ALEXANDRA SPIEGEL

Blockchain-basiertes virtuelles Geld

Schriften zum Recht der Digitalisierung

Mohr Siebeck

Schriften zum Recht der Digitalisierung

Herausgegeben von

Florian Möslein, Sebastian Omlor und Martin Will

3

Alexandra Spiegel

Blockchain-basiertes virtuelles Geld

Mohr Siebeck

Alexandra Spiegel, geboren 1991; Studium der Rechtswissenschaften an der Philipps-Universität Marburg; 2013–2015 Studentische Hilfskraft am Institut für Genossenschaftswesen Marburg bei Herrn Prof. Dr. Volker Beuthien; 2016 Erste Juristische Prüfung; 2016–2018 Wissenschaftliche Mitarbeiterin an der Philipps-Universität Marburg, Professur für Bürgerliches Recht, Handels- und Wirtschaftsrecht, Bankrecht sowie Rechtsvergleichung; 2018 Zweites juristisches Staatsexamen.

ISBN 978-3-16-159395-6 / eISBN 978-3-16-159396-3
DOI 10.1628/978-3-16-159396-3

ISSN 2700-1288 / eISSN 2700-1296 (Schriften zum Recht der Digitalisierung)

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliographie; detaillierte bibliographische Daten sind über *http://dnb.dnb.de* abrufbar. Dissertation am Fachbereich Rechtswissenschaften der Philipps-Universität Marburg.

Das Buch wurde von Gulde Druck in Tübingen gesetzt, auf alterungsbeständiges Werkdruckpapier gedruckt und gebunden.

Printed in Germany.

Meiner Familie

Vorwort

Die vorliegende Arbeit wurde im Wintersemester 2019/2020 vom Fachbereich Rechtswissenschaften der Philipps-Universität Marburg als Dissertation angenommen. Literatur und Rechtsprechung befindet sich auf dem Stand von Januar 2020, umfassend berücksichtigt werden konnte sie jedoch nur, sofern sie bis März 2019 veröffentlicht wurde.

Meine Promotionszeit an der Philipps-Universität Marburg, die sich zeitlich mit der Tätigkeit als wissenschaftliche Mitarbeiterin an der Professur für Bürgerliches Recht, Handels- und Wirtschaftsrecht, Bankrecht sowie Rechtsvergleichung, dem Referendariat sowie zuletzt der Einarbeitung als Richterin auf Probe überschnitt, war eine so wertvolle wie lehrreiche Zeit, für die ich mich bei meinem Doktorvater Herrn Prof. Dr. Sebastian Omlor, LL.M. (NYU), LL.M. Eur. von ganzem Herzen bedanken möchte. Sein „liberal-leistungsorientierter" Ansatz zur Anleitung seiner Doktoranden und des Lehrstuhls sowie seine überaus loyale und freundliche Art verhalfen mir zu höchster Motivation und Leistungsbereitschaft. Mein Dank gilt darüber hinaus Herrn Prof. Dr. Florian Möslein, LL.M. (London) für die Erstellung des Zweitgutachtens. Den Herausgebern gilt mein Dank für die Aufnahme der Arbeit in diese Schriftenreihe.

Vor allem möchte ich jedoch denjenigen danken, die mir nicht nur fachlich, sondern auch persönlich während der kräftezehrenden Zeit des Promovierens zur Seite standen. Dazu zählt meine gesamte Familie, insbesondere meine Eltern, denen ich sehr viel mehr zu verdanken habe und ohne die es mich nicht gäbe. Außerdem Frau Staatsanwältin Lisa Pohlmann, die die Mühen des Korrekturlesens auf sich nahm. Ganz besonders und von ganzem Herzen richtet sich mein Dank an meinen Ehemann Björn Niclas Spiegel, der mich sowohl in persönlicher als auch fachlicher Hinsicht immer ermutigt und motiviert hat und ohne dessen Unterstützung es diese Arbeit nicht gäbe.

Aschaffenburg, im Juni 2020 *Alexandra Spiegel*

Inhaltsübersicht

Inhaltsverzeichnis

A. Virtuelles Geld

I. Einleitung

Das Zivilrecht will die Rechtsverhältnisse zwischen zwei oder mehr gleichgeordneten Rechtssubjekten regeln und erfassen. Hierbei geht es weniger um Regeln, die die Rechtssubjekte einschränken sollen, schließlich ist die Wahrung der Privatautonomie Kennzeichen des Zivilrechts. Es geht vielmehr um eine Kategorisierung und Ordnung dessen, was tatsächlich passiert, sodass im Problemfall auf einen gesetzlich geregelten und dadurch für alle Subjekte gerechten Lösungsmechanismus zurückgegriffen werden kann. Sofern neue, beispielsweise technische, Phänomene auftreten und in der Welt der Rechtssubjekte eine Rolle spielen, bedarf es einer Überprüfung, ob die derzeit geltenden rechtlichen Regelungen das neue Phänomen noch erfassen können – wenn ja, wie – oder ob das Zivilrecht insoweit einer „Aktualisierung" bedarf. Eine Aktualisierung kann dabei nicht lediglich durch die Ergänzung eines weiteren auf das Phänomen zugeschnittenen Gesetzestextes geschehen, sondern kann auch darin liegen, einen bestehenden abstrakt-generell gefassten Text so auszulegen, dass er die neue Situation erfasst.

Mit der Entwicklung der Blockchain-Technologie im Jahr 2009 und des darauf basierenden virtuellen Geldes wurde das Zivilrecht vor eine neue Herausforderung gestellt. Virtuelles Geld, das rein digital existiert, spielt nunmehr eine Rolle zwischen Rechtssubjekten, indem sie sich virtuelles Geld verschaffen, es im Rechtsverkehr verwenden und dabei an andere Rechtssubjekte weitergeben.

Diese Arbeit widmet sich zunächst einer Darstellung der dem virtuellen Geld zugrundeliegenden technischen Funktionsweise und stellt am Beispiel von Bitcoins die Möglichkeiten des originären sowie derivativen Erwerbs derselben dar (B.). Im darauf folgenden geldtheoretischen Teil (C.) wird untersucht, ob das virtuelle „Geld" diesen Rechtsbegriff ausfüllt. Dabei wird dem Umstand Rechnung getragen, dass eine fest etablierte Definition des Begriffs nicht existiert, sondern dass es unterschiedliche Herangehensweisen hierfür gibt. Sodann wird auch der Begriff der Währung (D.), der aufgrund seiner hoheitlichen Bezüge deutlich weniger Spielraum zur Bezeichnung des virtuellen Geldes lässt, in den Blick genommen.

In Abschnitt E. folgt auf die geld- und währungstheoretischen Ausführungen die Erörterung, inwieweit einzelne, vor allem zivilrechtliche, Rechtsgebiete Regelungen für virtuelles Geld bereithalten. Dabei wird unter 1. zunächst darauf eingegangen, um „was" es sich bei virtuellem Geld anhand verschiedener Einordnungsmöglichkeiten handelt, und sodann unter 2. der Umgang mit virtuellem Geld am Beispiel von Bitcoins erörtert und kategorisiert.

In einem schuldrechtlichen Teil (a.) werden einerseits die verschiedenen Erwerbsmöglichkeiten sowie etwaige Besonderheiten und Störungen der Vertragsbeziehung durch Widerruf, Mängel, Anfechtung oder Wertveränderungen behandelt sowie andererseits erfüllungsrechtliche Fragen, insbesondere auch der Zahlungs- und Leistungsort (ee.), thematisiert. Im Bereich des Sachenrechts (b.) liegt der Schwerpunkt auf der Frage der Einordnung von virtuellem Geld unter den Eigentumsbegriff bzw. dessen Spannweite und analoge Anwendbarkeit. Mit deliktsrechtlichen Erwägungen (c.) schließt der Abschnitt zum BGB.

Die Durchsetzung der im zivilrechtlichen Abschnitt kategorisierten Ansprüche wird im nachfolgenden Kapitel zum Vollstreckungsrecht (II.) thematisiert, wobei zwischen der Zwangsvollstreckung wegen einer Geldforderung und wegen einer ausdrücklich in Bitcoins ausgedrückten Forderung unterschieden wird.

Sodann erfolgt – getrennt zum eingangs thematisierten währungstheoretischen Teil – ein nunmehr konkret gefasster währungsrechtlicher Abschnitt (III.) mit der Erörterung, inwieweit § 35 des Gesetzes über die deutsche Bundesbank auf virtuelles Geld anwendbar ist.

Bankenaufsichtsrechtlich besonders relevant ist in Bezug auf virtuelles Geld die Einordnung als Rechnungseinheit im Sinne des Kreditwesengesetzes. Im Abschnitt IV. wird deshalb die durch die Bundesanstalt für Finanzdienstleistungsaufsicht vorgenommene Positionierung hierzu untersucht und kritisch beleuchtet.

In Abschnitt V. wird deine der wenigen Entscheidungen zu virtuellem Geld vorgestellt, die der Europäische Gerichtshof im Jahr 2015 zum Steuerrecht getroffen hat.

Das letzte Kapitel der Arbeit (VI.) bilden rechtsvergleichende Ausführungen zu vier weiteren Rechtsordnungen: Frankreich, den Vereinigten Staaten von Amerika, England und China. Neben der Untersuchung der Rechtslage in einem geographisch angrenzenden Land (Frankreich) stehen die untersuchten Rechtsordnungen für einen eher offenen (USA, England) sowie einen eher restriktiven (China) Umgang mit virtuellem Geld. Dies stellt auch den Grund dar, warum die rechtsvergleichenden Ausführungen den Abschluss bilden: Jede Rechtsordnung geht anders mit technischen Neuerungen und den damit einhergehenden Herausforderungen für die Rechtslage um, was dadurch noch deutlicher herausgestellt werden kann.

II. Marktkapitalisierung

Die Begriffe virtuelles Geld und Blockchain-Technologie sind zwei zwingend miteinander verknüpfte Themenfelder.

Ersteres kommt ohne letztere nicht aus, da die Blockchain die Basis für die Gesamtheit der virtuellen Daten bildet, die für das Halten und Transferieren von virtuellem Geld benötigt werden, (näher unten zur technischen Funktionsweise von Bitcoins, S. 6 ff.). Auf Grundlage der Blockchain existieren fast 2.000 kryptographische Gelder[1], deren Marktkapitalisierung teilweise sehr beschränkt ist. Die virtuellen Gelder mit der größten Marktkapitalisierung sind in Abbildung 1 dargestellt:

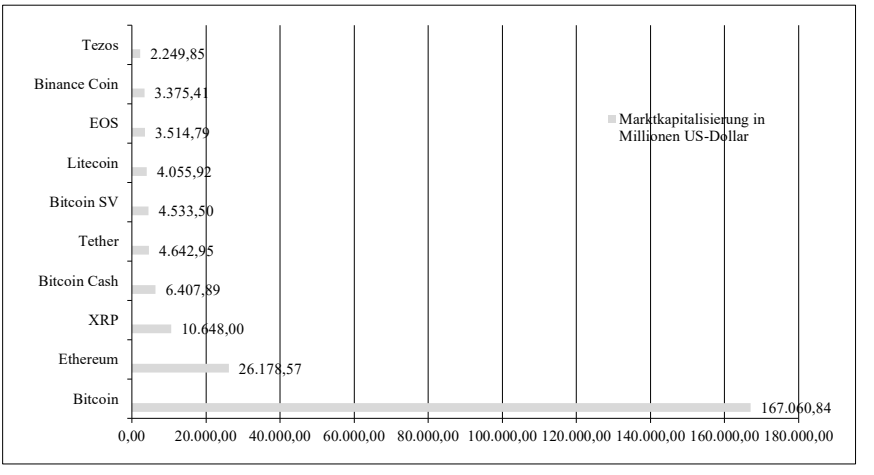

Abb. 1: Marktkapitalisierung verschiedener virtueller Gelder, Daten nach https://de.statista.com/statistik/daten/studie/296205/umfrage/marktkapitalisierung-digitaler-zahlungsmittel/

Mit Abstand die größte Marktkapitalisierung erfährt nach wie vor der Bitcoin. Die folgende Arbeit bezieht sich aus diesem Grund in erster Linie auf rechtlich relevante Aspekte für Bitcoins. Diese Grundsätze sind jedoch oftmals ohne weiteres auf die sogenannte Altcoins, die alternativen kryptographischen Gelder, übertragbar, da die wesentlichen Eckpunkte übereinstimmen: ausschließlich virtuelle, d. h. digitale Verfügbarkeit der Daten, die innerhalb eines Blockchain-Systems einzelnen Nutzern zugeordnet, mit einem Wert ausgestattet und übertragbar sind.

[1] www.coinmarketcap.com.

B. Die technische Seite der Bitcoins

Virtuelles Geld wird häufig mit dem Bitcoin assoziert. Während die Marktkapitalisierung, d. h. Multiplikation der Geldmenge mit dem Geldwert, anderer virtueller Gelder bei beispielsweise ca. 26 Milliarden US-Dollar (Ethereum) liegt, sind Bitcoin im Wert von über 167 Milliarden US-Dollar am Markt kapitalisiert (vgl. auch Abbildung 1).[1] Auch im Hinblick darauf, dass die am Markt kursierenden Alternativen zu Bitcoins oft lediglich Ableger mit minimalen Veränderungen der Bediensoftware sind,[2] ist die technische Orientierung und die sich daran anschließende rechtliche Untersuchung an diesem Geldphänomen am zielführendsten.

Die Gesamtkonzeption von Bitcoins und die Funktionsweise der Transaktionen basieren auf einer Idee, die über die bisher unbekannte Person bzw. Personengruppe „Satoshi Nakamoto" publiziert wurde. Ein grundlegendes Konzeptpapier wurde über diese (Pseudonym-)Bezeichnung am 31.10.2008 veröffentlicht und ist auch weiterhin im Internet abrufbar.[3] Bitcoins sollen danach in erster Linie eine Alternative zu dem von Regierungen und Banken kontrollierten Geld darstellen, die ohne zentrale Instanz auskommt.[4]

I. Bitcoins

Bitcoins selbst sind die im Bitcoin-System verwendeten Einheiten, die in staatliche Währungen wie Euro oder US-Dollar über Handelsbörsen umtauschbar sind und mit denen der Austausch von Waren und Dienstleistungen betrieben werden kann. Es existiert keine gegenständliche Verkörperung dieser ausschließlich di-

---

[1] Statista, Ranking der größten virtuellen Währungen nach Marktkapitalisierung im März 2019 (in Millionen US-Dollar) https://de.statista.com/statistik/daten/studie/296205/umfrage/marktkapitalisierung-digitaler-zahlungsmittel/ (22.04.2020).

[2] *Kerscher,* Bitcoin, 2. Auflage (2014), S. 47.

[3] Das sog. White Paper ist abrufbar unter: *Nakamoto,* Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf.

[4] *Djazayeri*, jurisPR-BKR 6/2014, 1.

gitalen Einheiten.[5] Das liegt auch daran, dass Bitcoins bis auf die achte Dezimalstelle aufgeteilt werden können; die kleinste Einheit, d. h. 0,00000001 Bitcoin, wird als ein Satoshi (nach dem Erfinderpseudonym) bezeichnet.

II. System – generelle Funktionsweise

Das System, über welches Bitcoins entstehen und transferiert werden können, ist ein dezentrales peer-to-peer-Netzwerk (P2P-Netzwerk), bestehend aus den teilnehmenden Computern (PCs, Laptops oder Smartphones bzw. Zusammenschlüsse von Rechner, sog. „Bitcoin-Farms"), auf denen dafür eine entsprechende Software („client"/„wallet") installiert ist. Es zeichnet sich dadurch aus, dass alle Teilnehmer („peers") gleichberechtigt miteinander verbunden sind und Informationen untereinander ausgetauscht werden, ohne dass eine zentrale Instanz die Verbreitung übernimmt.[6] Jeder partizipierende Nutzercomputer dient deshalb gleichzeitig als Verzeichnisserver für das Bitcoin-Netzwerk.[7] Die Verbindung zwischen den einzelnen Computern wird dabei über das Internet hergestellt. Die Software auf dem Computer dient dem Teilnehmer in erster Linie als digitale Geldbörse („wallet"), die dessen Zugriffsdaten (öffentliche und private Schlüssel) für die erworbenen Bitcoins speichert und aus der Ausgaben getätigt sowie in die Einnahmen empfangen werden können. Die digitalen Schlüssel in Form von Dateien können dabei lokal auf dem Computer gespeichert oder auf einem anderen Speichermedium (z. B. USB-Stick, externe Festplatte) gesichert werden.

Bei der Installation der Software werden Adressen zum Empfangen und Versenden von Bitcoins generiert. Dazu verwendet die Software ein digitales Signaturverfahren auf der Basis asymmetrischer Kryptografie.[8] Die Asymmetrie besteht insofern, als nicht derselbe Schlüssel für die Ver- und Entschlüsselung verwendet wird (ansonsten wäre es eine symmetrische Kryptografie).[9] Die Adressen basieren auf einem öffentlichen Schlüssel, der als Empfangsadresse weitergegeben werden kann und auf einem dazu passenden privaten Schlüssel, welcher höchst vertraulich aufbewahrt und nur zur Authentifizierung und Autorisierung von Zahlungsvorgängen verwendet werden sollte.[10] Jeder Nutzer kann dabei be-

---

[5] Die zumeist in Verkaufsstätten mit Bitcoin-Annahmemöglichkeit zu sehenden Bitcoin-Münzen sind auch dort lediglich zu Illustrationszwecken abgebildet.

[6] *Platzer,* Bitcoin – kurz & gut (2014), S. 17.

[7] *Schroeder*, JurPC Web-Dok. 104/2014, Abs. 1, 9; *Safferling/Rückert*, MMR 2015, 788, 789.

[8] *Kütük/Sorge*, MMR 2014, 643, 643; *Lerch*, ZBB 2015, 190, 193.

[9] *Kerscher,* Bitcoin, 2. Auflage (2014), S. 19.

[10] *Kerscher,* Bitcoin, 2. Auflage (2014), S. 54.

liebig viele Schlüsselpaare generieren.[11] Vom (weitergegebenen) öffentlichen Schlüssel können aufgrund der Komplexität des Algorithmus, der aus dem privaten den öffentlichen Schlüssel generiert, keine Rückschlüsse gezogen werden, sodass ein zumindest pseudonymer Transaktionsvorgang gewährleistet ist.[12]

III. Blockchain-Technologie

1. Blockchain

Als gemeinsamer Knotenpunkt aller Bitcoins besteht eine öffentlich einsehbare[13] chronologische Auflistung aller Vorgänge, die mit Bitcoins ausgeführt wurden („Blockchain"). Die Clients auf den Nutzercomputern sorgen über das P2P-Netzwerk für einen dauerhaften Abgleich der Blockchain untereinander. Neue Transaktionen werden zu Blöcken zusammengefasst und den bisherigen Blöcken chronologisch angefügt, sodass eine Kette der vorhandenen Blöcke („Blockchain") entsteht. Jede Transaktion erhält über den Block einen exakten Zeitstempel, sodass jederzeit gewährleistet ist, dass die Blockchain zuverlässig Auskunft darüber gibt, welcher Adresse welcher Bitcoin aktuell zugeordnet ist. Diese Auskunft ist zudem über den Zusammenhang mit den vorherigen Blöcken der Kette auch überprüfbar, da jede Transaktion der Vergangenheit einsehbar ist.[14]

2. Sicherung der Richtigkeit der Blockchain

Die Sicherheit und Richtigkeit dieser Aufzeichnung wird dadurch gewährleistet, dass die Aufnahme einer Transaktion in die Auflistung erst nach einer Überprüfung der Transaktion erfolgt. Diese Überprüfung wird dezentral durch die Nutzer durchgeführt, die ihre Rechenleistung zur Verfügung stellen und versuchen, die vom System gestellte „Rechenaufgabe" unter Verwendung eines Algorithmus zu lösen und damit die Transaktionen zu verifizieren.[15] Ziel der Rechenaufgabe ist die Erstellung eines Blocks. Inhaltlich besteht die Rechenaufgabe aus sog. „one-way-hashes". Deren Besonderheit liegt darin, dass ihre Berechnung außerordentlich kompliziert ist, ein feststehendes Ergebnis jedoch sehr einfach auf seine Richtigkeit überprüft werden kann.[16]

---

[11] *Boehm/Pesch*, MMR 2014, 75 f.
[12] *Kerscher,* Bitcoin, 2. Auflage (2014), S. 54.
[13] Abrufbar unter https://blockchain.info/.
[14] *Platzer,* Bitcoin – kurz & gut (2014), S. 21.
[15] *Kerscher,* Bitcoin, 2. Auflage (2014), S. 82 ff.
[16] *Platzer,* Bitcoin – kurz & gut (2014), S. 23.

3. Verhinderung des doppelten Ausgebens

Insbesondere liegt der Fokus darauf, bereits ausgegebene Bitcoins nicht noch einmal ausgeben zu können („double spending“).[17] Für eine Überweisung benötigt der Absender neben dem öffentlichen Schlüssel des Empfängers (als Empfangskonto) eine Signatur des Vorgangs. Zur Verifikation dieser Signatur ist lediglich eine vorher auf dem öffentlichen Schlüssel des Absenders (Absenderkonto) eingegangene Transaktion in mindestens derselben Höhe erforderlich. Der Überweisende verweist somit immer zwingend auf einen vorherigen Bitcoin-Eingang.[18] Um zu verhindern, dass ein Absender seine Signatur mehrfach verifizieren kann, kommt die Blockchain-Technologie zum Einsatz.[19] Hierbei werden alle initiierten Transaktionen über das Netzwerk an alle Teilnehmer gesendet und in Blöcken gesammelt. Die Teilnehmer können nun (freiwilllig) versuchen, einen Arbeitsbeweis („proof of work“) in Form eines komplizierten mathematischen Problems (basierend auf kryptografischen Algorithmen) zu berechnen.[20] Bei erfolgreicher Berechnung sendet der Teilnehmer den Block inklusive Arbeitsbeweis an alle anderen Teilnehmer. Der Erfolg, den Arbeitsbeweis als erstes zu erbringen, hängt maßgeblich von der durch den Teilnehmer eingesetzten Rechnerleistung ab; je mehr Leistung er einsetzt, desto höher ist die statistische Wahrscheinlichkeit der erfolgreichen ersten Verifikation. Der betriebene Aufwand besteht dabei neben dem Einsatz von Geld für die ausreichende Hardware-Ausstattung auch in den Stromkosten für den Rechnerbetrieb.[21] Beachtlich ist daneben, dass die aufzuwendende Rechnerleistung mit steigender Anzahl der Bitcoins durch die erhöhte Komplexität der Rechenaufgaben ebenfalls ansteigt.[22] Dem Anstieg der Komplexität liegt die Verengung der Parameter, innerhalb derer das Ergebnis der Rechenaufgabe liegen darf, zugrunde.[23] Der durch einen Teilnehmer bestätigte Block wird an die anderen Netzwerkteilnehmer gesendet, welche wiederum versuchen können, weitere Blöcke zu errechnen und darauf aufzubauen.[24] Dadurch, dass der Block jeweils auch die Verlaufsgeschichte der vorangegangen Transaktionen enthält, entstehen Ketten von Transaktionsblöcken. Die

---

[17] *Safferling/Rückert*, MMR 2015, 788, 790.

[18] *Sorge/Krohn-Grimberghe*, DuD 2012, 479, 480.

[19] *Sorge/Krohn-Grimberghe*, DuD 2012, 479, 480.

[20] *Safferling/Rückert*, MMR 2015, 788, 790; *Beck*, NJW 2015, 580, 581; *Boehm/Pesch*, MMR 2014, 75, 76.

[21] *Kuhlmann*, CR 2014, 691, 692.

[22] *Djazayeri*, jurisPR-BKR 6/2014, 1; *Hafke*, in: Herausforderungen an Staat und Verfassung (2015), 106, 109.

[23] *Beck*, NJW 2015, 580, 581.

[24] *Safferling/Rückert*, MMR 2015, 788, 790.

längste Kette gilt als die korrekte und findet Eingang in die Blockchain.[25] Für Manipulationen an einer Transaktion müsste ein Angreifer folglich den betreffenden Block modifizieren und inklusive seiner gesamten Kette neu berechnen, bevor das Kollektiv der anderen Nutzer weitere Blöcke an die längste Kette anhängt.[26] Das Bitcoin-Netzwerk sieht eine Transaktion als vollständig abgeschlossen und unumkehrbar an, wenn mindestens sechs weitere Blöcke auf ihr aufbauen.[27] Jeder Bitcoin besteht folglich aus einer langen Kette digitaler Signaturen.[28] Die Technologie basiert damit auf dem Vertrauen, dass alle redlichen Teilnehmer zusammen mehr Rechnerleistung zur Verifikation aufbringen können, als ein einzelner Teilnehmer zur Manipulation.[29]

4. Belohnung für die Verifikation eines Blocks

Als Belohnung erhält der erste, der den gesamten Block verifiziert hat, Bitcoins gutgeschrieben („mining"). Für den o.g. Arbeitsbeweis werden der schnellsten Rechnereinheit eine bestimme Menge Bitcoins als Prämie zugewiesen.[30] Der hinter den Aufgaben stehende Algorithmus ist allerdings derart konzipiert, dass sich mit steigender Anzahl der bereits erzeugten Bitcoins die Parameter für die Lösung der Rechenaufgabe verengen und damit die Berechnung komplexer und langwieriger wird.[31] Einer inflationären Ausschüttung von Bitcoins wirkt auch entgegen, dass die Emission einer Belohnung nur ungefähr alle zehn Minuten stattfindet.[32] Zusätzlich wird die Belohnung in regelmäßigen Abständen verringert. Hintergrund dieses Konzepts ist die vom Netzwerk vorgegebene Höchstzahl von 21 Millionen Bitcoins.

5. Anderweitige Nutzung der Blockchain-Technolgie

Die Blockchain-Technologie, die das Herzstück der Funktionsweise der Bitcoins darstellt, wurde einerseits vielfach von Bitcoin-Nachahmern (z. B. Litecoin, Dogecoin) imitiert. Diese virtuellen Gelder weichen in ihrer Funktionsweise meist nur minimal vom Original ab.[33]

---

[25] *Safferling/Rückert*, MMR 2015, 788, 790; *Sorge/Krohn-Grimberghe*, DuD 2012, 479, 480.
[26] *Sorge/Krohn-Grimberghe*, DuD 2012, 479, 480.
[27] *Kerscher,* Bitcoin, 2. Auflage (2014), S. 58.
[28] *Lerch*, ZBB 2015, 190, 194.
[29] *Kütük/Sorge*, MMR 2014, 643, 644.
[30] *Schroeder*, JurPC Web-Dok. 104/2014, Abs. 1, 13.
[31] *Beck*, NJW 2015, 580, 582.
[32] *Kuhlmann*, CR 2014, 691, 692.
[33] *Kerscher,* Bitcoin, 2. Auflage (2014), S. 47.

Andererseits haben sich zahlreiche Finanzunternehmen (z. B. Goldman Sachs, J.P. Morgan, Barclays, Credit Suisse u.v.m.) zur R3-Gruppe (R3Cev)[34] zusammengeschlossen, um herauszufinden, inwieweit die Blockchain-Technologie auch für Banken genutzt werden kann. Die Vorteile sehen die dort mitarbeitenden Finanzmarktexperten unter der Leitung des Gründers David Rutter in dem enormen Potential von Transaktionskosteneinsparungen, Fehlerreduktion und Sicherheitszuwachs.[35] Elf Großbanken haben in einem abgeschlossenen, weltumspannenden Blockchain-Netzwerk auch bereits erste Finanztransaktionen ausgeführt.[36] Entscheidender Unterschied in der forschenden Entwicklung eines Blockchain-Konzepts der Banken ist jedoch die Schaffung einer zentralen Verwaltungsstelle. In Rede steht dabei auch die Schaffung eines Netzwerks, das zwar öffentlich ist, jedoch nur für bestimmte, zuvor zugelassene Nutzer.[37]

Auch die Bundesregierung hat im September 2019 unter Zusammenarbeit des Bundesministeriums für Wirtschaft und Energie und des Bundesministeriums der Finanzen eine Strategie zum weiteren Umgang mit der Blockchain-Technologie veröffentlicht.[38] Ein Schwerpunkt in der Erarbeitung soll u. a. darin liegen, verlässliche Rahmenbedingungen für eine hinreichende Investitionssicherheit zu bieten, ohne die Blockchain-Technologie gegenüber anderen Technologien zu benachteiligen oder zu bevorzugen.[39]

Verwendung kann die Technologie auch im Bereich von „smart contracts" finden. Dabei kann auf Basis der Blockchain-Technologie ein Mechanismus programmiert werden, der bei dem Eintritt definierter Bedingungen manipulationssicher eine Reaktion ausführt. Möglich wäre damit beispielsweise die Festlegung, unter welcher zuvor definierten (logischen) Bedingung eine Waschmaschine autonom den Kauf von Waschpulver bei einem Onlinehändler aus-

---

[34] *New York Times*, Bitcoin Technology Piques Interest on Wall St., Artikel vom 28.08.2015, abrufbar unter http://www.nytimes.com/2015/08/31/business/dealbook/bitcoin-technology-piques-interest-on-wall-st.html?_r=0.

[35] *Reuters*, Nine of world's biggest banks join to form blockchain partnership, Artikel vom 15.09.2015, abrufbar unter http://www.reuters.com/article/us-banks-blockchain-idUSKCN0RF24M20150915.

[36] *Frankfurter Allgemeine Zeitung,* Digitale Währung: Das Geld der Zukunft, http://www.faz.net/aktuell/finanzen/digital-bezahlen/blockchain-heisst-die-technik-hinter-der-internetwaehrung-bitcoin-14063245.html.

[37] *Coindesk*, Beyond Banking: R3's Expanding Vision for Global Blockchain, Artikel vom 13.04.2018, abrufbar unter https://www.coindesk.com/beyond-banking-r3-expanding-vision-global-blockchain.

[38] *Bundesministerium für Wirtschaft und Energie*, Blockchain-Strategie der Bundesregierung, abrufbar unter https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/blockchain-strategie.pdf?__blob=publicationFile&v=10.

[39] *Bundesministerium für Wirtschaft und Energie*, Blockchain-Strategie der Bundesregierung, S. 12 f.

Sachregister