Arbeitsvertrag ausgestattet, nicht mehr die Zeit zu den dafür notwendigen Kürzungen und Überarbeitungen.

Diese ausdrücklich als Forum für Studien- und Diplomarbeiten deklarierte Reihe ermöglicht es, weiterführende studentische Analysen und Berichte unredigiert herauszugeben.

Prof. Dr. iur. Heribert M. Anzinger, Professor für Wirtschafts- und Steuerrecht

Vorwort

Virtuelle Währungen werden von einer breiten Öffentlichkeit durch die Verbreitung von Bitcoin wahrgenommen. Daneben entstehen aber beinahe täglich neue Formen, deren Technologien sich verändern und deren Anwendungspotential unterschiedlich beurteilt wird. Ihr Vorverständnis unterscheidet sich in den drei Lagern, der leidenschaftlichen Enthusiasten, vorsichtig Neugierigen und warnenden Skeptiker.

Aufgabe der Universitäten ist es, neuen technologischen Möglichkeiten aufgeschlossen gegenüber zu stehen, die Empirie zu ergründen, einzuordnen und Potentiale zu ergründen. Aus der Perspektive der Rechtswissenschaft gehört dazu auch die rechtliche Einordnung.

Die als Bachelorarbeit im Studiengang Wirtschaftswissenschaften im Dezember 2017 an der Universität Ulm vorgelegte Ausarbeitung von Felix Schmid vermittelt einen hervorragenden Einblick in den Stand der Technik sowie die Chancen und Risiken virtueller Währungen. Damit schafft sie Grundlagen, um die rechtliche Regulierung in ausgewählten Staaten bewerten und Regulierungsbedarf einschätzen zu können.

Die Arbeit ist überzeugend strukturiert und trifft im Rahmen einer Bachelorarbeit das richtige Maß zwischen einführenden, zielführenden und kritischen Teilen. Felix Schmid hat verschiedene Fragestellungen sinnvoll kombiniert und eine strukturierte Analyse der Chancen und Risiken virtueller Währungen vorbereitet. Dabei hat er sein Thema sinnvoll eingegrenzt.

Felix Schmid hat dabei nicht nur dokumentiertes Wissen zusammengetragen, sondern auch eigene Daten ermittelt, etwa zur tatsächlichen Transaktionskapazität des Bitcoin-Netzwerks. Er hat nicht nur Meinungsbilder zusammengeführt, sondern auch eigene Wertungen vorgenommen und überzeugend begründet. Dies und der skizzierte Überblick über erste Regulierungsansätze in einzelnen Staaten empfehlen die Arbeit zur einführenden Lektüre in das Thema Virtuelle Währungen.

Im Dezember 2018

Prof. Dr. Heribert Anzinger, Universität Ulm

Zusammenfassung / Abstract

Heutzutage existieren neben der bekanntesten Kryptowährung “Bitcoin” noch viele weitere virtuelle Währungen. Ziel dieser Arbeit ist es, zu untersuchen, ob virtuelle Währungen das Potenzial haben, das Zahlungsmittel der Zukunft zu werden und inwiefern es einer Regulierung bedarf. Der erste Teil der Arbeit widmet sich ausschließlich der ursprünglich einzigen Kryptowährung Bitcoin und erläutert deren Funktionsweise. Anschließend geraten auch die alternativen Kryptowährungen, die sogenannten Altcoins, in den Fokus. Mittlerweile gibt es an die Tausend verschiedene virtuelle Währungen.

Virtuelle Währungen weisen große Unterschiede zu den herkömmlichen Währungen auf. Ökonomen sprechen jedoch nur dann von einer Währung, wenn die drei Geldfunktionen erfüllt sind, deshalb wird im weiteren Verlauf untersucht, inwiefern die Zahlungsmittelfunktion, Wertaufbewahrungsfunktion und Recheneinheitsfunktion von virtuellen Währungen erfüllt wird.

Da virtuelle Währungen ein sehr junges und neues Themengebiet sind, existiert derzeit noch keine einheitliche Herangehensweise für die Regulierung. Aufgrund der extrem schnell voranschreitenden Entwicklung im Bereich der Kryptowährungen gibt es aktuell weder einen umfassenden Verbraucherschutz, noch Maßnahmen zur Verhinderung von kriminellen Aktivitäten. Diese Risiken werden aufgezeigt.

Einige Staaten haben bereits Maßnahmen zur Regulierung getroffen, sodass die Arbeit mit dem Aufzeigen bereits getroffener Regulierungsmaßnahmen in der EU und in den USA abgeschlossen wird.

Inhaltsverzeichnis

Inhaltsverzeichnis……X

Abbildungsverzeichnis…….....XII

Tabellenverzeichnis……..……...XIII

Abkürzungsverzeichnis…….……..XIV

A. Einleitung……1

B. Einordnung virtueller Währungen……2

C. Kryptowährungen……...7

I. Der Prototyp Bitcoin……...7

1. Was ist Bitcoin?.....7
2. Funktionsweise der Blockchain-Technologie……9
3. Die Quellen für den Erwerb von Bitcoin……...14

II. Kryptowährungen im Überblick……20

III. Unterschiede verschiedener Kryptowährungen..23

IV. Bitcoin Cash, Ethereum und Ripple……...……..25

1. Bitcoin Cash……25
2. Ethereum……..26
3. Ripple…….……27

D. Virtuelle Währungen und die Geldfunktionen……..28

I. Zahlungsmittelfunktion.....29

II. Wertaufbewahrungsfunktion…….……..35

III. Recheneinheitsfunktion…….……..40

E. Rechtliche Regulierung virtueller Währungen……41

I. Risiken……...41

II. Regulierungsmaßnahmen in der EU und den USA ……....45

F. Fazit……49

Literaturverzeichnis……...52

Abbildungsverzeichnis

Abb. 1: Schematischer Überblick digitale Währungen……4

Abb. 2: Entstehung einer Bitcoin Adresse……11

Abb. 3: Struktur eines Blocks……..12

Abb. 4: Funktionsweise Proof-of-Work……..14

Abb. 5: Ausschnitt von Berlin aus coinmap……...17

Abb. 6: Prognostizierte Gesamtanzahl von Bitcoins über die Zeit……...19

Abb. 7: Gesamte Marktkapitalisierung vom 28.04.2013 bis zum 13.09.2017…….22

Abb. 8: Relativer Anteil einzelner Kryptowährungen an der ges. Marktkapitalisierung…….22

Abb. 9: Zahl der täglichen Bitcoin-Transaktionen…….30

Abb. 10: Kursentwicklung Bitcoin……37

Abb. 11: Volatilität von diversen Währungen……38

Tabellenverzeichnis

Tab. 1: Kategorisierung virtueller Währungen 6

Tab. 2: Marktkapitalisierung der zehn größten Kryptowährungen am 11.09.2017 20

Abkürzungsverzeichnis

Abb.	Abbildung
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
bzw.	beziehungsweise
ca.	circa
d. h.	das heißt
DLT	Distributed-Ledger-Technologie
et al.	et alia
EU	Europäische Union
EZB	Europäische Zentralbank
Hrsg.	Herausgeber
id.	Idem
i. d. R.	in der Regel
KWG	Kreditwesengesetz
MB	Megabyte
MSBs	money services businesses
PoW	Proof-of-Work
PoS	Proof-of-Stake
S.	Seite
SegWit	Segregated Witness
Std.	Stunden
USA	United States of America
USD	United States Dollar
UTC	koordinierte Weltzeit
Vgl.	Vergleiche
Vol.	Volume

A. Einleitung

„The man with a new idea is a crank until the idea succeeds."

Mark Twain (1835-1910)

Satoshi Nakomoto war solch ein Mann mit einer neuen Idee. Ob diese das Potenzial hat, in der Zukunft erfolgreich zu sein, soll in dieser Arbeit untersucht werden.

Satoshi Nakomoto gilt als Erfinder der Kryptowährung Bitcoin. Am dritten Januar 2009 begann mit der Generierung des ersten Blocks der Blockchain die praktische Umsetzung der Kryptowährung Bitcoin mit dem Ziel, eine Währung zu schaffen, die virtuell erzeugt und gehandelt wird, ganz ohne die Hilfe einer zentralen Instanz.[1] Dies soll mit Hilfe der sogenannten Blockchain- bzw. Distributed-Ledger-Technologie gelingen.

Neben Bitcoin wurden in den letzten Jahren viele weitere innovative Kryptowährungen entwickelt. Parallel zu den neuen Entwicklungen wurden auch immer mehr mögliche Schwachstellen der Kryptowährungen offengelegt. Dennoch stieg die Marktkapitalisierung in den letzten Jahren stetig an, sodass virtuelle Währungen weiter an Bedeutung und Bekanntheit gewinnen.

Ziel dieser Arbeit ist es, zu untersuchen, ob virtuelle Währungen das Potenzial haben, das Zahlungsmittel der Zukunft zu werden und inwiefern es einer Regulierung bedarf. Der erste Teil der Arbeit widmet sich ausschließlich der ursprünglich einzigen Kryptowährung Bitcoin und erläutert deren Funktionsweise. Anschließend geraten auch die alternativen Kryptowährungen, die sogenannten Altcoins, in den Fokus. Mittlerweile gibt es an die Tausend verschiedene virtuelle Währungen. In dieser Arbeit wird neben Bitcoin jedoch nur noch auf die Währungen Ethereum, Bitcoin Cash und Ripple näher eingegangen. Ethereum und Ripple werden im Besonderen

[1] Siehe *Nakomoto, S.* (2008), S. 1.

erwähnt, da sie sich durch ihre Anwendungsmöglichkeiten grundlegend von Bitcoin unterscheiden und dabei nach Bitcoin die höchste Marktkapitalisierung aufweisen.

Virtuelle Währungen weisen große Unterschiede zu den herkömmlichen Währungen auf. Ökonomen sprechen jedoch nur dann von einer Währung, wenn die drei Geldfunktionen erfüllt sind, deshalb wird im weiteren Verlauf untersucht, inwiefern die Zahlungsmittelfunktion, Wertaufbewahrungsfunktion und Recheneinheitsfunktion von virtuellen Währungen erfüllt wird.

Da virtuelle Währungen ein sehr junges und neues Themengebiet sind, existiert derzeit noch keine einheitliche Herangehensweise für die Regulierung. Aufgrund der extrem schnell voranschreitenden Entwicklung im Bereich der Kryptowährungen gibt es aktuell weder einen umfassenden Verbraucherschutz, noch Maßnahmen zur Verhinderung von kriminellen Aktivitäten. Diese Risiken werden aufgezeigt.

Einige Staaten haben bereits Maßnahmen zur Regulierung getroffen, sodass die Arbeit mit dem Aufzeigen bereits getroffener Regulierungsmaßnahmen in der EU und in den USA abgeschlossen wird.

B. Einordnung virtueller Währungen

Digitale Währung - virtuelle Währung – Kryptowährung - Bitcoin.

Bei der Recherche zu diesem Thema fällt sehr schnell auf, dass verschiedene Autoren bzw. Institutionen diese Begriffe austauschbar verwenden[2], obwohl es eindeutige Unterschiede gibt.

Wie in Abb.1 zu sehen, sind digitale Währungen der Überbegriff für elektronisches Geld (auch E-Geld genannt) und virtuelle Währungen.[3] Das Europäische Parlament und der Rat der Europäischen Union definieren E-Geld als „jeden elektronisch — darunter auch magnetisch — gespeicherten monetären

[2] Vgl. *Lam, P. N./Lee, D. K. C.* (2015a), S. 6; *Financial Action Task Force (Hrsg.)* (2014), S. 4.
[3] Dazu *Financial Action Task Force (Hrsg.)* (2014), S. 4.

Wert in Form einer Forderung gegenüber dem Emittenten, der gegen Zahlung eines Geldbetrags ausgestellt wird […] und der auch von anderen natürlichen oder juristischen Personen als dem E-Geld-Emittenten angenommen wird."[4] E-Geld ist also eine digitale Darstellung von Fiat-Währungen[5], welche für elektronische Transaktionen verwendet wird.[6]

Eine einheitliche Definition virtueller Währung gibt es derzeit noch nicht[7], verschiedene Institutionen haben jedoch in der Vergangenheit versucht, diese zu definieren. So hat die EZB 2012 virtuelle Währung als unreguliertes digitales Geld, welches normalerweise von ihren Entwicklern herausgegeben und kontrolliert wird und von einer speziellen virtuellen Gesellschaft genutzt und akzeptiert wird, definiert.[8] 2015 hat die EZB es für nötig gehalten, ihre Definition zu aktualisieren und in gewissen Aspekten abzuändern.[9] Demnach können virtuelle Währungen als digitale Darstellung eines Wertes definiert werden, der nicht von Zentralbanken, Kreditinstitutionen oder E-Geld Institutionen herausgegeben wird und unter Umständen als eine Alternative zu Geld genutzt werden kann.[10] Diese Auffassung stimmt mit der des Internationalen Währungsfonds überein, welcher noch hinzufügt, dass virtuelle Währungen ihre eigene Währungseinheit besitzen.[11] Auch die Europäische Bankenaufsichtsbehörde und die Europäische Kommission definieren virtuelle Währungen als digitale Darstellung eines Wertes, der weder von einer Zentralbank noch von einer öffentlichen Behörde ausgegeben wird mit dem Zusatz, dass er nicht zwingend mit einer Fiat-Währung verknüpft sein muss, aber von natürlichen und juristischen Personen als Zahlungsmittel anerkannt wird und elektronisch übertragen, gespeichert

---

[4] *Europäische Union (Hrsg.)* (2009), S. 11.
[5] Fiat-Geld ist Kreditgeld, das seinen Wert nicht aus sich heraus, sondern durch Zuweisung i. d. R. durch gesetzliche Vorschriften erhält und als Währung verwendet wird. Das heutige Geld der Zentralbanken (z. B. Euro, USD) stellt Fiat-Geld dar.
[6] Dazu *Financial Action Task Force (Hrsg.)* (2014), S. 4.
[7] Siehe *Lam, P. N./Lee, D. K. C.* (2015a), S. 310.
[8] Vgl. *Europäische Zentralbank (Hrsg.)* (2012), S. 13.
[9] Vgl. *Europäische Zentralbank (Hrsg.)* (2015), S. 25.
[10] Id.
[11] Siehe. *Internationaler Währungsfonds (Hrsg.)* (2016), S. 7.

und gehandelt werden kann.[12] Zusätzlich ist noch festzuhalten, dass virtuelle Währungen kein gesetzliches Zahlungsmittel sind.[13]

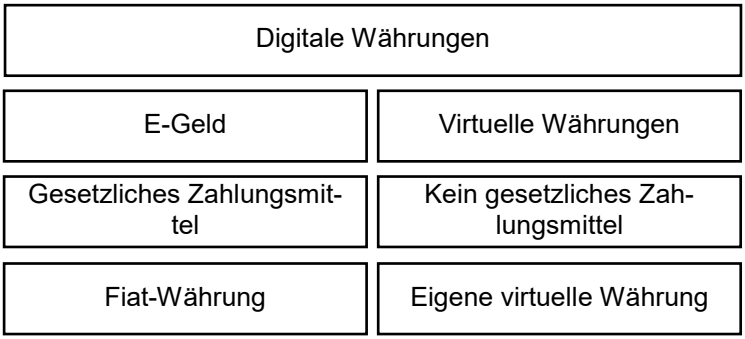

Abb. 1: Schematischer Überblick digitale Währungen

Grundsätzlich kann man virtuelle Währungen in konvertierbar und nicht-konvertierbar aufteilen.[14]

Konvertierbare virtuelle Währungen haben einen entsprechenden Wert in einer Fiat-Währung und können gegen diese hin und her getauscht werden.[15]

Nicht-konvertierbare virtuelle Währungen agieren ausschließlich innerhalb einer in sich geschlossenen virtuellen Welt und können nicht in Fiat-Währungen umgetauscht werden.[16] Ein Beispiel hierfür ist die virtuelle Währung „World of Warcraft Gold“, mit der im bekannten Multiplayer-Online-Spiel „World of Warcraft“ bezahlt wird.

---

[12] Vgl. *Europäische Kommission (Hrsg.)* (2016), S.35; *Europäische Bankenaufsichtsbehörde (Hrsg.)* (2014), S. 11.
[13] Vgl. *Financial Action Task Force (Hrsg.)* (2014), S. 4; *Europäische Zentralbank (Hrsg.)* (2012), S. 16; *Europäische Bankenaufsichtsbehörde (Hrsg.)* (2014), S. 13.
[14] Diese Kategorisierung unterscheidet sich von der der EZB. Die EZB unterteilt virtuelle Währungen in drei Schemen. Geschlossen, mit unidirektionalem Fluss und mit bidirektionalem Fluss.
[15] Vgl. *Financial Action Task Force (Hrsg.)* (2014), S. 4.
[16] Siehe *Internationaler Währungsfonds (Hrsg.)* (2016), S. 8.

Konvertierbare virtuelle Währungen können zusätzlich in zentrale und dezentrale virtuelle Währungen aufgeteilt werden, wohingegen alle nicht-konvertierbaren virtuellen Währungen per Definition zentral sind.[17] Zentrale virtuelle Währungen verfügen über eine einzelne verwaltende Instanz (auch Administrator genannt), die das System kontrolliert. Ein Beispiel für eine virtuelle Währung, die von einer zentralen Instanz verwaltet wird und konvertierbar ist, ist der „Linden Dollar“, das Zahlungsmittel im Online-Computerspiel „Second Life“. Hier kann man sich die im Spiel erwirtschafteten „Linden Dollar“ in USD auszahlen lassen.

[17] Vgl. *Financial Action Task Force (Hrsg.)* (2014), S. 5.

	Zentral	Dezentral
Konvertierbar	▪ Kontrolliert von einem Administrator ▪ Tauschbar in Fiat-Währung ▪ Beispiel: Second Life Linden Dollar	▪ Kontrolliert von den Teilnehmern ▪ Tauschbar in Fiat-Währung ▪ Beispiel: Bitcoin **= Kryptowährung**
Nicht-konvertierbar	▪ Kontrolliert von einem Administrator ▪ Nicht tauschbar in Fiat-Währung ▪ Beispiel: World of Warcraft Gold	Existiert nicht

Tab. 1: Kategorisierung virtueller Währungen
(in Anlehnung an: *Financial Action Task Force (Hrsg.)* (2014), S. 8.)

Dagegen werden dezentrale virtuelle Währungen, welche man auch als Kryptowährung[18] bezeichnet, nicht von einem Administrator verwaltet, sondern vielmehr durch die Teilnehmer selbst.[19] Der Vollständigkeit halber seien noch hybride Schemen[20] genannt, in denen ein Teil der Funktionen von einer zentralen Autorität geleistet wird und ein Teil dezentral von den Teilnehmern selbst.[21]

Da Kryptowährungen die jüngste Art virtueller Währung sind, die gleichzeitig das größte Potenzial, aber auch die meisten Risiken besitzen, wird sich diese Arbeit auf die Analyse von Kryptowährungen beschränken – im Speziellen wird auf die Kryptowährung Bitcoin eingegangen, da diese als der Prototyp aller Kryptowährungen bezeichnet werden kann und deshalb die bekannteste ist.

C. Kryptowährungen

I. Der Prototyp Bitcoin

1. Was ist Bitcoin?

Kryptowährungen sind auf Mathematik basierende, dezentrale, konvertierbare virtuelle Währungen, die mit Hilfe von Kryptografie verschlüsselt werden.[22] Die erste und bekannteste Kryptowährung ist Bitcoin und wurde am ersten November 2008 zum ersten Mal in dem Whitepaper „Bitcoin: A Peer-to-Peer Electronic Cash System“[23] von Satoshi Nakomoto erwähnt.[24] Wer sich hinter dem Pseudonym Satoshi Nakomoto[25] verbirgt, ist bis heute nicht bekannt.[26]

---

[18] Die Bezeichnungen (dezentrale) virtuelle Währungen und Kryptowährungen werden in dieser Arbeit als Synonyme verwendet.
[19] Siehe *Financial Action Task Force (Hrsg.)* (2014), S. 4.
[20] Beispielsweise Ripple.
[21] Vgl. *Internationaler Währungsfonds (Hrsg.)* (2016), S. 8-9.
[22] Vgl. *Financial Action Task Force (Hrsg.)* (2014), S. 5.
[23] *Nakomoto, S.* (2008), S. 1.
[24] Siehe *Wallace, B.* (2011).

Das Wort BITCOIN setzt sich aus den beiden englischen Begriffen Bit, der kleinsten Maßeinheit für eine Datenmenge und coin, in Deutsch Münze, zusammen.[27] Der Begriff Bitcoin bezeichnet zwei unterschiedliche Dinge. Zum einen das komplette Währungssystem, d. h. die Technologie und das globale Netzwerk und zum anderen die Währungseinheit an sich. Dabei bezeichnet „Bitcoin“ mit einem Großbuchstaben das gesamte Währungssystem und „bitcoin(s)“ die Währungseinheit an sich. Die Währung wird auch als „BTC“ bzw. an manchen Börsen mit „XBT“ abgekürzt.[28]
Bitcoin basiert auf einem Peer-to-Peer-Netzwerk. Dieses besteht aus Teilnehmern, die alle eine bestimmte Software - den „Bitcoin-Client“ - verwenden.[29] Diese ist eine Open-Source-Software und somit für jedermann frei zugänglich.[30]
Die Erfindung von Bitcoin ist revolutionär, da es zum ersten Mal möglich ist, eine digitale Währung von einer Person zu einer anderen zu schicken, ohne dass dabei dritte Parteien, wie Finanzinstitute, involviert werden müssen.[31] Es gelang erstmals eine Lösung des Double-Spending-Problems ohne die Hilfe von vertrauenswürdigen Dritten[32]. Das Double-Spending-Problem ist folgendes: Vor Bitcoin waren digitale Währungen beliebig oft kopierbar und es gab keine Möglichkeit, ohne die Hilfe eines zentralen Intermediärs sicherzustellen, dass ein Teil des Geldes nicht schon einmal ausgegeben wurde. Vertrauenswürdige Dritte mussten Buch über die getätigten Transaktionen führen, um zu gewährleisten, dass alle

---

[25] Es wird davon ausgegangen, dass Satoshi Nakomoto in Japan lebt. Ob es sich dabei um nur eine Person oder um eine Gruppe handelt ist jedoch unbekannt.
[26] Dazu *Tu, K. V./Meredith, M. W.* (2014), S. 279-280.
[27] Vgl. *Kerscher, D.* (2014), S. 10.
[28] Dazu *Lam, P. N./Lee, D. K. C.* (2015a), S. 14.
[29] Vgl. *Kerscher, D.* (2014), S. 11.
[30] Siehe *Münzer, J.* (2014), S. 26; *Lam, P. N./Lee, D. K. C.* (2015a), S. 11.
[31] Vgl. *Nakomoto, S.* (2008), S. 1; *Europäische Zentralbank (Hrsg.)* (2012), S. 21.
[32] Siehe *Nakomoto, S.* (2008), S. 1.

Teile des digitalen Geldes nur ein Mal ausgegeben wurden.[33] Bitcoin löst dieses Problem mit Hilfe der Blockchain-Technologie, die auf dem Prinzip eines verteilten Hauptbuches mit Transaktionskonten („Distributed Ledger“) beruht.[34]

2. Funktionsweise der Blockchain-Technologie

Die Blockchain ist, wie der Name schon sagt, eine Kette aus aneinandergereihten Blöcken, in denen alle Transaktionen gespeichert sind. Dabei bezieht sich jeder Block auf den zuvor generierten Block und bestätigt dessen Richtigkeit.[35] Da sich jeder neue Block auf den Vorgängerblock bezieht, ergibt sich eine fortlaufende Kette von Blöcken, die aufeinander aufbauen.[36] Die Bitcoin Blockchain besteht aktuell (Stand 30.08.2017, 8:45 Uhr) aus 482.597 Blöcken.[37] Der erste Block („Genesis Block“) wurde am 3. Januar 2009 generiert.[38]

Bitcoin bzw. die Blockchain-Technologie verwendet ein Public-Key-Kryptosystem[39], um die Sicherheit der Transaktionen zu gewährleisten.[40] Die Funktionsweise der Blockchain-Technologie lässt sich am besten anhand einer Beispieltransaktion erklären. Will beispielsweise Alice ein Bitcoin an Bob verschicken, so müssen beide im Besitz eines Bitcoin-Clients sein. Diese Client-Software wird auch als Wallet bezeichnet.[41] Um ein Bitcoin-Wallet zu eröffnen, kann die Software kostenlos und anonym heruntergeladen werden, ohne das Einrichten eines Benutzerkontos.[42] Mittlerweile gibt es eine Vielzahl verschiedener Wallet-Lösungen. Der Hauptunterschied besteht darin, dass der Bitcoin-Nutzer entweder nur die Basisfunktio-

---

[33] Hierzu *Swan, M.* (2015), Abschnitt: The Double-Spend and Byzantine Generals’ Computing Problems.
[34] Vgl. *Brühl, V.* (2017), S. 1.
[35] Ähnlich *Bhaskar, N. D./Lee, D. K. C.* (2015), S.49.
[36] Dazu *Kerscher, D. (2014), S. 82-83.*
[37] Siehe beispielsweise *Blockchain.info (Hrsg.)* (2017a).
[38] Vgl. *Caetano, R.* (2015), Abschnitt: The Genesis Block.
[39] Da die Kryptografie die Grundlage der dezentralen virtuellen Währungen bildet, werden diese auch Kryptowährung genannt.
[40] Ähnlich *Kerscher, D.* (2014), S. 20.
[41] Dazu *Kerscher, D.* (2014), S. 49.
[42] Id.

nen nutzen kann – Bitcoin-Adressen verwalten und Transaktionen tätigen – oder, dass der Nutzer zusätzlich die Funktion eines vollständigen Bitcoin-Klienten („full node“) übernimmt. Als „full node“ hat ein Bitcoin-Klient zusätzlich die Aufgabe, Transaktionen zu verifizieren.[43]

Anschließend erstellt Alice eine Nachricht („message“), welche die Transaktionsdetails beinhaltet, vereinfacht beispielsweise „Ich will ein Bitcoin an Bob transferieren“. Zusätzlich beinhaltet die Nachricht einen sogenannten „hash“ von der letzten Transaktion, in welcher dieser Bitcoin verwendet wurde. Sobald die Transaktion zwischen Alice und Bob vollendet ist, wird auch diese Transaktion einen Hash erzeugen, der benötigt wird, wenn Bob seinen Bitcoin an eine weitere Person überweisen möchte. Auf diese Weise lassen sich alle Bitcoins bis zu ihrem Ursprung zurückverfolgen.[44]

Für eine Transaktion benötigt man einen privaten Schlüssel („private key“) und einen öffentlichen Schlüssel („public key“) bzw. eine Bitcoin Adresse („bitcoin address“). Zuerst erzeugt der Bitcoin-Client einen privaten Schlüssel. Dieser besteht aus einer zufälligen 256-bit Binärzahl[45], welche anschließend in ein Hexadezimalsystem mit 64 Ziffern umgewandelt wird. Zum Beispiel: 1E99423A4ED27608A15A2616A2B0E9E52CED330AC530EDCC32C8FFC6A526AEDD.[46] Mit Hilfe eines Algorithmus (Elliptic Curve Digital Signature Algorithms (ECDSA)) wird aus dem privaten Schlüssel ein passender öffentlicher Schlüssel erstellt.[47] Die Bitcoin Adresse erhält man durch das Zerlegen des öffentlichen Schlüssels mit den Verschlüsselungsmethoden SHA256[48] und RIPEMD-160.[49] Eine Bitcoin Adresse existiert aus 26-35 Zeichen, bestehend aus Zahlen,

---

[43] Vgl. *Brühl, V.* (2017), S. 136.
[44] Ähnlich *Lee, L.* (2015), S. 95.
[45] Die generierte 256-bit Binärzahl besteht aus 256 zufälligen Ziffern aus Nullen und Einsen.
[46] Vgl. *Lee, L.* (2015), S. 96.
[47] Dazu *Caetano, R.* (2015), Abschnitt: Elliptic Curve Cryptography; *Kerscher, D.* (2014), S. 54.
[48] SHA steht für Secure Hash Algorithm.
[49] Siehe *Bhaskar, N. D./Lee, D. K. C.* (2015), S. 51.

Groß- und Kleinbuchstaben.[50] Bitcoin Adressen besitzen eine eingebaute Fehlerkontrolle durch eine Prüfsumme, sodass Adressen mit einem Schreibfehler abgelehnt werden.[51] Anders als bei Konten wird in der Regel für jede Transaktion eine neue Bitcoin Adresse verwendet.[52]

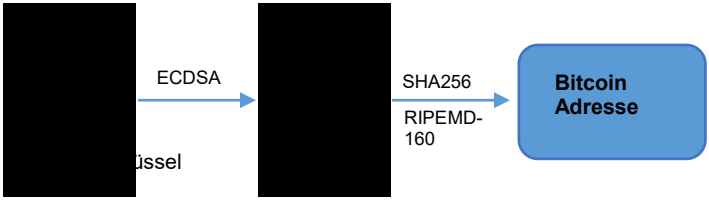

Abb. 3: Entstehung einer Bitcoin Adresse

Sobald Alice im Besitz der Nachricht („Ich will ein Bitcoin an Bob transferieren“ + Hash der letzten Transaktion) und der Bitcoin Adresse von Bob ist, signiert Alice die Transaktion mit Hilfe ihrer digitalen Signatur.[53] Die digitale Signatur entsteht durch einen kryptografischen Signierungsalgorithmus aus der Nachricht und dem privaten Schlüssel.[54]

Bis zu diesem Punkt konnte alles offline ausgeführt werden. Jetzt muss sich Alice online mit dem Bitcoin Netzwerk verbinden, um eine Anfrage zur Ausführung der Transaktion (einen Bitcoin an Bob zu transferieren) an alle vollständigen Netzwerkknoten („full nodes“) zu versenden.[55] Diese haben nun die Aufgabe, die Validität der Transaktion dezentral zu überprüfen und die Transaktion im gesamten Peer-to-Peer Netzwerk an die anderen Netzwerkknoten weiterzuleiten.[56]

Sobald die Transaktion verifiziert wurde, wartet sie in einem sogenannten „Mempool“ darauf, mit den anderen wartenden

---

[50] Um Verwechslungen zu vermeiden existieren die Zeichen O,0, I und l nicht.
[51] Dazu *Caetano, R.* (2015), Abschnitt: Explaining Bitcoin addresses.
[52] Vgl. *Brühl, V.* (2017), S. 136.
[53] Vgl. *Lee, L.* (2015), S. 98.
[54] Dazu *Brühl, V.* (2017), S. 136; *Lee, L.* (2015), S. 98.
[55] Ähnlich *Lee, L.* (2015), S. 98.
[56] Siehe *Brühl, V.* (2017), S. 136-137.

Transaktionen in einen Block verpackt und bestätigt zu werden.[57] Dies ist die Aufgabe der sogenannten „Miner“ (Name abgeleitet vom Schürfen von Rohstoffen wie beispielsweise Gold). Beim „Mining“ suchen die Miner die Lösung für eine mathematische Aufgabe, sodass ein neuer Block generiert werden kann, der dann in die Blockchain aufgenommen wird. Dieser Vorgang wird „Proof-of-Work“ genannt.

Kopfteil	Version	02000000
	Hash des vorherigen Blocks	0000000000000001ef42d93177gf…
	Merkle Root	46e7a942fb425c3837d52f198452…
	Zeitstempel	358b0553
	Bits	535f0119
	Nonce	48750833
	Anzahl der Transaktionen	1493
Hauptteil	Transaktionen	

Abb. 4: Struktur eines Blocks (in Anlehnung an: *Bhaskar, N. D./Lee, D. K. C.* (2015), S.48.)

Im Folgenden wird beschrieben, wie ein solcher Block aufgebaut ist. Wie in Abb. 3 zu sehen, besteht er aus einem Kopfteil („header“) und einem Hauptteil („body“).[58] Während der Hauptteil die Transaktionen beinhaltet, besteht der Kopfteil aus folgenden sieben Feldern: Versionsnummer, Hash des vorheri-

[57] Vgl. *Lee, L.* (2015), S. 100.
[58] Vgl. *Bhaskar, N. D./Lee, D. K. C.* (2015), S. 48.

gen Blocks, Merkle Root, Zeitstempel, Bits, Nonce und Anzahl der Transaktionen.

Die Versionsnummer eines Blocks hängt von der Version der Software, die zur Generierung des Blocks verwendet wurde, ab.[59] Der Hash des vorherigen Blocks ist ein 256-bit Wert und dient als Referenz auf den vorherigen Block der Blockchain.[60] Die Merkle Root entsteht, indem die Transaktionen des Hauptteils zuerst einzeln und dann paarweise so lange mit dem SHA256 Algorithmus verschlüsselt, also „gehasht" werden, bis ein einzelner Hashwert, die Merkle Root, verbleibt.[61] Die Merkle Root wird dann mit dem Hash des vorherigen Blocks erneut durch den SHA256 Algorithmus zu einem sogenannten „challenge string" gehasht.

Damit ein neuer Block generiert werden kann, müssen die Miner durch einen algorithmischen Suchprozess solange Zufallszahlen für das „Nonce"- Feld suchen, bis eine gefor-derte Zielgröße für den Hashwert des neuen Blocks unterschritten ist.[62] Dabei stellt das „Bits"- Feld die aktuell geforderte Zielgröße, auch Schwierigkeit („difficulty") genannt, dar.[63] Je höher die Schwierigkeit, desto kleiner ist die Zielgröße und somit auch der Hashwert. Dieser beginnt immer mit Nullen und mit steigender Schwierigkeit erhöht sich somit die Anzahl an führenden Nullen.[64] Der Hashwert des neuen Blocks entsteht, indem der „challenge string" und die Nonce (auch „proof string" genannt) gehasht werden.[65] Da die erfolgreiche Generierung eines gültigen Hashwertes den Einsatz entsprechender Rechnerkapazitäten erfordert und damit Kosten verursacht, bezeichnet man diesen Vorgang als Proof-of-Work.[66]

---

[59] Id.
[60] Id.
[61] Vgl. *Brühl, V.* (2017), S. 137.
[62] Ähnlich *Brühl, V.* (2017), S. 137.
[63] Dazu *Bhaskar, N. D./Lee, D. K. C.* (2015), S. 48, *Caetano, R.* (2015), Abschnitt: Proof of work.
[64] Siehe *Bhaskar, N. D./Lee, D. K. C.* (2015), S. 50.
[65] Vgl. *Lee, L.* (2015), S. 101-102.
[66] Siehe *Brühl, V.* (2017), S. 137.

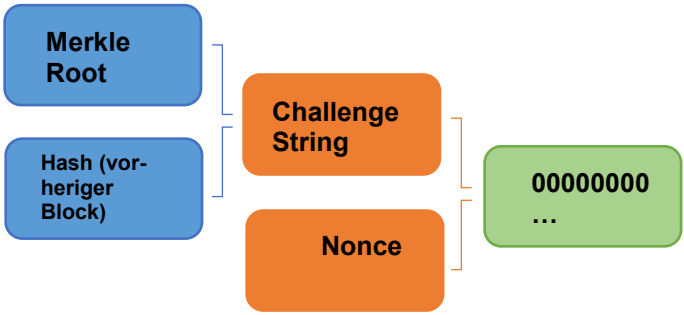

Abb. 5: Funktionsweise Proof-of-Work

Der Zeitstempel („timestamp“) gibt die aktuelle Zeit in Sekunden seit dem 01.01.1970 um 0:00 Uhr (UTC) an und bestätigt die Hinzufügung zur Blockchain zu einem spezifischen Zeitpunkt.[67] Die Anzahl der im Block enthaltenen Transaktionen wird durch das letzte Feld im Kopfteil angezeigt.

Eine Bitcoin Transaktion besteht aus einem oder mehreren Inputs und einem oder mehreren Outputs. Dabei verweisen die Inputs auf die Outputs vergangener Transaktionen, die zuvor dem Aussteller der aktuellen Transaktion geschickt wurden.[68] Die Summe aller Inputs muss immer größer oder gleich der Summe aller Outputs betragen. Besteht eine Differenz zwischen den Summen, so wird dies als Transaktionsgebühr verstanden und geht an den „Miner“, der die Transaktion bestätigt.[69]

3. Die Quellen für den Erwerb von Bitcoin

Aktuell können Bitcoins auf drei verschiedene Arten erlangt werden. Die einfachste Art ist, Bitcoins auf Handelsplattformen online gegen eine Fiat-Währung einzutauschen.[70] Handelsplattformen können Börsen, Marktplätze oder Wechselstuben

---

[67] Dazu Nakomoto, S. (2008), S. 2; *Bhaskar, N. D./Lee, D. K. C.* (2015), S. 48.
[68] Dazu *Kerscher, D.* (2014), S. 57.
[69] Ähnlich *Tschorsch, F./Scheuermann, B.* (2016), S. 2089.
[70] Vgl. *Plassaras, N. A.* (2013), S. 386.

sein.[71] Kurz nach der Gründung von Bitcoin im Jahr 2009 wurden auch die ersten Handelsplattformen geschaffen. Die erste und lange Zeit wichtigste Börse für Bitcoin war die japanische Börse Mt.Gox[72].[73] Mittlerweile gibt es über 100 verschiedene Kryptowährungsbörsen weltweit.[74] Während der Handel auf Börsen automatisiert abläuft, muss man auf Marktplätzen selbst nach einem passenden Kaufs- bzw. Verkaufsangebot suchen. Der Kurs, zu dem Kryptowährungen gekauft oder verkauft werden, kommt wie jeder andere Kurs für ein Wirtschaftsgut durch Angebot und Nachfrage zustande.[75] Bei Wechselstuben können Kryptowährungen direkt vom jeweiligen Betreiber zu einem bestimmten Preis erworben werden.[76]

Eine weitere Möglichkeit Bitcoins zu erlangen, ist das Verkaufen von Waren oder Dienstleistungen im Austausch gegen Bitcoins. Bei wie vielen verschiedenen Händlern es aktuell möglich ist, mit Bitcoin zu bezahlen, kann nur geschätzt werden. Es gibt viele Verzeichnisse, die Bitcoin Akzeptanzstellen listen, wobei keines jemals wirklich vollständig ist. Laut einem Bericht von Coinalytics akzeptierten im September 2015 weltweit rund 106.000 Händler Bitcoin als Zahlungsmethode.[77] Aus dem Bericht geht auch hervor, dass die Zahl der Händler, die Bitcoins akzeptieren, im Jahr 2015 noch gestiegen ist.[78] Dahingegen meinte im Juli 2017 James Faucette, Analytiker bei Morgan Stanley, in einem Bericht, dass „die Akzeptanz von Bitcoin schrumpfend und praktisch null ist.“[79] [Übersetzung des Verfassers] Gemäß Morgan Stanley wurde 2016 Bitcoin noch von fünf der 500 größten Onlinehändler akzep-

---

[71] Vgl. *Finanzen.net (Hrsg.)* (2017).
[72] Der Name Mt.Gox ist eine Abkürzung für „Magic: The Gathering Online Exchange“, da Mt.Gox ursprünglich eine Handelsplattform für Spielkarten des Fantasy-Spiels „Magic: The Gathering“ war.
[73] Hierzu *Caetano, R.* (2015), Abschnitt: Comparing Bitcoin exchanges.
[74] Siehe *CryptoCoinCharts (Hrsg.)* (2017).
[75] Vgl. *Kerscher, D.* (2014), S. 69.
[76] Siehe *Finanzen.net (Hrsg.)* (2017).
[77] Vgl. *Coindesk (Hrsg.)* (2015), Folie 8.
[78] Id.
[79] “bitcoin acceptance is virtually zero and shrinking” (*Chaparro, F.* (2017)).

tiert. 2017 allerdings nur noch von drei von 500.[80] Trotz Bitcoins steigender Beliebtheit erlauben nur wenige der großen Onlinehändler Bitcoin als Zahlungsmittel. Als Beispiel sind Overstock.com, Microsoft oder Expedia zu nennen.[81] Von den über 100.000 Händlern, die Bitcoin als Zahlungsmittel akzeptieren, sind die meisten kleine Unternehmen und der Großteil beschränkt sich auf Onlinehändler, die keine lokalen Geschäfte haben.

Zur Bestimmung physischer Akzeptanzstellen existiert beispielsweise die Internetseite coinmap.org.[82] Coinmap zeigt auf einer Weltkarte Geschäfte, Geldautomaten und viele andere lokale Akzeptanzstellen für Bitcoin. Zusätzlich sind auch Standorte gelistet, die Forschung unter anderem zu dem Thema Bitcoin betreiben, wie z. B. das Prometheus Institut in Berlin.[83] Die Gesamtanzahl der dort gelisteten Akzeptanzstellen beträgt am 7. September 2017 genau 9754. Bei Betrachtung der Karte wird schnell klar, dass die Bitcoin-Infrastruktur noch weit davon entfernt ist, ein lückenloses Netzwerk von Einkaufsmöglichkeiten aufzuweisen. Zudem beschränken sich die Nutzungsmöglichkeiten überwiegend, aber nicht ausschließlich, auf große Städte. In Deutschland beispielsweise auf Berlin, Hamburg, Frankfurt oder München. In der Universitätsstadt Ulm mit rund 120.000 Einwohnern gibt es laut coinmap dahingegen keine einzige Möglichkeit mit Bitcoin zu bezahlen.

---

[80] Siehe dazu *Chaparro, F.* (2017); *Katz, L.* (2017).
[81] Dazu *Chokun, J.* (2017).
[82] Vgl. *coinmap (Hrsg.)* (2017).
[83] Id.

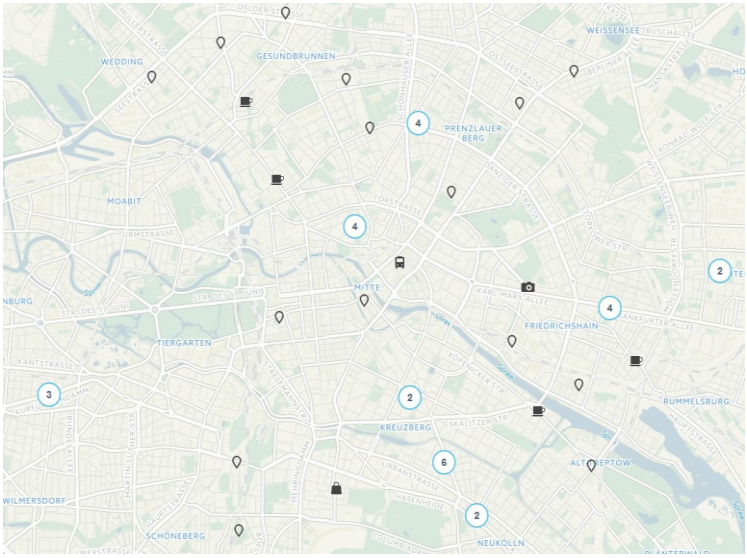

Abb. 6: Ausschnitt von Berlin aus coinmap
(Quelle: *coinmap (Hrsg.)* (2017))

Als Beispiel zeigt obige Abbildung 5 einen Kartenausschnitt aus Berlin. Es zeigt sich, dass auch in Deutschlands Bitcoin Hotspot Berlin kein lückenloses Netz aus Akzeptanzstellen existiert. Die Geschäftsfelder, die Bitcoin als Zahlungsmittel akzeptieren, sind breit gestreut. So gibt es in Berlin mehrere Restaurants, Bars und Cafés, aber auch beispielsweise zwei Arztpraxen und zwei Rechtsanwaltskanzleien.[84] Wichtig zu beachten ist, dass sich auf coinmap alle Bitcoin Akzeptanzstellen selbstständig auf der Internetseite eintragen müssen. Somit ist die Liste niemals komplett vollständig und aktuell, sondern dient eher als Überblick über die aktuelle Händlerinfrastruktur.

In Japan kann man vielleicht schon bald bei über 260.000 Händlern mit Bitcoins zahlen.[85] Japans Regierung erkennt seit dem 1. April 2017 Bitcoin und andere virtuelle Währungen als offizielles Zahlungsmittel an und seit dem 1. Juli 2017 muss

[84] Id.
[85] Hierzu *Helms, K.* (2017).

keine Konsumsteuer mehr auf Bitcoin-Transaktionen in Japan gezahlt werden.[86] Im April 2017 kam es zu einer Partnerschaft zwischen dem Unternehmen Recruit Lifestyle Co., Ltd. und der größten japanischen Kryptowährungsbörse Coincheck. Mithilfe der Point of Sale (POS) App „AirRegi“ von Recruit Lifestyle Co., Ltd. können Läden, die Zahlungen mit AirRegi abwickeln, seit dem 3. Juli 2017 auch Bitcoin als Zahlungsmittel akzeptieren.[87] Derzeit nutzen ungefähr 260.000 Händler AirRegi in Japan und hätten somit die Möglichkeit, auch Bitcoin als Zahlungsmittel zu akzeptieren.[88] Die japanische Ladenkette Megane Super mit 334 Filialen akzeptiert beispielsweise seit dem 10. Juli 2017 Bitcoin über die App AirRegi.[89] Außerdem kann man unabhängig von der App seit Juli 2017 in allen Filialen des japanischen Technikkaufhaus Bic Camera mit Bitcoins bezahlen.[90]

Die dritte Option Bitcoins zu erhalten, ist die Generierung neuer Münzen durch den oben beschriebenen Miningprozess. Wie schon in Abschnitt 2. „Funktionsweise der Blockchain-Technologie“ beschrieben, wird ein Anreizsystem benötigt, damit die Miner freiwillig Rechenleistung aufbringen, um Blöcke der Blockchain und somit Transaktionen zu verifizieren. Die Ausschüttung neuer Bitcoins als Belohnung für die erfolgreiche Generierung eines gültigen Hashwertes ist das Anreizsystem von Bitcoin.[91]

Da das Bitcoin Protokoll vorsieht, dass im Durchschnitt alle zehn Minuten ein Block ge-

neriert wird, passt sich der Schwierigkeitsgrad für das Lösen des mathematischen Problems alle 2016 Blöcke an.[92] Dies entspricht ungefähr einem Zeitraum von zwei Wochen. Werden die Blöcke zu schnell generiert, wird die Schwierigkeit erhöht. Somit benötigen die Miner länger, um eine gültige

---

[86] Siehe *bitFlyer (Hrsg.)* (2017a) und *bitFlyer (Hrsg.)* (2017b).
[87] Vgl. *Helms, K.* (2017).
[88] Id.
[89] Id.
[90] *Bic Camera (Hrsg.)* (2017); *Nikkei Asian Review (Hrsg.)* (2017).
[91] Ähnlich *Kerscher, D.* (2014), S.80.
[92] Dazu *Kerscher, D.* (2014), S.83.

Nonce zu finden und die Generierung neuer Blöcke passt sich wieder näher an die vorgegebenen zehn Minuten an.[93] Während die Generierungsrate neuer Blöcke konstant ist, nimmt die Anzahl neu ausgeschütteter Bitcoins geometrisch ab.[94]

Alle 210.000 Blöcke[95] halbiert sich der Wert, angefangen bei 50 BTC pro Block im Jahr 2009.[96] Dies hat zur Folge, dass die Obergrenze jemals existierender Bitcoins 21 Millionen[97] beträgt, welche ungefähr im Jahr 2140 erreicht wird.[98]

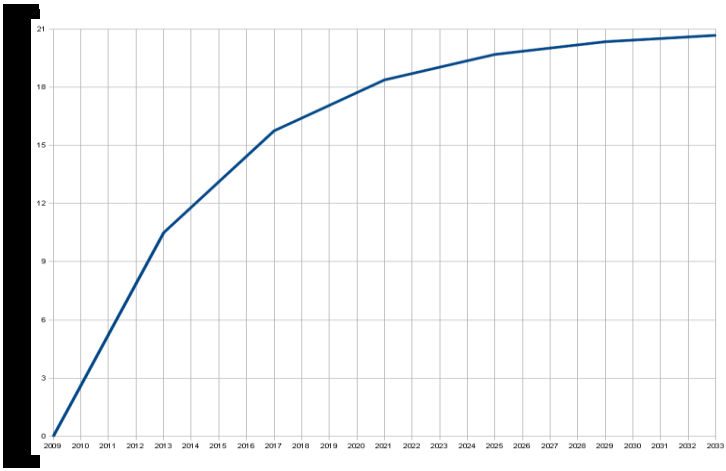

Abb. 7: Prognostizierte Gesamtanzahl von Bitcoins über die Zeit (in Anlehnung an: *Bitcoin Wiki (Hrsg.)* (2011))

Wie in Abb. 6 zu sehen, werden jedoch voraussichtlich bereits im Jahr 2032 ungefähr 99,2% aller Bitcoins generiert sein.[99] Dies hat zur Folge, dass mit sinkender Blockbelohnung die Transaktionskosten steigen werden, da die Miner weiterhin ein

---

[93] In Anlehnung an *Kerscher, D.* (2014), S. 83-84.
[94] Vgl. *Europäische Zentralbank (Hrsg.)* (2012), S. 25.
[95] 210.000*10min ≈ 4 Jahre.
[96] Vgl. *Franco, P.* (2015), S. 143.
[97] 20,999,999.9769 Bitcoins ist der exakte Wert.
[98] Siehe *Bitcoin Wiki (Hrsg.)* (2017b), Projected Bitcoins Long Term.
[99] Id.

Anreizsystem benötigen, damit sie Rechenleistung freiwillig zur Verfügung stellen.[100]

Aktuell, im September 2017, befinden sich etwas mehr als 16,5 Millionen Bitcoins im Umlauf und die Blockbelohnung beträgt 12,5 BTC pro Block.[101]

II. Kryptowährungen im Überblick

Rang	Währung	Marktkapitalisierung in USD	Preis pro Coin in USD
1	Bitcoin	68.676.365.041	4147,54
2	Ethereum	27.524.786.435	291,09
3	Bitcoin Cash	8.791.850.639	530,47
4	Ripple	8.323.182.726	0,217067
5	Litecoin	3.483.427.632	65,87
6	Dash	2.396.803.638	317,41
7	NEM	2.278.224.000	0,253136
8	Monero	1.685.664.456	111,88
9	Ethereum Classic	1.400.577.818	14,68
10	IOTA	1.378.074.437	0,495794

Tab. 2: Marktkapitalisierung der zehn größten Kryptowährungen am 11.09.2017
(In Anlehnung an: *CoinMarketCap (Hrsg.)* (2017a))

Neben Bitcoin haben sich mittlerweile noch viele andere Kryptowährungen etabliert, die umgangssprachlich Altcoins, also alternative Coins genannt werden.[102] Der Quellcode von Bitcoin ist öffentlich frei zugänglich, sodass Programmierer welt-

[100] Siehe *Gora, V.* (2015), S. 820.
[101] Vgl. *Bitcoincharts (Hrsg.)* (2017), Bitcoin Network.
[102] Hierzu *Europäische Zentralbank (Hrsg.)* (2015), S. 9.

weit die Möglichkeit haben, eine eigene Kryptowährung, basierend auf dem Bitcoin Protokoll zu erfinden.[103] Gemäß der Internetseite CoinMarketCap existieren derzeit 866 verschiedene Kryptowährungen, die alle an mindestens einer öffentlichen Börse aktiv handelbar sind.[104]Kryptowährungen, die früher existiert haben, heute jedoch nicht mehr gehandelt werden, zählen somit nicht dazu.[105] Tab. 2 listet die zehn größten Kryptowährungen, gemessen nach ihrer Marktkapitalisierung, auf. Dabei berechnet sich die Marktkapitalisierung, indem der aktuelle Preis (gewichteter Durchschnitt aller Preise von allen Märkten) mit der Anzahl an Coins (die sich aktuell im Umlauf befinden) multipliziert wird.[106]

Derzeit weisen elf virtuelle Währungen eine Marktkapitalisierung von mehr als einer Milliarde USD auf und über 30 virtuelle Währungen eine Marktkapitalisierung über 100 Millionen USD.[107]

Der Kryptowährungsmarkt wächst rapide und der aktuelle Trend ist eine steigende Anzahl an Kryptowährungen sowie eine starke Wertsteigerung.[108] Wie in Abb. 7 zu sehen, erreichte der Kryptowährungsmarkt am 2. September 2017 seinen bislang höchsten Wert mit einer Marktkapitalisierung von ca. 179,8 Milliarden USD. Dies bedeutet, dass sich die Marktkapitalisierung in jüngster Vergangenheit vom 1. Januar 2017 bis zum 2. September 2017 ziemlich exakt verzehnfacht hat.[109]. Die Grafik aus Abb. 7 beginnt am 28. April 2013 mit einer Marktkapitalisierung von knapp 1,6 Milliarden USD und endet am 13. September 2017 mit einer Marktkapitalisierung in Höhe von 137,9 USD.[110]

---

[103] Vgl. *Ong, B. et al.* (2015), S. 82.
[104] Siehe *CoinMarketCap (Hrsg.)* (2017b).
[105] Hierzu *Ong, B. et al.* (2015), S. 82-83.
[106] Vgl. *CoinMarketCap (Hrsg.)* (2017b).
[107] Siehe *CoinMarketCap (Hrsg.)* (2017a).
[108] Dazu *CoinMarketCap (Hrsg.)* (2017c), Total Market Capitalization und *CoinMarketCap (Hrsg.)* (2017d).
[109] Marktkapitalisierung am 01.01.2017 betrug ca. 17,7 Milliarden USD.
[110] *CoinMarketCap (Hrsg.)* (2017c), Total Market Capitalization.

Abb. 8: Gesamte Marktkapitalisierung vom 28.04.2013 bis zum 13.09.2017
(Quelle: *CoinMarketCap (Hrsg.)* (2017c), Total Market Capitalization)

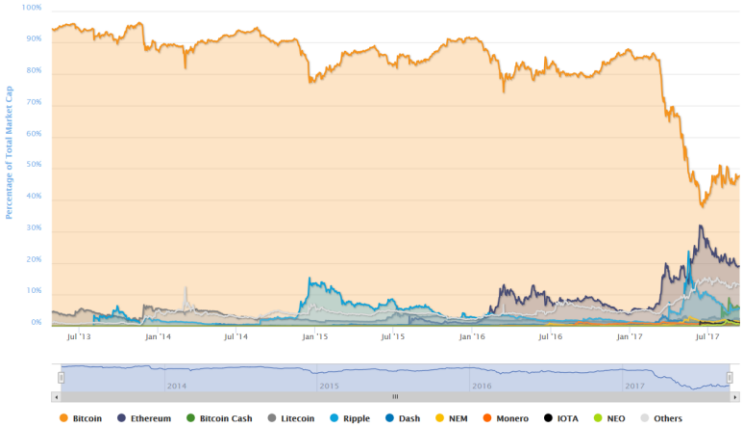

Abb. 9: Relativer Anteil einzelner Kryptowährungen an der ges. Marktkapitalisierung
(Quelle: *CoinMarketCap (Hrsg.)* (2017c), Percentage of Total Market Capitalization (Dominance))

Mit dem Durchbruch von Ripple und Ethereum im März 2017 hat die Dominanz Bitcoins gegenüber den Altcoins stark abgenommen (siehe Abb. 8). Während Bitcoin am 1. Januar 2017 noch ungefähr 87,6% der gesamten Marktkapitalisierung

in Anspruch nahm, sind es zum Zeitpunkt des Schreibens dieser Arbeit (13.09.2017) nur noch 47,7%.

Bitcoin ist zwar nach wie vor die wichtigste und bekannteste Kryptowährung, allerdings nicht mehr die einzige.

Da Ethereum, Bitcoin Cash und Ripple die bedeutendsten Altcoins sind und wesentliche Unterschiede zu Bitcoin aufweisen (abgesehen von Bitcoin Cash), wird auf diese in Abschnitt C. IV. näher eingegangen.

III. Unterschiede verschiedener Kryptowährungen

Obwohl Altcoins in den unterschiedlichsten Varianten existieren, basieren sie alle auf der fundamentalen Erfindung von Bitcoin, der Distributed-Ledger-Technologie (DLT), jedoch basieren nicht alle Kryptowährungen auf der Blockchain-Technologie.[111] Die Blockchain ist nur eine Variante der DLT.[112] Die primären technischen und funktionellen Unterschiede der verschiedenen Kryptowährungen lassen sich in folgende vier Kategorien einteilen:

Die erste und wahrscheinlich wichtigste Kategorie ist der Validierungsmechanismus.[113] Außer Proof-of-Work (PoW) gibt es noch zahlreiche andere Mechanismen, um Transaktionen zu verifizieren und somit neue Coins zu erschaffen. Neben Proof-of-Work ist Proof-of-Stake (PoS) ein alternativer, oft genutzter Validierungsmechanismus.[114] Bei dem PoW-Mechanismus hängt die Wahrscheinlichkeit, einen neuen Block zu generieren von der Höhe der zur Verfügung gestellten Rechenleistung ab. Beim PoS-Mechanismus hängt sie hingegen von der Anzahl der Coins ab, die man besitzt.[115] Jemand der 1% der gesamten Coins besitzt, kann somit auch 1% der Blöcke generieren.[116] Zusätzlich lassen sich DLT-Systeme in offene

---

[111] Siehe *Ong, B. et al.* (2015), S. 83.
[112] Ähnlich *Hildner, A.* (2016), S. 487.
[113] Dazu *Europäische Zentralbank (Hrsg.)* (2015), S. 10.
[114] Vgl. *Lee, L.* (2015), S. 108.
[115] Dazu *Bitcoin Wiki (Hrsg.)* (2015).
[116] Id.

(„permissionless“) und zugangsbeschränkte („permissioned“) DLT-Systeme gliedern.[117] Da bei dem PoW-Mechanismus grundsätzlich jeder Rechenleistung dem Netzwerk zur Verfügung stellen kann, der im Besitz der öffentlich frei zugänglichen Software ist, liegen diesem offene DLT-Systeme zugrunde.[118] Bei dem PoS-Mechanismus (wörtlich „Beteiligungsnachweis“) muss jeder Transaktionsteilnehmer nachweisen, dass er über eine spezielle Berechtigung zur Teilnahme an dem System verfügt. Diesen Berechtigungsnachweis erhält er von einer zentralen Legitimationsstelle, also von der Institution, die das System kontrolliert.[119] Aus diesem Grund liegen dem PoS-Mechanismus zugangsbeschränkte DLT-Systeme zugrunde. Außerdem gibt es hybride Systeme, die beispielsweise PoW und PoS kombinieren.[120]

Eine weitere Kategorie bildet die Nutzung verschiedener Algorithmen und die damit verbundenen Auswirkungen auf die Blockchain, wie zum Beispiel die Veränderung des Zeitabstands zwischen den einzelnen Blöcken oder die Häufigkeit der Anpassung des Schwierigkeitsgrads. [121] Neben Bitcoins SHA256 ist Scrypt der meist verwendete Algorithmus. Die Kryptowährungen Litecoin und Dogecoin verwenden zum Beispiel Scrypt.[122]Jedoch basiert die zweitgrößte Kryptowährung Ethereum auf dem Ethash Algorithmus.[123]

Die dritte Kategorie, in der sich verschiedene Kryptowährungen unterscheiden, ist die Anzahl der (maximal) herausgegebenen Coins.[124] Während sich bei Bitcoin jemals maximal 21 Millionen Coins im Umlauf befinden werden, sind es bei Ripple beispielsweise 100 Milliarden.[125]

---

[117] In Anlehnung an *Geiling, L.* (2016), S. 30.
[118] Dazu *Brühl, V.* (2017), S. 140.
[119] Vgl. *Geiling, L.* (2016), S. 30.
[120] Siehe *Europäische Zentralbank (Hrsg.)* (2015), S. 10.
[121] Id.
[122] Id.
[123] Vgl. *Ethereum Homestead (Hrsg.)* (2017a), The algorithm.
[124] Hierzu *Europäische Zentralbank (Hrsg.)* (2015), S. 11.
[125] Siehe *CoinMarketCap (Hrsg.)* (2017e).

Kryptowährungen, die sich durch neue Ideen funktionell unterscheiden, bilden die letzte Kategorie.[126] Bestes Beispiel hierfür ist die virtuelle Währung Ethereum, die im Folgenden näher beschrieben wird.

IV. Bitcoin Cash, Ethereum und Ripple

Neben Bitcoin sind die Altcoins Bitcoin Cash, Ethereum und Ripple aufgrund ihrer hohen Marktkapitalisierung am bekanntesten und sollen deswegen im Folgenden kurz beschrieben werden.

1. Bitcoin Cash

Bitcoin Cash entstand am ersten August 2017 durch eine Aufspaltung („hard fork") der Bitcoin Blockchain und ist der Kryptowährung Bitcoin sehr ähnlich.[127] Die Bitcoin Blockchain spaltete sich am 01.08.2017 mit Block 478558 in zwei „Ketten" auf.[128] Seit dem ersten August werden auf der Nebenkette alle Bitcoin Cash-Transaktionen verzeichnet. Der Grund für die Aufspaltung war eine Meinungsverschiedenheit verschiedener Teilnehmer des Bitcoin-Netzwerks darüber, wie das Skalierungsproblem[129] gelöst werden soll.

Der Hauptunterschied zwischen Bitcoin und Bitcoin Cash liegt in der Blockgröße. Während ein Block auf der Bitcoin Blockchain maximal 1 MB groß sein darf, wurde bei Bitcoin Cash die Blockgröße auf 8 MB erhöht.[130] Um „Replay Attacks" zu verhindern wurde zusätzlich der Ablauf des Transaktionsprozesses bei Bitcoin Cash leicht abgeändert.[131] Unter einem Replay Attack versteht man die Replikation einer Transaktion. Da die Nutzer für beide Währungen die gleichen privaten

---

[126] Vgl. *Europäische Zentralbank (Hrsg.)* (2015), S. 11; *Ong, B. et al.* (2015), S. 83-84.
[127] Vgl. *Bitcoin.com (Hrsg.)* (2017), What is Bitcoin Cash?.
[128] Dazu *BitcoinCash.org (Hrsg.)* (2017), Frequently Asked Questions.
[129] Dazu mehr in Abschnitt D. I. „Zahlungsmittelfunktion".
[130] Siehe *BitcoinCash.org (Hrsg.)* (2017), New Features.
[131] Id.

Schlüssel verwenden, wäre es grundsätzlich möglich, dass ein Angreifer eine fremde Transaktion repliziert.[132] Will beispielsweise Alice Bitcoins an Bob transferieren, könnte ein Angreifer die Transaktionsdetails wiederverwenden, um die Transaktion auch im Bitcoin Cash Netzwerk durchzuführen. Durch getroffene Schutzmaßnahmen ist dies zwischen Bitcoin und Bitcoin Cash jedoch nicht möglich.[133]

2. Ethereum

Ethereum ist eine öffentlich, frei zugängliche Plattform, die es jedem ermöglicht, dezentralisierte Applikationen und Smart Contracts zu entwerfen und zu verwenden.[134] Smart Contracts sind automatisierte Programme, die bei der Erfüllung spezifischer Bedingungen, digitale Werte transferieren.[135] Anders ausgedrückt sind Smart Contracts Verträge, bei denen Rechte und Pflichten, aber auch Bedingungen und Folgen so strukturiert in Algorithmen abgebildet werden, dass diese als Anwendungen auf der Blockchain implementiert werden können.[136] Dies ist im Ethereum-Netzwerk möglich, da die Blockchain eine Turing-vollständige Programmiersprache beinhaltet.[137] Smart Contracts können praktisch für alles genutzt werden, was man persönlich besitzen kann. Dazu zählen materielle Güter wie Autos, Häuser oder Computer, aber auch immaterielle Güter wie Rechte des geistigen Eigentums.[138]

Ethereums Währungseinheit wird Ether genannt und ist ein notwendiges Element der Ethereum Plattform, da es als Treibstoff funktioniert.[139] Die Nutzung von Smart Contracts kostet nämlich Ether als Gebühr.[140] 60 Millionen Ether wurden

---

[132] Dazu *Khatwani, S.* (2017), What is a Bitcoin Replay Attack?.
[133] Vgl. *BitcoinCash.org (Hrsg.)* (2017), New Features.
[134] Siehe *Ethereum Homestead (Hrsg.)* (2017b), What is Ethereum?; *GitHub Inc. (Hrsg.)* (2017a), Ethereum.
[135] Vgl. *Fairfield, J. A. T.* (2014), S. 38.
[136] Siehe *Brühl, V.* (2017), S. 138.
[137] Hierzu *GitHub Inc. (Hrsg.)* (2017a), Ethereum.
[138] Ähnlich *Lee, L.* (2015), S. 114.
[139] Vgl. *Ethereum Foundation (Hrsg.)* (2017),What is Ether?.
[140] Dazu *Ethereum Foundation (Hrsg.)* (2017), Who needs ether?.

2014 an die Investoren, die am Vorverkauf teilgenommen haben, ausgeschüttet. Weitere 12 Millionen gingen an die Entwickler und ein Teil an die Ethereum Foundation. Aktuell werden alle 15-17 Sekunden fünf Ether für die Generierung eines neuen Blocks erzeugt.[141] Ethereums Validierungsmechanismus ist, genau wie bei Bitcoin, Proof-of-Work. Allerdings ist eine Änderung des Validierungsmechanismus geplant. Anstelle von PoW soll in der Zukunft eine Art des PoS-Mechanismus treten. Dieser wird von der Ethereum Foundation Casper genannt und befindet sich derzeit noch in der Entwicklung.[142]

3. Ripple

Gemessen an ihrer Marktkapitalisierung ist Ripple die viertgrößte Kryptowährung. Sie wurde 2012 von dem US-Unternehmen Ripple Labs entwickelt.[143] Während es sich bei fast allen Kryptowährungen um dezentrale virtuelle Währungen handelt, wird Ripple oft als zentrale virtuelle Währung betrachtet.[144] Dies liegt jedoch nicht daran, dass eine zentrale Institution alle Transaktionen speichert und bestätigt, sondern an der Art, wie neue Coins herausgegeben werden. Ripple basiert auf den Prinzipien der Blockchain.[145] Ein aus Computern bestehendes Netzwerk erfasst und speichert automatisch alle Transaktionen in einer verteilten Datenbank, genannt „Ripple Consensus Ledger".[146]

Im Gegensatz zu Bitcoin oder Ethereum werden allerdings keine neuen Coins durch das Mining erschaffen. Stattdessen wurden 100 Milliarden XRP (Name der Währungseinheit) bei der Gründung produziert.[147] Davon wurden 20 Milliarden von

---

[141] Siehe *Ethereum Foundation (Hrsg.)* (2017), How are ethers created?.
[142] Vgl. *Ethereum Foundation (Hrsg.)* (2017): Ether, Is the ether supply infinite?.
[143] Vgl. *Ripple Labs (Hrsg.)* (2014), S. 4.
[144] Dazu *Europäische Zentralbank (Hrsg.)* (2015), S. 11.
[145] Vgl. *Ripple (Hrsg.)* (2017), Distributed.
[146] Siehe *GitHub Inc. (Hrsg.)* (2017b), What is Ripple.
[147] Vgl. *Ammous, S.* (2016), S. 16.

den Gründern, Entwicklern und Investoren aus Risikokapitalgesellschaften einbehalten und 80 Milliarden XRP gingen an Ripple Labs, der somit zentraler Emittent der Währung ist.[148]

Ripple hat auch nicht wie Bitcoin das Ziel, eine eigene richtige virtuelle Währung zu sein, sondern dient viel mehr als Brückenwährung für illiquide Währungspaare.[149] Im Ripple-Netzwerk kann jede Fiat-Währung oder virtuelle Währung mittels eines IOU-Systems[150] übertragen werden.[151] Um eine Währung in eine andere zu transferieren, werden sogenannte „gateways“ eingesetzt. Ripple benötigt finanzielle Institutionen, um als „gateway“ in und aus dem Ripple-Netzwerk zu fungieren.[152] Bei einer Transaktion im Ripple-Netzwerk tauscht ein „gateway“ beispielsweise USD in XRP. XRP dient als Brückenwährung und ermöglicht es einem anderen „gateway“ XRP in beispielsweise Euro zurückzutauschen.[153]

Damit werden Transaktionsgebühren vermieden, da man Währungen nicht mehr paarweise tauschen muss. Ein weiterer Vorteil der Brückenwährung ist, dass Zahlungsvorgänge innerhalb von wenigen Sekunden abgeschlossen werden können. Dies macht Ripple-Transaktionen um einiges schneller als herkömmliche Transaktionen durch Banken und auch Bitcoin und Ethereum benötigen dafür mehr Zeit.[154]

D. Virtuelle Währungen und die Geldfunktionen

Damit ein Medium als Geld bzw. Währung bezeichnet werden kann, muss es die drei Geldfunktionen erfüllen. Ökonomen definieren diese als Zahlungsmittelfunktion, Wertaufbewahrungsfunktion und Recheneinheitsfunktion.[155] In der Literatur

---

[148] Hierzu *Europäische Zentralbank (Hrsg.)* (2015), S. 11.
[149] Siehe *Ripple Labs (Hrsg.)* (2014), S. 15.
[150] „IOU“ steht für informal certificate of debt“, d. h. eine Person erklärt gegenüber einer anderen Person, dass sie ihr einen bestimmten Betrag schuldet.
[151] Vgl. *Hildner, A.* (2016), S. 491.
[152] Ähnlich *Ripple Labs (Hrsg.)* (2014), S. 9.
[153] Vgl. *Lee, L.* (2015), S. 111-112.
[154] Siehe *Ripple (Hrsg.)* (2017), Benefits.
[155] Vgl. *Mankiw, N. G.* (2012), S. 80.

gibt es zwei konkurrierende Ansichten, ob virtuelle Währungen - insbesondere Bitcoin – die drei Geldfunktionen erfüllen.[156] Ein Teil der Literatur argumentiert, dass Bitcoin die Eigenschaften einer realen Währung nicht aufweist, sondern eher als ein spekulatives Investment zu betrachten ist.[157] Andere Forschungslinien stellen Bitcoins Potenzial in den Vordergrund und behandeln Bitcoin als globale Währung mit hohem zukünftigen Potenzial.[158] Inwiefern Bitcoin die verschiedenen Geldfunktionen erfüllt und welche Vor- und Nachteile die virtuelle Währung im Zusammenhang mit den verschiedenen Geldfunktionen aufweist, wird im Folgenden analysiert.

I. Zahlungsmittelfunktion

Um die Zahlungsmittelfunktion bzw. Tauschmittelfunktion zu erfüllen, müsste Bitcoin von einer hinreichenden Anzahl an Nutzern akzeptiert werden.[159] Wie schon in Abschnitt C. I. 3. beschrieben, ist dies jedoch noch nicht der Fall.

Eine Hürde für die Akzeptanz des Bitcoins als Zahlungsmittel ist die Tatsache, dass Kryptowährungen ein Netzwerk-Gut sind.[160] Netzwerkeffekte treten auf, wenn der Wert eines Gutes oder einer Leistung von der gesamten Nutzeranzahl abhängig ist.[161] Zahlungsmittel sind gekennzeichnet durch Netzwerkeffekte, da sie nur in dem Ausmaß nützlich sind, in dem Tauschpartner bereit sind, diese zu akzeptieren.[162] Netzwerkeffekte und Wechselkosten stärken die Position der amtierenden Währungen. Damit Bitcoin überhaupt die Chance hat, eine amtierende Währung zu ersetzen, muss die Kryptowährung hinreichend besser sein als die amtierende Währung, um

---

[156] Vgl. *Kancs, d'Artis/Ciaian, P./Rajcaniova, M.* (2015), S. 7.
[157] Siehe beispielsweise *Velde, F. R.* (2013); *Hanley, B. P.* (2015); *Yermack, D.* (2015); *Lo, S./Wang, J. C.* (2014).
[158] Siehe beispielsweise *Plassaras, N. A.* (2013); *Luther, W. J./White, L. H.* (2014).
[159] In Anlehnung an *Lo, S./Wang, J. C.* (2014), S. 3.
[160] Dazu *Hanl, A./Michaelis, J.* (2017), S. 364.
[161] Ähnlich *Luther, W. J.* (2016c), S. 398.
[162] Id.

Netzwerkeffekte und Wechselkosten zu überwinden.[163] Nahezu alle derzeit amtierenden Währungen werden durch Regierungen unterstützt und sind ein gesetzliches Zahlungsmittel. Da dies bei Kryptowährungen nicht der Fall ist, werden die Netzwerkeffekte zusätzlich verstärkt.[164]

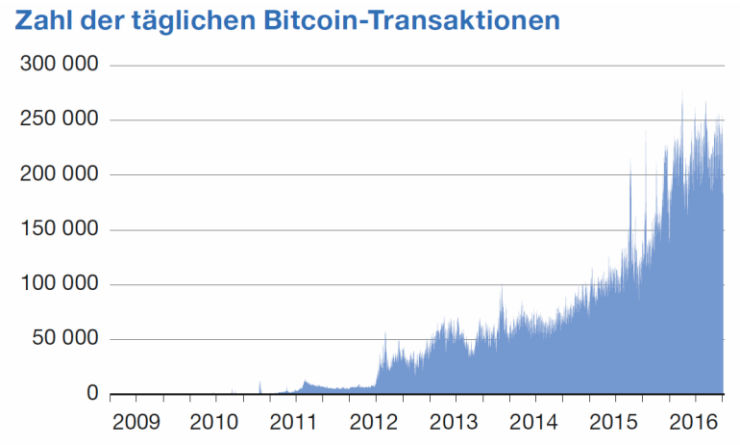

Abb. 10: Zahl der täglichen Bitcoin-Transaktionen
(Quelle: *Brühl, V.* (2017), S. 139)

Die Verwendung einer Zahlungstechnologie ist jedoch in den meisten Fällen keine 0-1-Entscheidung. Der typische Konsument nutzt zwei oder drei Methoden,m beispielsweise eine Kreditkarte für größere Transaktionen und Bargeld für kleinere Einkäufe im täglichen Leben. Daher muss eine neue Zahlungsmethode wie Bitcoin nicht für alle Transaktionen nach allen Kriterien wie Kosten, Geschwindigkeit oder Sicherheit überlegen sein. Die Überlegenheit in einem Teilbereich reicht aus, um substanzielle Verbreitung zu finden.[165] Wie empirische Studien zeigen, reagieren Konsumenten durchaus sensibel bei der Wahl der Zahlungsmethode, wenn die neue

---

[163] Id.
[164] *Europäische Bankenaufsichtsbehörde (Hrsg.)* (2014), S. 12-13 und *Luther, W. J.* (2016c), S. 398.
[165] Vgl. *Hanl, A./Michaelis, J.* (2017), S. 364.

Technologie besser zu ihren Bedürfnissen passt.[166] Wie in Abb. 9 zu sehen, hat in den letzten Jahren die Anzahl der täglichen Bitcoin-Transaktionen stark zugenommen. Derzeit (Stand September 2017) werden weltweit knapp 300.000 Transaktionen pro Tag mithilfe des Bitcoin-Netzwerks getätigt und damit ist die technische Kapazität schon nahezu ausgeschöpft.[167] Obwohl in der Literatur oft die Annahme getroffen wird, dass das Bitcoin-Netzwerk ungefähr sieben Transaktionen pro Sekunde bewältigen kann, ist dies in der Praxis nicht immer der Fall.[168] Vergleicht man Theorie und Praxis und schaut sich die Daten der Bitcoin Blockchain genauer an, sieht man, dass die Kapazität in der Praxis teilweise deutlich geringer ist. Laut der Seite Blockchain.info wurden in den 24 Stunden zwischen dem 18.09.2017 um 15:05 Uhr und dem 19.09.2017 um 15:05 Uhr 258.796 Transaktionen bestätigt.[169] In den gesamten 24 Stunden betrug die Größe des Mempools mehrere Megabyte bzw. warteten mehrere Tausend Transaktionen im Mempool auf ihre Bestätigung. Das heißt, es wären eigentlich genügend Transaktionen zur Bestätigung bereit gestanden, um die in der Literatur genannte Kapazität von sieben Transaktionen pro Sekunde (entspricht 604.800 Transaktionen / 24 Std.) auszuschöpfen. In dem von mir betrachteten 24 Stunden Intervall wurden 128 neue Blöcke gefunden, wodurch die Zeit zwischen den Blöcken etwas mehr als zehn Minuten betrug.[170] Die generierten Blöcke hatten eine durchschnittliche Größe von 1 MB und somit das Maximum. Mit diesen Daten lässt sich nun leicht berechnen, dass in dem gewählten Zeitintervall ziemlich exakt nur drei Transaktionen pro Sekunde[171] bestätigt wurden, obwohl eigentlich genügend zu bestätigende Transaktionen zur Verfügung standen.

---

[166] Siehe *Koulayev, S. et al.* (2016).
[167] Vgl. *Blockchain.info (Hrsg.)* (2017b), TRANSACTION SUMMARY.
[168] Dazu *Bonneau, J. et al.* (2015), S. 114; *Hanl, A./Michaelis, J.* (2017), S. 364.
[169] *Blockchain.info (Hrsg.)* (2017b), TRANSACTION SUMMARY.
[170] Wird wie vorgesehen ein Block alle zehn Minuten generiert, werden in 24 Stunden 144 (statt 128) neue Blöcke generiert.
[171] 258.796/(24*60*60) ≈ 2,9953.

Doch auch im Falle, dass tatsächlich sieben Transaktionen pro Sekunde realisierbar sind, bleibt das Skalierungsproblem bestehen. Allein in Deutschland werden werktäglich ca. 25 Millionen Überweisungen durchgeführt.[172] Visa bewältigt im Durchschnitt ungefähr 2000 Transaktionen pro Sekunde und ist in der Lage, bis zu 65000 Transaktionen pro Sekunde zu bearbeiten. [173] Um als weltweites Zahlungsmittel zu agieren, sind sieben Transaktionen pro Sekunde viel zu wenig.

Eine Lösung wäre die Erhöhung der Blockgröße, sodass mehr Transaktionen in einem Block bestätigt werden können. Allerdings würde dies die Dezentralität des Netzwerks gefährden, da die operativen Kosten der Miner steigen würden und sich das Mining somit nicht mehr für alle bisherigen Miner rentieren würde.[174] Außerdem kann eine Erhöhung der Blockgröße zu einem „hard fork" führen. Hierbei gabelt sich die Blockchain in zwei unterschiedliche Ketten, falls eine signifikante Anzahl an Nodes ihren Client nicht aktualisieren und es würde dadurch zwei Versionen von Bitcoin[175] geben.[176]

Eine andere Lösung für das Skalierungsproblem soll Segregated Witness liefern. Segregated Witness, abgekürzt SegWit, ist ein Update für den Quellcode von Bitcoin, wodurch die Blockgröße erhöht wird und die Implementierung einer Second-Layer-Lösung ermöglicht wird.[177] Vereinfacht ausgedrückt, wird durch SegWit jedem Block, neben dem durch die Transaktionen gebildeten Merkle Tree, ein „Witness" (Zeuge) zur Seite gestellt. Dieser enthält alle Daten um die Validität einer Transaktion überprüfen zu können.[178] Im Endeffekt er-

---

[172] Hierzu *Hanl, A./Michaelis, J.* (2017), S. 364.
[173] Vgl. *Bitcoin Wiki (Hrsg.)* (2017a), Scalability targets und *Visa Inc. (Hrsg.)* (2017), S.2.
[174] Vgl. *Giese, P.* (2017), Der Anfang aller Überlegungen – die Skalierungsdebatte.
[175] So entstand beispielsweise Bitcoin Cash.
[176] Hierzu *Giese, P.* (2017), Der Anfang aller Überlegungen – die Skalierungsdebatte.
[177] Dazu *Preuss, M.* (2017), Welchen Lösungsansatz bietet SegWit für das Skalierungsproblem?
[178] Siehe *Giese, P.* (2017), Segregated Witness – mehr als eine Lösung des Skalierungsproblems.

höht sich durch den „Witness“ die effektive Anzahl an Transaktionen, die in einem Block gespeichert werden können. Es wird also die Anzahl der Transaktionen pro Block erhöht, ohne eine tatsächliche Erhöhung der Blockgröße.[179] Ein weiterer wichtiger Vorteil ist, dass durch SegWit bedenkenlos mit unbestätigten Transaktionen gearbeitet werden kann. Dies hilft nicht nur der Sicherheit des Netzes, sondern ebnet auch den Weg für das Lightning Network.[180] Das Lightning Network wird oftmals als die ultimative Lösung des Skalierungsproblems gesehen, da man mit dessen Hilfe einen Großteil der Transaktionen „offchain“, also abseits der Blockchain abwickeln könnte und somit das Netzwerk entlastet.[181] SegWit wurde mit dem Block 481.823 im August 2017 offiziell aktiviert.[182] Da die Nutzung von SegWit bei einer Transaktion freiwillig ist, wird es jedoch noch selten verwendet. Derzeit (Stand 21.09.2017) unterstützen nur knapp 4% aller Bitcoin Transaktionen SegWit.[183]

Neben den bereits genannten Nachteilen von Kryptowährungen im Hinblick auf deren Zahlungsmittelfunktion gibt es aber auch Vorteile gegenüber den herkömmlichen Zahlungsmitteln.

Ein großer Vorteil von Bitcoin ist die vergleichsweise schnelle Transaktionsgeschwindigkeit. Auf traditionellem Weg vorgenommene Überweisungen dauern innerhalb der EU einen Werktag, bei Überweisungen in die USA rund fünf Werktage und bei Überweisungen in Entwicklungsländer teilweise bis zu 20 Werktage.[184] Im Bitcoin-Netzwerk gilt eine Transaktion üblicherweise nach sechs Blöcken als bestätigt. Unter der Voraussetzung, dass eine aufgegebene Transaktion direkt in den folgenden Block integriert wird, ist also eine Transaktion innerhalb von einer Stunde als sicher und unumkehrbar anzusehen.[185] Da jedoch Bitcoin mittlerweile an seine Belastungs-

---

[179] Id.
[180] Id.
[181] Vgl. *Preuss, M.* (2017), Welchen Lösungsansatz bietet SegWit für das Skalierungsproblem?
[182] Hierzu *Bergmann, C.* (2017b).
[183] Vgl. *CountSegwit (Hrsg.)* (2017).
[184] Siehe *Hanl, A./Michaelis, J.* (2017), S. 366.
[185] Id.

grenze stößt (Skalierungsproblem), kam es in der Vergangenheit auch schon zu Staus auf der Blockchain, sodass Transaktionen teilweise mehrere Tage im Mempool auf ihre Bestätigung warteten.[186]

Ein weiterer Vorteil von Bitcoin als Zahlungsmittel sind die niedrigen Transaktionskosten. Da virtuelle Währungen unabhängig von dritten Parteien sind, entfallen auch sämtliche Kosten, die im Zusammenhang mit Intermediären anfallen.[187]

Bei einer Bitcoin-Transaktion hat jeder Nutzer die Möglichkeit, eine freiwillige Transaktionsgebühr zu hinterlegen, welche an den Miner geht, der die Transaktion erfolgreich in einen neuen Block integriert. Dementsprechend bevorzugen Miner Transaktionen mit hohen Transaktionsgebühren gegenüber Transaktionen mit keinen bzw. niedrigen Transaktionsgebühren. Zusätzlich zu den Transaktionsgebühren bekommen die Miner aktuell 12,5 neu generierte Bitcoins pro Block. Da die Zahl der neu generierten Bitcoins mit der Zeit abnehmen wird, ist davon auszugehen, dass die Miner in der Zukunft stärker von den Transaktionsgebühren abhängig sein werden.[188] Deshalb ist es angemessen, von steigenden Transaktionskosten in der Zukunft auszugehen.[189] Zum Zeitpunkt des Schreibens (Stand: 22.09.2017) beziehen Miner knapp 95% ihrer Einnahmen aus der Generierung neuer Bitcoins und ca. fünf Prozent durch die Transaktionsgebühren.[190] Die Höhe der Transaktionskosten[191] in Abhängigkeit vom Transaktionsvolumen schwankte im Jahr 2017 zwischen 0,32% und 1,67%.[192] Im Vergleich dazu betrugen die globalen durchschnittlichen Transaktionskosten bei herkömmlichen Überweisungen 7,45% des Transaktionsvolumens im ersten Quartal 2017.[193] Die meisten Händler, die

---

[186] *Bergmann, C.* (2017a).
[187] Dazu *Kancs, d'Artis/Ciaian, P./Rajcaniova, M.* (2015), S. 7.
[188] Dazu *Europäische Bankenaufsichtsbehörde (Hrsg.)* (2014), S. 17.
[189] Id.
[190] Vgl. *Blockchain.info (Hrsg.)* (2017b), MINING-KOSTEN.
[191] Dabei setzen sich die Transaktionskosten aus den freiwilligen Gebühren der Nutzer und den Kosten durch die Generierung neuer bitcoins zusammen.
[192] Siehe *Blockchain.info (Hrsg.)* (2017c).
[193] Vgl. *The World Bank Group (Hrsg.)* (2017), S. 2.

Bitcoin als Zahlungsmittel akzeptieren, tendieren dazu, erhaltene Bitcoins direkt in ihre lokale Fiat-Währung umzutauschen. Dadurch entstehen weitere Kosten in Höhe von ungefähr einem Prozent.[194] Wichtig zu beachten ist jedoch, dass der Transaktionskostenvorteil von Bitcoin innerhalb des einheitlichen Euro-Zahlungsverkehrsraumes (SEPA[195]) eine weitaus geringere Rolle spielt.[196]

Um Bitcoin zu verstehen und nutzen zu können, werden relativ hohe Computerkenntnisse vorausgesetzt.[197] Bitcoin basiert auf einem sehr komplexen Code, der nur von ein paar Personen verstanden und von noch weniger Personen (Programmierer), die das gesamte System überblicken, kontrolliert wird.[198] Dies könnte eine Barriere für viele potenzielle Nutzer darstellen und damit die Verbreitung des Bitcoins als Zahlungsmittel erschweren.

II. Wertaufbewahrungsfunktion

Wenn eine Währung die Funktion als Wertaufbewahrungsmittel erfüllt, kann sie zu einem beliebigen Zeitpunkt in der Zukunft gegen Güter und Dienstleistungen eingetauscht werden. Dabei darf der ökonomische Wert in der Zukunft nicht stark von dem in der Gegenwart abweichen.[199]

Bitcoin hat gegenüber Fiat-Währungen einen klaren Vorteil, um als Wertaufbewahrungsmittel zu agieren. Während die meisten Fiat-Währungen inflationär sind, ihr Wert sich also mit der Zeit reduziert und somit die Erfüllung der Funktion als Wertaufbewahrungsmittel erschwert wird, ist Bitcoin deflationären Spannungen ausgesetzt.[200] Die maximale Anzahl an existierenden Bitcoins ist auf 21 Millionen beschränkt. Nutzen

---

[194] Hierzu *Europäische Bankenaufsichtsbehörde (Hrsg.)* (2014), S. 17.
[195] SEPA steht für Single Euro Payments Area und besteht aus 34 Ländern, wozu unter anderem die 28 Mitgliedsstaaten der EU zählen.
[196] Dazu *Europäische Bankenaufsichtsbehörde (Hrsg.)* (2014), S. 17.
[197] Vgl. *Kancs, d'Artis/Ciaian, P./Rajcaniova, M.* (2015), S. 10.
[198] Siehe *Velde, F. R.* (2013), S. 3.
[199] Dazu *Mankiw, N. G.* (2012), S. 80, *Yermack, D.* (2015), S. 39.
[200] Dazu *Kancs, d'Artis/Ciaian, P./Rajcaniova, M.* (2015), S. 13-14.

immer mehr Teilnehmer das Bitcoin-System, während die Menge an Bitcoins jedoch gleich bleibt, wird deren Wert steigen und es kommt zu einer Deflation, falls die Bitcoin Besitzer nicht mehr bereit sind, ihre Bitcoins gegen andere Währungen oder Waren einzutauschen.[201] Zusätzlich können Bitcoins, die versehentlich verloren oder zerstört wurden, nicht mehr ersetzt werden, sodass die Anzahl an verfügbaren Bitcoins schrumpfen wird.[202]

Auf der einen Seite ist Deflation vorteilhaft für die Bitcoin-Besitzer, da sie durch die Wertsteigerung reicher werden. Auf der anderen Seite könnte die Erwartung eines höheren zukünftigen Wertes dazu führen, dass Bitcoins gehortet werden.[203] Dies führt dazu, dass die Verwendung von Bitcoin als Zahlungsmittel stark beschränkt wird. Außerdem birgt eine Deflation das Risiko einer wirtschaftlichen Depression, falls die Wirtschaft in eine Deflationsspirale gerät.[204] Tatsächlich ist die Funktion als Wertanlage neben dem Interesse an einer neuen Technologie das bedeutsamste Motiv für das Halten von Bitcoins. Zumindest für US-Konsumenten ist die Funktion als Wertanlage wichtiger als die Nachfrage nach Bitcoins, um Käufe von Gütern und Dienstleistungen abzuwickeln.[205]

Ein großes Problem für die Wertaufbewahrungsfunktion ist die hohe Volatilität des Bitcoin Preises. Da sich der Wert von Kryptowährungen ausschließlich durch Angebot und Nachfrage ergibt, schwankt der Bitcoin Preis sehr stark.[206] Abb. 10 zeigt die Kursentwicklung des Bitcoins gegen den USD von August 2011 bis September 2017. Die Daten stammen von der Kryptowährungsbörse BitStamp, welche derzeit eine der größten Handelsplattformen für Bitcoin ist. Man sieht auf einen Blick, dass der Wert von Bitcoin alles andere als stabil ist. Allein im Jahr 2017 hat sich der Wert bis September mehr als

---

[201] Hierzu *Kerscher, D.* (2014), S. 125.
[202] Vgl. *Kancs, d'Artis/Ciaian, P./Rajcaniova, M.* (2015), S. 14.
[203] Id.
[204] Dazu *Kerscher, D.* (2015), S. 125; *Vandezande, N.* (2017), S. 343.
[205] Ähnlich *Hanl, A./Michaelis, J.* (2017), S. 364; *Schuh, S./Shy, O.* (2016), S. 27.
[206] Siehe *Plassaras, N. A.* (2013), S. 383.

vervierfacht, wobei sich der Preis mehrere Male innerhalb weniger Tage drastisch verändert hat.

Abb. 11: Kursentwicklung Bitcoin
(Quelle: *ARIVA.DE (Hrsg.)* (2017))

Eine weitere Untersuchung zur Wertstabilität führte Yermack zwischen dem 01.01.2013 und 29.11.2013 durch. Wie in Abbildung 11 zu sehen, untersuchte er die Volatilität der Wechselkurse von vier verschiedenen Fiat-Währungen, Gold und Bitcoin gegen den US Dollar. Die Ordinate zeigt die annualisierte Volatilität in Prozent. Neben Bitcoin und Gold wurden außerdem die Währungen Euro, Yen, Schweizer Franken und Britische Pfund betrachtet. Es zeigt sich, dass die Volatilität von Bitcoin um ein Vielfaches höher ist als die der anderen Währungen. Im Jahr 2013 wiesen die realen Währungen eine Volatilität zwischen 7% und 12% auf.[207] Gold stellt eine plausible Alternative zu den realen Währungen als Wertaufbewahrungsmittel dar und hatte 2013 basierend auf dem Dollarwechselkurs eine Volatilität von 22%.[208] Dahingegen schwankte der Bitcoin Preis mit einer Volatilität von 142% sehr viel stärker.[209] Für risikoaverse Konsumenten könnte die hohe Kursvolatilität ein hinreichender Grund sein, Kryptowährungen wie Bitcoin komplett zu vermeiden. Um als ein Wertaufbewahrungsmittel zu dienen, müssen Kryptowährungen sicher aufbewahrt werden können. Allerdings stellt die Sicher-

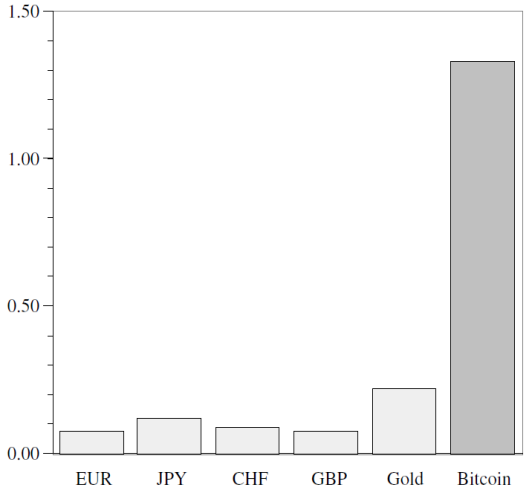

Abb. 12: Volatilität von diversen Währungen (Quelle: *Yermack D.* (2015), S. 40)

[207] Vgl. *Yermack, D.* (2015), S. 40.
[208] Id.
[209] Vgl. *Yermack, D.* (2015), S. 40.

heit ein reales Problem dar. Die Risiken, die die Sicherheit betreffen, lassen sich in zwei Gruppen einteilen. Zum einen in Risiken, die innerhalb des Netzwerks entstehen und zum anderen in Risiken, die an der Schnittstelle, also an der Verwendung des Netzwerks entstehen.[210] Zu den inneren Risiken gehören zum Beispiel die Sicherheit der Kryptografie und das Risiko einer sogenannten 51%-Attacke, die ein „double spending" ermöglichen würde.[211] Gelingt es einem Miner oder einem Mining Pool[212] mehr als 50 Prozent der gesamten Rechenleistung zu kontrollieren, kann dieser die anderen Miner auskonkurrieren und dadurch eigenständig Transaktionen rückgängig machen oder neue Transaktionen nicht mehr zulassen.[213] Die Bitcoin Blockchain wird mittlerweile seit knapp neun Jahren genutzt und bisher sind keine substanziellen technischen Fehlfunktionen bekannt geworden. Obwohl die Sicherheit der Kryptografie ein grundsätzliches Problem ist, wird die von Nakomoto gewählte Verschlüsselungstechnik (bisher) als sicher eingestuft.[214] Deutlich kritischer für die Sicherheit sind die Schnittstellen-Risiken. In der Vergangenheit wurde bereits das virtuelle Geld von einigen Bitcoin Besitzern gestohlen. Um das Bitcoin System nutzen zu können, wird ein Wallet benötigt und um Bitcoins zu erlangen, sind die meisten Nutzer auf Handelsplattformen angewiesen. Außerdem zeigt mittlerweile die Praxis, dass die meisten Transaktionen unter Zuhilfenahme von Zahlungsdienstleistern abgewickelt werden, sodass Nutzer von Kryptowährungen teilweise doch abhängig von Intermediären sind.[215] Diese bilden für Hacker ein potenzielles Angriffsziel, sodass in der Vergangenheit diverse Kryptowährungs-Börsen erfolgreich gehackt wurden.[216]

---

[210] Siehe *Hanl, A./Michaelis, J.* (2017), S. 366.
[211] Id.
[212] Einzelne Miner schließen sich oftmals zu Mining Pools zusammen um die Wahrscheinlichkeit einen neuen Block erfolgreich zu generieren zu erhöhen und dadurch die Varianz ihrer Einnahmen zu reduzieren.
[213] Hierzu *Bonneau, J. et al.* (2015), S. 108.
[214] Vgl. *Brito, J./Castillo, A.* (2016), S. 34; *Hanl, A./Michaelis, J.* (2017), S. 366-367.
[215] Siehe *Hanl, A./Michaelis, J.* (2017), S. 367.
[216] Dazu *Brito, J./Castillo, A.* (2016), S. 35.

III. Recheneinheitsfunktion

Damit eine Währung die Recheneinheitsfunktion erfüllt, muss der relative Wert von Gütern, Dienstleistungen und anderen Transaktionen bestimmbar sein. Außerdem ist die Teilbarkeit in hinreichend kleine Einheiten notwendig, damit Transaktionen in den verschiedensten Größen möglich sind.[217]

Ein Bitcoin lässt sich in acht Dezimalstellen unterteilen. Damit entspricht 0,00000001 BTC der kleinstmöglichen Einheit und zu Ehren des Erfinders Satoshi Nakomoto wird diese kleinste Einheit als ein „satoshi" bezeichnet.[218] Da 21 Millionen bitcoins (maximale Anzahl) multipliziert mit 100.000.000 satoshis pro bitcoin 2.100.000.000.000.000 (2,1 Billiarden) ergibt, ist die Funktion der Teilbarkeit in hinreichend kleine Einheiten erfüllt.[219] Falls diese Menge nicht mehr ausreichen sollte, kann die Kommastelle im System von den Entwicklern weiter versetzt werden, um eine noch kleinere Stückelung zu ermöglichen.[220]Ist beispielsweise ein Bitcoin 4000 USD Wert, so würde ein Brötchen im Wert von 50 US cents 0,000125 BTC bzw. 12500 satoshis entsprechen. Preisangaben mit mehreren Dezimalstellen sind jedoch sehr gewöhnungsbedürftig und könnten Konsumenten verwirren, sodass Probleme bei der Bestimmung des relativen Wertes von Gütern auftreten.[221]

Doch aufgrund der bereits erwähnten hohen Volatilität eignet sich Bitcoin nicht bzw. nur bedingt als Recheneinheit.[222] Die meisten Händler, die Bitcoin als Zahlungsmittel akzeptieren, nehmen aufgrund der hohen Volatilität die Dienstleistung eines Zahlungsdienstleisters in Anspruch. Bei einer Transaktion erhalten Zahlungsdienstleister wie Coinbase oder BitPay im Auftrag des Verkäufers Bitcoins und transferieren denselben Betrag in der lokalen Währung zum aktuellen Wechselkurs an den Verkäufer.[223] Anstelle der Verkäufer tragen die Zahlungs-

---

[217] Ähnlich *Kancs, d'Artis/Ciaian, P./Rajcaniova, M.* (2015), S. 12.
[218] Dazu *Hanley, B. P.* (2015), S. 6.
[219] Id.
[220] Vgl. *Kerscher, D.* (2014), S. 125.
[221] Dazu *Yermack, D.* (2015); S. 38-39.
[222] Hierzu *Hanl, A./Michaelis, J.* (2017), S. 365.
[223] Siehe *Luther, W. J./White, L. H.* (2014), S. 5.

dienstleister das Wechselkursrisiko und im Ausgleich dafür wird eine Gebühr in Höhe von ungefähr einem Prozent erhoben.[224] Wegen der hohen Kursschwankungen formulieren Unternehmen, die Bitcoin akzeptieren, ihre Preise in der lokalen Fiat-Währung. Der Bitcoin Preis ergibt sich erst nach der Umrechnung mit dem aktuellen Wechselkurs.[225]

E. Rechtliche Regulierung virtueller Währungen

I. Risiken

Das Hauptziel finanzieller Regulierungsbehörden ist es, Risiken, die durch finanzielle Aktivitäten auftreten, zu identifizieren und, falls nötig, angemessene Maßnahmen zu ergreifen.[226] So haben eine Reihe internationaler Behörden die Risiken, die im Zusammenhang mit virtuellen Währungen auftreten, analysiert und vor den Risiken gewarnt. Beispielsweise hat die Europäische Bankenaufsichtsbehörde 2014 eine Risikoanalyse durchgeführt und dabei 70 verschiedene von Kryptowährungen ausgehende Risiken entdeckt.[227]

Eine weitere Risikoanalyse wurde von der Bitcoin Foundation veröffentlicht.[228] Auch die Financial Action Task Force[229] und der Internationale Währungsfonds[230] äußerten sich in Berichten zu den Risiken von Kryptowährungen. Ebenso warnten einige Zentralbanken vor den Gefahren.[231] Einige der Risiken könnten durch eine angemessene Regulierung minimiert werden. Bei der Regulierungsdebatte sind die Risiken für die Nut-

---

[224] Id.
[225] Hierzu *Hanl, A./Michaelis, J.* (2017), S. 365.
[226] Siehe *Europäische Bankenaufsichtsbehörde (Hrsg.)* (2014), S. 21.
[227] Vgl. *Europäische Bankenaufsichtsbehörde (Hrsg.)* (2014).
[228] Vgl. *The Bitcoin Foundation (Hrsg.)* (2014).
[229] Vgl. *Financial Action Task Force (Hrsg.)* (2014).
[230] Vgl. *Internationaler Währungsfonds (Hrsg.)* (2016).
[231] Siehe *Europäische Zentralbank (Hrsg.)* (2015), S. 30.

zer und die außerhalb des Bitcoin-Netzwerks liegenden Risiken entscheidend.[232]

Ein Hauptrisiko für die Nutzer ist das Verlustrisiko.[233] Dabei kann der Verlust auf zwei verschiedene Arten auftreten. Erstens durch das Verlieren des privaten Schlüssels, wodurch der Zugang zu den Bitcoins für immer unmöglich wird und zweitens durch Hackerangriffe.[234] Virtuelle Währungen - besonders die Serviceanbieter - sind durch Hackerangriffe gefährdet. Zusätzlich riskieren Nutzer, die ihre Computer und Wallets nicht ausreichend sichern, dass ihre privaten Schlüssel und Bitcoins gestohlen werden.[235]

Das Fehlen eines Intermediärs führt dazu, dass durchgeführte Transaktionen endgültig sind, d. h. sie können nicht, wie es z. B. bei Lastschriftrückgaben möglich ist, rückgängig gemacht werden.[236] Auch dann nicht, wenn eine Transaktion fehlerhaft erfolgte. Außerdem können Bitcoin-Nutzer sich nicht darauf verlassen, dass Bitcoins als Zahlungsmittel akzeptiert werden, da sie kein gesetzliches Zahlungsmittel sind.[237] Ebenso wenig ist die Konvertierbarkeit in eine Fiat-Währung garantiert.[238]

Wie bereits beschrieben, sind Kryptowährungen extrem volatil. Die hohe Volatilität ist ein weiteres Risiko, dem die Nutzer, speziell die Investoren, ausgesetzt sind.[239] Bei Bitcoin könnte es sich um ein Schneeballsystem („Ponzi scheme“) bzw. eine

---

[232] Die *Europäische Bankenaufsichtsbehörde (Hrsg.)* (2014), S. 22 differenziert die Risiken kleinteiliger nach (A) „Risks to users“, (B) „Risks to non-user-market-participants“ („exchanges“, „merchants“ und „others“), (C) „Risks to financial integrity“, (D) „Risks to payment systems in FCs“ und (E) „Risks to regulatoy authorities“. Das hier zugrunde gelegte Verständnis fasst den “Nutzerbegriff” weiter, so dass darunter die Gruppen A, B und D fallen. Die außerhalb des Netzwerks liegenden Risiken umfassen dann die Gruppen C und E.
[233] Siehe *Lam, P. N./Lee, D. K. C.* (2015b), S. 313.
[234] Dazu *Lam, P. N./Lee, D. K. C.* (2015b), S. 313; *Luther, W. J.* (2016a), S. 8-9.
[235] Vgl. *Lam, P. N./Lee, D. K. C.* (2015b), S. 313.
[236] Hierzu *Luther, W. J.* (2016a), S. 11; *Lerch, M. P.* (2015), S. 197.
[237] Siehe *Europäische Bankenaufsichtsbehörde (Hrsg.)* (2014), S. 27.
[238] Id.
[239] Dazu *Luther, W. J.* (2016a), S. 4.

„Blase“ handeln und es besteht das Risiko, dass der Kurs einbricht und die Währung somit wertlos wird.[240]

Risiken im Zusammenhang mit Bitcoin treten auch außerhalb des Systems auf, wobei sie selbstverständlich mit den Risiken des Bitcoin-Netzwerks zusammenhängen.[241] Dabei hängen die größten Risiken – Geldwäsche, Terrorismusfinanzierung und Kriminalität – mit der Anonymität bzw. Pseudoanonymität von virtuellen Währungen zusammen.[242] Bargeld bietet die „perfekte“ Anonymität gegenüber Außenstehenden, da nur die am Tausch Beteiligten involviert sind.[243] Den Gegensatz dazu bilden herkömmliche Banküberweisungen, bei denen die Einsichtnahme und das Zurückverfolgen von Transaktionen zumindest für die jeweilige Bank unproblematisch sind, sodass die Weitergabe beispielsweise an staatliche Behörden wie das Finanzamt kaum zu unterbinden ist.[244] Virtuelle Währungen beschreiten hier einen Mittelweg. Alle Transaktionen werden auf der Blockchain gespeichert und sind für jeden Transaktionsteilnehmer öffentlich einsehbar.[245] Allerdings liegen die Transaktionen nur unter Pseudonymen vor. Schließlich sind lediglich Bitcoin-Adressen bekannt, für deren Erstellung die Nutzer keine persönlichen Daten von sich angeben müssen.[246] Begünstigt wird die kriminelle Verwendung von Bitcoins durch die Internationalität des Netzwerks und der Unumkehrbarkeit von Transaktionen.[247]

So können virtuelle Währungen für rechtmäßige und rechtswidrige Aktivitäten genutzt werden.[248] Beispielsweise konnten im Zeitraum zwischen Februar 2011 und Oktober 2013 im Dark Web auf dem Online-Marktplatz „Silk Road“ illegale Gü-

---

[240] Ähnlich *Lerch, M. P.* (2015), S. 198; *Europäische Zentralbank (Hrsg.)* (2015), S. 27.
[241] Hierzu *Lerch, M. P.* (2015), S. 198.
[242] *Europäische Zentralbank (Hrsg.)* (2015), S. 32.
[243] Vgl. *Hanl, A./Michaelis, J.* (2017), S. 367.
[244] Id.
[245] Dazu *Luther, W. J.* (2016a), S. 13.
[246] Siehe *Financial Action Task Force (Hrsg.)* (2014), S. 9.
[247] Vgl. *Lerch, M. P.* (2015), S. 198.
[248] Hierzu *Lam, P. N./Lee, D. K. C.* (2015b), S. 313.

ter gehandelt werden.[249] Die Website Silk Road akzeptierte ausschließlich Bitcoin als Zahlungsmittel und bot eine Vielzahl an Gütern an, wobei der Drogenhandel klar im Fokus der Seite stand.[250] Eine Studie ergab, dass über Silk Road monatlich Transaktionen in Höhe von ungefähr 1,2 Millionen USD abgewickelt wurden.[251] Neuere Schätzungen gehen von monatlich 4,7 Millionen USD aus.[252] Für einen globalen Marktplatz ergeben beide Schätzungen ein relativ geringes Transaktionsvolumen. Ferner betrug im gleichen Zeitraum das monatliche Transaktionsvolumen für das gesamte Bitcoin-System durchschnittlich ca. 206,33 Millionen USD, sodass Transaktionen auf Silk Road „nur" knapp 2,28 Prozent aller Bitcoin-Transaktionen ausmachten.[253] Ein weiteres ganz aktuelles Beispiel für die Verwendung von Bitcoin in einem kriminellen Zusammenhang war die Erpressung zahlreicher Betroffener im Mai 2017. Bei einer Cyberattacke mit Schadsoftware forderten die Erpresser die Zahlung des Lösegelds ausschließlich in Bitcoin.

Neben der Verwendung von Bitcoin für kriminelle Geschäfte, haben Politiker und Regulierungsbehörden Bedenken, dass Bitcoin zur Geldwäsche und Terrorismusfinanzierung verwendet werden kann.[254] Das Eintauschen von Fiat-Währung aus kriminellen Aktivitäten in Bitcoin ist der erste Schritt bei einer klassischen Geldwäsche. Anschließend werden einige Bitcoin-Transaktionen ausgeführt, um die Herkunft des Geldes zu verschleiern. Dabei wird für jede Transaktion eine neue Bitcoin-Adresse verwendet. Schließlich werden die „gewaschenen" Bitcoins wieder in eine Fiat-Währung zurückgetauscht und in das Wirtschaftssystem integriert.[255] Obwohl die Sorgen der Geldwäsche und Terrorfinanzierung durch virtuelle Wäh-

---

[249] Siehe *Brito, J./Castillo, A.* (2016), S. 37.
[250] Dazu *Christin, N.* (2012), S. 2.
[251] Vgl. *Christin, N.* (2012), S. 17.
[252] Hierzu *Luther, W. J.* (2016a), S. 13.
[253] Id.
[254] Siehe *Brito, J./Castillo, A.* (2016), S. 39; *Europäische Bankenaufsichtsbehörde (Hrsg.)* (2014), S. 32; *Financial Action Task Force (Hrsg.)* (2014), S. 9.
[255] Ähnlich *Lam, P. N./Lee, D. K. C.* (2015b), S. 313.

rungen derzeit eher theoretischer als praktischer Natur sind, ist die Möglichkeit durchaus gegeben und die Gefahr real.[256]

Es scheint zudem denkbar, dass virtuelle Währungen Auswirkungen auf die Geldpolitik und Preisstabilität haben könnten.[257] Allerdings ist dies aufgrund des vergleichsweise geringen Transaktionsvolumens virtueller Währungen noch nicht der Fall.[258]

II. Regulierungsmaßnahmen in der EU und den USA

Aufgrund der schnellen Entwicklung und Verbreitung virtueller Währungen haben inzwischen verschiedene Länder eine Regulierung von virtuellen Währungen in Betracht gezogen.[259] Da sich Technologien jedoch immer schneller entwickeln als die Gesetzgebung, existieren aktuell noch keine umfassenden oder einheitlichen Herangehensweisen für die Regulierung.[260] Behörden haben weltweit unterschiedliche Auffassungen darüber, wie virtuelle Währungen zu regulieren sind.[261]

In diesem Abschnitt werden die Vorgehensweisen und bisher getroffenen Maßnahmen in der EU bzw. in Deutschland und den USA aufgezeigt:

Für die Europäische Union existiert derzeit noch keine einheitliche Regulierung, was eine Herausforderung für die Mitgliedsstaaten bei der Bekämpfung illegaler Aktivitäten wie Geldwäsche darstellt.[262] Zudem wird die Einordnung virtueller Währungen in die bestehenden EU-Richtlinien der Electronic Money Directive (2009/110/EC) und der Payment Service Directive (2007/64/EC) verneint.[263] Des Weiteren sind virtuelle Währungen kein Bestandteil der vierten europäischen Geld-

---

[256] Vgl. *Brito, J./Castillo, A.* (2016), S. 39.
[257] Hierzu *Europäische Zentralbank (Hrsg.)* (2012), S. 26.
[258] Dazu *Europäische Zentralbank (Hrsg.)* (2015), S. 37.
[259] Siehe *Lam, P. N./Lee, D. K. C.* (2015b), S. 314.
[260] Dazu *Vandezande, N.* (2017), S. 343; *Lam, P. N./Lee, D. K. C.* (2015b), S. 314.
[261] Vgl. *Arnfield, R.* (2015), S. 3.
[262] Hierzu *Europäische Zentralbank (Hrsg.)* (2012), S. 45.
[263] Siehe *Europäische Zentralbank (Hrsg.)* (2012), S. 43.

wäscherichtlinie (2015/849), welche am 20. Mai 2015 von dem Europäischen Parlament und dem Rat der Europäischen Union verabschiedet wurde.[264]

Angesichts der bestehenden Rechtsunsicherheit und einer fehlenden Regulierung ist das Europäische Parlament der Auffassung, dass es einer Ausweitung der bestehenden Regelungen auf virtuelle Währungen oder einer zusätzlichen neuen Gesetzgebung innerhalb der EU bedarf.[265] Das Parlament verlangt die Einrichtung einer Task Force, die von der Kommission geleitet wird und Empfehlungen für eine Regulierung auf EU-Ebene erarbeiten soll, ohne dass neue Innovationen im Keim erstickt werden.[266] Ferner hat die Europäische Kommission im Juli 2016 einen Antrag zur Änderung der vierten europäischen Geldwäscherichtlinie (2015/849) gestellt. Der Antrag fordert, dass Handelsplattformen und Wallet-Anbieter von virtuellen Währungen ebenfalls als Instanzen angesehen werden, die den Bedingungen der vierten europäischen Geldwäscherichtlinie unterliegen.[267] Jüngst hat sich auch EZB-Präsident Mario Draghi in einem öffentlichen Brief an das Europäische Parlament zu dem Thema virtueller Währungen geäußert.[268] In diesem wies er darauf hin, dass die EZB 2012 und 2015 jeweils einen Bericht veröffentlichte, der die Unterschiede und Risiken virtueller Währungen aufzeigt. Darüber hinaus schrieb er, dass die Berichte zu dem Ergebnis kommen, dass virtuelle Währungen aufgrund ihrer begrenzenten Verbindung zu der realen Ökonomie, ihrem geringen Transaktionsvolumen und aufgrund der geringen Akzeptanz derzeit keine Bedrohung für die Finanzstabilität seien. Draghi ist der Meinung, dass - obwohl die Marktkapitalisierung virtueller Währungen seit der Veröffentlichung der Berichte zugenommen hat – es keine Hinweise gibt, die suggerieren, dass die Verbindung zwischen virtuellen Währungen und der realen

---

[264] Vgl. *Vandezande, N.* (2017), S. 348; *Europäische Union (Hrsg.)* (2015).
[265] *Europäisches Parlament* (2016), Rn. 14.
[266] *Europäisches Parlament* (2016), Rn. 22.
[267] *Europäische Kommission (Hrsg.)* (2016), S. 12.
[268] *Draghi, M.* (2017).

Ökonomie erheblich gestiegen sei.[269] Da eine zukünftige Zunahme der Nutzung und Akzeptanz virtueller Währungen durchaus denkbar ist, ist laut Draghi die Überwachung der Entwicklung von virtuellen Währungen wichtig.[270]

In Deutschland ist die Einstufung durch die Aufsichtsbehörde BaFin (Bundesanstalt für Finanzdienstleistungsaufsicht) maßgeblich. Bereits 2011 definierte die Aufsichtsbehörde Bitcoin und andere digitale Zahlungsmittel als privatrechtlich ausgegebene Komplementärwährungen und ordnete diese als Rechnungseinheit ein.[271] Somit gelten sie nach § 1 Absatz 11 Satz 1 KWG als Finanzinstrumente.[272] Der gewerbliche Umgang mit virtuellen Währungen kann eine Erlaubnispflicht nach dem Kreditwesengesetz auslösen. Gemäß § 32 Absatz 1 KWG benötigt jeder, der gewerbsmäßig Finanzdienstleistungen erbringen will, eine schriftliche Erlaubnis der BaFin (BaFin-Lizenz).[273]

Keine erlaubnispflichtige Tätigkeit ist die bloße Nutzung von virtuellen Währungen als Ersatz für Bar- oder Buchgeld zur Teilnahme am Wirtschaftskreislauf im Austauschgeschäft. Auch das Mining von virtuellen Währungen stellt an sich keine erlaubnispflichtige Tätigkeit dar, da der Miner die virtuelle Währung nicht selbst emittiert.[274] Allerdings unterliegen Mining Pools, die gewerblich Erlösanteile aus geschürften und veräußerten virtuellen Währungen anbieten, der Erlaubnispflicht.[275] Ebenso ist der Betrieb von Handelsplattformen erlaubnispflichtig.[276] Wer ein erlaubnispflichtiges Geschäft ohne eine BaFin-

---

[269] Siehe *Draghi, M.* (2017), S. 1-2.
[270] Dazu *Draghi, M.* (2017), S.2.
[271] Vgl. *BaFin (Hrsg.)* (2011), 2. hh).
[272] Siehe *BaFin (Hrsg.)* (2016), Anfragen an die BaFin.
[273] Vgl. § 32 Absatz 1 KWG.
[274] Ähnlich *BaFin (Hrsg.)* (2016), Erlaubnispflicht.
[275] Dazu *BaFin (Hrsg.)* (2016), Erlaubnispflichten beim Mining, An- und Verkauf.
[276] Hierzu *WINHELLER Rechtsanwaltsgesellschaft mbH (Hrsg.)* (2017), Bitcoin Exchanges erlaubnispflichtig.

Lizenz betreib, macht sich strafbar – selbst im Fall des nur fahrlässigen Handelns.[277]

In den USA wurden virtuelle Währungen auf der föderalen Ebene durch das Financial Crimes Enforcement Network (FinCEN) reguliert.[278] Zusätzliche Regulierungsmaßnahmen wurden von einigen Staaten, wie beispielsweise New York, getroffen.

Das FinCEN ist unter anderem für die Regulierung von sogenannten „money services businesses“ (MSBs) und „money transmitters“ zuständig.[279] Am 18. März 2013 veröffentlichte das FinCEN eine Richtlinie[280], die klärt, wer im Zusammenhang mit virtuellen Währungen ein MSB führt und wer nicht.[281] Darin wird zwischen den Kategorien „user“, „exchanger“ und „administrator“ unterschieden.[282] Ein „user“ ist eine Person, die eine virtuelle Währung bezieht, um Güter und Dienstleistungen zu kaufen.[283] Der Begriff „exchanger“ bezeichnet eine Person oder Organisation, die virtuelle Währungen gegen Fiat-Währungen oder andere virtuelle Währungen tauscht.[284] Personen oder Organisationen, die die Befugnis haben, eine virtuelle Währung zu erlassen oder einzuziehen, werden als „administrator“ bezeichnet.[285] In den USA werden gemäß dem FinCEN „user“ nicht als MSBs angesehen. Dagegen sind „exchangers“ und „adminsitrators“ „money transmitters“ und unterliegen deshalb den Vorschriften von MSBs.[286]

Somit müssen sich amerikanische Handelsplattformen, bei denen virtuelle Währungen gehandelt werden können, an die Vorschriften, die für MSBs gelten, halten.[287] Zu diesen Vor-

---

[277] Vgl. *WINHELLER Rechtsanwaltsgesellschaft mbH (Hrsg.)* (2017), Folge einer fehlenden BaFin-Lizenz.
[278] Hierzu *Levin, R. B./O´Brien, A. A./Zuberi, M. M.* (2015), S. 336.
[279] Id.
[280] *FinCEN (Hrsg.)* (2013).
[281] Ähnlich *Middlebrook, S. T./Hughes, S. J.* (2014), S. 828.
[282] Vgl. *FinCEN (Hrsg.)* (2013), S. 2.
[283] Id.
[284] Id.
[285] Id.
[286] Siehe *FinCEN (Hrsg.)* (2013), S. 3; *Arnfield, R.* (2015), S. 8.
[287] Dazu *Lam P. N./Lee D. K. C.* (2015b), S. 320.

schriften zählt neben der Pflicht zur Registrierung, Buchführung und Berichterstattung, die Implementierung eines Plans zur Geldwäschebekämpfung.[288]

Eine weitere Regulierungsmaßnahme hat der Bundesstaat New York am 23. Juli 2014 mit der Einführung der sogenannten „BitLicense“ getroffen.[289] Das New York State Department of Financial Services veranlasste, dass jede Person, die Geschäfte mit virtuellen Währungen betreibt, eine Lizenz in Form einer BitLicense benötigt.[290] Den Anknüpfungspunkt zur Erfordernis einer BitLicense bilden Tätigkeiten mit Bezug zu New York oder zu einer in New York ansässigen Person.[291]

F. Fazit

Die kritische Betrachtung dezentraler virtueller Währungen zeigte die Stärken und Schwächen der innovativen Währungen auf. Es lässt sich nicht abstreiten, dass zum jetzigen Zeitpunkt die Schwächen noch überwiegen. Allerdings befindet sich die Technologie der Kryptowährungen noch im Anfangsstadium, sodass abzuwarten bleibt, wie diese sich entwickeln wird. Schon im Februar 2010 war sich Satoshi Nakomoto, der Gründer von Bitcoin, sicher, dass es in 20 Jahren entweder ein sehr hohes Transaktionsvolumen oder gar kein Transaktionsvolumen mehr geben wird.[292]

Die Anzahl der Bitcoin-Transaktionen hat in den letzten Jahren stark zugenommen. Aktuell werden täglich knapp 300.000 Bitcoin-Transaktionen ausgeführt und somit wird das Skalierungsproblem immer mehr zu einem Problem, das in naher Zukunft gelöst werden muss. Auch Altcoins wurden in den letzten Jahren immer beliebter und bekannter, wobei einige dieser Kryptowährungen ein paar der bestehenden Probleme von Bitcoin schon gelöst haben. Dennoch beansprucht Bitcoin

---

[288] Vgl. *Arnfield, R.* (2015), S. 9.
[289] Siehe *Schenk, J./Grieser, S. G.* (2015), S. 29.
[290] Vgl. *NYSDFS (Hrsg.)* (2015), S. 7; *Schenk, J./Grieser, S. G.* (2015), S. 29-30.
[291] Hierzu *Schenk, J./Grieser, S. G.* (2015), S. 30.
[292] Vgl. *Bitcoin Forum (Hrsg.)* (2010).

ungefähr die Hälfte der gesamten Marktkapitalisierung aller Kryptowährungen und ist damit die wichtigste.

Die drei Geldfunktionen werden von den virtuellen Währungen aktuell nur bedingt oder nicht erfüllt. Da die verbreitetste Kryptowährung Bitcoin weltweit geschätzt nur von gut 100.000 Händlern akzeptiert wird, ist man noch weit davon entfernt, ein lückenloses Netzwerk von Einkaufsmöglichkeiten in Anspruch nehmen zu können. Somit kann von einer Erfüllung der Zahlungsmittelfunktion nicht gesprochen werden. Auch die Vorteile der niedrigeren Transaktionskosten und höheren Transaktionsgeschwindigkeit gegenüber herkömmlichen Banküberweisungen sind in der Praxis bei Weitem nicht so vorteilhaft, wie man meinen könnte. Das größte Problem von virtuellen Währungen in Bezug auf die Wertaufbewahrungsfunktion und Recheneinheitsfunktion ist die extrem hohe Volatilität des Wechselkurses.

Von einer einheitlichen Regulierung der virtuellen Währungen ist man noch weit entfernt. Behörden haben weltweit unterschiedliche Auffassungen darüber, wie virtuelle Währungen zu regulieren sind. Die deutsche Finanzaufsichtsbehörde BaFin und das amerikanische Financial Crimes Enforcement Network (FinCEN) gehen bei der Regulierung jedoch ähnlich vor. Da die Blockchain an sich nicht reguliert werden kann, versuchen beide Behörden, die in den Handel von virtuellen Währungen involvierten Unternehmen einer Regulierung zu unterwerfen.

Die Frage, ob virtuelle Währungen das Zahlungsmittel der Zukunft werden, kann niemand mit absoluter Sicherheit sagen. Meine persönliche Meinung und auch die Meinung diverser Autoren ist, dass aufgrund der beschriebenen Risiken und Problemen virtuelle Währungen höchstwahrscheinlich nur eine Nischenwährung ohne weltweite Akzeptanz werden.[293]

Allerdings bin ich der Meinung, dass die Blockchain-Technologie aufgrund der hohen Sicherheit durch Dezentralität durchaus sehr viel Potenzial besitzt und in der Zukunft

---

[293] Siehe beispielsweise *Luther, W. J.* (2016b), S. 553; *Luther, W. J.* (2016c), S. 403.

noch in anderen Bereichen eine wichtige Rolle spielen wird, nämlich immer dann, wenn es darum geht, eine große Datenmenge dezentral, sicher und automatisiert abzuspeichern.

Literaturverzeichnis

Ammous, S. (2016): Can cryptocurrencies fulfil the functions of money?, Working Paper No. 92, August 2016, unter: http://capitalism.columbia.edu/files/ccs/workingpage/2017/ammous_cryptocurrencies_and_the_functions_of_money.pdf (Stand: 14.09.2017).

ARIVA.DE (Hrsg.): BTC/USD (Bitstamp), unter: http://www.ariva.de/btc-usd-bitcoin-us-dollar-kurs/chart?compare=None&avgVal1=0&t=all&avgType1=None&scale=lin&resolution=auto&type=CloseLine&displayHighLow=0&band=None&resolutionInfo=604800&typ=cur&typ=cur&typ=cur&grid=1&grid=0&boer-se_id=167&volume=0&antiAlias=1&antiAlias=0&go=Ok&savg=0&events=None&indicator=None (Stand: 26.09.2017).

Arnfield, R. (2015): Regulation of Virtual Currencies: A Global Overview, unter: http://www.nfcidea.pl/wp-content/uploads/2015/02/Regulation-if-Virtual-Currancies-by-Jumio.pdf (Stand: 05.10.2017).

BaFin (Hrsg.) (2011): Merkblatt Finanzinstrumente (Aktien, Vermögensanlagen, Schuldtitel, sonstige Rechte, Anteile an Investmentvermögen, Geldmarktinstru-mente, Devisen und Rechnungseinheiten), unter: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Merkblatt/mb_111220_finanzinstrumente.html (Stand: 07.10.2017).

BaFin (Hrsg.) (2016): Virtuelle Währungen/Virtual Currency (VC), unter: https://www.bafin.de/DE/Aufsicht/FinTech/VirtualCurrency/virtual_currency_node.html (Stand: 03.11.2017).

Bergmann, C. (2017a): Bitcoin erreicht sein Limit: Absurde Folgen des Fee-Markets, in BitcoinBlog.de (Hrsg.), unter: https://bitcoinblog.de/2017/03/07/bitcoin-erreicht-sein-limit-absurde-folgen-des-fee-markets/ (Stand: 21.09.2017).

Bergmann, C. (2017b): SegWit ist live. Endlich., in Bitcoin-Blog.de (Hrsg.), unter: https://bitcoinblog.de/2017/08/24/segwit-ist-live-endlich/ (Stand: 21.09.2017).

Bic Camera (Hrsg.) (2017), unter: http://www.biccamera.co.jp.e.lj.hp.transer.com/shopguide/campaign/bitcoin/index.html (Stand: 08.09.2017).

Bitcoin.com (Hrsg.) (2017): Differences Between Bitcoin Cash and Bitcoin, unter: https://www.bitcoin.com/info/differences-between-bitcoin-cash-bcc-and-bitcoin-btc (Stand: 18.09.2017).

BitcoinCash.org (Hrsg.) (2017), unter: https://www.bitcoincash.org/ (Stand: 18.09.2017).

Bitcoincharts (Hrsg.) (2017): Bitcoin Network, unter: https://bitcoincharts.com/bitcoin/ (Stand: 12.09.2017).

Bitcoin Forum (Hrsg.) (2010), unter: https://bitcointalk.org/index.php?topic=48.msg329#msg329 (Stand: 30.10.2017).

Bitcoin Wiki (Hrsg.) (2011): Datei:Total bitcoins over time graph.png, unter: https://de.bitcoin.it/wiki/Datei:Total_bitcoins_over_time_graph.png (Stand:11.09.2017).

Bitcoin Wiki (Hrsg.) (2015): Proof of Stake, unter: https://en.bitcoin.it/wiki/Proof_of_Stake (Stand: 13.09.2017).

Bitcoin Wiki (Hrsg.) (2017a): Scalability, unter: https://en.bitcoin.it/wiki/Scalability (Stand: 21.09.2017).

Bitcoin Wiki (Hrsg.) (2017b): Controlled supply, unter: https://en.bitcoin.it/wiki/Controlled_supply (Stand: 03.11.2017).

bitFlyer (Hrsg.) (2017a): The Virtual Currency Act explained, unter: https://bitflyer.jp/en/virtual-currency-act (Stand: 07.09.2017).

bitFlyer (Hrsg.) (2017b): Regarding taxes & virtual currency, unter: https://bitflyer.jp/digital-currency-tax (Stand: 07.09.2017).

Bhaskar, N. D./Lee, D. K. C. (2015): Bitocin Mining Technology, in: Lee, D. K. C. (Hrsg.): Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data, Amsterdam.

Blockchain.info (Hrsg.) (2017a), unter: https://blockchain.info/ (Stand: 30.08.2017).

Blockchain.info (Hrsg.) (2017b): Währungs Statistik, unter: https://blockchain.info/de/stats (Stand: 19.09.2017).

Blockchain.info (Hrsg.) (2017c): Cost % of Transaction Volume, unter: https://blockchain.info/de/charts/cost-per-transaction-percent (Stand: 22.09.2017).

Bonneau, J./Miller, A./Clark, J./Narayanan, A./Kroll, J. A./Felten, E. W. (2015): SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies, unter: http://www.ieee-security.org/TC/SP2015/papers-archived/6949a104.pdf (Stand: 21.09.2017).

Brito, J./Castillo, A. (2016): Bitcoin: A Primer for Policymakers, 2. Auflage, Arlington, unter: https://www.mercatus.org/system/files/GMU_Bitcoin_042516_WEBv2_0.pdf (Stand: 28.09.2017).

Brühl, V. (2016): Bitcoins, Blockchain und Distributed Ledgers: Funktionsweise, Marktentwicklungen und Zukunftsperspektiven, in: Wirtschaftsdienst (Hrsg.), Jg. 97, Heft 2, S. 135-142.

Caetano, R. (2015): Learning Bitcoin, E-Book, unter: http://proquest.tech.safaribooksonline.de/book/web-applications-and-services/9781785287305 (Stand: 04.11.2017).

Chaparro, F. (2017): Morgan Stanley: 'Bitcoin acceptance is virtually zero and shrink-ing', in: Business Insider (Hrsg.), unter: http://www.businessinsider.de/bitcoin-price-rises-but-retailers-wont-accept-it-7-

2017?utm_source=Triggermail&utm_medium=email&utm_campaign=Post%20Blast%20(biipayments):%20Merchants%20aren%27t%20accepting%20bitcoin%20%E2%80%94%20Mobile%20money%20has%20a%20major%20role%20in%20Africa%20%E2%80%94%20Flywire%20growth%20accelerates&utm_term=BII%20List%20Payments%20ALL&r=US&IR=T (Stand: 06.09.2017).

Chokun, J. (2017): Who Accepts Bitcoins As Payment? List of Companies, Stores, Shops, in: 99Bitcoins (Hrsg.), unter: https://99bitcoins.com/who-accepts-bitcoins-payment-companies-stores-take-bitcoins/ (Stand: 06.09.2017).

Christin, N. (2012): Traveling the Silk Road: A measurement analysis of a large anony-mous online marketplace, Working paper, unter: https://www.andrew.cmu.edu/user/nicolasc/publications/TR-CMU-CyLab-12-018.pdf (Stand: 01.10.2017).

Coindesk (Hrsg.) (2015): State of Bitcoin and Blockchain Q3 2015, unter: https://de.slideshare.net/CoinDesk/v3-state-of-bitcoin-and-blockchain-q3-2015 (Stand: 06.09.2017).

coinmap (Hrsg.) (2017), unter: https://coinmap.org/#/map/52.47169740/13.49807739/11 (Stand: 07.09.2017).

CoinMarketCap (Hrsg.) (2017a): Cryptocurrency Market Capitalizations, unter: https://coinmarketcap.com/coins/ (Stand: 11.09.2017).

CoinMarketCap (Hrsg.) (2017b): Frequently Asked Questions, unter: https://coinmarketcap.com/faq/ Stand: 12.09.2017).

CoinMarketCap (Hrsg.) (2017c): Global Charts, unter: https://coinmarketcap.com/charts/ (Stand: 13.09.2017).

CoinMarketCap (Hrsg.) (2017d): Historical Snapshots, unter: https://coinmarketcap.com/historical/ (Stand: 13.09.2017).

CoinMarketCap (Hrsg.) (2017e): Ripple, unter: https://coinmarketcap.com/currencies/ripple/ (Stand: 14.09.2017).

CountSegwit (Hrsg.) (2017), unter: http://www.countsegwit.com/countsegwit.html (Stand: 21.09.2017).

CryptoCoinCharts (Hrsg.) (2017), unter: https://cryptocoincharts.info/markets/info (Stand: 06.09.2017).

Draghi, M. (2017), unter: https://www.ecb.europa.eu/pub/pdf/other/ecb.mepletter170720_bermejo_viegas.en.pdf?afc1b44a8ebe0d7b13ae025cd986920f (Stand: 05.11.2017).

Ethereum Foundation (Hrsg.) (2017): Ether, unter: https://www.ethereum.org/ether (Stand: 15.09.2017).

Ethereum Homestead (Hrsg.) (2017a)*:* The algorithm, unter: http://ethdocs.org/en/latest/mining.html#the-algorithm (Stand: 14.09.2017).

Ethereum Homestead (Hrsg.) (2017b): What is Ethereum?, unter: http://ethdocs.org/en/latest/introduction/what-is-ethereum.html (Stand: 15.09.2017).

Europäische Bankenaufsichtsbehörde (Hrsg.) (2014): EBA Opinion on 'virtual curren-cies', unter: https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf (Stand: 25.08.2017).

Europäische Kommission (Hrsg.) (2016): COM (2016) 450 final, unter: https://ec.europa.eu/transparency/regdoc/rep/1/2016/DE/1-2016-450-DE-F1-1.PDF (Stand: 25.08.2017).

Europäisches Parlament (2016): European Parliament resolution of 26 May 2016 on virtual currencies,

P8_TA(2016)0228, unter: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2016-0228+0+DOC+XML+V0//EN (Stand: 07.10.2017).

Europäische Union (Hrsg.) (2009): Richtlinie 2009/110/EG, unter: http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32009L0110&from=DE (Stand: 08.09.2017).

Europäische Union (Hrsg.) (2015): Richtlinie (EU) 2015/849, unter: http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32015L0849&from=DE (Stand: 06.10.2017).

Europäische Zentralbank (Hrsg.) (2012): Virtual currency schemes, unter: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf (Stand: 25.08.2017).

Europäische Zentralbank (Hrsg.) (2015): Virtual currency schemes – a further analysis, unter: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf (Stand: 25.08.2017).

Fairfield, J. A. T. (2014): Smart Contracts, Bitcoin Bots, and Consumer Protection, in: Washington and Lee Law Review Online (Hrsg.), Volume 71, Issue 2, unter: http://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=1003&context=wlulr-online (Stand: 15.09.2017).

Financial Action Task Force (Hrsg.) (2014): Virtual Currencies Key Definitions and Potential AML/CFT Risks, FATF Report, unter: http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf (Stand: 25.08.2017).

Finanzen.net (Hrsg.) (2017), unter http://www.finanzen.net/ratgeber/kryptowaehrung/bitcoin-kaufen (Stand: 06.09.2017).

FinCEN (Hrsg.) (2013): FIN-2013-G001, unter: https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf (Stand: 06.11.2017)

Franco, P. (2015): Understanding Bitcoin: Cryptography, engineering, and economics, Online-Ausgabe, Chichester, unter: http://onlinelibrary.wiley.com/book/10.1002/9781119019138 (Stand: 11.09.2017).

Geiling, L. (2016): Distributed Ledger: Die Technologie hinter den virtuellen Währun-gen am Beispiel der Blockchain, in: BaFin Journal (Hrsg.), Februar 2016, unter: http://www.bafin.de/SharedDocs/Downloads/DE/BaFinJournal/2016/bj_1602.pdf?__blob=publicationFile&v=3 (Stand: 13.09.2017).

Giese, P. (2017): SegWit, SegWit2x, UASF – Was ist das? (Teil 1), in: BTC-ECHO (Hrsg.), unter: https://www.btc-echo.de/segwit-segwit2x-uasf-was-ist-das-teil-1/ (Stand: 21.09.2017).

GitHub Inc. (Hrsg.) (2017a)*:* Ethereum Whitepaper, unter: https://github.com/ethereum/wiki/wiki/White-Paper (Stand: 15.09.2017).

GitHub Inc. (Hrsg.) (2017b)*:* rippled, unter: https://github.com/ripple/rippled (Stand: 14.09.2017).

Gora, V. (2015): Cryptocurrencies: Are Disruptive Financial Innovations Here?, in: Modern Economy (Hrsg.), 6, S. 816-832.

Hanl, A./Michaelis, J. (2017): Kryptowährungen - ein Problem für die Geldpolitik?, in Wirtschaftsdienst, Volume 97, Issue 5, S. 363 – 370.

Hanley, B. P. (2015): The False Premises and Promises of Bitcoin, unter: https://arxiv.org/ftp/arxiv/papers/1312/1312.2048.pdf (Stand: 23.09.2017).

Helms, K. (2017): Rollout of 260,000+ Bitcoin-Accepting Stores in Japan Begins, in: Bitcoin.com, unter:

https://news.bitcoin.com/rollout-of-260000-bitcoin-accepting-stores-in-japan-begins/ (Stand: 07.09.2017).

Hildner, A. (2016): Bitcoins auf dem Vormarsch: Schaffung eines regulatorischen Level Playing Fields?, in BKR – Zeitschrift für Bank und Kapitalmarktrecht, Heft 12, S. 485-495.

Internationaler Währungsfonds (Hrsg.) (2016): Virtual Currencies and Beyond: Initial Considerations, IMF Staff Discussion Note, unter: https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf (Stand: 25.08.2017).

Kancs, d'Artis/Ciaian, P./Rajcaniova, M. (2015): The Digital Agenda of Virtual Cur-rencies: Can BitCoin Become a Global Currency?, in: Europäische Kommission JRC (Hrsg.), unter: http://publications.jrc.ec.europa.eu/repository/bitstream/JRC97043/the%20digital%20agenda%20of%20virtual%20currencies_final.pdf (Stand: 08.10.2017).

Katz, L. (2017): Bitcoin Acceptance Among Retailers Is Low and Getting Lower, in: Bloomberg (Hrsg.), unter: https://www.bloomberg.com/news/articles/2017-07-12/bitcoin-acceptance-among-retailers-is-low-and-getting-lower (Stand: 06.09.2017).

Kerscher, D. (2014): Bitcoin. Funktionsweise, Risiken und Chancen der digitalen Wäh-rung, 2. Auflage, Dingolfing.

Khatwani, S. (2017): Bitcoin Fork Coming: How To Prepare For Replay Attacks (What are replay attacks?), in: CoinSutra (Hrsg.), unter: https://coinsutra.com/what-are-replay-attacks/ (Stand: 05.11.2017).

Koulayev, S./Rysman, M./Schuh, S./Stavins, J. (2016): Explaining adoption and use of payment instruments by US consumers, in: RAND Journal of Economics (Hrsg.), Vol. 47, No. 2.

KWG (2017): Gesetz über das Kreditwesen, unter: https://www.gesetze-im-internet.de/kredwg/KWG.pdf (Stand: 28.10.2017).

Lam, P. N./Lee, D. K. C. (2015a): Introduction to Bitcoin, in: Lee, D. K. C. (Hrsg.):Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data, Amsterdam.

Lam, P. N./Lee, D. K. C. (2015b): A Light Touch of Regulation for Virtual Currencies, in: Lee, D. K. C. (Hrsg.): Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data, Amsterdam.

Lee, L (2016): New Kids on the Blockchain: How Bitcoin's Technology Could Reinvent the Stock Market, in: Hastings Business Law Journal, Volume 12, Number 2, S. 81-132.

Lerch, M. P. (2015): Bitcoin als Evolution des Geldes: Herausforderungen, Risiken und Regulierungsfragen, in: ZBB (Hrsg.), Heft 3, S. 190-204.

Levin, R. B./O´Brien, A. A./Zuberi, M. M. (2015): Real Regulation of Virtual Currencies, in: Lee, D. K. C. (Hrsg.): Handbook of Digital Currency: Bitcoin, Innova-tion, Financial Instruments, and Big Data, Amsterdam.

Lo, S./Wang, J. C. (2014): Bitcoin as Money?, No. 14-4, unter: https://www.bostonfed.org/-/media/Documents/Workingpapers/PDF/cpp1404.pdf (Stand: 06.11.2017)

Luther, W. J. (2016a): Regulating Bitcoin: On What Grounds?, Working Paper, unter: https://poseidon01.ssrn.com/delivery.php?ID=120106117091006029075072087116000106053087095019051075010070113104064080086099127025120122060118005029010126001110094122100123103051037075027073003121019088106004069037089078092126117122067112067026084021070084025118069076021093108118082092125064002090&EXT=pdf (Stand: 30.10.2017).

Luther, W. J. (2016b): CRYPTOCURRENCIES, NETWORK EFFECTS, AND SWITCHING COSTS, in: Contemporary Economic Policy, Vol. 34, No. 3, S. 553-571.

Luther, W. J. (2016c): Bitcoin and the Future of Digital Payments, in: The Independent Review (Hrsg.), v. 20, n. 3, S. 397-404.

Luther, W. J./White, L. H. (2014): Can Bitcoin Become a Major Currency?, GMU Working Paper in Economics No. 14-17, unter: https://poseidon01.ssrn.com/delivery.php?ID=228120074126094086013122119067001123113033089067083026007071077066002071004084095077016096063033044063062006031118009009088122042014014018044030073123091122013021113056055054119025098007099082107092016083067026084078090000096120080091000099018103006119&EXT=pdf (Stand: 23.09.2017).

Mankiw, N. G. (2012): Macroeconomics, 8. Auflage, New York.

Middlebrook, S. T./Hughes, S. J. (2014): Regulating Cryptocurrencies in the United States: Current Issues and Future Directions, in: William Mitchell Law Review (Hrsg.), Volume 40, Issue 2, Article 11, S. 813-848.

Münzer, J. (2014): Bitcoins: Aufsichtliche Bewertung und Risiken für Nutzer, in: BaFin Journal (Hrsg.), Januar 2014.

Nakomoto, S. (2008): Bitcoin: A Peer-to-Peer Electronic Cash System, unter: https://bitcoin.org/bitcoin.pdf (Stand: 26.08.2017).

Nikkei Asian Review (Hrsg.) (2017): Japan's Bic Camera to accept bitcoin nationwide, unter: https://asia.nikkei.com/Business/Companies/Japan-s-Bic-Camera-to-accept-bitcoin-nationwide (Stand: 08.09.2017).

NYSDFS (Hrsg.) (2015): Part 200. Virtual Currencies, unter: http://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf (Stand: 05.10.2017).

Ong, B./Lee, T. M./Li, G./Lee, D. K. C. (2015): Evaluating the Potential of Alternative Cryptocurrencies, in: Lee, D. K. C. (Hrsg.): Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data, Amsterdam.

Plassaras, N. A. (2013): Regulating Digital Currencies: Bringing Bitcoin within the Reach of the IMF, in: Chicago Journal of International Law (Hrsg.), Vol. 14: No. 1, Article 12, S. 377-407.

Preuss, M. (2017): Was ist Segregated Witness?, in: BTC-ECHO, unter: https://www.btc-echo.de/was-ist-segregated-witness/ (Stand: 21.09.2017).

Ripple (Hrsg.) (2017): XRP, unter: https://ripple.com/xrp/ (Stand: 14.09.2017).

Ripple Labs (Hrsg.) (2014): The Ripple Protocol: A Deep Dive for Finance Professionals, unter: http://www.the-blockchain.com/docs/Ripple%20Protocol%20-%20Deep%20Dive%20For%20Financial%20Professionals.pdf (Stand: 14.09.2017).

Schenk, J./Grieser, S. G. (2015): Regulierung von Bitcoins – zwei Ansätze im Ver-gleich, in: Recht der Finanzinstrumente (Hrsg.) (2015), Heft 1, S. 29-36.

Schuh, S./Shy, O. (2016): U.S. Consumers' Adoption and Use of Bitcoin and Other Vir-tual Currencies, unter: https://www.dnb.nl/en/binaries/Consumer%20VC%20paper_DNB_FINAL_corrected_tcm47-344530.pdf?2016083013 (Stand: 26.09.2017).

Swan, M. (2015): Blueprint for a New Economy, E-Book, unter: http://proquest.tech.safaribooksonline.de/book/web-development/ecommerce/9781491920480 (Stand: 28.08.2017).

The Bitcoin Foundation (Hrsg.) (2014): Removing Impediments to Bitcoin's Success: A Risk Management Study, Bitcoin Foundation Research Brief No. 1, unter: https://bitcoinfoundation.org/wp-

content/uploads/2014/07/Bitcoin-Risk-Management-Study-Spring-2014.pdf (Stand: 29.09.2017).

The World Bank Group (Hrsg.) (2017): Remittance Prices Worldwide, Issue 21, March 2017, unter: https://remittanceprices.worldbank.org/sites/default/files/rpw_report_march_2017.pdf (Stand: 22.09.2017).

Tschorsch, F./Scheuermann, B. (2016): Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies, IEEE Communications Surveys & Tutorials, Volume 18, Issue 3, thirdquarter 2016.

Tu, K. V./Meredith, M. W. (2015): Rethinking Virtual Currency Regulation in the Bitcoin Age, in: Washington Law Review (Hrsg.), Vol. 90, S. 271-347.

Vandezande, N. (2017): Virtual currencies under EU anti-money laundering law, in: Computer Law & Security Review (Hrsg.), Volume 33, Issue 3, S. 341-353.

Velde, F. R. (2013): Bitcoin: A primer, in: Chicago Fed Letter (Hrsg.), No. 317, Decem-ber 2013, unter: https://www.chicagofed.org/~/media/publications/chicago-fed-letter/2013/cfldecember2013-317-pdf.pdf (Stand: 22.09.2017).

Visa Inc. (Hrsg.) (2017): Visa Inc. Facts & Figures, unter: https://usa.visa.com/dam/VCOM/global/about-visa/documents/visa-facts-figures-jan-2017.pdf (Stand: 21.09.2017).

Wallace, B (2011): The Rise and Fall of Bitcoin, in: Wired Magazine (Hrsg.), unter: https://www.wired.com/2011/11/mf_bitcoin/ (Stand: 25.08.2017).

WINHELLER Rechtsanwaltsgesellschaft mbH (Hrsg.) (2017): Bitcoin und BaFin, unter: https://www.winheller.com/bankrecht-finanzrecht/bitcointrading/bitcoin-und-bafin.html (Stand: 28.10.2017).

Yermack, D. (2015): Is Bitcoin a Real Currency? An Economic Appraisal, in: Lee, D. K. C. (Hrsg.): Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data, Amsterdam.