TILL VON POSER

Haftungsadressaten in DLT-Netzwerken

Schriften zum Recht der Digitalisierung
18

Mohr Siebeck

Schriften zum Recht der Digitalisierung

Herausgegeben von

Florian Möslein, Sebastian Omlor und Martin Will

18

Till von Poser

Haftungsadressaten in DLT-Netzwerken

Mohr Siebeck

Till von Poser, geboren 1993; Bankausbildung; Studium der Rechtswissenschaften in Heidelberg, Lausanne und Münster; Wissenschaftlicher Mitarbeiter am Institut für das Recht der Digitalisierung an der Universität Marburg; 2022 Promotion; Referendariat am Landgericht Frankfurt am Main.
orcid.org/0009-0005-2169-9767

Zugleich Dissertation am Fachbereich Rechtswissenschaft der Philipps-Universität Marburg

ISBN 978-3-16-162425-4/ eISBN 978-3-16-162662-3
DOI 10.1628/978-3-16-162662-3

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 *https://dnb.de* abrufbar.

Das Buch wurde von Beltz Grafische Betriebe in Bad Langensalza auf alterungsbeständiges Werkdruckpapier gedruckt und dort gebunden.

Printed in Germany.

Meinen Eltern

Vorwort

Die vorliegende Arbeit wurde im Wintersemester 2022/2023 durch den Fachbereich Rechtswissenschaften der Universität Marburg als Dissertation angenommen. Rechtsprechung, Literatur und technologischer Stand konnten im Wesentlichen bis Anfang 2022 berücksichtigt werden. Seit der Beginn meiner Auseinandersetzung mit der Blockchain Ende 2019 hat sich die Materie stark verändert und wird dies auch weiterhin tun – ich hoffe trotzdem, dass sich viele der Erkenntnisse bei Änderung der technologischen Voraussetzungen und der Rechtslage auch in Zukunft verwerten lassen.

Betreut wurde die Arbeit von meinem verehrten Doktorvater Prof. Dr. Florian Möslein, LL.M. (London). Ich bin ihm nicht nur für seine intensive Betreuung und jederzeitige Diskussionsbereitschaft, sondern auch für die unglaublich bereichernde Zeit an seinem Lehrstuhl zu tiefem Dank verpflichtet. Prof. Dr. Sebastian Omlor, LL.M. (NYU) danke ich nicht nur für die zügige Erstellung des Zweitgutachtens, sondern gemeinsam mit Florian Möslein für die absolut geniale Zeit am Institut für das Recht der Digitalisierung mit all seinen Tagungen, Reisen, Treffen, innovativen Forschungsprojekten usw. usf. IRDi rocks!

Dank geht auch an die Friedrich-Naumann-Stiftung, die mich finanziell und ideell während der Hauptphase der Promotion gefördert und so zum Gelingen der Arbeit maßgeblich beigetragen hat. Der Swiat-GmbH danke ich für die äußerst großzügige Übernahme eines Großteils der Druckkosten. Dem Mohr Siebeck Verlag danke ich für die Aufnahme der Arbeit in seine Schriftenreihe „Schriften zum Recht der Digitalisierung“ und die Betreuung während der Drucklegung.

Ich danke der Vielzahl von Kommilitonen, Wissenschaftlern und Praktikern, die mich bei der Anfertigung der Arbeit begleitet haben. Insbesondere soll hier stellvertretend die Wissenschaftliche Gesellschaft für Recht und Blockchain-Technologie e.V. genannt werden, mit deren Mitgliedern ich die unvermeidlichen Täler einer Promotionsphase gemeinsam durchschreiten konnte.

Auch Freunden und Familie kann ich nicht genug danken. Insbesondere gilt dies für meine Ehefrau Helena – sie war der Grund, warum ich mich im Corona-Lockdown jeden Morgen an den Schreibtisch gesetzt habe. Zuletzt danke ich meinen Eltern, die mich – jeder auf seine eigene Art – nicht nur während der Promotion, sondern während allen Phasen meiner juristischen Laufbahn von Herzen unterstützt haben. Ihnen widme ich diese Arbeit.

Inhaltsübersicht

Inhaltsverzeichnis

Einleitung

A. Problemstellung

Ethereum, Chiliz, Cardano, EOS, IOTA, Tezos… Die Distributed-Ledger-Technologie, vor allem durch die Kategorie der „Blockchains" bekannt, hat sich längst von ihrem prominentesten Anwendungsfall – dem Bitcoin – gelöst. Als Basistechnologie für eine Vielzahl unterschiedlicher Anwendungen lässt sie sich überall dort einsetzen, wo Vertrauen zwischen einander unbekannten Marktakteuren notwendig ist. DLT-Netzwerke beruhen in ihrer Grundkonzeption auf einem Datenaustausch mehrerer gleichberechtigter Personen über das Internet, einem sogenannten Peer-to-Peer-Netzwerk. Da diese „Peers" maßgeblicher Betreiber der Technologie sind, übernehmen sie gleichzeitig die technische Verantwortung für den Inhalt der auf DLT-Netzwerken gespeicherten Daten.

Es gibt nicht „das DLT-Netzwerk", wie es etwa „das Internet" gibt. Vielleicht für manchen Beobachter etwas überraschend, hat sich auch 2023 kein universales Netzwerk durchgesetzt, in dem alle DLT-basierten Anwendungen betrieben werden. Es herrscht vielmehr ein fragmentierter Markt, in dem unterschiedliche DLT-Netzwerke mit unterschiedlichen technischen Ausgestaltungen, aber auch unterschiedlichem thematischem Bezug[1] auf sich aufmerksam machen wollen und um neue Nutzer werben.[2] Die Vielzahl dieser Netzwerke, die auf den gleichen technischen und verhaltensökonomischen Grundlagen beruhen, werfen die abstrakte Frage nach ihrem Rechtscharakter, vor allem aber nach der Haftung für das Netzwerk selbst auf. Die Haftung für Ereignisse im Netzwerk kann angesichts der immensen Werte, die mittlerweile DLT-basiert bewegt werden, für die Entscheidung von Unternehmen, aber auch von Privatpersonen für oder gegen die Nutzung von DLT-Technologie zum ausschlaggebenden Faktor werden.

Die Arbeit erörtert demzufolge, welchem zivilrechtlichen Normregime die einzelnen Akteure – namentlich Betreiber, Nutzer und Entwickler – in den un-

---

[1] Siehe etwa die Blockchain Chiliz (chiliz.com) mit einem Fokus auf Sport und Unterhaltung.

[2] Eine Übersicht über alle existenten DLT-Netzwerke ist nicht ersichtlich. Einen Anhaltspunkt bietet die Übersicht unter https://coinmarketcap.com/de/all/views/all/. Da DLT-Netzwerke nicht zwangsläufig Kryptowährungen unterstützen, Kryptowährungen aber wiederum auch als DLT-Anwendungen ausgestaltet werden können, kann diese Liste nur eine erste Orientierung bieten.

terschiedlichen Gestaltungsformen von DLT-Netzwerken ausgesetzt sind. Kern der Untersuchung sind dabei die Abgrenzung und Zuordnung von Verantwortungsbereichen der verschiedenen Akteure, welche im deliktischen Bereich maßgeblich durch das Bestehen von Verkehrspflichten erfolgen. Die Bedeutung der Feststellung von Verkehrspflichten liegt in der Konkretisierung der Grenze zwischen erlaubtem und pönalisiertem Verhalten. Zwingender Bestandteil einer haftungsrechtlichen Untersuchung ist dabei die ebenfalls ungeklärte, aber in der Literatur oftmals angerissene Frage, ob sich die technikbasierten DLT-Netzwerke als rechtliche Gesamtheit erfassen lassen.

Für die auf Smart Contracts basierenden „DAOs" existieren schon diverse Untersuchungen, für DLT-Netzwerke selbst steht eine vertiefte Betrachtung aber noch aus. Die Arbeit untersucht demzufolge in einem ersten Schritt, ob die Kooperation der Teilnehmer von DLT-Netzwerken in die Kategorien rechtlicher Gemeinschaften, insbesondere die Gesellschaft bürgerlichen Rechts nach § 705 BGB oder aber – anknüpfend an ein Recht oder Rechtsgut – in die Gemeinschaft nach § 741 BGB einzuordnen ist. Die durch diese Normen angebotenen Organisationsregeln sind eher von untergeordneter Bedeutung, da die Funktionsweise eines DLT-Netzwerks stets durch ihre Programmierung technisch vorgegeben ist.

Entscheidend ist daher vielmehr, ob es sich bei DLT-Netzwerken um Haftungsverbünde und möglicherweise sogar um Rechtspersönlichkeiten handelt. Gleichzeitig ist eine solche Einordnung nicht zwingend: Real existierende Verbände können durchaus kooperative Strukturen bilden, ohne dass diese Strukturen durch die Rechtsordnung erfasst werden müssen.[3] Entscheidend für diese Erfassung ist daher die Anerkennung der real existierenden Strukturen durch die Rechtsordnung, die wiederum den rechtlichen Verbund als solchen legitimiert.[4] Insbesondere bei den sogenannten offenen[5] DLT-Netzwerken sind die Akteure der einzelnen Netzwerke häufig weltweit verteilt. Hinzu kommt die durch die Eigenheit der Technologie hinzutretende Pseudonymisierung. Die dadurch entstehenden Rechtsdurchsetzungsdefizite gehen mit der Technologie Hand in Hand. Für die Gewährleistung praxistauglicher und auch gerechter Ergebnisse sollen diese Rechtsdurchsetzungsdefizite daher in die Betrachtung miteinbezogen werden.

„Insgesamt stellen dezentrale Systeme eine neue Erscheinungsform sozialer Interaktion dar, bei der die individuelle Verantwortlichkeit und/oder gemeinschaftlichen Verantwortlichkeiten der Beteiligten noch ungeklärt sind und deren sachgerechte Erfassung in vielerlei Hinsicht ein Überdenken der bislang bekannten Instrumente rechtlicher Gestaltung erfordert."[6]

---

[3] *Ott*, Recht und Realität der Unternehmenskooperation, 86.
[4] *Ott*, Recht und Realität der Unternehmenskooperation, 86.
[5] Siehe dazu unten Teil 1, A., II., 2.
[6] *Siedler* in Möslein/Omlor, Fintech-HdB, § 5, Rn. 7.

Aussagen wie diesen begegnet man in der Betrachtung von DLT-Netzwerken häufig. Bevor man freilich über die Implementierung neuartiger Instrumente in die Rechtsordnung nachdenkt, sollte zunächst die Tauglichkeit bestehender Rechtsinstitute überprüft werden. Diesen Schritt will diese Arbeit leisten.

B. Untersuchungsgegenstand und Gang der Untersuchung

DLT-Technologie wirft mittlerweile in jedem denkbaren Rechtsgebiet Rechtsfragen auf. Im Sinne der oben beschriebenen Zielsetzung ist der Untersuchungsgegenstand der Arbeit sowohl aus tatsächlich-technischer als auch aus rechtlicher Perspektive beschränkt.

I. Tatsächlicher Untersuchungsgegenstand

DLT-Netzwerke sind die Basis für eine Vielzahl von Anwendungen, die ebenso wie die DLT-Technologie selbst eine Innovation darstellen. Dies betrifft insbesondere die Konzepte der sogenannten Coins oder Token, die als Wertrepräsentative herkömmliche Wertpapiere faktisch ersetzen können und auch die in Deutschland dafür notwendige Anerkennung durch den Gesetzgeber im eWpG inzwischen erfahren haben. Die Arbeit nimmt – soweit möglich – die Rechtsfragen, die sich aus dem speziellen Charakter der auf DLT-Netzwerken basierenden Anwendungen ergeben, aus dem Untersuchungsgegenstand heraus. Wegen des Erfordernisses einer Rechtsgutsverletzung als Anknüpfungspunkt deliktischer Haftung ist es zwar erforderlich, die Frage nach dem Charakter gewisser Anwendungen als absolutes Recht zu beantworten. Darüber hinaus beschränkt sich die Arbeit aber explizit auf die Frage nach der Verantwortlichkeit für die Technologie selbst, nicht innerhalb gewisser Anwendungen. Rund um diese Anwendungen wie „Kryptoassets“ oder „DAOs“ hat sich ein komplexes Ökosystem mit diversen Marktteilnehmern und insbesondere Handelsplattformen entwickelt, die selbst wieder innovativ und DLT-basiert sein können.[7] DLT ist aber nicht nur Kapitalmarkt, sondern bietet in vielen anderen Bereichen Anwendungspotenzial.[8]

Im Vordergrund steht daher maßgeblich das Zusammenwirken der die Technologie betreibenden Akteure, die sich technisch auf der als „Layer 1“ bezeichneten Ebene bewegen. Diese strikte Trennung zwischen Technologie und Anwendung geht einher mit der Entdeckung des Potenzials von DLT-Anwendungen

[7] Für eine umfassende Betrachtung dieser Strukturen siehe *Hoch* in Rechtshandbuch Kryptowerte, § 7, Rn. 4 ff.

[8] Statt vieler Beispiele siehe nur die Lieferkettenlösung Azhos, Börsenzeitung vom 15.03.2021, abrufbar unter https://www.boersen-zeitung.de/finanzen-technik/bei-azhos-stimmt-die-chemie-077ee1e0-7db1-11eb-8aac-17a68efb4aa7.

infolge des Einsatzes als Basistechnologie für Kryptowährungen im Allgemeinen.

Beschränkt wird der Untersuchungsgegenstand weiter durch das Erfordernis faktischer Dezentralität. DLT-Netzwerke, deren Verwaltung durch eine Person im Rechtssinne geschieht (im Folgenden als „proprietäre Lösungen" bezeichnet), werfen nicht die oben dargestellten neuartigen haftungsrechtlichen Problemstellungen auf. Obwohl es sich aus technischer Sicht um identische Systeme handelt, entstehen die tatsächlichen und rechtlichen Vorteile von DLT-Netzwerken erst unter Beteiligung von mindestens zwei Rechtspersonen, die einander nicht vertrauen.[9]

Außerdem soll an dieser Stelle betont werden, dass sich die Frage der Haftung und des rechtlichen Charakters maßgeblich nach der technischen Rolle bemisst, die ein Akteur einnimmt. Für die Zwecke dieser Arbeit werden die verschiedenen Akteure so untersucht, als handle es sich bei ihnen um unterschiedliche Personen. In der Praxis fallen diese verschiedenen Positionen allerdings oftmals zusammen. Dieser Zusammenhang wird für die präzise Darstellung der rechtlichen Strukturen und Haftungszusammenhänge getrennt, in der abschließenden Betrachtung aber zusammen gewürdigt.

Der Fokus auf die Technologie selbst ermöglicht es zuletzt, die bislang nur sehr dürftig untersuchten Formen zugangsbeschränkter DLT-Netzwerke in den Blick zu nehmen. Im Verlauf der Arbeit wird sich gleichwohl zeigen, dass gerade die Ausgestaltung bestimmter zugangsbeschränkter DLT-Netzwerke häufig auf individuellen Vertragskonstellationen beruht. Eine umfassende rechtliche Bewertung dieser Vertragskonstruktionen wird erst dann möglich sein, wenn durch gerichtliche Kasuistik die entsprechenden vertraglichen Regelungen nachprüfbar veröffentlicht werden. Gerade in diesem Bereich ist daher nur eine vorsichtige erste Bewertung deren Bedeutung sich vor allem aus dem Vergleich mit anderen Konzeptionen der Nutzung von DLT-Netzwerken ergibt.

II. Rechtlicher Untersuchungsgegenstand

Es handelt sich um eine Arbeit rein zum zivilrechtlichen Charakter und zur Haftung von DLT-Netzwerken. Damit entfällt insbesondere die aufsichtsrechtliche Perspektive als Untersuchungsgegenstand. Das Aufsichtsrecht über DLT-Technologien wird in Zukunft auf europarechtlicher Ebene durch die VO 2019/1937 „MiCa" und auf nationaler Ebene durch das jüngst beschlossene Gesetz zur Einführung von elektronischen Wertpapieren (eWpG) geprägt sein. In beiden Normen finden sich allerdings auch Haftungsregeln, deren Analyse Teil dieser Arbeit ist. In den Untersuchungsgegenstand fällt auch das Immaterialgüterrecht als Teil des Zivilrechts. Die Untersuchung setzt gleichwohl die Anwendbarkeit deutschen Rechts voraus, dessen tiefergehende Betrachtung den Rahmen dieser Arbeit überschreiten würde.

[9] Siehe vertiefend dazu auch unten Teil 1, A., II., 5.

III. Gang der Untersuchung

Teil I widmet sich zunächst den technischen Grundlagen von DLT-Netzwerken und mündet in einer Systematisierung der verschiedenen Akteure. Es folgt dann eine kurze Analyse vergleichbarer Technologien, bevor aus der abstrakten Perspektive das Problem effektiver Rechtsdurchsetzung in offenen DLT-Netzwerken dargestellt und eingeordnet wird.

In Teil II wird die Frage nach dem Charakter von DLT-Netzwerken als Rechtsgesamtheit gestellt. Dies geschieht zunächst durch eine Analyse der Nutzungsverhältnisse in Bezug auf das DLT-Netzwerk als solches, bevor dann die Voraussetzungen der Gesellschaft bürgerlichen Rechts nach § 705 BGB in den verschiedenen Konstellationen offener und geschlossener Netzwerke untersucht werden. Anschließend erfolgt eine Untersuchung von § 741 BGB i. V. m. § 87a UrhG mit einer schwerpunktmäßigen Betrachtung offener Netzwerke.

In Teil III widmet sich die Arbeit den speziellen haftungsrechtlichen Fragen. Zunächst soll dafür die allgemeine Frage nach dem rechtlichen Charakter von DLT-basierten Anwendungen beantwortet werden, die als häufig betroffenes Schutzobjekt auch für die Betrachtung der „Layer-1-Ebene“ erforderlich ist. Darauf aufbauend soll der haftungsrechtliche Rahmen für die verschiedenen relevanten Akteure, namentlich der Nutzer, der Betreiber und zuletzt der Entwickler untersucht werden. In ersterer Gruppe wird die Normgebung im nationalen und europarechtlichen Bereich für die DLT-Technologie auf die Regelungen hin zu untersuchen sein, die Aussagen über die Haftung und Verantwortlichkeit selbst treffen.

Teil 1

Grundlagen und Einordnungen

A. Technischer Hintergrund und Systematisierungen

I. Entwicklungshintergrund

Satoshi Nakamoto hat 2008 mit seinem Bitcoin-Whitepaper[1] das Konzept der Datenbankführungen revolutioniert: Das Whitepaper räumt die letzten Schwierigkeiten aus, die bis dahin bei der Führung von Datenbanken mit mehreren Beteiligten bestanden, ohne dass es dafür eines Intermediärs als vertrauensstiftende Institution bedarf. Solche Datenbanken sind im technischen Sinne verteilt und gleichzeitig dezentral – ein Distributed-Ledger.

Kernproblem solcher Datenbanken war bis dato die Manipulationsmöglichkeit durch einzelne Beteiligte, das „Double-Spending-Problem".[2] Ein verteiltes und dezentrales System ohne einen Intermediär muss verhindern, dass ein böswilliger Teilnehmer bei mehreren anderen Teilnehmern gleichzeitig unterschiedliche Datenbankeintragsänderungen veranlasst, um sich einen Vorteil zu verschaffen. Dieses Problem lässt sich am Beispiel einer dezentral organisierten Kryptowährung verdeutlichen: Laut Datenbank hat A einen Kontostand von 3 Einheiten. Er veranlasst die Überweisung von drei Einheiten an B und von drei Einheiten an C. Da es keine zentrale Instanz zur Überprüfung gibt, werden B und C die Transaktion zunächst akzeptieren. Bis B und C sich untereinander ausgetauscht haben und der Betrug auffällt, ist A verschwunden. Irgendwann wird die Manipulation auffallen, aber bis dahin hat A irgendeine realwertige Gegenleistung erlangt und das Netzwerk verlassen.

Dabei wurde schon 1982 allgemein bewiesen, dass jedes Netzwerk auch bei völliger Anonymität der Teilnehmer fälschungssicher ist, solange nur mehr als 2/3 der Teilnehmer keine Betrüger sind (die sogenannte byzantinische Fehlertoleranz).[3] Seit dieser Erkenntnis waren die Bemühungen forschender Entwickler dabei vor allem auf die Schaffung einer dezentralen Kryptowährung als Anwendungsfall einer solchen Datenbank ohne Intermediär gerichtet. In dem Zusam-

---

[1] Abrufbar unter https://Bitcoin.org/Bitcoin.pdf.

[2] Gesehen wurde das Problem erstmals von *Chaum*, 8 Sci. Am. 1992, 96 ff.

[3] *Lamport*/*Shostak*/*Pease*, ACM Transactions on Programming Languages and Systems, Vol. 4, Iss. 3, 1982. Hierbei handelt es sich um das sogenannte Byzantinische Fehlerproblem: Jedes entwickelte DLT muss dieses Problem neu lösen, die benutzen Lösungen variieren nach Art des zugrunde liegenden DLT.

menhang mag die in der Onlinecommunity angeblich vorherrschende Ablehnung von klassischen Institutionen eine Rolle gespielt haben, vor allem ist aber die Rolle des Intermediärs (also der Banken) bei der Ausgabe von Geld besonders offensichtlich und einflussreich.

Zentrale Innovation des Whitepapers von Satoshi Nakamoto[4] „Bitcoin: A Peer-to-Peer Electronic Cash System"[5] ist die Beschreibung eines dezentralen Rechensystems zum Finden eines Konsensus über den Stand des Netzwerks, der sogenannte Proof-of-Work-Algorithmus. Der Erfolg von Bitcoin und die Entdeckung des wirtschaftlichen Potenzials führte allerdings zur Entwicklung von weiteren Lösungen des „Double-Spending-Problems", sodass „Proof-of-Work" heutzutage nicht mehr die einzige Lösung des Double-Spending-Problems darstellt. DLT-Technologien werden heutzutage sowohl von verschiedenen privaten und kommerziellen Anbietern als auch von offenen Communities betrieben. Ihre Anwendungsfälle haben sich dabei längst von simplen Kryptowährungen weiterentwickelt.

Das größte und praktisch relevanteste dieser komplexeren Netzwerke ist dabei die Blockchain[6] Ethereum, der aufgrund ihrer Vorreiterrolle bei DLT-basierten Anwendungen in dieser Arbeit ein besonderer Schwerpunkt zukommt. Es ist zu erwarten, dass sich der Markt konsolidiert und nach der Entwicklung funktionsfähiger Konzepte ein Netzwerkeffekt eintritt, sich die Nutzer also auf Software konzentrieren, die aufgrund anderer Teilnehmer die größte Reichweite erreicht.[7] Allerdings befinden sich DLT-Technologien noch in einer Phase der Vertrauensbildung und der Erprobung verschiedener Konzepte, da sich einzelne Lösungen noch nicht herausgebildet haben.

II. Funktionsweise und technische Umsetzung

Im Folgenden werden diejenigen technischen Aspekte herausgearbeitet, die DLT-Netzwerke grundsätzlich kennzeichnen. Zugrunde gelegt wird dabei die vorherrschende Programmierung und die nach dem ISO-Komitee geltende Begriffsdefinition.[8] Die Darstellung fokussiert dabei auf die Bereiche, die letztendlich für die rechtlichen Fragestellungen von Relevanz sind. Insbesondere sollen die kryptografischen Grundlagen – die von essenzieller Bedeutung für die Funktionsweise eines DLT-Netzwerks sind – nur kurz dargestellt werden, da ihr Verständnis für die hiesigen rechtliche Fragestellungen von untergeordneter Bedeutung ist.

---

[4] Dabei handelt es sich um ein Pseudonym, dessen Identität bis heute ungeklärt ist.

[5] Abrufbar unter https://Bitcoin.org/Bitcoin.pdf.

[6] Bei einer Blockchain handelt es sich um eine Sonderform von DLT-Netzwerken, siehe unten Teil 1, A., II., 1., e), bb).

[7] *Seemann*, Technology Review 10/2018, 46.

[8] Siehe zu den folgenden Begriffen daher auch die Definitionsliste unter ISO-Standard 22739:2020; abrufbar unter https://www.iso.org/obp/ui/#iso:std:iso:22739:ed-1:v1:en.

1. Aufbau eines DLT-Netzwerks[9]

a) Dezentrale Speicherung

Bei einem Distributed-Ledger-Netzwerk wird der aktuelle Stand des Registers („Ledger") bei jedem Teilnehmer des Netzwerks hinterlegt. Jeder Teilnehmer kann jederzeit bei sämtlichen anderen Teilnehmern den Stand des Ledgers abfragen. Veränderungen in der Buchführung werden bei jedem Teilnehmer aufgezeichnet. Dadurch ist das System zunächst grundsätzlich fälschungssicher: Verändert einer der Teilnehmer seine Aufzeichnungen, ohne dass dies vom Netzwerk autorisiert ist, so stimmt sein Ledger nicht mit den anderen Ledgern überein und er kann als Betrüger identifiziert werden.

b) Full Nodes

Diese Register werden auf einem Netzwerk von Computern abgelegt, die in der Regel als Nodes[10] (zu Deutsch: „Knotenpunkt") bezeichnet werden.[11] Jeder dieser Computer kommuniziert mit den anderen über eine Software.[12] Nicht jeder Node muss mit jedem anderen Node im Netzwerk in Verbindung stehen, ausreichend ist der Kontakt des Nodes zu einigen anderen Nodes. Grundsätzlich[13] herrscht eine Gleichberechtigung der verschiedenen Nodes.[14] Es gibt keinen zentralen Node, auf den sich das Netzwerk konzentriert.[15] Demzufolge besteht bei Ausfall einzelner Nodes keine Gefahr für die Funktionsfähigkeit des Netzwerks. Diese Charakteristika der Teilnehmer sind sämtlich nicht DLT-spezifisch, sondern zeichnen vielmehr jedes Peer-to-Peer-Netzwerk aus.[16]

---

[9] Siehe auch die Darstellungen von *Kaulartz* in Möslein/Omlor, Fintech-HdB, § 5 und *Fromberger*/*Zimmermann* in Rechtshandbuch Kryptowerte, § 1.

[10] Es werden die englischen Begriffe verwendet, da allein diese faktisch genutzt werden und daher relevant sind.

[11] So die Definition der ISO (Fn. 8, Teil 1, A.). Siehe dazu *Fazekas* in Köhler-Schute (Hrsg.), Blockchains und DLT-Technologien in Unternehmen, 38, 41.

[12] *Fazekas* in Köhler-Schute (Hrsg.), Blockchains und DLT-Technologien in Unternehmen, 38, 41.

[13] Es gibt allerdings auch abweichende Systeme, in denen sogenannte Masternodes technisch vollumfänglich zur Kontrolle der anderen Nodes berechtigt sind. Sie sind keine DLT-Systeme im hier verstandenen Sinne, da die technischen Berechtigungen nicht dezentral verteilt sind.

[14] Technisch können die Nodes allerdings unterschiedlich ausgestaltet sein. Danach bemisst sich aber nicht ihr Einfluss im Netzwerk, siehe z. B. für Bitcoin *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, 8.

[15] *Fazekas* in Köhler-Schute (Hrsg.), Blockchains und DLT-Technologien in Unternehmen, 38, 41.

[16] Grundlegend zu den Charakteristika von Peer-to-Peer-Netzwerken siehe *Steinmetz*/*Wehrle*, Informatik-Spektrum 27, 51.

Die Kommunikation zwischen den Nodes verläuft je nach DLT unterschiedlich.[17] Die Nodes können entweder punktuell Informationen austauschen (z. B. in Hyperledger Fabric) oder aber eine dauerhafte Verbindung zueinander aufrechterhalten (so beispielsweise in Ethereum). Die Nodes müssen sich nicht zwangsläufig untereinander in ihrer Gesamtheit bekannt sein.

Ein Node ist nicht mit einer natürlichen Person im Rechtssinn gleichzusetzen. Beide stehen nicht in einer abhängigen Beziehung zueinander, d. h. mehrere Personen können über einen einzigen Node am Netzwerk teilnehmen. Beispielsweise können sich zwei natürliche Personen einen Computer und die Software darauf teilen und abwechselnd Handlungen im Netzwerk vornehmen. Andersherum kann eine Person mehrere Nodes gleichzeitig betreiben. Diese Konstellationen sind für die anderen Beteiligten nicht erkennbar, da der Node nur mittels seiner Adresse identifiziert wird.

In manchen DLT-Netzwerken werden für die noch zu erläuternde Freigabe von Transaktionen auch solche Peers bezeichnet, die nicht die komplette Datenbank, sondern lediglich einen Ausschnitt davon speichern. Solche Nodes bezeichnet man auch als „Light Nodes". Light Nodes sind für den grundsätzlichen Betrieb eines DLT-Netzwerks weder notwendig noch ausreichend.[18] Nodes, die hingegen die komplette Datenbank speichern und für den Betrieb eines DLT-Netzwerks essenziell sind, werden daher zur Abgrenzung als „Full Nodes" bezeichnet.

c) Adressen

Nodes speichern also den aktuellen Stand des Ledgers. Sie sind aber nicht die einzigen Akteure in einem DLT-Netzwerk, hinter denen Personen im Rechtssinne stehen können. Für die Kommunikation mit dem Netzwerk ist es bei den meisten DLT-Netzwerken nicht erforderlich, dass ein Node betrieben wird. Vielmehr ist dafür allein eine Adresse vonnöten. Wer beispielsweise Bitcoin nutzen will, braucht dafür nur einen sogenannten key, also eine Adresse, die dem Netzwerk bekannt ist.[19] Er muss nicht die komplette Blockchain speichern und als Node fungieren. Wie bei den Nodes ist auch eine Adresse nicht mit einer natürlichen Person gleichzusetzen, vielmehr wird die Nutzung mehrerer Adressen durch eine Person aus Sicherheitsgründen sogar empfohlen.[20] Außerhalb der Nodes kann so eine viel größere Anzahl von Personen mit einem DLT-Netzwerk interagieren. Diese Personen speichern selbst nicht das komplette Netzwerk. Vielmehr werden Daten über ihre Handlungen im DLT-Netzwerk hinterlegt, sodass sie eintragungsfähig sind. Sie können daher das Netzwerk nutzen und Informationen hin-

---

[17] *Fazekas* in Köhler-Schute (Hrsg.), Blockchains und DLT-Technologien in Unternehmen, 38, 41.

[18] *Fromberger/Zimmermann* in Rechtshandbuch Kryptowerte, § 1, Rn. 9.

[19] *Antonopoulos*, Bitcoin & Blockchain, 6.

[20] Siehe nur beispielhaft etwa https://bitcoin.org/de/schuetzen-sie-ihre-privatsphaere.

Sachregister