EDUARD HOFERT

Regulierung der Blockchains

Internet und Gesellschaft
14

Mohr Siebeck

Internet und Gesellschaft

Schriften des Alexander von Humboldt Institut
für Internet und Gesellschaft

Herausgegeben von

Jeanette Hofmann, Ingolf Pernice,
Thomas Schildhauer und Wolfgang Schulz

14

Eduard Hofert

Regulierung der Blockchains

Hoheitliche Steuerung der Netzwerke im Zahlungskontext

Mohr Siebeck

Eduard Hofert, geboren 1988; Studium der Rechtswissenschaften an der Universität Hamburg; 2018 Promotion; derzeit Rechtsreferendar am Hanseatischen Oberlandesgericht Hamburg.

ISBN 978-3-16-156391-1 / eISBN 978-3-16-156459-8
DOI 10.1628/978-3-16-156459-8

ISSN 2199-0344 / eISSN 2569-4081 (Internet und Gesellschaft)

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliographie; detaillierte bibliographische Daten sind im Internet über *http://dnb.dnb.de* abrufbar.

Das Buch wurde von epline in Böblingen aus der Times New Roman gesetzt und von Gulde-Druck in Tübingen auf alterungsbeständiges Werkdruckpapier gedruckt und gebunden.

Printed in Germany.

Vorwort

Die vorliegende Arbeit wurde Wintersemester 2017/2018 von der Fakultät für Rechtswissenschaften der Universität Hamburg als Dissertation angenommen und anschließend im Hinblick auf die Drucklegung auf den Stand März 2018 aktualisiert. Ein ganz besonderer Dank gilt meinem Doktorvater Herrn Prof. Dr. Roland Broemel. Seine wertvollen Ratschläge und der konstruktive Austausch in sämtlichen Phasen der Promotion haben erheblich zum Gelingen der Arbeit beigetragen. Außerdem möchte ich Frau Prof. Dr. Marion Albers für die zügige Erstellung des Zweitgutachtens danken.

Ferner gilt mein Dank dem Verlag Mohr Siebeck, insbesondere Frau Daniela Taudt, sowie Herrn Prof. Dr. Ingolf Pernice und Herrn Jörg Pohle für ihre hilfreichen Hinweise. Für die vielen anregenden Gespräche und Bemerkungen von technischer Seite danke ich Alexander Bassmanow.

Ganz besonders bedanken möchte ich mich bei meiner Mutter für ihre Unterstützung. Ihr ist dieses Buch gewidmet.

Hamburg, im Juli 2018 Eduard Hofert

Inhaltsübersicht

Inhaltsverzeichnis

Abkürzungsverzeichnis

ABl.	Amtsblatt
AEUV	Vertrag über die Arbeitsweise der europäischen Union
AML	Anti-money laundering
AnlEntG	Anlegerentschädigungsgesetz
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BaFöG	Bundegesetz über individuelle Förderung der Ausbildung
BBankG	Gesetz über die Deutsche Bundesbank
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BörsenG	Börsengesetz
BSI-Gesetz	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
BT-Drs.	Bundestagsdrucksache
BTC	Bitcoin
BVerfGE	Sammlung der Entscheidungen des Bundesverfassungsgerichts
CFT	Countering the financing of terrorism
CRR	Capital Requirements Regulation
DAO	Decentralized Autonomous Organisation
DepotG	Gesetz über die Verwahrung und Anschaffung von Wertpapieren
DNS	Domainnamensystem
EBA	Europäische Bankenaufsichtsbehörde
EinSiG	Einlagensicherungsgesetz
ESZB-Satzung	Protokoll über die Satzung des Europäischen Systems der Zentralbanken und der Europäischen Zentralbank
EZB	Europäische Zentralbank
FATF	Financial Action Task Force on Money Laundering
GBO	Grundbuchordnung
GG	Grundgesetz
GrCh	Charta der Grundrechte der Europäischen Union
HGB	Handelsgesetzbuch
ICANN	Internet Corporation for Assigned Names and Numbers
IWF	Internationaler Währungsfonds
KWG	Gesetz über das Kreditwesen
MaKonV	Verordnung zur Konkretisierung des Verbotes der Marktmanipulation
NSI	Network Solutions Incorporated
OTC	Over the counter
RGBl.	Reichsgesetzblatt
TCP/IP	Transmission Control Protocol/Internet Protocol
UDRP	Uniform Domain-Name Dispute-Resolution Policy
UrhG	Gesetz über Urheberrecht und verwandte Schutzrechte

VC	Virtual Currency
VCS	Virtual Currency Schemes
WpHG	Gesetz über den Wertpapierhandel
ZAG	Gesetz über die Beaufsichtigung von Zahlungsdiensten
ZIEV	Verordnung über die angemessene Eigenkapitalausstattung von Zahlungsinstituten und E-Geld-Instituten nach dem Zahlungsdiensteaufsichtsgesetz

A. Einleitung

Ein Blick auf die junge Geschichte der Blockchains zeigt, dass die rechtliche Diskussion und die Fortentwicklung der Technologie in ausgeprägter Form von Narrativen beeinflusst werden.[1] Der Ausgangspunkt der Entwicklungen ist die sogenannte Cypherpunk-Bewegung und deren Bemühungen, ein kryptografisches Zahlungssystem für das Internet zu entwickeln.[2] Vor diesem Hintergrund wurde die Blockchain-Technologie im Jahre 2008 unter dem Pseudonym „Satoshi Nakamoto"[3] als „Peer-to-Peer Electronic Cash System" in Form der Kryptowährung Bitcoin veröffentlicht.[4] Im Vordergrund stand der Gedanke eines staatlich nicht manipulierbaren, monetären Nebenkreislaufs bzw. der Idee eines „entstaatlichten Geldes" abseits konventioneller Intermediation in der Wirtschaft.[5] Der Leitgedanke des Projekts folgte auch aus dem Code der ersten Transaktion des Systems, die im sogenannten „Genesis-Block" archiviert eine Referenz auf den Artikel einer britischen Tageszeitung zur sich anbahnenden Eurokrise enthält: „Chancellor on Brink of Second Bailout for Banks".[6] Abseits derartiger wirtschaftsphilosophischer Erwägungen kann die Blockchain-Technologie bereits im Nutzungskontext des Zahlungsverkehrs signifikante Effizienzsteigerungen in der Wirtschaft bewirken.[7] Kosten für die Infrastruktur

---

[1] Siehe auch *Fairfield*, 88 S. Cal. L. Rev. (2015), 805, 829 ff.

[2] Siehe hierzu nur *Eric Hughes*, A Cypherpunk's Manifesto, 1993, unter https://w2.eff.org/Privacy/Crypto/Crypto_misc/cypherpunk.manifesto (alle genannten Internetseiten wurden zuletzt am 14. 01. 2017 abgerufen): „We the Cypherpunks are dedicated to building anonymous systems. We are defending our privacy with cryptography, with anonymous mail forwarding systems, with digital signatures, and with electronic money."

[3] Es ist nach wie vor ungeklärt, welche Person oder Gruppe hinter dem Pseudonym „Satoshi Nakamoto" steht. Siehe hierzu nur *Kirby*, 93 N. C. L. Rev. (2014), 189, 192; *Doguet*, 73 La. L. Rev. (2013), 1119, 1120; *Burge*, 67 Hastings L. J. (2016), 1493, 1528 f.; *Kulms*, 51 Pravo i privreda 4–6 (2014), 288, 294.

[4] *Satoshi Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, unter https://bitcoin.org/bitcoin.pdf.

[5] Auf die Übereinstimmungen des Konzepts mit der sogenannten Österreichischen Schule der Ökonomie verweisen *Lerch*, ZBB 2015, 190, 203 und *Groshoff*, 5 Wm. & Mary Bus. L. Rev. (2014), 489, 506 ff.

[6] Siehe für die Referenz auf den Artikel aus der britischen Tageszeitung „The Times" vom 03. 09. 2009 Bitcoin Wiki, Genesis block, unter https://en.bitcoin.it/wiki/Genesis_block.

[7] Finanzinstitute könnten mit der Nutzung der Blockchain-Technologie alleine im Bereich der Compliance Schätzungen zufolge Kosten in Höhe von bis zu 20 Milliarden Dollar im Jahr auf globaler Ebene einsparen: *Schneider et al.*, Blockchain: Putting Theory into Prac-

und Verluste in der Umlaufgeschwindigkeit ergeben sich derzeit insbesondere aus der komplexen Struktur des globalen Zahlungsverkehrs. Transaktionen werden von einer Vielzahl von Intermediären in unterschiedlichen Jurisdiktionen prozessiert, deren Register aufwendig miteinander im Einklang gehalten werden müssen.[8] Im Kern adressiert das Bitcoin-Konzept diese Ineffizienzen, indem es die Notwendigkeit zentraler Registrars im Kontext des elektronischen Zahlungsverkehrs beseitigt. Die Integrität des System soll ersatzweise über den Algorithmus gewährleistet werden: „What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party."[9] Die Entwickler des verteilten Transaktionsraums zielten in dieser Form darauf ab, ein funktionelles Äquivalent zum komplexen normativen System des (körperlosen) Buch- und E-Geldes zu schaffen, dessen Grundlage einerseits ein strenges hoheitliches Regulierungsregime – insbesondere in Form der Geldmengensteuerung über dezidierte Kapitalanforderungen – und andererseits ein dichtes Vertragsgeflecht im Interbankenverhältnis, aber auch im Verhältnis zwischen den Intermediären und den Institutskunden bildet. Pointiert lässt sich das Konzept der Kryptowährung Bitcoin mittels des Oxymorons „Trustless Trust"[10] beschreiben. Einerseits stellt das Vertrauen in den Blockchain-Code eine wesentliche Funktionsbedingung der Systeme dar. Andererseits beseitigt die Blockchain-Governance die im Zusammenhang mit der Integrität der Infrastrukturträger (Staat oder Wirtschaftssubjekte) stehende Vertrauenssensibilität der Systeme.[11] Die Integrität einer Blockchain-Transaktion folgt bereits aus der technischen Programmierung des Systems, ohne dass es auf die Vertrauenswürdigkeit einzelner Teilnehmer ankommt.[12]

Satoshi Nakamotos Papier setzt den Fokus somit zwar auf die Anwendung der Technologie im Zahlungsverkehr. Die Tragweite seines Konzepts geht allerdings weit über den monetären Bereich hinaus. Der Entwickler beschreibt

---

tice, Goldman Sachs Equity Research Report, 2016, S. 5, unter http://www.the-blockchain.com/docs/Goldman-Sachs-report-Blockchain-Putting-Theory-into-Practice.pdf; Wild et al., Technology: Banks seek the key to blockchain, Financial Times Online, 01. 11. 2015, abrufbar unter: https://www.ft.com/content/eb1f8256-7b4b-11e5-a1fe-567b37f80b64.

[8] Siehe *Werbach*, Trustless Trust, S. 34 f.

[9] *Satoshi Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008 (Fn. 4, in diesem Abschnitt), S. 1.

[10] *Reid Hofman*, The Future of the Bitcoin Ecosystem and "Trustless Trust" – Why I Invested in Blockstream, LinkedIn Pulse, 17. 11. 2014, unter https://www.linkedin.com/pulse/20141117154558-1213-the-future-of-the-bitcoin-ecosystem-and-trustless-trust-why-i-invested-in-blockstream.

[11] Siehe *Werbach*, Trustless Trust, S. 37 f.

[12] *Nick Szabo*, The Dawn of Trustworthy Computing, Unenumerated, 11. 12. 2014, unter http://unenumerated.blogspot.de/2014/12/the-dawn-of-trustworthy-computing.html: "Trust-minimized code means you can trust the code without trusting the owners of any particular remote computer."

als Grundlage der Kryptowährung die „Blockchain“[13] oder „Decentralized Ledger Technology“[14] bzw. „Distributed Ledger Technology“[15] genannte Technik nicht-proprietärer Governance im Internet.[16] Allgemein betrachtet generiert die Blockchain-Governance lediglich die Entscheidung darüber, ob eine Nachricht zwischen zwei Blockchain-Adressen übermittelt und dann registriert werden soll oder nicht.[17] Das kann ein Zahlungsvorgang sein. Zwingend ist dies allerdings nicht. Im Fall der Autorisierung durch das Netzwerk wird eine Rechnungseinheit[18] der betreffenden Blockchain-Adresse zugewiesen, um die Transaktion zu determinieren. Der Eintrag in der allgemein zugänglichen Blockchain gibt den Vorgang wieder. Blockchains lassen sich auf dieser Ebene als „Kontoauszüge“ für Erklärungen zwischen Computern beschreiben.[19] Die Durchschlagskraft der Technologie folgt daraus, dass die Entscheidungen nunmehr in verteilter Form von der Allgemeinheit getroffen werden können.[20] Ver-

[13] Siehe für die Einführung der verteilten Registerführung in die juristische Diskussion etwa *Kaulartz*, Die Blockchain-Technologie, CR 2016, 474–480 oder *Fairfield*, Bitproperty, 88 S. Cal. L. Rev. (2015), 805–874.

[14] Siehe für den Begriff *Reyes*, Moving Beyond Bitcoin to an Endogenous Theory of Decentralized Ledger Technology Regulation: An Initial Proposal, 61 Vill. L. Rev. (2016), 191–234; Weltwirtschaftsforum, The future of financial infrastructure – An ambitious look at how blockchain can reshape financial services, 2016, unter http://www3.weforum.org/docs/WEF_The_future_of_financial_infrastructure.pdf.

[15] Eingehend Kaulartz, CR 2016, 474.

[16] *Satoshi Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008 (Fn. 4, in diesem Abschnitt), S. 2 ff.

[17] Voraussetzung ist lediglich, dass der Anweisende über das notwendige Zugriffsrecht zu den seiner Adresse zugewiesenen Rechnungseinheiten verfügt. Die Nachrichten, dazu sogleich mehr, können in Verbindung mit den Rechnungseinheiten anderen Adressen zugesendet werden.

[18] Gegebenenfalls werden Meta-Daten mit der Rechnungseinheit verbunden, etwa eine Kennziffer, die auf ein bestimmtes digitales Gut verweist. Die Transaktion kann etwa lauten, dass das Wertpapier X von der Blockchain-Adresse 1 auf die Blockchain-Adresse 2 übertragen wird. Hierzu transferiert der Inhaber des Zugriffsrechts zur Adresse 1 eine diesem Punkt zugewiesene Rechnungseinheit in Verbindung mit dem Meta-Datum Inhaberschaft an Wertpapier X an den Inhaber des Zugriffsrechts zur Adresse 2.

[19] Treffend *Kaulartz/Heckmann*, CR 2016, 618, 619.

[20] Ferner lässt sich eine verteilte Registerführung in geschlossener Form organisieren, was von dem ursprünglichen Blockchain-Konzept Bitcoins abweicht. Es handelt sich dann um sogenannte „permissioned ledgers“. Derartige Datenbanken verfügen zwar über eine mit Bitcoin vergleichbare, verteilte Datenstruktur, so dass jede Entität des Netzwerks als Registrar agiert, dennoch voneinander abweichende Register technisch ausgeschlossen und somit keine Verrechnungseinheiten erforderlich sind. Sie müssen allerdings nicht zwingend in Form einer Blockchain ausgestaltet sein. Die Kontrolle über das Register obliegt dann etwa Zentralbanken oder Unternehmensgruppen. Der Zugang zum Register kann bei dieser Ausgestaltung beschränkt sein – die Identität der Teilnehmer ist im Rahmen dieser Variante bekannt. Der Vorteil liegt darin, dass die Notwendigkeit einer zentralen Clearing-Stelle entfällt. Auch diese Erscheinungsform wird in der vorliegenden Arbeit analysiert, wenngleich, erstens, die Herausforderungen an den Staat hier gegenüber verteilten Registern weniger signifikant und, zweitens, die Abweichungen zu konventionellen Registern wie dem Buchgeld-System oder Grundbüchern geringer sind. Viele (öffentlich-rechtliche) Regulierungsfragen resultieren gerade aus

teilte Registerführung scheiterte bislang am sogenannten Double-spending-Problem. Die Funktionsfähigkeit eines Registers ist nur dann gewährleistet, wenn der Absender einer Transaktion über den betreffenden Wert nicht mehrfach verfügen kann oder wie Satoshi Nakamoto es im Kontext der Kryptowährung Bitcoin formuliert: „The problem of course is the payee can't verify that one of the owners did not double-spend the coin".[21] Das Problem folgt schon daraus, dass digitale Güter wie Musikdateien oder eben Einträge in Datenbanken sich nahezu ohne Grenzkosten duplizieren lassen.[22] Die Möglichkeit der Duplikation eines Registereintrags in der Form, dass der Absender den virtuellen Wert mehrfach an unterschiedliche Empfänger transferiert, stellt die Integrität des Systems in Frage. Die Aufgabe eines Registers, „[…] to resolve competing claims to the same item or interest"[23], kann vor diesem Hintergrund nicht mehr erfüllt werden. In konventionellen Systemen gewährleistet eine zentrale Administration die Integrität.[24] Blockchains entgegnen Manipulationsversuchen der beschriebenen Art mittels einer neuartigen Form verteilter Koordination. Die Ausgestaltung der Blockchains wirkt auf den ersten Blick paradox: Einerseits zeigt sich eine *logische* Zentralisierung in der Form, dass im jeweiligen System lediglich eine Version des Registers Gültigkeit besitzt. Andererseits ist die *Koordination* der Transaktionsräume in der Hinsicht verteilt ausgestaltet, als jeder Teilnehmer über die Möglichkeit verfügt, eine Kopie der Blockchain zu erhalten und das Register um weitere Vorgänge zu ergänzen.[25] Die mittels Blockchain-Technik bewältigte Hürde liegt in der Synchronisation der in den Netzwerken kommunizierten Register-Versionen.[26]

Auf dieser Grundlage ist etwa die Allokation von (digitalen) Vermögenswerten in verteilter Form realisierbar, ohne dass auf hoheitliche Vollstreckungsmechanismen oder einen registerführenden Intermediär zurückgegriffen werden

---

der nicht-proprietären Internet-Governance *offener* Blockchains. Siehe für die Unterscheidung zwischen offenen und zugangspflichtigen Registersystemen (Blockchains oder allgemeiner: „distributed ledgers") z. B. *Werbach*, Trustless Trust, S. 23, Fn. 109; *Swanson*, Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems.

[21] *Satoshi Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008 (Fn. 4, in diesem Abschnitt), S. 2.

[22] *Fairfield*, 88 S. Cal. L. Rev. (2015), 805, 817.

[23] Siehe für Grundanforderungen an Registersysteme *Frisch*, 72 Iowa L. Rev. (1987), 531, 531.

[24] In dieser Hinsicht lässt sich eine Vielzahl an Beispielen nennen, etwa die amtliche Administration von Grundbüchern oder die Intermediation der Kreditinstitute im Giralgeld-System. Siehe nur *Fairfield*, 88 S. Cal. L. Rev. (2015), 805, 817 ff.; *Kaplanov*, 25 Loy. Consumer L. Rev. (2012), 111, 117 f.

[25] Siehe für die Unterscheidung zwischen logischer Zentralisierung und organisatorischer Verteilung der Netzwerke *Albert Wenger*, Bitcoin: Clarifying the Foundational Innovation of the Blockchain, Continuations, 15. 12. 2014, unter http://continuations.com/post/105272022635/bitcoin-clarifying-the-foundational-innovation-of.

[26] Siehe *Werbach*, Trustless Trust, S. 23 ff.

muss.[27] Blockchains bieten den Nutzern die Möglichkeit, Vereinbarungen wie Kaufverträge im E-Commerce, Ereignisse wie Warenlieferungen oder Rechtsverhältnisse wie Nutzungsrechte an Musikwerken eingriffssicher in einer öffentlichen Datenbank festzuhalten.[28] Vor diesem Hintergrund ist darauf hinzuweisen, dass eine begriffliche Differenzierung zwischen „virtuellen Währungen" oder „Kryptowährungen" und „Blockchains" erforderlich ist, die etwa im System Ethereum aufgegriffen wird. Die *Ethereum*-Blockchain wird von der Kryptowährung *Ether* unterschieden, wobei das zweitgenannte Element einen wesentlichen Bestandteil des erstgenannten bildet.[29] Die vorliegende Untersuchung wird sich mit der Notwendigkeit systemimmanenten Geldes in der Blockchain-Governance auseinandersetzen.[30] Der Begriff „virtuelle Währung"[31] liegt insofern nah, als das Protokoll des Systems im Hinblick auf dieses Teilelement mit dem normativen Konstrukt der hoheitlichen Regulierung des Geldwesens vergleichbar ist. In beiden Fällen soll das Regelwerk den monetären Kreislauf ausgestalten und als Grundlage für die Wertstabilisierung des Geldes dienen. Der Begriff „Kryptowährung" wird in der Regel synonym verwendet[32] und rekurriert auf das basale Element der asymmetrischen Kryptografie, das den Transaktionsräumen zugrunde liegt. Der Begriff „Blockchain" beschreibt hingegen das verteilte Registersystem, welches, wie oben beschrieben, nicht nur für Zahlungsvorgänge genutzt werden kann, sondern gerade anwendungsoffen ausgestaltet ist.[33] Kryptowährungen und verteilte Blockchain-Governance sind somit zwar voneinander zu unterscheiden, ohne allerdings den funktionalen Zusammenhang zwischen den beiden Elementen auszublenden.

Einträge in der Blockchain sind vor diesem Hintergrund differenziert zu betrachten. Transaktionen können sich auf *physische* Güter beziehen und etwa den Lieferweg eines Arzneimittels wiedergeben, um die stoffliche Identität oder

---

[27] *Abramowicz*, 58 Ariz. L. Rev. (2016), 359, 361: „But what makes Bitcoin remarkable is that it settles the most controversial issue – who owns wealth – without need for a law enforcement apparatus."

[28] Siehe für Anschauungsbeispiele der Blockchain-Technologie *Wright/De Filippi*, Decentralized Blockchain Technology and the Rise of Lex Cryptographia.

[29] Siehe für die Unterscheidung https://www.ethereum.org/ether. Offene Blockchains funktionieren lediglich auf Basis systemimmanenten Geld und enthalten somit einen eigenen „Geldkreislauf". Die Auseinandersetzung mit den technischen Wesenszügen der verteilten Register wird den Zusammenhang illustrieren.

[30] Siehe hierzu insbesondere S. 14 ff. für die technische Funktionsweise offener Blockchains und S. 25 ff. für eine Auseinandersetzung mit der Governance-Struktur der Systeme im Kontext der nicht-propietären Resourcen-Allokation Elinor Ostroms.

[31] Der Begriff der Währung beschreibt „die Gesamtheit des der Bundesrepublik zuzurechnenden Geldes", siehe z. B. *Uhle*, in: Maunz/Dürig, GG, 81. Ergänzungslieferung, Art. 73, Text bei und Verweis in Fn. 6.

[32] Siehe *Burge*, 67 Hastings L. J. (2016), 1493, 1528; *Lee et al.*, 16 Bus. L. Int'l (2015), 21, 21.

[33] Siehe auch *Abramowicz*, 58 Ariz. L. Rev. (2016), 359, 361.

den Ursprung eines zulassungspflichtigen Medizinprodukts sicherzustellen.[34] Ferner können sie die Inhaberschaft an *virtuellen* Ressourcen wie etwa Derivaten oder anderen Wertpapieren anzeigen. In zweitgenannter Hinsicht sind digitale „Börsengänge"[35] in Form der „Intial Coin Offerings" in aller Munde.[36] Der Umstand, dass Blockchains sich nicht eindimensional als Zahlungssysteme und Blockchain-Transaktionen nicht in jedem Fall als Zahlungsvorgänge klassifizieren lassen, bedeutet allerdings nicht, dass die bisherige (juristische) Diskussion um die Einordnung des Phänomens ins Leere läuft. Die Fragestellungen sind allerdings stets im Kontext der betreffenden Anwendung zu formulieren. Bitcoins *können* etwa „als Tausch- bzw. Zahlungsmittel zum Erwerb von Waren wie auch zur Beschaffung von Gebrauchs- oder sonstigen Nutzungsvorteilen eingesetzt werden."[37] Die Bitcoin-Blockchain wird in diesem Verwendungskontext als Zahlungsraum beansprucht. Dann stellt sich etwa die Frage nach der vertragstypologischen Einordnung der Rechtsbeziehung zwischen den Vertragsparteien.[38] Oder es stellt sich die allgemeinere Frage, wie Bitcoins oder andere Kryptowährungen in diesem Zusammenhang als Gegenstand von sekundären Leistungspflichten zu behandeln sind.[39] Im Schuldrecht steht bei der Klassifizierung der Parteiwille und die Privatautonomie im Vordergrund.[40]

Im Aufsichtsrecht verhindert eine differenzierte Sichtweise die Herausbildung eines sachfremden Regimes.[41] Die Diskussion um den rechtlichen Umgang mit der Technologie knüpfte zunächst an die von Satoshi Nakamoto hervorgehobene Finanzierungsfunktion der Systeme sowie das Ökosystem um die Kryptowährungen an.[42] Tatsächlich zeigt sich in diesem Zusammenhang ein nicht unerheblicher Regulierungsbedarf, der in der vorliegenden Untersuchung herausgestellt wird. Dass die Rechnungseinheiten kapitalintensiver Systeme wie Bitcoin dazu geeignet sind, dem Inhaber abstrakte, unkörperliche Vermögensmacht zu verschaffen,[43] lässt sich nicht von der Hand weisen.[44] Vor

---

[34] Dazu *Lantz*, TEDxHamburg, New Kids on the Blockchain, 2016, unter http://www.tedxhamburg.de/lorne-lantz-new-kids-on-the-blockchain.

[35] *Vogel et al.*, AG 2017, R333.

[36] Eingehend *Hacker/Thomale*, Crypto-Securities Regulation; anderen Crowdfunding-Modi gegenüberstellend *Borkert*, ITRB 2018, 39.

[37] *Beck/König*, JZ 2015, 130, 133 ff.

[38] Dieser Fragestellung widmen sich etwa *Beck/König*, JZ 2015, 130, 133 ff.; *Spindler/Bille*, WM 2014, 1357, 1362 f.; *Engelhardt/Klein*, MMR 2014, 355, 358 f.

[39] Hierzu *Beck/König*, AcP 215 (2015), 655 ff. Ferner geht *Beck*, NJW 2015, 580 ff. der Frage nach, ob sich Bitcoins als Geld im rechtlichen Sinne klassifizieren lassen.

[40] *Beck/König*, JZ 2015, 130, 133 ff.; *Beck*, NJW 2015, 580, 585 f.

[41] Siehe auch *Fairfield*, 88 S. Cal. L. Rev. (2015), 805, 869 f.

[42] Siehe nur *Reyes*, 61 Vill. L. Rev. (2016), 191, 194, 203, 221 ff.; *Fairfield*, 88 S. Cal. L. Rev. (2015), 805, 829 ff., Verweise in Fn. 7.

[43] In dieser Form wird im vertragstypologischen Kontext der (rechtliche) Begriff des Geldes ausgefüllt. Siehe hierzu etwa *Isele*, AcP 129 (1928), 129, 181; *Simitis*, AcP 159 (1960), 406, 443; *Hahn/Häde*, Währungsrecht, S. 19.

[44] So auch *Beck/König*, JZ 2015, 130, 136; *Beck*, NJW 2015, 580, 582 ff.

diesem Hintergrund setzt die Arbeit den Fokus auf die Verwendung der Blockchain-Technologie im Finanzsystem. Die Frage in diesem Zusammenhang ist, ob die gegenwärtig überwiegende Differenzierung zwischen Finanzdienstleistungen in Bezug auf hoheitliches Geld und Finanzdienstleistungen, die an virtuelle Währungen anknüpfen, einer Korrektur bedarf. Ferner stellt sich die Frage, inwieweit in dieser Hinsicht die Blockchain-Governance selbst von hoheitlicher Seite zu adressieren ist.[45]

Die Untersuchung steht vor dem Hintergrund eines wachsenden Marktes blockchainbasierter Finanzierungsdienste unterschiedlicher Art. Das Ökosystem weist möglicherweise ein Risikopotential auf, das von hoheitlicher Seite adressiert werden sollte. Kryptowährungen basieren auf grundlegender Ebene auf einem verteilten Netzwerk zwischen den Teilnehmern des Systems, in dessen Rahmen (auf Grundlage der betreffenden Blockchain) Transaktionen verifiziert werden und virtuelles Geld emittiert wird. Die Bedeutung der Blockchain-Technologie in diesem Anwendungskontext zeigen die vielfältigen auf Kryptowährungen basierenden Geschäftsmodelle, die im weiten Sinne den Transaktionssystemen zugerechnet werden können.[46]

Den Finanzdienstleistungen mit virtuellem Geld liegt in aller Regel eine elektronische Geldbörse (sogenannte „*wallet*“) zugrunde. Hierbei handelt es sich um eine unmittelbar mit der Blockchain verbundene Applikation, welche als Depot oder algorithmisches Kontokorrent beschrieben werden kann. „Wallets“ werden zum Teil auch als eigenständige Dienstleistungen angeboten. Die Anbieter derartiger Dienste werden „*wallet provider*“ genannt.[47] Der Nutzer einer Kryptowährung kann allerdings im Kontrast zu konventionellen Geldsystemen auf die Einschaltung eines Intermediärs verzichten und auf eine dezentrale Applikation zurückgreifen, die er etwa auf dem eigenen Computer oder im Webbrowser einrichtet.[48] In dieser Hinsicht kann von dezentralen „wallets“ gesprochen werden. Der Nutzer verfügt bei dieser Verwahrmethode die volle Kontrolle über das virtuelle Geld. Nichtsdestotrotz begründet die Inanspruchnahme von zentralen Wallet-Anbietern, also zentralen Verwahrmethoden, zahlreiche Vorteile, so dass es einerseits nicht überrascht, dass ein entsprechendes Nachfragepotential bereits zu beobachten ist, und andererseits damit weiter-

[45] Die Europäische Bankenaufsichtsbehörde etwa hat nicht nur die Ausweitung der Finanzaufsicht auf Intermediäre auf dem Markt der Kryptowährungen gefordert, sondern darüber hinaus hoheitliche Akte in Bezug auf die verteilten Systeme selbst. Siehe für die Regulierungsidee der Behörde S. 73 ff.

[46] *Lerch*, ZBB 2015, 190, 194.

[47] Siehe hierzu EBA, Opinion on „virtual currencies“, 2014, S. 15, Ziff. 39, unter https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf; EZB, Virtual currency schemes – a further analysis, 2015, S. 8, unter https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf.

[48] Siehe EZB, Virtual currency schemes – a further analysis, 2015 (Fn. 47, in diesem Abschnitt), S. 8.

hin zu rechnen ist. So werden sich viele Nutzer etwa nicht mit der komplexen technischen Infrastruktur der virtuellen Währungen beschäftigen wollen und erhalten über die Dienstleister eine an ihren Bedürfnissen angepasste Benutzerschnittstelle. Ferner werden sich zahlreiche Netzwerkteilnehmer aus Sicherheitsgründen, als Schutzmaßnahme gegen informationstechnische Eingriffe, an Intermediäre wenden.[49] Ein anderer Grund für die Übergabe virtuellen Geldes an Intermediäre liegt darin, dass diese eine notwendige Bedingung darstellt, um weitere Dienste in Anspruch nehmen zu können. Hier stellt die elektronische Geldbörse gleichsam einen Teildienst dar. Das zeigt sich etwa am Beispiel *virtueller* „*Wechselstuben*", die in den Zahlungssystemen eine wesentliche Funktion erfüllen.[50] Als Schnittstelle zum hoheitlichen Währungssystem ermöglichen sie den Erwerb des virtuellen Geldes und den Rücktausch in Buchgeld, das bekanntermaßen auf hoheitliches Geld lautet.[51] Auf multilateralen Handelsplattformen wie Bitcoin Deutschland oder Kraken werden Anbieter und Nachfrager der virtuellen Währungen nach festgelegten Bestimmungen zum Vertragsschluss zusammengeführt. Der Betreiber der Plattform tritt dagegen nicht selbst als Marktteilnehmer auf.[52]

Die Möglichkeit des lokalen OTC-Handels bieten Plattformen wie LocalBitcoins. Die Anbieter sogenannter „*mining pools*" richten sich an Netzwerkteilnehmer, die ihre Rechenleistung als Blockchain-Registrars zur Verarbeitung und Verifikation von Transaktionen einsetzen wollen („miners"). Die Registrars können auf solchen Plattformen Zusammenschlüsse bilden, um ihre Chancen auf den Erhalt einer Belohnung in Form der betreffenden Kryptowährung zu erhöhen.[53] Der Betreiber schüttet die „geschürften" Geldeinheiten im Erfolgsfall an die Teilnehmer aus.[54]

Blockchainbasierte Zahlungsdienste („*processing service providers*") wie z. B. Coinbase, BitPay oder GoCoin implementieren die virtuellen Währungen in die Zahlungssysteme von E-Commerce-Händlern.[55] Den Verbrauchern eröffnet dies die Möglichkeit, Waren und Dienstleistungen mit den digitalen Geldeinheiten bei Anbietern zu erwerben, die keine eigene Geldbörse („wallet") unterhalten möchten. Die Kryptowährung fließt in diesem Rahmen dem Zahlungsdienstleister zu, welcher den Händler dann in aller Regel mit her-

---

[49] Siehe *Böhme et al*, 29 J. Econ. Perspect. (2015), 213, 220 f.

[50] Siehe für diese Finanzdienstleister *Münzer*, BaFin Journal 01/2014, 26.

[51] EBA, Opinion on „virtual currencies", 2014 (Fn. 47), S. 14, Ziffer 35 f.

[52] Siehe für diese Geschäftsart *Münzer*, BaFin Journal 01/2014, 26, 28 f.

[53] Das Geschäftsmodell ist mit Lottogemeinschaften vergleichbar und setzt die Verwendung der Methode des sogenannten Arbeitsnachweises voraus. Das ist etwa im Transaktionssystem Bitcoin der Fall. Siehe hierzu unten S. 24 ff. und 40 ff.

[54] Siehe *Spindler/Bille*, WM 2014, 1357, 1365 oder https://www.bitcoinmining.com/bitcoin-mining-pools/.

[55] Siehe für diese Dienstleistung etwa EZB, Virtual currency schemes – a further analysis, 2015 (Fn. 47, in diesem Abschnitt), S. 8.

kömmlichem Fiatgeld auszahlt.[56] Der Verkäufer kann dem Kunden einerseits eine weitere Zahlungsmethode anbieten und bleibt andererseits vor den Wertschwankungen der virtuellen Währungen geschützt. Verbraucher hingegen profitieren bei einer Inanspruchnahme der Zahlungsdienstleister von den informationstechnischen Systemen der Intermediäre und einer erleichterten Benutzerschnittstelle.

Weder in Deutschland noch anderweitig im Euroraum wurde bis zum gegenwärtigen Zeitpunkt ein spezieller Rechtsrahmen für virtuelle Währungen erlassen.[57] Demgegenüber existiert in Brasilien bereits seit Oktober 2013 ein spezifisches Gesetz in Bezug auf Transaktionen in virtuellen Währungen. Die Grundsätze und Standards für Zahlungsdienstleistungen mit konventionellen Zahlungsmitteln wurden mit dem legislativen Akt auf Kryptowährungen transferiert.[58] Überdies hat das New York Department of Financial Services ein Regelwerk für virtuelle Währungen erlassen.[59] Danach ist etwa die Administration sowie Emission einer virtuellen Währung erlaubnispflichtig, aber auch der Umtausch der digitalen Zahlungsmittel in Fiatgeld.[60] Prohibition scheint dagegen lediglich in China und Russland die Leitschnur zu sein.[61] In China ist Finanzintermediären der Handel und das Erbringen von Zahlungsdienstleistungen im Zusammenhang mit Bitcoins bereits seit Dezember 2013 untersagt.[62] Die Debatte um die hoheitliche Regulierung des Phänomens scheint sich in Russland ebenso auf ein Verbot zu verdichten. Schranken seien nach Auffassung der Zentralbank der Russischen Föderation schon aus der umfassenden Emissionshoheit des russischen Staates abzuleiten, weil jene sowohl der Einführung als auch der Nutzung anderer Währungseinheiten als dem Rubel entgegenstehe.[63] Ferner wird eine Pönalisierung der Beteiligung an Transaktionen mit virtuellen Währungen diskutiert.[64] Allerdings mehren sich in der Diskussion bereits kriti-

---

[56] Siehe *White*, 35 Cato J. (2015), 383, 385.

[57] Siehe European Parliamentary Research Service, Bitcoin: Markets, economics and regulation, Briefing vom 11. 04. 2014, S. 7, unter http://www.europarl.europa.eu/RegData/bibliotheque/briefing/2014/140793/LDM_BRI(2014)140793_REV1_EN.pdf.

[58] *De Filippi*, 3 Internet Policy Review (2014), 1, 5.

[59] Siehe für den bereits verkündeten Regulierungsrahmen http://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf.

[60] Siehe § 200.3 Abs. (a) der BitLicense zur Erlaubnispflicht sowie § 200.2 Abs. (q) zur Definition erlaubnispflichtiger Geschäfte mit virtuellen Währungen.

[61] Siehe European Parliamentary Research Service, Bitcoin: Markets, economics and regulation (Fn. 57 in diesem Abschnitt), S. 9, Annex B.

[62] *De Filippi*, 3 Internet Policy Review (2014), 1, 5.

[63] Siehe Presseerklärung der der Zentralbank der Russischen Föderation vom 27. 01. 2016 zur Verwendung von virtuellen Währungen wie insbesondere Bitcoin bei Transaktionen (Центральный банк Российской Федерации, Информация, Об использовании при совершении сделок „виртуальных валют“, в частности, Биткойн), unter http://www.cbr.ru/press/PR.aspx?file=27012014_1825052.htm.

[64] Siehe Library of Congress, Regulation of Bitcoin in Selected Jurisdictions, unter https://www.loc.gov/law/help/bitcoin-survey.

sche Stimmen, die darauf verweisen, dass vor dem Hintergrund des erwähnten funktionellen Zusammenhangs ein Verbot der Kryptowährungen die Entwicklung der Blockchain-Technologie als solche bzw. die Integrität der Systeme gefährden würde.[65]

Abseits derartiger Bestrebungen werden in zahlreichen Berichten und Stellungnahmen staatlicher Institute und Arbeitsgruppen sowohl auf nationaler als auch auf internationaler Ebene die Herausforderungen an den Staat thematisiert und differenzierte Ansätze entwickelt.

Die EZB beleuchtet in ihrer ersten Studie zu den „virtual currency schemes" die Implikationen und Risiken für die Preisstabilität[66], die Stabilität des Finanzsystems[67] und die Stabilität der Zahlungssysteme[68]. In einer zweiten Studie führt die EZB eine Definition für das monetäre Phänomen ein. Virtuelle Währungen seien demnach zu definieren „as a digital representation of value, not issued by a central bank, credit institution or e-money institution, which, in some circumstances, can be used as an alternative to money."[69] Damit wird die Eigenschaft der Blockchain-Rechnungseinheiten in den Vordergrund gestellt, als monetäres Werttransportvehikel zu fungieren.[70] In kursorischer Form werden ferner die Risiken für die Verwender des virtuellen Geldes aufgezeigt.[71] Eingehend analysiert wird das Risikopotentials in einer Stellungnahme der Europäischen Bankenaufsichtsbehörde.[72] Das Aufsichtsorgan entwickelt überdies bereits erste Regulierungsideen.[73]

Auf die Gefahren der Geldwäsche sowie der Terrorismusfinanzierung aufgrund der systemischen Anonymität oder Pseudonymität der Nutzer virtueller Währungen weist der erste Bericht der Financial Action Task Force hin.[74] In einem zweiten Papier stellt die Arbeitsgruppe eine erste Leitlinie zum strukturierten Umgang mit den Risiken dar. Der Fokus liege aus ihrer Sicht bei den konvertiblen virtuellen Währungen, also jenen, die auf dem „Währungsmarkt" von und in staatliches Geld umgetauscht werden können. In diesem Rahmen stelle die virtuelle „Wechselstube" das Einfallstor zum regulierten Fi-

---

[65] Näher *Kupriyanov*, 7 Ugolovnyj process 2016, 8–9.

[66] EZB, Virtual currency schemes, 2012, S. 33 ff., Ziffer 4.1, unter https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf.

[67] EZB, Virtual currency schemes, 2012 (Fn. 66, in diesem Abschnitt), S. 37 ff., Ziffer 4.2.

[68] EZB, Virtual currency schemes, 2012 (Fn. 66, in diesem Abschnitt), S. 40 ff., Ziffer 4.3.

[69] EZB, Virtual currency schemes – a further analysis, 2015 (Fn. 66, in diesem Abschnitt), S. 25, Ziffer 2.2.

[70] Ebendort.

[71] EZB, Virtual currency schemes – a further analysis, 2015 (Fn. 47, in diesem Abschnitt), S. 18 ff., Ziffer 1.6.

[72] EBA, Opinion on „virtual currencies", 2014 (Fn. 47, in diesem Abschnitt).

[73] EBA, Opinion on „virtual currencies", 2014 (Fn. 47, in diesem Abschnitt), S. 39 ff.

[74] FATF, Virtual Currencies – Key Definitions and Potential AML/CFT Risks, 2014, unter http://www.fatf-gafi.org/media/fatf/documents/reports/virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.

Sachregister