BERLINER RECHTSZEITSCHRIFT

JURISTISCHE FACHZEITSCHRIFT AN DER FREIEN UNIVERSITÄT BERLIN

AUS DER PRAXIS

Dr. Jakob Degen und Kristin Dortans
Arbeitsrecht skurril – Geschichten, die das Leben schreibt

ZIVILRECHT

Helena Ferber
Corporate Digital Responsibility –
Einsatz von KI in der Unternehmensleitung

ÖFFENTLICHES RECHT

Jakob S. Feddersen
Keine Steuern für Digitalkonzerne? – zur beihilfenrechtlichen Kontrolle von Steuervorteilen für Internetgiganten

Adrian Kaufmann
Öffentliche Blockchains im Spannungsfeld zur datenschutzrechtlichen Verantwortlichkeit der DSGVO

STRAFRECHT

Jan Breede
Die einverständliche Fremdgefährdung

GRUNDLAGEN DES RECHTS

Jann Maatz
Willensfreiheit und Privatrecht

Charles E. Müller
Die Sozialbindung des Eigentums –
Rudolf von Jherings Vorarbeit für § 906 BGB

3. Jahrgang | Seiten 89–176
www.berlinerrechtszeitschrift.de
ISSN (Print) 2699-948X | ISSN (Online) 2699-2132

AUSGABE 2/2022

Adrian Kaufmann[*]

Öffentliche Blockchains im Spannungsfeld zur datenschutzrechtlichen Verantwortlichkeit der DSGVO

Den Verantwortlichen für den Datenschutz zu bestimmen, ist nicht nur für die Datenschutzbehörden und die Betroffenen wichtig, sondern auch für die Zukunft der Blockchain-Technologie. Etwaige Innovationsbremsen können nur dann von Entwicklern und der Politik gelöst werden, wenn Rechtssicherheit darüber besteht, wer nach den derzeitigen technischen und rechtlichen Gegebenheiten die datenschutzrechtliche Verantwortung trägt. Diese Arbeit soll hierzu beitragen, indem sie nach einem kurzen Blick auf die Grundlagen der Blockchain-Technologie die gegenwärtige Diskussion über die Person des Verantwortlichen zusammenfasst und unter Berücksichtigung der aktuellen Rechtsprechung des EuGH die verantwortlichen Personen ermittelt. Dabei soll der Blick allein auf die öffentlichen, zulassungsfreien Blockchains gerichtet werden, da bei ihnen die Dezentralität und damit auch das Spannungsfeld zum Datenschutzrecht am stärksten ausgeprägt ist.

Inhaltsübersicht

A. Einleitung 130
B. Grundlagen der Blockchain-Technologie 131
I. Technische Grundlagen der Blockchain 131
1. Verkettete Liste 131
2. Proof of Work 131
3. Prinzip der längsten Kette 131
4. Public und Private Key 131
5. Ablauf der Datenspeicherung 131
II. Einordnung von Blockchains in Kategorien 131
III. Zusammenfassung 132
C. Sachlicher Anwendungsbereich der DSGVO 132
I. Personenbezogene Daten 132
II. Stand der derzeitigen Diskussion 132
III. Verarbeitung 132
IV. Zusammenfassung 132
D. Verantwortliche im Kontext der DSGVO 132
I. Begriffsdefinition 133
II. Gemeinsame Verantwortlichkeit 133
E. Verantwortlichkeit in einer öffentlichen Blockchain 133
I. Betrachtungsrichtungen 133
II. Mikroperspektive 134
1. Nutzer 134
2. Miner 135
3. Nodes 136
4. Zwischenergebnis Mikroperspektive 137
III. Makroperspektive 137
1. Bedeutung des Protokolls 137
2. Entwickler 137
3. Miner und Nodes 138
4. Zwischenergebnis Markoperspektive 139
IV. Verhältnismäßigkeit 139
1. Unmittelbare Konsequenzen des Ergebnisses .. 139
2. Abwägung 139
V. Stellungnahme: Reformbedarf? 140
F. Ergebnis 140

A. Einleitung

Die Blockchain stellt eine neue, innovative und vielversprechende Technologie dar. Sie ermöglicht es, Informationen sicher zu speichern, ohne Vertrauen in eine Person setzen zu müssen. Wesensmerkmale der Blockchain-Technologie sind – jedenfalls in ihrer „reinsten" Ausprägung – die dezentrale Speicherung und die grundsätzliche Unveränderbarkeit der Daten. Informationen werden nicht auf einem einzelnen Server gespeichert, sondern auf vielen unterschiedlichen Computern (sog. *Nodes*).[1] Die Inhaber dieser Computer können die Daten nicht allein verändern oder in anderer Weise nutzen. Bei der Blockchain muss der Nutzer deshalb nicht einem Serverinhaber, sondern dem System vertrauen. Diese Dezentralität lässt jedoch ein neues Spannungsfeld zum Datenschutzrecht entstehen.[2] So setzt etwa die DSGVO[3] gerade voraus, dass mindestens eine Person als Verantwortlicher für die Einhaltung der datenschutzrechtlichen Vorschriften einzustehen hat.[4]

Diese Arbeit soll der Frage nachgehen, wer in einer öffentlichen Blockchain Verantwortlicher im Sinne der DSGVO ist. Zuerst werden die dafür relevanten, technischen Grundlagen der Blockchain-Technologie zusammengefasst (B.). Anschließend wird ein Blick auf den sachlichen Anwendungsbereich der DSGVO (C.) und den Begriff der Verantwortlichkeit in der DSGVO (D.) geworfen. Aufgrund der dort erarbeiteten Kriterien werden sodann die Akteure darauf untersucht, ob sie zum Kreis der Verantwortlichen gehören (E.). Zuletzt werden die gewonnenen Erkenntnisse zusammengefasst (F.).

[*] Der *Verfasser*, Adrian Kaufmann, studiert im 8. Semester Rechtswissenschaft an der Christian-Albrechts-Universität zu Kiel. Der Beitrag beruht auf einer Seminararbeit bei Professorin Dr. *Susanne Gössl* LL.M. (Tulane) aus dem Seminar „Themen der Digitalisierung im SoSe 2021".

[1] *Kaulartz*, CR 2016, 474 (475).

[2] *Schrey/Thalhofer*, NJW 2017, 1431 (1433).

[3] Verordnung (EU) 2016/679 v. 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. EU Nr. L 119, S. 1.

[4] Vgl. *Schrey/Thalhofer*, NJW 2017, 1431 (1433).

B. Grundlagen der Blockchain-Technologie

I. Technische Grundlagen der Blockchain

Die Vorteile der Blockchain ergeben sich aus den charakteristischen Merkmalen der Dezentralität und Unveränderbarkeit. Im Gegensatz zu herkömmlichen Speichern, wie etwa in einer *Cloud*, gibt es keine zentrale Instanz.[5] Die Daten werden stattdessen auf einer Vielzahl von Computern (sog. *Nodes*) gespeichert.[6]

1. Verkettete Liste

Die Informationen werden zu Blöcken zusammengefasst und aneinander angehängt. Dadurch entsteht eine Kette von Blöcken, die der Blockchain ihren Namen gibt. Angehängt werden die Blöcke, indem sie auf den *Hash*-Wert des vorherigen Blocks verweisen.[7] Der *Hash*-Wert ist eine Art „Prüfsumme"[8] und praktisch einzigartig.[9] Werden die Daten eines Blocks geändert, der Block gelöscht oder ein weiterer Block dazwischengeschoben, ist die Kette unterbrochen. Wenn sich der Inhalt des Blocks ändert, ändert sich auch dessen *Hash*-Wert. Der nachfolgende Block setzt die Kette nicht mehr fort. Ändert man den Verweis in diesem Block, verändert sich wiederum sein *Hash*-Wert und der nächste Datenblock bricht die Kette. Will man die Daten der Kette nachträglich verändern, muss daher die gesamte Kette angepasst werden.[10]

2. Proof of Work

Die Verweise der folgenden Blöcke zu ändern, wäre an sich noch nicht aufwändig genug, um nachträgliche Änderungen auszuschließen. Daher wird das Prinzip um das *proof-of-work*-Verfahren erweitert. Jeder Block enthält eine algorithmische Aufgabe, die durch die sog. *Miner* gelöst wird. Die Aufgabe ist so gestaltet, dass sie schwierig und nur durch viel Rechenleistung zu lösen, aber einfach zu verifizieren ist.[11] Aufgabe und Lösung sind vom Inhalt des Blocks abhängig. Die Lösung muss bei einer Änderung daher nicht nur für den konkreten Block, sondern auch für alle folgenden Blöcke erneut berechnet werden.

3. Prinzip der längsten Kette

Die Änderung des Blocks wird von den übrigen *Nodes* erst übernommen, wenn er in der längsten Kette des Netzwerkes steht.[12] Die Verkettung braucht durch das *proof-of-work*-Verfahren immer einen Arbeitsnachweis in Form von Rechenleistung. Allein um eine ebenso lange Kette zu erhalten, muss er dafür zwangsläufig genauso viel Rechenleistung aufbringen, wie das gesamte übrige Netzwerk aufgebracht hatte, um die Blöcke zu errichten.[13]

4. Public und Private Key

Für die Funktion der Blockchain von deutlich größerer Bedeutung als für die Frage nach dem datenschutzrechtlich Verantwortlichen sind der *public* und *private key*. Der *public key* ist eine Signatur, die insbesondere bei Kryptowährungen mit einer Kontonummer verglichen werden kann.[14] Der *private key* ist die Ermächtigung, Informationen zu übermitteln, und daher mit einer Unterschrift vergleichbar.[15]

5. Ablauf der Datenspeicherung

Daten werden auf Initiative eines Nutzers auf der Blockchain gespeichert. Bei der Kryptowährung *Bitcoin* etwa vollzieht ein Nutzer eine Transaktion, infolgedessen die Transaktionsdaten gespeichert werden. Die Informationen werden an eine *Node* weitergeleitet. Diese gibt sie an *Miner* weiter, die eine oder mehrere Informationen in Blöcken zusammenfassen und um die Lösung des algorithmischen Rätsels ergänzen. Anschließend gibt die *Node* den Block im gesamten Netzwerk bekannt. Die übrigen *Nodes* verifizieren den Block anhand formaler Kriterien und hängen den Block anschließend in ihrer Kopie der Blockchain an.[16]

II. Einordnung von Blockchains in Kategorien

Blockchains können unterschiedlich ausgestaltet werden. Grob lassen sie sich danach kategorisieren, ob Lesezugriff besteht und in welcher Weise eine Person Schreibzugriff auf die Blockchain erhält: Bei öffentlichen Blockchains kann jeder die (verschlüsselten) Informationen einsehen.[17] In einer privaten Blockchain gibt es einen Administrator, der entscheidet, wer Zugang erhält und wer nicht.[18]

Anhand des Schreibzugriffs lässt sich zwischen zulassungspflichtigen und zulassungsfreien Blockchains unterscheiden.[19] Bei zulassungsfreien Blockchains kann jede Person die entsprechende Software herunterladen und als

[5] *Kaulartz*, CR 2016, 474 (475).
[6] *Kaulartz*, CR 2016, 474 (475).
[7] *Böhme/Pesch*, DuD 2017, 473 (474).
[8] *Böhme/Pesch*, DuD 2017, 473 (474).
[9] *Kaulartz*, CR 2016, 474 (475).
[10] *Pachernegg*, Die Blockchain-Technologie im Fokus der DSGVO, S. 20, https://epub.jku.at/obvulihs/content/titleinfo/4898963, zuletzt abgerufen am 18.8.2022; *Böhme/Pesch*, DuD 2017, 473 (474).
[11] *Böhme/Pesch*, DuD 2017, 473 (474 f.).
[12] *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, S. 3, https://bitcoin.org/bitcoin.pdf, zuletzt abgerufen am 18.8.2022.
[13] *Böhme/Pesch*, DuD 2017, 473 (475); *Schrey/Thalhofer*, NJW 2017, 1431 (1432).
[14] *Kaulartz*, CR 2016, 474 (475).
[15] *Kaulartz*, CR 2016, 474 (476).
[16] *Buocz et al.*, Computer Law and Security Review 2019, 182 zitiert nach SSRN3297531, dort S. 24.
[17] *Finck*, Blockchain and the General Data Protection Regulation, European Parliamentary Research Service, PE 634.445, S. 5, https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019).634445_EN.pdf, zuletzt abgerufen am 18.8.2022; *dies*., European Data Protection Law Review (EDPL) 2018, 17 (19 f.); *Martini/Weinzierl*, NVwZ 2017, 1251 (1252); *Hein/Wellbrock/Hein,* Rechtliche Herausforderungen von Blockchain-Anwendungen, 2019, S. 12.
[18] *Finck*, EDPL 2018, 17 (19).
[19] *Welzel et al.*, Mythos Blockchain: Herausforderungen für den öffentlichen Sektor 2017, S. 15, https://www.oeffentliche-it.de/documents/1018

Miner oder *Node* am Netzwerk mitwirken, während bei zulassungsbeschränkten Blockchains die Teilnehmer von einem Administrator ausgewählt werden.[20]

III. Zusammenfassung[21]

Bei den öffentlichen, zulassungsfreien Blockchains gibt es keine zentrale Stelle, die eine herausgehobene und mit besonderer Entscheidungsgewalt versehene Stellung innehat. Stattdessen gibt es eine Vielzahl an Beteiligten, die als Verantwortliche in Frage kommen.

Nachfolgend wird der Blick auf das Datenschutzrecht gelegt, um die Kriterien zu bestimmen, die für die Ermittlung der Verantwortlichen entscheidend sind.

C. Sachlicher Anwendungsbereich der DSGVO

Die Daten auf einer Blockchain werden in der Regel verschlüsselt und die Nutzer treten unter Pseudonymen auf. Führt dies dazu, dass die DSGVO nicht anwendbar ist, stellt sich die Frage nach dem Verantwortlichen gar nicht erst.

Sachlich anwendbar ist die DSGVO gemäß Art. 2 Abs. 1 für die automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

I. Personenbezogene Daten

Eine Definition der personenbezogenen Daten enthält wiederum Art. 4 Nr. 1 Hs. 1 DSGVO. Danach sind personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Bei Blockchains hängt der Personenbezug vom Inhalt der Daten ab, die auf ihr gespeichert werden. Je nach Anwendungsbereich der Blockchain können deshalb mal mehr und mal weniger personenbezogene Daten enthalten sein. Unter den vielen Anwendungsmöglichkeiten existieren einige, etwa digitale Personalausweise im Identitätsmanagement, die zwangsläufig personenbezogene Daten speichern müssen.

II. Stand der derzeitigen Diskussion

In der Literatur wird diskutiert, ob die natürlichen Personen hinter den Daten identifizierbar sind.[22] Zur Identifizierung einer Person gibt es einige Anhaltspunkte: *Public key*s können ggf. mit Informationen (z.B. bei Einkäufen mit Kreditkarten) oder IP-Adressen verbunden werden.[23] Und auch die gespeicherten Informationen können einer konkreten Person zugeordnet werden, wenn sie unverschlüsselt oder ungenügend verschlüsselt abgelegt werden.[24] Die vielfältigen Anwendungsmöglichkeiten lassen hier keine einheitliche Bewertung zu. Die Anonymisierung von Daten stellt aber bereits eine Möglichkeit dar, die Blockchain datenschutzkonform auszugestalten, ohne die Frage nach dem Verantwortlichen stellen zu müssen.[25]

III. Verarbeitung

Die zweite Voraussetzung für die sachliche Anwendbarkeit der DSGVO ist die Verarbeitung der Daten. Verarbeitung ist jeder „mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, […] die Speicherung, […] das Auslesen, […] die Offenlegung durch Übermittlung“ (Art. 4 Nr. 2 DSGVO). Damit ist nahezu jeder Vorgang mit personenbezogenen Daten eine Verarbeitung.[26]

Auf die Blockchain bezogen ist die Speicherung der Daten auf den *Nodes* eine Verarbeitung. Aber auch die Aufgabe der *Miner* ist von den Daten abhängig, die auf dem vorangegangenen Block gespeichert sind. Denn daraus ergibt sich der *Hash*-Wert des Blocks. Die Lösung der algorithmischen Aufgabe durch die *Miner* kommt daher auch für die Verarbeitung in Frage.

Zudem kommt auch die Verarbeitung der Daten durch Weitergabe an die anderen *Nodes* in Betracht. Ordnet man die *Nodes* als gemeinsam verantwortlich ein, stellt die Weitergabe eine Verwendung der Daten dar; andernfalls ist es eine Offenlegung.[27]

IV. Zusammenfassung

Die Zuordnung der Informationen zu einer konkreten Person ist im Rahmen der Blockchain durchaus möglich. Da diese Informationen von *Nodes* und *Minern* verarbeitet werden, ist die DSGVO sachlich anwendbar und es stellt sich die Frage nach dem Verantwortlichen.

D. Verantwortliche im Kontext der DSGVO

Art. 8 GRCh und Art. 16 AEUV enthalten Gewährleistungen für den Schutz von persönlichen Daten bei ihrer Verarbeitung. Die DSGVO kommt dem nach, indem sie Verantwortliche benennt, die als zentrale Figur für die Einhaltung

1/14412/Mythos+Blockchain+-+Herausforderung+für+den+Öffentliche n+Sektor, zuletzt aufgerufen am 18.8.2022.

[20] *Welzel et al.* (Fn. 19), S. 15.

[21] Weiterführend *Böhme/Pesch,* DuD 2017, 473.

[22] Etwa *Erbguth/Fasching*, ZD 2017, 560 (562 f.); *Kaulartz*, CR 2016, 474 (479 f.); *Quiel*, DuD 2018, 566 (568); *Schrey/Thalhofer*, NJW 2017, 1431 (1433).

[23] *Pachernegg* (Fn. 10), S. 51.

[24] Vgl. zum Interesse an unverschlüsselten Daten *Quiel*, DuD 2018, 566 (568).

[25] Siehe etwa *Erbguth*, Datenschutz auf öffentlichen Blockchains, https://erbguth.ch/Erbguth_DatenschutzBlockchains.pdf, zuletzt abgerufen am 18.8.2022; *Finck* (Fn. 17), S. 32 ff.

[26] *Schreiber,* in: Plath, DSGVO/BDSG, 3. Aufl. 2018, Art. 4 DSGVO Rn. 9; *Schild,* in: BeckOK-Datenschutzrecht, 39. Ed. 2021, Art. 4 DS-GVO Rn. 32.

[27] *Ernst,* in: Paal/Pauly, DS-GVO, 3. Aufl. 2021, Art. 4 DS-GVO Rn. 29.

des Datenschutzes verantwortlich sind.[28] Verantwortliche sind Adressaten der datenschutzrechtlichen Pflichten (z.B. Art. 5 Abs. 2 DSGVO) und der Betroffenenrechte. Um den Schutz effektiv auszugestalten, ist die Rolle des Verantwortlichen klar zugeteilt.[29]

I. Begriffsdefinition

Definiert wird der Begriff des Verantwortlichen in Art. 4 Nr. 7 Hs. 1 DSGVO als „die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet". Der Verantwortliche ist vom Auftragsverarbeiter abzugrenzen. Letzterer verarbeitet die personenbezogenen Daten im Auftrag des Verantwortlichen (Art. 4 Nr. 8 DSGVO) und kann durch seine Weisungsgebundenheit abgegrenzt werden.[30]

Die zentrale Voraussetzung für die Verantwortlichkeit ist das Entscheiden über die Zwecke und Mittel der Verarbeitung. Denn hinter jedem Beteiligten der Blockchain lässt sich letztlich immer eine natürliche oder juristische Person oder andere Stelle ausmachen, sodass diesem Kriterium keine Bedeutung zukommt.

Das Entscheiden über Zwecke und Mittel lässt sich wiederum in drei Bereiche zerlegen: das *Entscheiden*, die *Zwecke* und die *Mittel*. *Entscheiden* erfordert faktischen Einfluss auf die Zwecke und Mittel der Datenverarbeitung.[31] Wie sich aus dem Zusammenhang zu Art. 26 Abs. 1 S. 1 DSGVO und den anderen Sprachfassungen der DSGVO ergibt, ist *Entscheiden* eher als *Festlegen* zu verstehen.[32] Der *Zweck* ist das erwartete Ergebnis, das beabsichtigt wird oder die geplanten Aktionen leitet.[33] Die *Mittel* bezeichnen die Art und Weise, auf der ein Ergebnis oder Ziel erreicht wird.[34] Damit knüpft die Definition des Mittels an die des Zwecks an.

II. Gemeinsame Verantwortlichkeit

Wie die Definition des Verantwortlichen in Art. 4 Nr. 7 Hs. 1 DSGVO nahelegt, können auch mehrere Personen gemeinsam verantwortlich sein, wenn sie gemeinsam die Zwecke und Mittel der Verarbeitung festlegen (Art. 26 Abs. 1 S. 1 DSGVO). Die gemeinsame Verantwortlichkeit muss von der bloßen Mitursächlichkeit abgegrenzt werden. Entscheidend ist, dass die jeweiligen Personen hinreichend Einfluss auf die Ziele und die Art und Weise der Datenverarbeitung haben. Um einen möglichst wirksamen Schutz der personenbezogenen Daten zu ermöglichen, ist es hingegen nicht erforderlich, dass alle Personen gleichwertigen Einfluss haben.[35] Der Grad der Verantwortlichkeit einer jeden Person muss letztendlich im Einzelfall beurteilt werden.[36]

Wichtig war dem Verordnungsgesetzgeber, die Verantwortung klar zuzuteilen.[37] Dies ist notwendig, um den Schutz der personenbezogenen Daten in zweierlei Hinsicht effektiv auszugestalten: Zum einen ist der Verantwortliche Adressat der Betroffenenrechte. Will ein Betroffener seine Rechte geltend machen, muss ihm der Adressat bekannt sein. Bei gemeinsamer Verantwortlichkeit verpflichtet Art. 26 Abs. 1 S. 2 DSGVO dazu, die interne Zuständigkeit transparent zu regeln. Hier kann auch eine Anlaufstelle für Ansprüche aus Betroffenenrechten genannt werden (Art. 26 Abs. 1 S. 3 DSGVO). Diese ist aber, wie Art. 26 Abs. 3 DSGVO zeigt, für die Betroffenen nicht verpflichtend. Sie können sich vielmehr weiterhin an alle Verantwortlichen halten. Damit erschwert die gemeinsame Verantwortlichkeit nicht die Durchsetzung von Betroffenenrechten.[38] Zum anderen wird der Schutz dadurch gewährleistet, dass die Aufsichtsbehörden ihrer Arbeit effektiv nachkommen können.[39] Diese können sich zwar nicht an alle Verantwortlichen wenden,[40] ihre Arbeit wird aber durch die transparent dargelegten internen Zuständigkeiten nach Art. 26 Abs. 1 S. 2 DSGVO erleichtert.

E. Verantwortlichkeit in einer öffentlichen Blockchain

Im Folgenden sind alle Beteiligten im Hinblick auf ihre Handlungs- und Entscheidungsmöglichkeiten zu untersuchen, um einen oder mehrere Verantwortliche zu bestimmen.

I. Betrachtungsrichtungen

Die Handlungs- und Entscheidungsmöglichkeiten der Beteiligten lassen sich in zwei Ebenen einordnen: die konkrete Datenverarbeitung (Mikroperspektive) und die Blockchain als Struktur der Datenverarbeitung (Makroperspektive).[41]

[28] Artikel-29-Datenschutzgruppe, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", Working Paper WP 169, S. 5 f., https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_de.pdf, zuletzt abgerufen am 18.8.2022.
[29] Erwägungsgrund 79 DSGVO.
[30] Artikel-29-Datenschutzgruppe (Fn. 28), S. 31; *Schwartmann/Hermann,* in: HK-DS-GVO/BDSG, 2018, Art. 4 DS-GVO Rn. 132.
[31] Artikel-29-Datenschutzgruppe (Fn. 28), S. 12.
[32] *Peitz*, Datenschutzrechtliche Verantwortlichkeit in Blockchain-Systemen, 2020, S. 181 f.
[33] *Schwartmann/Mühlenbeck,* in: HK-DS-GVO/BDSG (Fn. 30), Art. 4 DS-GVO Rn. 121.
[34] Art-29-Datenschutzgruppe (Fn. 28), S. 16.
[35] EuGH, Urt. v. 5.6.2018, Wirtschaftsakademie Schleswig-Holstein, C-210/16; ECLI:EU:C:2018:388, Rn. 44; EuGH, Urt. v. 10.7.2018, Zeugen Jehovas, C-25/17; ECLI:EU:C:2018:551, Rn. 66; EuGH, Urt. v. 29.7.2019, Fashion ID, C-40/17; ECLI:EU:C:2019:629, Rn. 103.
[36] EuGH, Urt. v. 29.7.2019, Fashion ID, C-40/17; ECLI:EU:C:2019:629, Rn. 70.
[37] Erwägungsgrund 79 DSGVO.
[38] *Dovas*, ZD 2016, 512 (514).
[39] Erwägungsgrund 79 DSGVO.
[40] *Kremer*, in: HK-DS-GVO/BDSG (Fn. 30), Art. 26 DSGVO Rn. 44.
[41] *Bacon et al*., Blockchain Demystified, Queen Mary School of Law Legal Studies Research Paper No. 268/2017, S. 41 f., https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3091218, zuletzt abgerufen am 18.8.2022.

II. Mikroperspektive

Da die Anknüpfungspunkte aus Mikroperspektive näher an der konkreten Datenverarbeitung liegen, sollen sie zuerst untersucht werden.

1. Nutzer

Der Nutzer ist die Person, die die Speicherung auf der Blockchain und damit auch die weiteren Datenverarbeitungsschritte anstößt, etwa indem er eine *Bitcoin*-Transaktion vornimmt. Nur er entscheidet darüber, ob die konkreten Informationen an irgendeine *Node* gelangen.[42]

Im Gegensatz zu zentralen Systemen verfügen die Personen, die hinter dem System stehen, nur über wenig Einfluss auf die Datenverarbeitung. Der Eintrag wird nur beschränkt gegengeprüft und *Nodes* und *Miner* können den Eintrag kaum nachträglich beeinflussen. Die Entscheidungsmacht des Nutzers ist denen dieser Systembetreiber nicht mehr so untergeordnet, wie es bei zentralen Systemen der Fall ist. Der Nutzer könnte daher nicht nur als Nutzer, sondern als aktiver Teil des Systems gesehen werden,[43] der einen solchen Einfluss auf Zwecke und Mittel der Datenverarbeitung hat, dass sich die Verantwortung von den übrigen Beteiligten auf den Nutzer verschiebt.[44] Hinsichtlich seiner eigenen personenbezogenen Daten wäre er dadurch datenschutzrechtlich gleichzeitig als Betroffener und als Verantwortlicher einzuordnen.[45]

a) Zweck und Mittel

Der Zweck der Datenverarbeitung wird dann mit dem Zweck der Nutzung – etwa einer *Bitcoin*-Transaktion – gleichgesetzt.[46] Das „Bestimmen" über die Mittel wird dann zum Teil darin gesehen, dass der Nutzer sich für eine bestimmte Blockchain – einschließlich ihrer Mittel der Datenverarbeitung – entschieden hat.[47] Dieser Entscheidung des Nutzers folgend werden die Daten dann von *Minern* und *Nodes* verarbeitet.[48]

b) Entscheiden

Ob von einem „Entscheiden" gesprochen werden kann, richtet sich nach dem faktischen Einfluss, den der Nutzer auf die Datenverarbeitung hat. Hinsichtlich der Mittel der Datenverarbeitung kann der Nutzer (nur) zwischen den verschiedenen Blockchains wählen. Insoweit unterscheidet sich die Blockchain nicht von einem *Cloud*-Service, wo der Nutzer auch nur zwischen verschiedenen Anbietern wählen kann.[49] Die Unterschiede zur *Cloud* zeigen sich aber bei der Wahl des Zwecks: Auf der *Cloud* kann der Nutzer im Grunde alle möglichen Daten ablegen und dabei gänzlich unterschiedliche Zwecke verfolgen. Bei der Blockchain gilt dies typischerweise nicht. Es können zwar im Grundsatz alle Arten von Informationen auf Blockchains gespeichert werden, die einzelnen Blockchains sind aber in der Regel auf eine bestimmte Art von Information zugeschnitten. So werden etwa auf der *Bitcoin*-Blockchain ausschließlich Transaktionen abgespeichert. Der Nutzer hat dadurch eine so eingeschränkte Entscheidungsbefugnis, dass der Zweck im Wesentlichen vom System vorgegeben wird.[50]

Dies zeigt sich auch bei dem Vergleich von dem Nutzer einer Blockchain mit dem Betreiber einer Facebookseite: In seinem Urteil „Wirtschaftsakademie Schleswig-Holstein" argumentierte der EuGH, dass der Betreiber einer Facebookseite (fast gänzlich frei) festlegen könne, nach welchen Kriterien Statistiken über die Besucher der Seite erstellt werden.[51] Bei einer Blockchain hat der Nutzer kaum eine Möglichkeit, die Art der Informationen, die auf der Blockchain abgelegt werden, zu beeinflussen. Bei dem Vergleich mit dem Betreiber einer Facebookseite ergibt sich darüber hinaus ein weiteres Problem: Der Blockchain-Nutzer verliert jeglichen Einfluss, sobald er eine Information an das Blockchain-Netzwerk gesendet hat.[52] Der Betreiber der Facebookseite kann hingegen seine Kriterien jederzeit ändern.

c) Problematik der Identität von Verantwortlichem und Betroffenem

Aber selbst wenn man den Nutzer als Verantwortlichen ansehen würde, hätte man das Problem nur aufgeschoben. Um Art. 8 GRCh gerecht zu werden, wäre es notwendig, dass mindestens eine weitere Person verantwortlich ist. Andernfalls würde durch neue Technik ein Raum geschaffen werden, in dem man sich gänzlich der Verantwortlichkeit für das System entziehen kann.[53] Es wäre deshalb mindestens eine weitere verantwortliche Person notwendig, gegen die der Betroffene seine Rechte geltend machen kann. Den Nutzer als Verantwortlichen einzuordnen wäre daher nicht zielführend.

[42] *Erbguth/Fasching*, ZD 2017, 560 (564).
[43] *Giannopoulou/Ferrari*, in: Internet Science, INSCI 2018. Lecture Notes in Computer Science, 2019, S. 203 zitiert nach SSRN3316954, dort S. 10.
[44] *De Filippi*, The Interplay between Decentralization and Privacy: The Case of Blockchain Technologies, S. 15, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2852689, zuletzt abgerufen am 18.8.2022; vgl. auch *Finck*, EDPL 2018, 17 (27).
[45] *Barsan*, Revue Trimestrielle de Droit Financier 2020, 58 (61); *Finck*, EDPL 2018, 17 (27).
[46] *Bacon et al.* (Fn. 41), S. 44; *Barsan*, Revue Trimestrielle de Droit Financier 2020, 58 (58).
[47] *Bacon et al.* (Fn. 41), S. 44.
[48] *Barsan,* Revue Trimestrielle de Droit Financier 2020, 58 (58).
[49] *Bacon et al.* (Fn. 41), S. 44 f.; *Finck*, (Fn. 17), S. 48.
[50] *Buocz et al.* (Fn. 16), zitiert nach SSRN3297531, dort S. 24.
[51] EuGH, Urt. v. 5.6.2018, Wirtschaftsakademie Schleswig-Holstein, C-210/16; ECLI:EU:C:2018:388, Rn. 36.
[52] *Hein/Wellbrock/Hein* (Fn. 17), S. 30.
[53] *Moerel*, European Review of Private Law 2019, 825 (843); *Wirth/Kolain*, Reports of the European Society for Socially Embedded Technologies 6 (2018), 1 (6).

d) Zwischenergebnis

Die Wahlmöglichkeiten des Nutzers sind stark eingeschränkt, weshalb es schwerfällt, ihm einen hinreichenden Einfluss auf Zwecke und Mittel der Datenverarbeitung zuzuschreiben. Der Nutzer kann deshalb nicht als Verantwortlicher angesehen werden.

2. Miner

Der einzelne *Miner* fasst eine oder mehrere Informationen in einem Block zusammen und versucht das algorithmische Rätsel zu lösen. Findet er die Lösung, fügt er sie in den Block ein und leitet den Block an die *Nodes* weiter. Er profitiert unmittelbar davon, indem er eine Belohnung (bei Kryptowährungen etwa *Coins*) erhält, wenn er als Erster das Rätsel gelöst hat. Diesen Profit zieht er damit unmittelbar aus der Datenverarbeitung.[54]

a) Handlungs- und Entscheidungsproblem

Der *Miner* hat allerdings keine Möglichkeit, auf die Daten, die er verarbeitet, einzuwirken.[55] Ändert er die Daten, wird sein Block von den übrigen *Minern* verworfen.[56] Er kann die Arbeit an einem bestimmten Block verweigern. Dies führt aber nicht dazu, dass die Information nicht mehr auf der Blockchain gespeichert wird. Die Information gelangt zurück in den Pool, aus dem *Miner* die Informationen in Blöcken abspeichern. Der einzelne *Miner* und auch alle anderen *Miner* können die Information weiterhin in einem Block speichern, das algorithmische Rätsel lösen und an die *Nodes* senden.[57] Bezogen auf eine konkrete Information kann der *Miner* also entscheiden, ob er für sie einen Block schaffen möchte.[58]

Auf die Speicherung der Daten bei den *Nodes* hat er keinerlei Einfluss. Er kann nur Blöcke an die *Nodes* senden, damit sie die Blöcke an die Kette anfügen. Umgekehrt kann er aber nicht anregen, Daten in Blöcken zu ändern oder Blöcke zu löschen. Ohne Einfluss ist es ihm auch nicht möglich, über die Verarbeitung dieser Daten zu „entscheiden".

b) Entscheiden über Zweck und Mittel

Zentrale Motivation für die Arbeit des *Miner*s ist die Belohnung. So werden etwa bei Kryptowährungen von *Minern* teilweise Informationen (konkret: Transaktionen) bevorzugt, bei denen sie höhere Transaktionsgebühren erhalten können.[59] Einen übergeordneten Zweck verfolgen die *Miner* mit der Verarbeitung der Daten hingegen nicht. Hinsichtlich der Mittel der Datenverarbeitung sieht es ähnlich aus: Der *Miner* kann sich nur dazu entscheiden, das Protokoll auszuführen oder nicht auszuführen. Führt er es aus, verarbeitet er die Daten so, wie es das Protokoll als Software vorsieht. Da er das Protokoll nicht für die konkrete Datenverarbeitung anpassen kann, hat er auch keine Entscheidungsgewalt über die Mittel der Datenverarbeitung.[60] Auch die kurzzeitige Kontrolle über den Block (samt Inhalt) führt nicht dazu, dass der *Miner* als Verantwortlicher einzuordnen ist.[61] Denn die Verantwortlichkeit setzt nicht an der Person an, die den Datenverarbeitungsvorgang ausführt, sondern an der Person, die über Zwecke und Mittel der Datenverarbeitung entscheidet (Art. 4 Nr. 7 Hs. 1 DSGVO).

c) Gemeinsame Verantwortlichkeit

Ein Zusammenschluss aller *Miner* oder einer hinreichenden Mehrheit von *Minern* hat einen deutlich höheren Einfluss auf die Blockchain. Sie können nicht nur darüber entscheiden, ob ein Block erstellt wird, sondern auch den Inhalt eines Blocks abändern. Sie verfügen nämlich über mehr Rechenleistung als der Rest der *Miner*, erstellen schneller Blöcke und damit auch die längere Kette. Ihre Entscheidungsmacht ist allerdings auch in diesem Fall eingeschränkt: Die *Nodes* prüfen die Blöcke anhand formaler Kriterien.[62] Daher kann auch eine hinreichende Mehrheit an *Minern* die Zwecke nicht frei festlegen.

In der Praxis erfolgt ein Zusammenschluss häufig in sog. *Mining-Pools*.[63] Diese achten aber darauf, dass sie nie die Mehrheit an Rechenleistung vereinen, da dies das *proof-of-work*-Verfahren und damit das Vertrauen im Netzwerk zerstören würde.[64] Eine gemeinsame Verantwortlichkeit aufgrund eines Zusammenschlusses der *Miner* scheidet deshalb in der Praxis aus und soll auch hier nicht in den Fokus gestellt werden.

d) Zwischenergebnis

Die *Miner* sind sehr weitgehend an die Regeln der Blockchain gebunden. Diese schränken ihren Entscheidungsspielraum derart ein, dass sie nicht genug Einfluss auf die Zwecke und Mittel haben, um die Verantwortung für die Datenverarbeitung zu übernehmen.

[54] *Martini/Weinzierl*, NVwZ 2017, 1251 (1254).
[55] *Erbguth/Fasching*, ZD 2017, 560 (564); *Ramos/Silva*, International Conference Series on Theory and Practice of Electronic Governance 2019, 342, zitiert nach SSRN3478036, dort S. 4; *Stadler/Bischler,* ZIIR 2019, 382 (388).
[56] *Erbguth/Fasching*, ZD 2017, 560 (564).
[57] *Hein/Wellbrock/Hein* (Fn. 17), S. 28.
[58] *Erbguth/Fasching*, ZD 2017, 560 (564).
[59] *Erbguth/Fasching*, ZD 2017, 560 (564).
[60] *Buocz et al.* (Fn 16), zitiert nach SSRN3297531, dort S. 25; *Pachernegg* (Fn. 10), S. 59.
[61] The Opinion of the Hungarian National Authority for Data Protection and Freedom of Information on Blockchain Technology in the Context of Data Protection, https://naih.hu/data-protection/decisions/file/312-the-opinion-of-the-hungarian-national-authority-for-data-protection-and-freedom-of-information-on-blockchain-technology-in-the-context-of-data-protection, zuletzt abgerufen am 18.8.2022.
[62] *Buocz et al.* (Fn. 16), zitiert nach SSRN3297531, dort S. 24; *Finck*, (Fn. 17), S. 46.
[63] *Pachernegg* (Fn. 10), S. 67.
[64] *Pachernegg* (Fn. 10), S. 67.

3. Nodes

a) Anknüpfungspunkte

Die einzelne *Node* kann in zweierlei Hinsicht relevant werden: Möchte der Nutzer Daten abspeichern, muss er sich an eine *Node* wenden. Diese gibt die Informationen an die *Miner* weiter, die die Daten dann in Blöcke verpacken und das algorithmische Rätsel lösen. Anschließend werden die Daten den restlichen *Nodes* bekanntgegeben. Neben dieser Weitergabe der Daten speichert jede einzelne *Node* die Daten auf ihrer Kopie der Blockchain ab. Vorher verifiziert die *Node* den Datenblock.[65]

Angeknüpft werden kann daher an die Speicherung und Verifizierung der Daten sowie an die Weitergabe der Daten an die übrigen *Nodes*.

b) Speicherung und Verifizierung der Daten

Die *Node* verarbeitet durch die Speicherung auf ihrer Kopie der Blockchain unmittelbar Daten.[66] Dabei hat ausschließlich sie den faktischen Einfluss darauf, ob die Datenverarbeitung von ihr vorgenommen wird oder nicht.[67] Daraus wird teilweise geschlossen, dass die einzelne *Node* für diese Datenverarbeitung verantwortlich sein müsse.[68] Anknüpfungspunkt dafür ist die Entscheidung der *Node* für die Speicherung der Daten.[69] Daraus ergibt sich aber noch nicht, dass die *Node* über die Zwecke und Mittel der Datenverarbeitung bestimmen würde.

aa) Zweck und Mittel

Hinsichtlich des Zwecks wird vorgebracht, jede *Node* habe ihre eigene Zielsetzung bei der Speicherung.[70] Unklar ist aber, welche Zielsetzung das sein soll. Anders als die *Miner* bekommen die *Nodes* für ihre Arbeit keine Vergütung in Aussicht gestellt. Damit bleibt allgemein betrachtet nur die „Teilnahme am Netzwerk" als Zielsetzung.[71] Mit der Teilnahme am Netzwerk können dann wiederum unterschiedliche Ziele verfolgt werden (z.B. höhere Sicherheit eigener Bitcoin-Transaktionen).[72]

Die Mittel der Datenverarbeitung ergeben sich aus dem Protokoll der Blockchain, welches die *Node* durch das Ausführen der entsprechenden Software umsetzt.[73]

bb) Entscheiden

Ein „Entscheiden" über die Mittel kann darüber hergeleitet werden, dass die *Node* sich für eine bestimmte Blockchain entschieden hat.[74] Diese Entscheidung ist aber nicht gleichzusetzen mit einem „Festlegen" der Zwecke und Mittel, da die *Node* nicht darüber entscheidet, wie die Daten verarbeitet werden, sondern nur, ob sie (nach den vorgegebenen Kriterien) verarbeitet werden.[75] Wie bereits im Kontext des Nutzers diskutiert, engt dies bei der Blockchain den Entscheidungsspielraum sehr weitgehend ein. Denn auch die *Node* ist an die Grenzen der gewählten Blockchain gebunden. Handelt sie entgegen den formalen Kriterien, wird sie von den anderen *Nodes* im Netzwerk ausgeschlossen.[76] Dadurch fehlt ihr der Einfluss auf die Mittel der Datenverarbeitung.[77] Ohne Einfluss auf die Mittel kann nicht die Rede davon sein, dass sie über diese entscheidet.[78]

cc) Gemeinsame Verantwortlichkeit

Betrachtet man nicht die Datenverarbeitung bei einer einzelnen *Node*, sondern alle Datenverarbeitungen der konkreten personenbezogenen Daten, lässt sich sagen, dass die *Nodes* zu gleichen Teilen daran mitwirken.[79]

Damit *Nodes* gemeinsam verantwortlich sind, müssen sie zusammen über die Zwecke und Mittel der Datenverarbeitung bestimmen (Art. 4 Nr. 7, Art. 26 Abs. 1 S. 1 DSGVO). Der Abschluss einer transparenten Vereinbarung über die internen Zuständigkeiten nach Art. 26 Abs. 1 S. 2 DSGVO ist keine Voraussetzung, sondern vielmehr die Folge der gemeinsamen Verantwortlichkeit.[80]

Selbst wenn man davon ausgeht, dass *Nodes* Zwecke und Mittel der Datenverarbeitung bestimmen, fällt es schwer, eine gemeinsame Verantwortlichkeit zu begründen. Das Merkmal „gemeinsam" kann als „zusammen mit" oder „nicht alleine" ausgelegt werden.[81] Entscheidungen mehrerer Personen, die aber jeweils eigenständig und unabhängig

[65] *Buocz et al.* (Fn. 16), zitiert nach SSRN3297531, dort S. 24; *Finck*, (Fn. 17), S. 46.
[66] *Bechtolf/Vogt*, ZD 2018, 66 (69); *Nath*, Cryptocurrency and Privacy: Economic Analysis of Law, S. 16, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3661287, zuletzt abgerufen am 18.8.2022.
[67] *Pachernegg* (Fn. 10), S. 61; *Stadler/Bichler*, ZIIR 2019, 382 (386).
[68] *Commission Nationale de l'Informatique et des Libertés*, Blockchain et RGPD: quelles solutions pour un usage responsable en présence de données personnelles?, S. 2, https://www.cnil.fr/sites/default/files/atoms/files/la_blockchain.pdf, zuletzt abgerufen am 18.8.2022.
[69] *Schrey/Thalhofer*, NJW 2017, 1431 (1433 f.).
[70] *Finck*, EDPL 2018, 17 (26); *Pachernegg* (Fn. 10), S. 62.
[71] *Bacon et al.* (Fn. 41), S. 44; *Martini/Weinzierl*, NVwZ 2017, 1251 (1253 f.).
[72] *Pesch/Sillaber*, Computer Law Review International (CRi) 2017, 166 (170).
[73] *Duarte*, An Introduction to Blockchain Technology From a Legal Perspective and Its Tensions With the GDPR, S. 37, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3545331, zuletzt abgerufen am 18.8.2022.
[74] *Finck*, EDPL 2018, 17 (26); *Terpedijan*, Jurimetrics Journal 2020, 253, zitiert nach SSRN3638736, dort S. 40.
[75] *Erbguth/Fasching*, ZD 2017, 560 (563); *Richter,* Blockchain – Rechtliche Aspekte aus Sicht der Finanzindustrie, in: Briner/Funk, DGRI Jahrbuch 2017, 2018, Rn. 29.
[76] *Erbguth/Fasching*, ZD 2017, 560 (563); vgl. *Finck*, EDPL 2018, 17 (27).
[77] *Fasching*, Anwendungsbereiche und ausgewählte Rechtsfragen der Blockchain-Technologie, 2017, S. 21.
[78] *Erbguth/Fasching*, ZD 2017, 560 (563).
[79] *Bechtholf/Vogt*, ZD 2018, 66 (69).
[80] *Kremer*, CR 2019, 225 (226); *Söbbing*, IT-Rechtsberater (ITRB) 2020, 218 (221).
[81] Artikel-29-Datenschutzgruppe (Fn. 28), S. 10 ff; *Lezzi/Oberlin*, ZD 2018, 398 (400).

voneinander sind, reichen daher nicht aus.[82] Die *Nodes* arbeiten jedoch gänzlich unabhängig voneinander und die funktionsfähige Blockchain stellt in diesem Sinne nur das Ergebnis ihrer unabhängigen Verhalten dar.[83] Sie sind daher nur mitursächlich, was mit einem „gemeinsamen Festlegen" nicht gleichzusetzen ist.[84]

c) Weitergabe der personenbezogenen Daten

Der Handlungs- und Entscheidungsspielraum bei der Weitergabe der personenbezogenen Daten an die *Miner* und die anderen *Nodes* ist vergleichbar mit dem der Speicherung. Die *Nodes* haben nur die Wahl zwischen den verschiedenen Blockchains und ob sie die Software der Blockchain ausführen oder nicht. Die Zwecke und Mittel der Speicherung werden im Wesentlichen von der Blockchain vorgegeben und können von den *Nodes* (zumindest auf Mikroebene) nicht beeinflusst werden.

d) Zwischenergebnis

Wie auch die *Miner* werden die *Nodes* in ihrer Entscheidung durch die Blockchain eingeschränkt. Sie haben daher nur geringen Einfluss auf Zweck und Mittel der Datenverarbeitung und können aufgrund ihrer Entscheidungsmöglichkeiten aus Mikroperspektive nicht verantwortlich sein.

4. Zwischenergebnis Mikroperspektive

Die Mikroperspektive konnte nicht dabei helfen, einen Verantwortlichen zu bestimmen. Dafür waren die Entscheidungsbefugnisse der Beteiligten auf dieser Ebene zu stark eingeschränkt und Zweck und Mittel zu sehr vom System der Blockchain vorgegeben. Es muss daher aus Makroperspektive nach dem Verantwortlichen gesucht werden. Anknüpfungspunkt ist dabei der Einfluss auf das System der Blockchain.[85]

III. Makroperspektive

1. Bedeutung des Protokolls

Das Protokoll enthält die Regeln des Blockchain-Netzwerks und schränkt damit die Entscheidungsgewalt aller Beteiligten ein.[86] Diese Regeln legen die Aufgaben der Beteiligten fest, insbesondere die der *Nodes* und *Miner.* Gleichzeitig beschränkt es regelmäßig den Kreis der Daten, die auf der Blockchain abgelegt werden können (z.B. Transaktionsdaten bei *Bitcoin* oder persönliche Daten bei *Decentralized Identifiers*). Die Wahlmöglichkeiten auf Seiten der Nutzer, der *Miner* und der *Nodes*, sind derart eingeschränkt, dass sie nicht über die Zwecke und Mittel entscheiden. Sie entscheiden, *ob* sie die Verarbeitung vornehmen, aber nur in sehr eingeschränkter Form über das *Warum* und das *Wie*. Legt man dies zugrunde, kommt man zu dem Schluss, dass das Protokoll die Zwecke und Mittel der Datenverarbeitung festlegt.[87] Das Protokoll selbst ist weder natürliche noch juristische Person und kann deshalb nicht verantwortlich sein (vgl. Art. 4 Nr. 7 DSGVO). Daher sind die Personen zu betrachten, die die Möglichkeit haben, das Protokoll und damit die Zwecke und Mittel der Datenverarbeitung festzulegen.[88]

2. Entwickler

Die Geschichte einer Blockchain beginnt immer bei einem Entwickler oder mehreren Entwicklern. Sie haben die Möglichkeit, das Protokoll der Blockchain datenschutzkonform auszugestalten und werden in Erwägungsgrund 78 der DSGVO angehalten, dies auch zu tun. Eine Verantwortlichkeit wird allein dadurch aber nicht zugewiesen.[89]

Die einzelnen Phasen, in denen Entwickler Einfluss auf die Blockchain ausüben, sind daher näher zu betrachten, um eine Aussage über ihre Verantwortlichkeit treffen zu können.

a) Initiatoren

aa) Personenkreis

Zuerst gibt es die Entwickler, die den *Code* für die Blockchain-Anwendung geschrieben und ihn implementiert haben. Diese Initialentwickler haben durch den *Code* einen Rahmen von Regeln und Aufgaben für die *Miner* und *Nodes* geschaffen.[90] Die Aufgabe der *Nodes* und *Miner* umfasst – etwa durch die Speicherung – die Verarbeitung personenbezogener Daten. Damit werden die Mittel der Datenverarbeitung im Protokoll vorgeschrieben.

Erstellen die Entwickler das Protokoll und die Implementierung – etwa aufgrund eines Werkvertrages – für eine andere Person, scheiden sie als Verantwortliche aus.[91] In diesem Fall legt der Dritte die Aufgaben und Regeln fest, während die Initialentwickler nur das Programm erstellen.[92] Der Dritte ist dann der Initiator.

bb) Entscheiden über Zweck und Mittel

Die Initiatoren sind nicht an der konkreten Datenverarbeitung beteiligt. Dies führt aber nicht dazu, dass sie kategorisch als Verantwortliche ausscheiden.[93] Entscheidend ist

[82] *Kremer,* CR 2019, 225 (228).
[83] *Böhme/Pesch*, DuD 2017, 473 (479); *Finck*, EDPL 2018, 17 (26); *Richter* (Fn. 75), Rn. 30.
[84] *Bechtholf/Vogt*, ZD 2018, 66 (69); a.A. *Peitz* (Fn. 31), S. 225.
[85] *Bacon et al.* (Fn. 41), S. 41.
[86] *De Filippi/Loveluck*, Internet Policy Review, 3 (2016), 1 (10).
[87] *Buocz et al.,* (Fn. 16), zitiert nach SSRN3297531, dort S. 27.
[88] *Buocz et al.,* (Fn. 16), zitiert nach SSRN3297531, dort S. 27.
[89] *Jaccard/Tharin*, GDPR & Blockchain: The Swiss Take, S. 12, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3575231, zuletzt abgerufen am 18.8.2022.
[90] *Buocz et al.,* (Fn. 16), zitiert nach SSRN3297531, dort S. 25.
[91] *Stadler/Bichler*, ZIIR 2019, 382 (387).
[92] Vgl. *Martini/Weinzierl*, NVwZ 2017, 1251 (1253), die jedoch unterstellen, die Entwickler würden immer auf Anweisung eines Dritten handeln.
[93] So aber *Isler*, Datenschutz auf der Blockchain, Jusletter 4. Dezember 2017, Rn. 33, https://jusletter.weblaw.ch/juslissues/2017/917/datenschutz

nach Art. 4 Nr. 7 Hs. 1 DSGVO nicht die persönliche Durchführung der Datenverarbeitung oder der unmittelbare Einfluss im Zeitpunkt der Datenverarbeitung, sondern die Entscheidungsgewalt über die Zwecke und Mittel. Diese kann auch zeitlich deutlich vor der konkreten Datenverarbeitung ausgeübt werden.

Das Protokoll ist jedoch in der Regel nachträglich abänderbar. Alle Beteiligten haben ein Interesse daran, Fehler zu beheben und die Blockchain auch an neue Bedingungen anpassen zu können. Die Initiatoren geben ihren Einfluss auf das Protokoll damit faktisch aus der Hand.[94] Sie haben einmal über die Zwecke und Mittel der Verarbeitung entschieden. Sie sind aber zu späteren Zeitpunkten nicht mehr in der Lage, Entscheidungen über diese zu treffen bzw. abzuändern, wenn sie nicht zum Personenkreis gehören, der auch die nachträglichen Protokolländerungen durchführt. Art. 4 Nr. 7 DSGVO spricht vom „Entscheiden", also von der Gegenwart und nicht von einer Person, die früher einmal entschieden hat. Einer Personengruppe die Verantwortung zuzuweisen, die aktuell keine Möglichkeit (mehr) hat, über Zwecke und Mittel zu entscheiden, wäre auch verfehlt, da sie ohne Einfluss etwaige Datenschutzpflichten gar nicht umsetzen kann.[95]

cc) Problematik der Sterblichkeit

Daneben gäbe es ein weiteres Problem: Die Gruppe der Initiatoren ist in der Regel ein Kreis von natürlichen Personen, die nicht austauschbar sind. Die Sterblichkeit von natürlichen Personen würde dazu führen, dass es nach einer gewissen Zeit keine Initialentwickler mehr gäbe. Weist man ihnen die Verantwortlichkeit zu, wäre es ab dem Todeszeitpunkt des letzten Initiators zumindest problematisch einen Verantwortlichen auszumachen.[96] Ohne einen Verantwortlichen würde ein Raum entstehen, in dem die personenbezogenen Daten nicht geschützt werden, obwohl weiterhin Daten verarbeitet werden. Dies wäre mit Art. 8 GRCh nicht vereinbar.[97]

Insgesamt scheiden die Initiatoren damit als Verantwortliche aus.

b) Entwickler-Community

aa) Personenkreis

Das Recht, das Protokoll zu ändern, steht typischerweise einer Gruppe von Entwicklern zu. Die fortlaufende Entwicklung erfolgt häufig als *open source*. Die Organisation innerhalb der *Entwickler-Community* kann aber unterschiedlich ausfallen:

Die *Community* kann sich demokratisch organisieren. Dann ändert sich der Personenkreis stetig, der darüber entscheidet, welche Änderungen implementiert werden.[98] Bei *Bitcoin* gibt es demgegenüber eine Gruppe von *Core-Developern*, die darüber entscheiden, welche Änderungen implementiert werden und welche nicht. Alle anderen Entwickler in der *Community* können Stellungnahmen abgeben und diskutieren, haben aber letztlich keine Entscheidungsgewalt.[99] In dieser Organisation bildet sich damit eine zentrale Stelle.[100]

bb) Entscheiden über Zweck und Mittel

Aber auch die *Entwickler-Community* kann Änderungen am Protokoll nicht durchsetzen.[101] Das alte Protokoll kann von den *Minern* und den *Nodes* weiterverwendet werden.[102] Ohne durchsetzbaren Einfluss auf das System ist das Änderungsrecht der *Entwickler-Community* eher ein Vorschlagsrecht.[103] Wird die Änderung aber angenommen, hatten die Entwickler erheblichen Einfluss auf die Ausgestaltung des Protokolls, da sie das Monopol auf das Vorschlagsrecht haben. Die Netzwerk-Teilnehmer können ohne die Entwickler keine Änderungen anstoßen. Damit kommt der *Entwickler-Community* eine wesentliche Rolle bei der Änderung des Protokolls und somit auch bei der Entscheidung über die Zwecke und Mittel der Datenverarbeitung zu.

3. Miner und Nodes

Aus Makroperspektive haben *Miner* und *Nodes* dieselben Entscheidungsmöglichkeiten.

a) Notwendiger Personenkreis

Die Entwickler-Community kann dem Blockchain-Netzwerk die Änderung nicht aufzwingen, denn das alte Protokoll ist weiterhin funktionstüchtig.[104] Daher müssen *Nodes* und *Miner* das neue Protokoll in Form der neuen Software ausführen, damit die Änderungen umgesetzt werden.[105] Das alte Protokoll wird, wenn es mit dem neuen Protokoll kompatibel ist (sog. *soft Fork*[106]), praktisch unanwendbar, sobald einige *Nodes* sowie *Miner* mit über 50 % der Rechenleistung über das neue Protokoll arbeiten. Dies ergibt sich aus dem Grundsatz, dass immer die längste Blockchain die

-auf-der-_fbecc2b55b.html__ONCE&login=false, zuletzt abgerufen am 18.8.2022; *Quiel*, DuD 2018, 566 (569).
[94] *Pachernegg* (Fn. 10), S. 59.
[95] *Richter* (Fn.75), Rn. 29.
[96] *Fasching* (Fn. 77), S. 20.
[97] *Peitz* (Fn. 32), S. 193 f.
[98] *Buocz et al.* (Fn. 16), zitiert nach SSRN3297531, dort S. 26; *de Laat*, Journal of Management and Governance, 2007, 165 (169).
[99] *Buocz et al.* (Fn. 16), zitiert nach SSRN3297531, dort S. 26.
[100] *De Filippi/Loveluck*, Internet Policy Review, 3 (2016), 1 (12).
[101] *Buocz et al.* (Fn. 16), zitiert nach SSRN3297531, dort S. 26; *Erbguth/Fasching*, ZD 2017, 560 (564); *Martini/Weinzierl*, NVwZ 2017, 1251 (1253).
[102] *De Filippi/Loveluck*, Internet Policy Review, 3 (2016), 1 (14); *Finck*, (Fn. 17), S. 44.
[103] *Buocz et al.* (Fn. 16), zitiert nach SSRN3297531, dort S. 26.
[104] *Buocz et al.* (Fn. 16), zitiert nach SSRN3297531, dort S. 27.
[105] *Buocz et al.* (Fn. 16), zitiert nach SSRN3297531, dort S. 27.
[106] *Atik/Gerro*, Hard Forks on the Bitcoin Blockchain: Reversible Exit, Continuing Voice, S. 7, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3203893, zuletzt abgerufen am 18.8.2022.

gültige ist. *Miner* und *Nodes*, die nach dem alten Protokoll arbeiten, erstellen eine parallele Verkettung. Auf Dauer wird aber diejenige Kette die längere sein, der sich die *Miner* mit der meisten Rechenleistung angeschlossen haben, da für diese die Blöcke schneller generiert werden können.

b) Entscheidungsspielraum

Im Ergebnis bedarf es daher eines Zusammenspiels von Entwickler-Community, *Minern* und *Nodes*, um das Protokoll zu ändern. Sie sind mit unterschiedlichen Rechten ausgestattet. Gemein ist ihnen jedoch, dass sie alle die Möglichkeit haben, die Änderung zu blockieren: Die Entwickler haben das Initiativrecht und es bedarf der *Miner* und der *Nodes*, damit die Änderung vorgenommen wird.

Die Entscheidungsmacht der *Nodes* und *Miner* kann auch hier hinterfragt werden. Im Grunde können sie nur entscheiden, ob sie die Änderung umsetzen wollen. Ihnen fehlt auf den ersten Blick abermals die Möglichkeit, Einfluss auf die Gestaltung des Protokolls zu nehmen. Hier haben die *Miner* und *Nodes* aber durch ihr Blockaderecht faktischen Einfluss auf die Entwickler-Community und damit mittelbar auch auf die Ausgestaltung des Protokolls.

Ob man den Einfluss zwischen Entwickler-Community, *Minern* und *Nodes* nun gleich gewichtet oder Abstufungen vornimmt, ist für die Frage nach der Verantwortlichkeit nicht von Belang.[107] So können alle Personen, die einen hinreichenden Einfluss auf die Zwecke und Mittel der Datenverarbeitung haben, als Verantwortliche herangezogen werden, womit ein besserer Schutz der personenbezogenen Daten bewirkt werden soll.[108]

4. Zwischenergebnis Markoperspektive

Im Ergebnis haben Entwickler-Community, *Miner* und *Nodes* die Möglichkeit, gemeinsam das Protokoll zu ändern. Damit legen sie nach derzeitigem Stand die Zwecke und Mittel der Datenverarbeitung fest und sind gemeinsam verantwortlich.

IV. Verhältnismäßigkeit

1. Unmittelbare Konsequenzen des Ergebnisses

Die gemeinsame Verantwortlichkeit führt insbesondere zu zwei rechtlichen Folgen: Jeder Verantwortliche muss die datenschutzrechtlichen Pflichten erfüllen (Art. 26 Abs. 3 DSGVO). Dadurch ist jeder von ihnen insbesondere Adressat, wenn Betroffene ihre Rechte geltend machen wollen. Weiterhin erfordert die gemeinsame Verantwortlichkeit, dass die Verantwortlichen eine transparente Vereinbarung darüber treffen, wer im Innenverhältnis welchen datenschutzrechtlichen Pflichten nachkommt (Art. 26 Abs. 1 S. 2, 3 DSGVO).[109]

a) Keine Durchsetzbarkeit

Die Durchsetzung der datenschutzrechtlichen Pflichten ist sowohl für den Betroffenen als auch für die Verantwortlichen ein Problem: Der Betroffene muss einen Verantwortlichen ausfindig machen können. Dies stellt aber eine praktisch unlösbare Aufgabe dar, weil alle Verantwortlichen unter Pseudonymen agieren.[110] Zudem sind *Nodes*, *Miner* und Entwickler-Community Personengruppen, deren Mitglieder sich stetig ändern.[111] Ein einmal ausgemachter Verantwortlicher kann daher nicht unbedingt erneut herangezogen werden. Am ehesten ist ein Verantwortlicher noch im Kreis der Entwickler zu finden. Die Entwickler stehen unabhängig von ihrer Organisationsform typischerweise auf Foren in stetigem Kontakt miteinander, was die Kontaktaufnahme vereinfachen könnte. Damit verschiebt sich aber nur das Problem, denn auch die Verantwortlichen untereinander kennen sich nicht.[112] Ein Einzelner hat keinen Einfluss auf das Gesamtsystem und kann die datenschutzrechtlichen Pflichten daher nicht allein erfüllen.[113]

b) Keine Vereinbarung über interne Zuständigkeit

Die Unbekanntheit der anderen Verantwortlichen stellt auch das entscheidende Hindernis für die Vereinbarung über die internen Zuständigkeiten dar.[114] Denkbar wäre, dass eine solche Vereinbarung in das Protokoll aufgenommen werden kann.[115] Dies widerspricht aber der Vorstellung der Beteiligten an einer Blockchain von Anonymität bzw. Pseudonymität, sodass es fraglich ist, ob diese Lösung in der Praxis umgesetzt werden würde.[116]

2. Abwägung

Die Grundrechte binden im Grundsatz nur den jeweiligen Mitgliedstaat bzw. die EU und ihre Stellen (vgl. Art. 51 Abs. 1 GRCh). Über die Auslegung unbestimmter Rechtsbegriffe hinaus sind die betroffenen Grundrechte aber auch zwischen Bürgern relevant.[117] Kollidiert etwa das Grundrecht des Schutzes der personenbezogenen Daten (Art. 8 GRCh) mit einem oder mehreren anderen Grundrechten, muss es unter Beachtung des Verhältnismäßigkeitsprinzips mit diesen abgewogen werden.[118] Je nachdem,

[107] Dazu EuGH, Urt. v. 29.7.2019, Fashion ID, C-40/17 ECLI:EU:C:2019:629, Rn. 70; Artikel-29-Datenschutzgruppe (Fn. 28), S. 24.
[108] EuGH, Urt. v. 29.7.2019, Fashion ID, C-40/17 ECLI:EU:C:2019:629, Rn. 70.
[109] *Nink,* in: Spindler/Schuster, Recht der elektronischen Medien, 4. Aufl. 2019, Art. 26 DSGVO Rn. 10.
[110] *Böhme/Pesch*, DuD 2017, 473 (478); *Pesch/Sillaber*, CRi 2017, 166 (170).
[111] *Erbguth/Fasching*, ZD, 2017, 560 (564).
[112] *Buocz et al.* (Fn. 16), zitiert nach SSRN3297531, dort S. 27 f.
[113] *Bechtolf/Vogt*, ZD 2018, 66 (69).
[114] *Pesch/Sillaber*, CRi 2017, 166 (170); siehe auch *Pachernegg* (Fn. 10), S. 68.
[115] *Pesch/Sillaber*, CRi 2017, 166 (170).
[116] *Pesch/Sillaber*, CRi 2017, 166 (170).
[117] Vgl. EuGH, Urt. v. 20.5.2003, Österreichischer Rundfunk, C-465/00; Slg.2003, I-4989 Rn. 21, 68.
[118] Erwägungsgrund 4 DSGVO; *Ernst* (Fn. 27), Art. 1 DSGVO Rn. 8.

welches Ziel mit der Blockchain verfolgt wird, können dabei unterschiedliche Grundrechte der Netzwerk-Teilnehmer eingeschränkt werden.[119] Hat das Ergebnis der Auslegung des Begriffs „Verantwortlicher" zur Folge, dass ungerechtfertigterweise in Grundrechte eingegriffen wird, muss eine alternative, grundrechtskonforme Auslegung erfolgen.[120]

Mit Blick auf das Ergebnis, dass Entwickler-Community, *Miner* und *Nodes* datenschutzrechtlich verantwortlich sind, ist zu betonen, dass es sich auf die hier allein im Fokus stehende zulassungsfreie, öffentliche Blockchain beschränkt. Dabei mussten typische Strukturen unterstellt werden, auf die die Verantwortlichen Einfluss haben. Es gibt bereits zahlreiche Ansätze, die die datenschutzrechtlichen Problematiken durch technische Herangehensweisen (*Privacy by Design,* vgl. Art. 25 DSGVO) lösen könnten.[121] Außerdem muss festgehalten werden, dass die Probleme mit dem sinkenden Grad der Dezentralisierung abnehmen. Sobald sich nämlich zentrale Stellen mit entsprechend großem Einfluss auf die Datenverarbeitung bilden, wird diesen die Verantwortlichkeit zufallen.[122] *Nodes* und *Miner* sind dann unter Umständen nur Auftragsverarbeiter.[123] Wenn für die Netzwerk-Teilnehmer nur diese konkrete Form der Datenspeicherung *de facto* ausgeschlossen wird,[124] wiegt der Eingriff nicht sonderlich schwer. Im Vergleich zur massiven Einschränkung des Schutzes der persönlichen Daten, die mit Alternativen einherginge, lässt sich ein unverhältnismäßiger Eingriff in die Grundrechte der Netzwerk-Teilnehmer nicht feststellen.[125]

V. Stellungnahme: Reformbedarf?

Auf den ersten Blick scheint die Zuweisung der Verantwortlichkeit unbefriedigend.[126] Doch mit einer klaren Zuweisung können die Entwickler Möglichkeiten ermitteln, ein zufriedenstellendes Ergebnis zu erreichen. Die DSGVO ist *de lege lata* technologieneutral und will der Entwicklung der Technik nicht entgegenstehen, sofern der Datenschutz durch sie gewährleistet wird.[127] Bei öffentlichen, zulassungsfreien Blockchains kann dies auf der technischen Ebene, also durch *Privacy by Design*, gewährleistet werden. So kann etwa der Löschungsanspruch (Art. 17 DSGVO) durch sog. Chamäleon-Hashfunktionen nachgekommen werden.[128] Diese ermöglichen eine nachträgliche Änderung oder Löschung der auf der Blockchain gespeicherten Informationen.[129]

Es wäre zwar denkbar, die DSGVO zu ändern. Das Problem ist aber die Verantwortlichkeit als solche. Denn in der öffentlichen Blockchain gibt es keine Person oder Personengruppe, die für sich genommen zur Erfüllung der Pflichten in der Lage wäre. *De lege ferenda* ohne Verantwortlichkeit auszukommen, ist nicht aussichtsreich, wenn man Art. 8 GRCh Rechnung tragen will.[130] Der letzte Weg, der dann noch bleibt, ist der technische. Da Blockchains, die weniger dezentral ausgestaltet sind, zumindest weniger Probleme verursachen, ist auch nicht zu erwarten, dass die DSGVO die Entwicklung der Blockchain-Technologie bremsen wird. Reformen wären nur möglich, wenn man gewillt wäre, bestimmte Technologien, wie die Blockchain, zu bevorzugen.[131]

F. Ergebnis

Die Dezentralität kann in einer Blockchain unterschiedlich stark ausgeprägt sein. In ihrer „reinsten" Form, der öffentlichen, zulassungsfreien Blockchain, ist die Frage nach dem Verantwortlichen besonders problematisch. Ohne zentrale Ausprägung scheint es auf den ersten Blick so, als ob niemand verantwortlich wäre, was auch an der DSGVO liegt. Wo diese versucht einen Verantwortlichen zu bestimmen,[132] liegt die Idee der Dezentralisierung darin, einen Verantwortlichen in diesem Sinne nicht zu benötigen. Jeder ist „Diener des Systems" und niemand kann operativ entscheiden, zu welchem Zweck und in welcher Weise Daten verarbeitet werden. Die Lösung ist das Protokoll. Es gibt die Antwort darauf, warum und wie Daten verarbeitet werden, und ist der Grund, warum allen Beteiligten bei der konkreten Datenverarbeitung die Entscheidungsoptionen genommen werden. Verantwortlich sind daher die Personen, die das System fortwährend gestalten: Entwickler-Community, *Miner* und *Nodes*. Diese können die datenschutzrechtlichen Pflichten zwar nicht im Einzelnen erfüllen, sind aber in der Lage, das System durch die Änderung des Protokolls anzupassen. Über *Privacy-by-Design*-Ansätze können sie ihre Blockchain datenschutzkonform ausgestalten und die Probleme umgehen, die sich durch die gemeinsame Verantwortlichkeit der drei Personengruppen ergeben.

[119] *Pesch/Sillaber*, CRi 2017, 166 (171); dazu insgesamt: *Rueckert*, Journal of Cybersecurity 2019, 1.
[120] EuGH, Urt. v. 13.5.2014, Google Spain, C-131/12; ECLI:EU:C:2014: 317, Rn. 68; *Jarass,* in: Jarass, GRCh, 4. Aufl. 2021, Einleitung, Rn. 62.
[121] Siehe etwa *Erbguth* (Fn. 25); *Finck* (Fn. 17), S. 32 ff.
[122] *Martini/Weinzierl*, NVwZ 2017, 1251 (1254); *Quiel*, DuD 2018, 566 (570).
[123] *Martini/Weinzierl*, NVwZ 2017, 1251 (1254).
[124] *Pesch/Sillaber*, CRi 2017, 166 (171).
[125] Im Ergebnis a.A. *Pesch/Sillaber*, CRi 2017, 166 (171).
[126] So auch *Quiel*, DuD 2018, 566 (570).
[127] Erwägungsgründe 6 und 15 DSGVO.
[128] *Erbguth* (Fn. 25).
[129] *Erbguth* (Fn. 25).
[130] A.A. *Fridgen et al.,* Chancen und Herausforderungen von DLT (Blockchain) in Mobilität und Logistik, 2019, S. 148 ff.
[131] *Pesch/Sillaber*, CRi 2017, 166 (171).
[132] Vgl. Erwägungsgrund 79 DSGVO.