

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.

© 2023 Mohr Siebeck Tübingen. www.mohrsiebeck.com

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlags unzulässig und strafbar. Das gilt insbesondere für die Verbreitung, Vervielfältigung, Übersetzung und die Einspeicherung und Verarbeitung in elektronischen Systemen.

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

Vorwort	VII
Inhaltsverzeichnis	XI
Einleitung	1
<i>A. Problemstellung</i>	1
<i>B. Untersuchungsgegenstand und Gang der Untersuchung</i>	3
Teil 1: Grundlagen und Einordnungen	7
<i>A. Technischer Hintergrund und Systematisierungen</i>	7
<i>B. Zivilrechtliche Strukturen vergleichbarer technischer Phänomene</i>	37
<i>C. Offene DLT-Netzwerke als virtuelle rechtsfreie Räume?</i>	45
Teil 2: Rechtsnatur	59
<i>A. Nutzung eines DLT-Netzwerks auf vertraglicher oder tatsächlicher Basis</i>	60
<i>B. Gesellschaft nach § 705 BGB</i>	68
<i>C. Gemeinschaft nach § 741 BGB</i>	104
<i>D. Gesamtergebnis zu Teil 2 und Konsequenzen</i>	127
Teil 3: Haftung	129
<i>A. Einordnung DLT-basierter Anwendungen</i>	130
<i>B. Haftung der Nutzer</i>	139
<i>C. Haftung der Betreiber</i>	150
<i>D. Haftung der Entwickler</i>	174

Schluss	199
<i>A. Zusammenfassung</i>	<i>199</i>
<i>B. Schlussüberlegungen und Ausblick</i>	<i>203</i>
Literaturverzeichnis	205
Sachregister	213

Inhaltsverzeichnis

Vorwort	VII
Inhaltsübersicht	IX
Einleitung	1
<i>A. Problemstellung</i>	1
<i>B. Untersuchungsgegenstand und Gang der Untersuchung</i>	3
I. Tatsächlicher Untersuchungsgegenstand	3
II. Rechtlicher Untersuchungsgegenstand	4
III. Gang der Untersuchung	5
Teil 1: Grundlagen und Einordnungen	7
<i>A. Technischer Hintergrund und Systematisierungen</i>	7
I. Entwicklungshintergrund	7
II. Funktionsweise und technische Umsetzung	8
1. Aufbau eines DLT-Netzwerks	9
a) Dezentrale Speicherung	9
b) Full Nodes	9
c) Adressen	10
d) States und Oracles	11
e) Transaktionen	12
aa) Funktion und Konzeption der Transaktionen	12
bb) Speicherung der Transaktionen und der Unterschied zwischen Blockchain und anderen DLTs	13
(1) Herkömmliche Blockchains	13
(2) Lösungsansätze durch neue DLT-Verfahren	14
f) Zusammenfassung der technischen Funktionsweise	15
2. Geschlossene und offene Netzwerke	15
a) Herkömmliche Systematisierung	15
b) Hybride	16
3. Verifikationsprozess	17
a) Konsensmechanismen in geschlossenen Netzwerken	18
b) Konsensmechanismen in offenen Netzwerken	18

4. Unveränderbarkeit der Transaktionsgeschichte	19
a) Sicherungsmechanismen	20
b) Hard Forks und Soft Forks	20
c) Weiterentwicklung bestehender DLT-Netzwerke auf Basis alter Netzwerke	21
5. Dezentralitätsbegriff	21
6. DLT-Governance	22
a) Begriffsbestimmung	22
b) Sonderfall der „On-Chain-Governance“	22
7. Untersuchte DLT-Netzwerke	23
a) Bitcoin-Blockchain	24
b) Ethereum-Blockchain	24
c) Tezos-Blockchain	24
d) Hyperledger	25
e) Corda	26
III. DLT-basierte Anwendungen	26
1. Coins	27
a) Grundsatz	27
b) „Non-fungible-Token“ als Sonderfall der Coins	28
2. Token	29
a) Begriff	29
b) Disruptivität der Tokenisierung	30
c) Systematisierung	30
3. Smart Contracts und DApps	31
a) Technisches Begriffsverständnis als solches mit Technologiebezug	31
b) Rechtswissenschaftliches Begriffsverständnis als solches ohne Technologiebezug	32
c) Identische Problemstellungen bei dem Begriff der „DApps“	33
4. Komplexere Umgebungen innerhalb von DLT-Netzwerken, insbesondere DAOs	33
5. Zusammenfassung	34
IV. Abgrenzung der Beteiligungsformen in einem DLT-Netzwerk	35
1. Grundkonzepte der Beteiligung	35
a) Entwickler und Betreiber	35
b) Nutzer	36
2. Besonderheiten geschlossener Netzwerke	37
3. Teilnehmer und ihr Verhältnis zueinander	37
<i>B. Zivilrechtliche Strukturen vergleichbarer technischer Phänomene</i>	37
I. Internet	38
II. Open-Source-Systeme	40
III. Domainnamensystem	41

IV. Datenaustauschplattformen auf Peer-to-Peer-Basis	41
V. Standardisierte Normwerke	42
VI. Erkenntnisgewinn und Bedeutung für die Forschungsfrage	43
1. Diffusion rechtlicher Beziehungen	43
2. Privatrecht als Instrument der Selbstregulierung	44
3. Bilaterale Rechtsbeziehungen als rechtliche Basis technikbasierter Netze	44
C. <i>Offene DLT-Netzwerke als virtuelle rechtsfreie Räume?</i>	45
I. Materiellrechtliche Geltung des Rechts	46
II. Fehlende Rechtsgeltung durch Rechtsdurchsetzungsdefizite	48
1. Pseudonymität als Defizit der Privatrechtsdurchsetzung	48
a) Nutzer	48
b) Betreiber	49
2. Defizitverstärkung durch weltweite Verteilung der Server	49
III. Instrumente zur Begrenzung der Rechtsdurchsetzungsdefizite	50
1. Auskunftsansprüche	50
2. Perspektivische Entwicklung eines digitalen Identitätsmanagements	52
3. Der „Gatekeeper“ im eWpG	52
a) Ansatz	53
b) Bewertung	55
4. Zwischenergebnis	56
IV. Ergebnis	57
 Teil 2: Rechtsnatur	 59
A. <i>Nutzung eines DLT-Netzwerks auf vertraglicher oder tatsächlicher Basis</i>	 60
I. Offene Netzwerke	60
1. Keine schuldrechtliche Beziehung zum Netzwerk	60
2. Rechtsverhältnisse in anreizbasierten Systemen	61
3. Ergänzende Auslobung eines einzelnen Nutzers	62
4. Rechtsverhältnis zum Wallet-Betreiber	62
5. Rechtsverhältnis zur registerführenden Stelle	63
6. Zwischenergebnis	64
II. Geschlossene Netzwerke	64
1. Konsortiale DLT-Netzwerke	64
2. Andere geschlossene Netzwerke	65
a) Abgrenzung zum Vertrag über die Softwareüberlassung	66
b) Vertragstypologische Einordnung	66
c) Zwischenergebnis	67
III. Ergebnis	67

<i>B. Gesellschaft nach § 705 BGB</i>	68
I. Grundlagen der gesellschaftsrechtlichen Verbindung	69
1. Gemeinsamer Zweck und Förderpflicht	69
2. Rechtsbindungswille	70
a) Voraussetzungen des Rechtsbindungswillens	70
b) Zur Grenze zwischen technischer und rechtlicher Bindung	71
3. Ansatzpunkte im eWpG	73
II. Offene Netzwerke	74
1. Gesamtheit der Teilnehmer eines offenen DLT-Netzwerks als GbR	74
a) Kein gemeinsamer Zweck	74
aa) Anwendungsunbeschränkte Netzwerke	74
bb) Kein gemeinsamer Zweck bei anwendungsbeschränkten DLT-Netzwerken (Kryptowährungen)	76
b) Kein Rechtsbindungswille der Nutzer	76
c) Keine Gesellschaft auf Basis einzelner vertraglicher Beziehungen	77
d) Einordnung in die Rechtsfigur der Vertragsnetze	77
aa) Die Dogmatik der Vertragsnetze	77
bb) Selbstausführende Netzwerkregeln als funktionales Vertragsäquivalent	78
cc) Weitere Voraussetzungen für ein Vertragsnetz liegen nicht vor	78
e) Keine ähnlichen geschäftlichen Kontakte nach § 311 Abs. 2 Nr. 3 BGB	79
f) Kein Gefälligkeitsverhältnis	81
g) Berücksichtigung der Rechtsdurchsetzungsdefizite	81
2. Betreiber eines DLT-Netzwerks als Gesellschaft bürgerlichen Rechts	81
a) Gemeinsamer Zweck	82
aa) Trennung von Motiv und Zweck	82
bb) Fortführung eines DLT-Netzwerks als gemeinsamer Zweck	83
cc) § 4 XI eWpG	84
dd) Förderung des Netzwerks	84
ee) Zwischenergebnis	85
b) Rechtsbindungswille	85
aa) Vorab: Bösertige Validatoren	85
bb) Kein Rechtsbindungswille in Off-Chain-Netzwerken ...	86
(1) Nur technische Koordination, keine Kooperation	86
(2) Keine Rechtfertigung zur Ergebniskorrektur	87
cc) Sonderfall: Rechtsbindungswille in On-Chain- Netzwerken	87

(1) Dogmatische Betrachtung	88
(2) Parallelen von DAOs und On-Chain-DLT- Netzwerken	89
dd) Zwischenergebnis	90
c) Unbeständige Gesellschafterzahl und Unkenntnis der Gesellschafter voneinander	91
aa) Körperschaftliche Strukturmerkmale in DLT- Netzwerken	91
bb) Keine Einordnung als Körperschaft	92
cc) Einordnung als Personengesellschaft trotz körperschaftlicher Strukturmerkmale	93
dd) Reichweite der Rechtsdurchsetzungsdefizite	94
ee) Mögliche Rechtsfolgen	94
d) Abgrenzung von Nutzern und Betreibern als Gesellschaftern	95
e) Weitere Rechtsfolgen	96
aa) Außenrechtsfähigkeit liegt im Regelfall nicht vor	96
bb) Sonstige Rechtsfolgen	97
3. Ergebnis für offene Netzwerke	97
III. Konsortiale und geschlossene Netzwerke	98
1. Konsortiale Netzwerke	98
a) Gemeinsamer Zweck und Förderpflichten	98
b) Rechtsbindungswille	98
c) Ergebnis und mögliche Rechtsfolgen	99
2. Andere geschlossene Netzwerke	100
a) Kein gemeinsamer Zweck	101
b) Kein Sternvertrag	101
c) Vertrag zugunsten Dritter	102
d) Vertrag mit Schutzwirkung zugunsten Dritter	103
e) Kein Vertragsnetz	103
IV. Sonstige hybride Systeme	103
V. Ergebnis	104
<i>C. Gemeinschaft nach § 741 BGB</i>	104
I. Abgrenzung zu Anwendungen	104
II. DLT-Netzwerke als Sachen	105
III. DLT-Netzwerke als Immaterialgut im Sinne der §87a ff. UrhG	106
1. Tatbestandsvoraussetzungen	107
a) Abstraktionsgrad der Betrachtung	107
b) Sammlung, systematische Ordnung und Unabhängigkeit der einzelnen Elemente	108
c) Datenbankhersteller	109
d) Wesentliche Investition	110

aa) Auslegungsmaßstab	110
bb) Bezugspunkt der Investition	110
cc) Beschaffung, Überprüfung oder Darstellung	111
dd) Wesentlichkeit der Investition	112
ee) Zwischenergebnis	113
2. Innenverhältnis und gewährte Rechte	114
a) Verhältnis der Datenbankhersteller untereinander	114
b) § 744 II BGB als relevante Konsequenz	116
c) Schutzzumfang	118
aa) Kein Bearbeitungsrecht	118
bb) Vervielfältigungsrecht	119
(1) Nutzung	119
(2) Beitritt neuer Nodes	120
cc) Weiterwendungsrecht bzw. öffentliches Wiedergaberecht	121
dd) Zwischenergebnis	122
ee) Verzicht auf Leistungsschutz in offenen Netzwerken	122
ff) Exkurs: Schutz technischer Maßnahmen, § 95a UrhG	123
gg) Zusammenfassung und Zwischenergebnis	125
d) Geschlossene Netzwerke	125
3. Weitere Rechtsfolgen	125
a) Zeitlicher Schutz nach § 87d UrhG	125
b) Materielle Reziprozität	126
c) Zivilrechtliche Sanktionsnormen	126
4. Ergebnis	126
<i>D. Gesamtergebnis zu Teil 2 und Konsequenzen</i>	<i>127</i>
Teil 3: Haftung	129
<i>A. Einordnung DLT-basierter Anwendungen</i>	<i>130</i>
I. Kryptowährungseinheiten und Coins	130
1. Einordnung als sonstiger Gegenstand	130
2. Absolutes Recht im Sinne des § 823 I BGB	131
a) Stand der Diskussion	131
b) Bewertung	132
aa) Daten als von der Rechtsordnung geschützte Position	132
bb) Einflussmöglichkeit der Full Nodes	133
cc) Wille des Gesetzgebers in § 2 III eWPG	134
dd) Zwischenergebnis	135
3. Erfassung über Eingriffskondiktion?	135
II. Token	136
1. Herkömmliche Token	136
2. Sonderfall eWpG	137

III. Andere absolute Rechtspositionen, insbesondere Immaterialgüterrechte	137
IV. Ergebnis	138
<i>B. Haftung der Nutzer</i>	139
I. Grundsatz	139
1. Verteilung des Technologierisikos im bilateralen Vertragsverhältnis	139
2. Außervertragliche Ansprüche und Konstellationen	139
a) Keine Verkehrssicherungspflicht einzelner Nutzer nach § 823 I BGB	140
b) Andere gesetzliche Ansprüche	141
c) Berücksichtigung der Rechtsdurchsetzungsdefizite in offenen Netzwerken	142
d) Zwischenergebnis	142
II. Das Haftungskonzept nach dem eWpG	142
1. Haftungszuweisung durch § 7 eWpG	143
a) Formelles Verständnis der registerführenden Stelle	143
b) Nutzer als Zuordnungssubjekt der Haftung des eWpG	144
2. Ausgestaltung von § 7 eWpG	145
a) Inhalt und Umfang der Haftung	145
b) Kreis der Anspruchsberechtigten	145
3. Abschied vom Verursacherprinzip	146
4. Ergebnis	148
III. Einfluss der MiCA (VO 2019/1937)	148
1. Nutzerzentrierte Anknüpfung	149
2. Keine Zuordnung von Verantwortlichkeiten für das Technologierisiko	149
IV. Ergebnis	150
<i>C. Haftung der Betreiber</i>	150
I. Offene Netzwerke	150
1. Full Nodes	150
a) Eigenes Verhalten	151
aa) Ein- und Austritt	151
bb) Forking	152
b) Verantwortlichkeit für gespeicherte Inhalte	153
aa) Anspruchsgrundlage	154
(1) Die Störerhaftung und ihre ungeklärten dogmatischen Grundlagen	154
(2) Full Nodes als technisch verantwortliche Intermediäre	155
bb) Haftungsprivilegierungen nach TMG	156
(1) Anwendbarkeit der Haftungsprivilegien des TMG	157

(a) Grundlagen der telemedienrechtlichen Privilegierung	157
(b) Übertragung auf DLT-Netzwerke	158
(c) Keine Anwendung des UrhDaG	159
(2) Konkrete Voraussetzungen	159
(a) DLT-Netzwerk als Informations- und Kommunikationsdienst	159
(b) Full Nodes als Diensteanbieter	160
(c) Abgrenzung von eigenen und fremden Informationen	161
(d) Hostprovider nach § 10 TMG	163
(aa) Tatbestandsvoraussetzungen	163
(bb) Rechtsfolgen	164
cc) Negatorische Ansprüche	167
dd) Ergebnis der Haftung für Full Nodes	168
ee) Keine Haftung für unrichtige Transaktionshistorie	168
2. Validatoren	169
a) Eigenes Verhalten	169
aa) Koordinierte Mehrheitsangriffe	169
bb) Verzögerung des Validierungsprozesses durch einzelne Validatoren	169
b) Fremdes Verhalten	170
c) Zwischenergebnis	171
II. Geschlossene DLT-Netzwerke	171
1. Keine Verantwortlichkeit der Kontrollinstanz nach § 8 TMG	171
2. Full Nodes und Validatoren in geschlossenen Systemen	173
III. Ergebnis	174
<i>D. Haftung der Entwickler</i>	174
I. Praktische Bedeutung der Entwicklerhaftung	175
II. Entwickler als mittelbare Verursacher	177
III. Grundlagen der Inanspruchnahme	177
1. Open-Source-Lizenzen als Basis der Softwaredistribution	178
a) Open-Source-System	178
b) In DLT-Netzwerken verwendete Lizenzen	178
2. Vertragskonstellationen	179
a) Beteiligte	179
aa) Entwickler	179
(1) Miturhebergemeinschaft qua Gesetz	180
(2) Gesellschaft qua Vereinbarung	180
(3) Außenrechtsfähigkeit und daraus resultierende Haftung	181
(4) On-Chain-Netzwerke	182

bb) Nodebetreiber und Distributoren	182
b) Vertragsinhalt, insbesondere Gewährleistung	182
c) Vertrag zwischen Entwickler und Full Node	183
aa) Unwirksamkeit nach AGB-Recht	183
bb) Gewährleistung und Schadensersatz	184
(1) Updateverpflichtungen	184
(2) Ausschluss von Mangelfolgeschäden durch den Schutzzweck der Norm	185
cc) Erwerb über den haftungsprivilegierten Distributor	187
dd) Keine Differenzierung zwischen den Formen des Netzwerks	189
d) Zwischenergebnis	189
3. Außervertragliche Haftung	189
a) Produkthaftungsgesetz	190
aa) Produkt, § 2 ProdHaftG	190
bb) Ausschluss nach § 1 II Nr. 3 ProdHaftG	190
cc) Sachbeschädigung	191
(1) Sache	191
(2) Einschränkung durch § 1 S. 2 2. Hs ProdHaftG	191
(3) Zwischenergebnis	192
dd) Fazit für das Produkthaftungsgesetz	193
b) Allgemeines Deliktsrecht	193
aa) Anwendungsbereich	194
bb) Wertungswiderspruch zum Schenkungsrecht?	194
(1) Konkretisierung der Produzentenhaftung zur Update-Verpflichtung	195
(2) Haftung auf Schadensersatz?	196
(3) Lösung durch Beschränkung auf Gefahrenabwehr	196
IV. Conclusio: Entwickler als verantwortliche „key persons“ in offenen Netzwerken	197
Schluss	199
A. Zusammenfassung	199
B. Schlussüberlegungen und Ausblick	203
Literaturverzeichnis	205
Sachregister	213

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 unbekanntem Marktteilnehmern 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 Bezug¹ 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 Haftungsverbände 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 offenen⁵ 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 I, 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-Whitepaper¹ 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 benutzten 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 Nakamoto⁴ „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 Blockchain⁶ 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-Netzwerks⁹

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 Nodes¹⁰ (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. Grundsätzlich¹³ 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

- Adressen *siehe* Key
AGB 142 f., 183 f.
Auskunftsanspruch 50 ff.
Auslobung 61
- Betreiber 25, 150 ff.
Blockchain 13 f., 54 f., 76, *siehe auch*
DLT-Netzwerk
Bitcoin 24
- Code 22, 26, 179
– fehlerhafter 175
Coin 27 ff., 76, 95, 105, 130 ff., 135
– *Voting* 95
Corda 26, 36
- DAO 2, 33 f., 89 ff.
– The DAO 34, 48 f., 79, 140 f.
DApp 33
Daten 132
Datenbanken 7, 106 ff.
– Hersteller von 109 f., 114, 122
– Rechte an 118 ff.
Dezentralität 4, 9, 21 f., 47
Disruptivität 30
DLT-Netzwerk 39, 47, 73, 84, 91 ff.,
126, 158 ff., 178
– Funktionsweise 7 ff.
– konsortiale 64 f., 98
Domain 41
- Elektronische Wertpapiere 53 f.
– Gesetz zur Einführung elektronischer
Wertpapiere 53 f., 63, 73 f., 84,
134 ff., 142 ff.
Eingriffskondiktion 135
Entwickler 35, 174 ff.
Ethereum 8, 10, 24, 178, 180 ff., 194
- Fork 20 f., 152 f.
– Hard Fork 20, 88, 121, 123, 140
– Soft Fork 21
- Gatekeeper 52 ff., 55, 63
Gefälligkeit 71, 81
Gemeinschaft 104 ff.
– Innenverhältnis 114 ff.
Gesellschaft bürgerlichen Rechts 68 ff.,
93, 96, 180 f.
– Außenrechtsfähigkeit 96, 181
– gemeinsamer Zweck 69 f., 74 ff.,
82 ff., 98, 101
– Publikumsgesellschaft 93
Governance 22 f.
– Off-Chain 22, 88, 116, 165
– On-Chain 22 f., 87 ff., 89, 95, 165,
182 f.
- Haftung 129, 142 ff., 147, 168
– Privilegierung 156 ff., 187 ff.
– Produkt- 190 ff.
– Störer- 154 ff.,
Hyperledger 25 f., 178
- Internet 38 ff.
– Access-Provider 39, 66 f., 172
– Hostprovider 163 ff., 187 f.
– Serviceprovider 38
- Immaterialgüterrecht 106 ff., 137
Intermediär 46, 65, 146, 155 f.
IOTA 19, 36, 175
- Key 10 ff.
Körperschaft 91 ff.
Konsensmechanismus 17 f.
– Proof-of-Stake 19, 61, 95, 110, 112
– Proof-of-Work 8, 19, 61, 112

- Kryptowahrung *siehe* Coin
 Kryptowertpapierregister 53, 147
- Layer-1 54, 140
 Ledger 10
- MiCA 148 ff.
 Mining-Pools 36, 115, 170
- Netze *siehe* Netzwerk
 Netzwerk 141
 - geschlossenes 15, 18, 64 ff., 100, 125 f., 171 ff.
 - hybrides 16, 103
 - offenes 15, 18, 36, 60 ff., 74 f., 97 ff., 150 ff.
 - technikbasiertes 44 f.
- Nodes 9, 109 f.
 - Full Nodes 9 f., 35, 38, 60, 81 f., 86, 112 f., 114, 133, 150 ff., 160 ff., 164, 168, 183 f.
 - Light Nodes 10, 35, 113, 120
- Nutzer 36, 139 ff.
- Open-Source 35, 40 f., 89, 178 ff., 194
- Peer-to-Peer 1, 41 f., 60
 Plattform 36
 Pseudonymitat 48 ff.
- Recht, absolutes 131
 Rechtsbindungswille 61, 70 ff., 76, 87 ff., 90, 98, 115
 Rechtsdurchsetzungsdefizit 48 ff., 55, 81, 94, 142
 Register *siehe* Ledger
 Registerfuhrende Stelle 63, 68, 143 f.
- Sache 105, 130, 191 f.
 Schadensersatz 168, 179, 184, 196
 Schenkung 194 ff.
 Schutz technischer Manahmen 123
 Selbstregulierung 44, 49
 Smart Contracts 31 ff., 47
 Sternvertrag 101 f.
- Telemediengesetz 156 ff., 172 ff., 185
 Tezos 23 ff., 92 f.
 Transaktionen 10 ff., 19 ff., 108, 133, 139, 168
 Token 29 ff., 136 ff.
- Validator 81, 85 ff., 109, 114, 169 ff., 173
 Vertragsnetz 77 ff., 103
 Vertrag zugunsten Dritter 102
- Wallet
 - Anbieter 36, 51, 62,
 - Betreiber *siehe* Wallet-Anbieter
- Whitepaper 8, 24, 123