Typoskript im Sinne des § 38 Abs. 4 UrhG; das Original ist abgedruckt in der NVwZ 2017, 1251 ff.

Die Blockchain-Technologie und das Recht auf Vergessenwerden: zum Dilemma zwischen Nicht-Vergessen-Können und Vergessen-Müssen

Professor Dr. Mario Martini und Forschungsreferent Quirin Weinzierl*

Eine neue Technologie erobert die Welt: die Blockchain. Nicht nur Technik-Auguren trauen ihr zu, einen Quantensprung der digitalen Evolution auszulösen. Sie hat das Zeug, vertrauenswürdige Intermediäre wie Registraturbehörden oder Banken zu ersetzen. Denn sie formt einen effizienten technologischen Abwicklungsrahmen für Prozesse, die bislang noch relevante Transaktions- und Verwaltungskosten verschlingen. Doch scheinen IT-Pioniere ihre Rechnung ohne das Recht auf Vergessenwerden zu machen: Eine Blockchain ist wie der *Rain Man* in *Barry Levinsons* Filmdrama. Sie vergisst nicht. Entfernt man einzelne Bestandteile aus der kontinuierlichen Verknüpfung der Datenblöcke, droht die Datenkette zu reißen. Die Nutzung der Technologie gerät damit in ein Dilemma zwischen funktional unmöglichem Vergessen-Können und einem datenschutzrechtlich geforderten Vergessen-Müssen. Die Autoren suchen nach Auswegen.

I. Die Blockchain-Technologie zwischen Mysterium und Motor der digitalen Revolution

1. Funktionsweise

In ihrer technischen Grundfunktion ist eine Blockchain[1] als dezentral geführte Datenbank konzipiert: Sie speichert Informationen in aneinandergereihten Datenblöcken und verkettet

---

* *Mario Martini* ist Lehrstuhlinhaber an der Deutschen Universität für Verwaltungswissenschaften Speyer und Leiter des Programmbereichs „Digitalisierung“ am FÖV Speyer. *Quirin Weinzierl* ist dort Forschungsreferent. Die Autoren danken insbes. Herrn *Dr. Marcus M. Dapp* (fortiss) für seine kritische Durchsicht sowie Herrn *Michael Kolain* (FÖV) für die hervorragende inhaltliche Unterstützung. Die Internetquellen wurden zuletzt am 30.5.2017 aufgerufen.

[1] „*Die* Blockchain“ als solche gibt es nicht – vielmehr handelt es sich um ein Technologiekonzept mit zahlreichen Ausgestaltungsformen (s. I. 3.). Teilw. firmiert die Blockchain-Technologie auch unter „Distributed Ledger Technology“.

diese mittels digitaler Fingerabdrücke (sog. *Hashes*).[2] Jeder neue Block speichert den *Hash* des vorangehenden Blocks, so dass die sich fortschreibende Blockchain alle jemals gespeicherten Informationen bzw. vorgenommenen Veränderungen an hinterlegten Berechtigungen in chronologischer Reihenfolge protokolliert.[3] Die Datenkette ist nicht zentral auf einem Server hinterlegt, sondern auf den Rechnern aller Teilnehmer (sog. *Nodes*) verteilt gespeichert. Diese kommunizieren ohne zentrale Instanz untereinander und bilden so ein Peer-to-Peer (P2P)-Netzwerk, das auf der Grundlage der Gleichrangigkeit eine Einigung über geteilte Daten erzielt.[4]

Wer als *Node* Transaktionen vornehmen will, ist auf einen öffentlichen und einen korrespondierenden privaten Schlüssel angewiesen. Der öffentliche Schlüssel ist mit einer Kontonummer vergleichbar, die bestehende Berechtigungen nachweist. Der *Hash* des öffentlichen Schlüssels ist für jedermann sichtbar in der Blockchain abgelegt. Der private Schlüssel fungiert als Passwort. Mit seiner Hilfe signiert und legitimiert der Teilnehmer alle Transaktionen, die von seinem öffentlichen Schlüssel ausgehen. Die zugehörigen Transaktionsdaten sendet er an das gesamte Netzwerk. Aus ihnen kann jeder seiner Teilnehmer – nach einer Prüfung der getätigten Transaktionen auf Richtigkeit – neue Blöcke erstellen (sog. *Mining*).[5] Sobald die anderen *Nodes* einen Block (insbes. die enthaltenen Transaktionen) anhand ihrer Blockchain verifiziert haben, fügen sie ihn an ihre Version der Kette an.[6] Auf diese Weise erkennt das Netzwerk die Wirksamkeit der getätigten Transaktionen an. Eine zentrale Verifikationsstelle, wie das Grundbuchamt oder eine Bank, gibt es in einer Blockchain nicht und braucht es auch nicht. Die Verbindung aus kryptographischer Verkettung und dezentraler Speicherung macht die Blockchain zu einer Registratur des Vertrauens: Sie stellt Vertrauen zwischen Akteuren her, die einander nicht kennen.

2. Nutzungsmöglichkeiten in Wirtschaft und Verwaltung

Im Vergleich zu Systemen, die auf Vertrauensintermediäre angewiesen sind, ist die Blockchain-Technologie nicht nur besonders änderungsresistent und damit weitgehend

---

[2] S. auch die instruktive Beschreibung bei *Welzel/Eckert* et al., Mythos Blockchain: Herausforderung für den öffentlichen Sektor, 2017, 8 ff.
[3] Allen diesen Transaktionen ist der genaue Zeitpunkt ihrer Vornahme eingeprägt (*timestamping*).
[4] Vgl. *van Valkenburgh,* What is "Blockchain" anyway?, https://coincenter.org/entry/what-is-blockchain-anyway.
[5] Hierfür muss er eine erhebliche Rechenleistung aufwenden (als Anreiz bzw. Gegenleistung erhält er Bitcoins o. eine sonstige Vergütung). Dies verhindert, dass sich zusätzlich zu den bereits verifizierten, im Netzwerk verteilten Blöcken später alternative Blöcke in das Netzwerk einspeisen lassen, sog. *Proof-of-Work*-Mechanismus; andere Einsatzszenarien nutzen einen *Proof-of-Stake*-Mechanismus, der Stimmrechte nach Anteilen gewichtet; zu weiteren Konsensalgorithmen vgl. *Christidis/Devetsikiotis*, IEEEAccess 2016, 2292 (2294 f.).
[6] Bei mehreren parallel ausgesandten Blöcken setzt sich der rechenintensivste durch.

fälschungssicher. Aufgrund ihrer Automatisierungsleistung ist sie auch effizient und im Grundsatz kostensparend.[7]

Viele handeln die Technologie aus diesen Gründen als geeignete Grundlage des Internets der Dinge, als Heilsbringer im digitalen Identitätsmanagement oder gar als Nachfolger des *Domain Name Systems*. Im täglichen Geschäftsverkehr kann sie ihre Vorzüge außer bei der Anwendung als Kryptowährung (zB Bitcoin) etwa auch bei Transaktionen im Interbankenhandel oder der Verwaltung geistigen Eigentums ausspielen. Besonderes Potenzial entfaltet die Blockchain-Technologie auch als Abwicklungsinstrument im Rahmen so genannter *Smart Contracts*[8], die zB Zahlungen automatisiert anweisen, sobald eine vereinbarte Bedingung eingetreten ist.[9]

Auch im öffentlichen Sektor verheißen Blockchains segensreiche Innovationen. So ist es denkbar, die Registerführung, zB das Grundbuch oder das Handelsregister, mittels einer Blockchain-Anwendung abzuwickeln.[10] Die US-Regierung erwägt, die Technologie als Buchführungsinstrument über elektronische Gesundheitsdaten einzusetzen.[11] Aber auch die Zuteilung und Verwendung von Sozialhilfeleistungen lässt sich über ein Blockchain-System verwalten; das Vereinigte Königreich praktiziert das experimentell.[12] Nicht zuletzt testen die Vereinten Nationen im Pilotprogramm „Building Blocks" eine schnelle und sichere Auslieferung von Hilfsgütern mit Hilfe einer Blockchain.[13]

3. Ausgestaltungsformen

Unter dem Begriffsdach „Blockchain" sammelt sich ein vielschichtiges Konglomerat unterschiedlicher, an das jeweilige Einsatzszenario anpassbarer Spielarten einer technologischen Grundphilosophie.[14] In ihrer Basisform, insbes. der virtuellen Währung Bitcoin, kann jedermann als *Node* an dem P2P-Netzwerk teilnehmen, dh mittels einer Bediensoftware (sog. *Client*) die aktuelle Blockchain[15] eines anderen *Nodes* auf seinem Rechner speichern und Transaktionen sowie Mining-Dienste vornehmen (zulassungsfreie bzw. *öffentliche Blockchain*). Denkbar ist aber auch, nur einen bestimmten Nutzerkreis zur

---

[7] Problematisch ist jedoch die Skalierbarkeit: je mehr Transaktionen, desto höher das Datenvolumen und damit die Transaktionsdauer. Vgl. etwa *Croman/Decker* et al., in: *Clark/Meiklejohn/Ryan* u. a., On Scaling Decentralized Blockchains, 2016, S. 106 ff.

[8] *Smart Contracts* sind Programm-Codes, die Verträge abbilden u. (teilw.) automatisch abwickeln. Vgl. *Kaulartz/Heckmann*, CR 2016, 618 (passim).

[9] Zu weiteren Anwendungsmöglichkeiten *Welzel/Eckert* et al. (o. Fußn. 2), 18 ff.

[10] S. auch *Martini*, DÖV 2017, 443 (454).

[11] Vgl. *Office of the National Coordinator for Health Information Technology* (ONC), ONC announces Blockchain challenge winners, Pressemitteilung v. 1.9.2016.

[12] Vgl. *Cellan-Jones,* Blockchain and benefits - a dangerous mix?, http://www.bbc.com/news/technology-36785872.

[13] Vgl. *World Food Program,* What is 'Blockchain' and How is it Connected to Fighting Hunger?, https://insight.wfp.org/what-is-blockchain-and-how-is-it-connected-to-fighting-hunger-7f1b42da9fe.

[14] Vgl. die Klassifizierung nach *Welzel/Eckert* et al. (o. Fußn. 2), 15.

[15] Es gibt innerhalb eines Blockchain-P2P-Netzwerkes nicht „die eine aktuelle Blockchain", vielmehr führt jeder *Node* seine Datenkette autonom.

Teilnahme zuzulassen (zulassungsbeschränkte bzw. *private Blockchain*). [16] Diese Ausgestaltung eignet sich insbes. für staatliche Anwendungen.

Die Einsicht in die Datenblöcke kann entweder beliebigen Interessierten offen stehen (öffentlich einsehbare bzw. *open blockchain*). Sie kann aber auch ausschließlich zugelassenen Personen vorbehalten sein (*closed Blockchain*).

II. Konflikt mit dem Recht auf Vergessenwerden

Der Wesenszug einer Blockchain, Transaktionsprozesse lückenlos zu speichern, ist Fluch und Segen zugleich: Denn gerade ihre Veränderungsresistenz bringt die Technologie in Konflikt mit dem Recht auf Vergessenwerden. Diesem liegt ein einleuchtender Leitgedanke zugrunde: Einen Menschen an weit in die Vergangenheit zurückreichende Informationen festzuhalten – mögen sie auch der Wahrheit entsprechen –, kann seine Persönlichkeitsentwicklung beeinträchtigen. Ein Datenverarbeitungssystem muss auf die sich daraus ergebenden normativen Anforderungen an die Verarbeitung personenbezogener Daten reagieren (können).

1. Personenbezug der in einer Blockchain gespeicherten Daten

Eine Blockchain speichert (jedenfalls in ihres heutigen Nutzungskonzeption) nicht unmittelbar elektronische Gesundheitsdaten oder die Namen einzelner Grundstückseigentümer bzw. Sozialhilfeempfänger. Vielmehr hinterlegt sie lediglich *Hashes* der jeweiligen Daten und verwendet öffentliche Schlüssel als Nutzerkennungen. Ob solche Informationen sich auf eine „identifizierbare" Person beziehen und damit personenbezogene Daten sind (Art. 4 Nr. 1 Hs. 1 Alt. 2 DSGVO), beantwortet das Datenschutzrecht entlang der Trennlinie des relativen Personenbezugs: Eine Information ist für denjenigen personenbezogen, der über das notwendige Zusatzwissen verfügt, um sie mit verhältnismäßigen Mitteln einer bestimmten Person zuzuordnen.[17]

Bei einer *zulassungsbeschränkten* Blockchain lässt sich ein Personenbezug leicht herstellen: Derjenige, der die Nutzerkennung vergibt, ist in der Lage, auf die Person rückzuschließen, die sich hinter einem öffentlichen Schlüssel verbirgt. Seine Stellung ähnelt derjenigen eines *Internet Service Providers*. Dieser kann jederzeit den Nutzer einer IP-Adresse, dem er diese zugeteilt hat, zweifelsfrei identifizieren.[18]

Doch auch Personen, die auf eine *zulassungsfreie oder öffentlich einsehbare Blockchain* zugreifen können, sind unter Umständen in der Lage, mit verhältnismäßigen Mitteln einen

---

[16] Gleichzeitig können bestimmte Rechte innerhalb des Netzwerks (wie das Recht zur Aussendung von Informationen u. damit die Vornahme von Transaktionen o. das Recht zum *Mining*) allen o. nur einzelnen Teilnehmern offen stehen (Blockchain ohne/mit besonderen Berechtigungen bzw. *permissionless*/*permissioned Blockchain*), vgl. *Welzel/Eckert* et al. (o. Fußn. 2), 15.
[17] So grds. EuGH, EuZW 2016, 909 (911, Rn. 49); vgl. auch *Hofmann/Johannes*, ZD 2017, 221 (222 ff.).
[18] Vgl. EuGH, ZD 2012, 29 (32, Rn. 51); hieran anschließend BGH, Urt. v. 16.5.2017, Az. VI ZR 135/13.

Personenbezug herzustellen.[19] Am einfachsten ist dies bei bewusster Selbstoffenbarung: Nutzt ein Teilnehmer Dienste wie Bitcoin-Marktplätze, gibt er durch seine Anmeldung preis, hinter bestimmten öffentlichen Schlüsseln zu stecken. Darüber hinaus ermöglichen Big-Data-Analysen, insbes. spezielle, auch frei verfügbare Analysetools,[20] Blockchain-Teilnehmer mit immer geringerem Aufwand zu identifizieren.[21] So ist es bspw. möglich, die (personenbezogene) IP-Adresse des Rechners zu ermitteln, den ein Teilnehmer nutzt.[22] Anspruchsinhabern oder dem Staat können ferner rechtliche Mittel zustehen, um eine Herausgabe der Zuordnungsinformationen zu erreichen – zB um Straftaten aufzuklären oder Ansprüche (etwa gegen Bitcoin-Verkäufer oder Grundstückseigentümer) durchzusetzen.[23]

Nicht nur die Schlüsselverwaltung bei zulassungsbeschränkten Ausgestaltungen, sondern bereits die abgelegten *Hashes* und öffentlichen Schlüssel selbst ermöglichen es daher häufig – wenn auch mitunter nur mittelbar –, mit verhältnismäßigen Mitteln die natürliche Person zu identifizieren, die hinter diesen Daten steht.[24] Die mit dem Betrieb eines Blockchain-Netzwerks verbundenen Datenverarbeitungen (wie die Speicherung und Übermittlung) bedürfen dann nicht nur einer Verarbeitungsgrundlage (Art. 6 I DSGVO).[25] Die Daten unterliegen auch dem Recht auf Vergessenwerden.

2. Datenschutzrechtliche Verantwortlichkeit als Herausforderung in einem dezentral organisierten System

Weniger klar als der Personenbezug ist die datenschutzrechtliche Verantwortlichkeit in dem kollaborativen System einer Blockchain. Denn die Technologie fußt gerade auf dem Prinzip der dezentralen Speicherung und Bearbeitung. Sie errichtet gleichsam ein System „organisierter Verantwortungslosigkeit", das die herkömmlichen datenschutzrechtlichen Kategorien an ihre Grenzen bringt.

Als Verantwortlicher kommt eine Vielzahl beteiligter Akteure in Betracht: derjenige, der die Blockchain *programmiert* hat; die Stelle, welche die Blockchain *initiiert*; das Mitglied des Netzwerks, welches eine *Transaktion aussendet*; jeder, der als *Node* die Blockchain bei sich speichert; der *Miner*, der neue Blöcke errechnet. Nicht zuletzt ist auch eine *gemeinsame Verantwortlichkeit* mehrerer oder aller dieser Akteure denkbar.

---

[19] Das hängt im Einzelnen allerdings v. Einsatzszenario ab. Der Einsatz eines Tor- o. VPN-Netzwerks kann den Personenbezug torpedieren.
[20] Vgl. zB den Dienst *Chainanalysis*: https://www.chainalysis.com/.
[21] Vgl. grds. *Brisch/Pieper*, CR 2015, 724 (724 ff.).
[22] Vgl. *Biryukov/Khovratovich/Pustogarov*, in: *Ahn,* Deanonymisation of Clients in Bitcoin P2P Network, 2014, S. 15 ff.
[23] ZB ein Auskunftsanspruch nach § 14 II (iVm § 15 V 4) TMG iVm der jeweiligen Ermächtigungsgrundlage, vgl. auch Art. 2 NetzDG-E (BR-Drs. 315/17, 4).
[24] AA ohne nähere Begründung *Schrey/Thalhofer*, NJW 2017, 1431 (1433).
[25] Vgl. *Hofert*, ZD 2017, 161 (164 ff.), der jd. übersieht, dass bereits jede Speicherung durch *Nodes* rechtfertigungsbedürftig ist, nicht lediglich die Verarbeitung durch *Miner*; s. auch *Kaulartz*, CR 2016, 474 (479 f.).

a) Zulassungsfreie Blockchain: dezentrale Verantwortlichkeit.

Die DSGVO bestimmt den Verantwortlichen nach Maßgabe der (faktischen [26]) Bestimmungsmacht: Verantwortlich ist, wer allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet (Art. 4 Nr. 7 DSGVO).

In einer zulassungsfreien Blockchain gibt die initiierende (und programmierende) Stelle[27] mit der Veröffentlichung des Programmcodes die Kontrolle über die Mittel und den Zweck der Verarbeitung aus der Hand. Wie andere Softwareentwickler auch stellt sie lediglich ein Datenverarbeitungsprogramm zur Verfügung. Mit den einzelnen Verarbeitungsvorgängen hat sie nichts zu schaffen. Dass die programmierende Einheit in Extremfällen, etwa einem versuchten *Hack* oder der Notwendigkeit technischer Modifikationen, uU großen faktischen Einfluss auf die Fortschreibung der Blockchain sowie auf die Fortentwicklung der *Clients* hat, ändert daran nichts:[28] Das Netzwerk ist weder zur Gefolgschaft verpflichtet, noch lässt sich aus einer derartigen Ausnahmesituation eine generelle Verantwortlichkeit ableiten.

Wirtschaftlich betrachtet sind zwar die *Miner* in das Schicksal der Blockchain besonders involviert: Sie profitieren unmittelbar von ihrer Teilhabe am verteilten Netzwerk.[29] Doch erschöpft sich ihr Einfluss darin, neue Blöcke zu errechnen. Den konkreten Inhalt der verarbeiteten Daten beeinflussen sie nicht; sie sind gleichsam gehorsame Diener des Systems. Ihre Rolle ist partiell mit Telekommunikationsdienste-Anbietern vergleichbar: Ebenso wie diese nicht für die in durchgeleiteten Nachrichten enthaltenen personenbezogenen Daten verantwortlich sind, [30] sind *Miner* nicht für die personenbezogenen Inhalte ihrer Rechenergebnisse verantwortlich.

Gemessen am Maßstab der DSGVO ist Verantwortlicher vielmehr jeder *Node*, der eine Transaktion vornimmt (und damit Informationen an alle anderen Knoten verteilt) und/oder in seine Kopie der Blockchain eingetragen hat.[31] Denn er verfolgt damit einen eigenen Zweck: [32] die Teilnahme am Netzwerk. Er erhebt, erfasst, ordnet und speichert

---

[26] Vgl. *Artikel-29-Datenschutzgruppe,* Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortliche" und „Auftragsverarbeiter", WP 169, 16.2.2010, 1, 11 ff.
[27] Im Falle der Bitcoin-Blockchain ihr gedanklicher Vater *Satoshi Nakamoto* (ein Pseudonym); vgl. *Nakamoto,* Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf.
[28] Vgl. bspw. zum Einfluss der Ethereum-Programmierer *Kannenberg,* Nach dem DAO-Hack: Kryptogeld Ethereum steht vor hartem Fork, https://heise.de/-3272501.
[29] Zur Rolle der *Miner* s. bereits Fn. 5.
[30] Vgl. auch ErwGrd 47 S. 1 DSRL; die DSGVO enthält keine vergleichbaren Ausführungen mehr.
[31] Insoweit übertragbaren Bedenken des GA Jääskinen (BeckRS 2013, 81374 [Rn. 83]) ggü. einer Stellung der Suchmaschinenanbieter als Verantwortliche hat sich der EuGH (EuZW 2014, 541 [542, Rn. 28]) nicht angeschlossen.
[32] Soweit es sich dabei um rein persönliche oder familiäre Zwecke handelt, ist die DSGVO auf ihn jedoch nicht anwendbar (Art. 2 Abs. 2 lit. c DSGVO).

personenbezogene Daten, legt sie ggf. selbst offen und kann insgesamt frei über die bei sich gespeicherten Daten verfügen.[33]

Prinzipiell können mehrere *Nodes* auch gemeinsam Verantwortliche sein (Art. 26 DSGVO). Das setzt jedoch voraus, dass sie die Zwecke und Mittel der Verarbeitung gemeinsam festlegen. Regelmäßig fehlt es daran. Zwar ist die Nutzung einer Blockchain ohne andere Rechner praktisch sinnlos. Jedoch übt der einzelne *Node* typischerweise keinen rechtlichen oder tatsächlichen Einfluss auf das „Ob" und „Wie" der Datenverarbeitung der anderen Knoten des Netzwerks aus.[34]

b) Zulassungsbeschränkte Blockchain: zentrale Verantwortlichkeit.

Nicht alle Blockchain-Anwendungsszenarien folgen der cyberanarchistischen Idee der Verantwortungsdiffusion: Zulassungsbeschränkte Blockchains zentralisieren die Einflussmöglichkeiten auf das Netzwerk. Sie bündeln diese bei der Stelle, die über die Zuteilung der Zugangsrechte bestimmt und damit „entschieden hat, personenbezogene Daten für ihre eigenen Zwecke zu verarbeiten"[35]. Setzt der *Staat* eine Blockchain zB für Grundbuch-, Sozialhilfe- oder Gesundheitsdaten ein, sind daher nicht die beauftragten Programmierer, einzelne *Nodes* (etwa Transferleistungsempfänger oder medizinische Einrichtungen) oder gar (ggf. beauftragte) *Miner* verantwortlich, sondern die handelnde Behörde. Auch dann, wenn *Private* (zB Banken) eine zulassungsbeschränkte Blockchain mit zentraler Zulassungsverwaltung einsetzen, sind diese selbst (ggf. als Bankenkonsortium nach Art. 26 DSGVO gemeinsame) Verantwortliche.

Nodes und *Miner* werden dort demgegenüber grds. als Auftragsverarbeiter (Art. 4 Nr. 8, Art. 28 DSGVO) tätig.[36] Für ihr Handeln ist der durch die einsetzende Stelle verfolgte Zweck leitend, eine sachgemäße Datenverarbeitung wahrzunehmen. Sie erfüllen (insoweit mit Cloud-Anbietern vergleichbar)[37] die nach dem funktionellen Ansatz der Auftragsverarbeitung wesentlichen Kriterien der rechtlich selbstständigen Verarbeitung im Interesse des Verantwortlichen[38].

---

[33] So iE auch die Einordnung v. Suchmaschinenbetreibern, EuGH, EuZW 2014, 541 (542, Rn. 28 ff.).
[34] Anders könnte der Fall jedoch liegen, wenn der Zweck des Netzwerks ein dezidiert gemeinschaftlicher ist oder *Smart-Contract*-Organisationen eine Blockchain für ihre Zwecke nutzen. Doch auch hier agieren die *Nodes* grds. autonom.
[35] *Artikel-29-Datenschutzgruppe* (o. Fußn. 26), 17.
[36] Den das Handelsregister (§ 387 V FamFG) sowie das Grundbuch (§ 126 III GBO) führenden Gerichten ist es bereits heute erlaubt, die notwendige Datenverarbeitung im Auftrag durch andere Stellen vornehmen zu lassen. Unberührt hiervon bleibt die Frage nach der (verfassungsrechtlichen) Zulässigkeit einer evtl. Aufgabenverlagerung; vgl. *Spoerr,* in *Wolff/Brink,* BeckOK DatenschutzR, 20. Ed. (Stand: 1.5.2017), § 11 BDSG Rn. 9 ff.
[37] Vgl. *Artikel-29-Datenschutzgruppe,* Stellungnahme 05/2012 zum Cloud Computing, WP 196, 1.7.2012, 10.
[38] Vgl. zu den Voraussetzungen *Artikel-29-Datenschutzgruppe* (o. Fußn. 26), 30 f., 33.

3. Pflichten des Verantwortlichen aus Art. 17 und Art. 19 DSGVO

Als Ausfluss des Rechts auf Vergessenwerden treffen den (jeweiligen) Verantwortlichen zwei wesentliche Pflichten: die Löschungspflicht aus Art. 17 I DSGVO und die flankierende Informationspflicht aus Art. 17 II DSGVO.[39]

Art. 17 I DSGVO erlegt dem Verantwortlichen auf, Daten zu löschen, die sich in seinem Verantwortungsbereich befinden. Er hat also sicherzustellen, dass der Zugriff auf die Daten nicht mehr oder nur noch mit unverhältnismäßig hohem Aufwand möglich ist. Ein Stornieren oder Zurückbuchen getätigter Transaktionen genügt dem noch nicht. Denn diese Maßnahmen eliminieren die ursprüngliche Information nicht aus der Datenkette. Sie bleiben vielmehr gespeichert. Normativ geboten ist aber ein Entfernen der Daten selbst aus der (jeweiligen Kopie der) Blockchain auf dem Speichermedium des *Nodes*.[40]

Die Pflicht des *Art. 17 II DSGVO*, Dritte über das Löschungsverlangen zu informieren, bezieht sich auf alle dem Verantwortlichen *unbekannten* Personen,[41] die Daten aus einer über das Internet[42] veröffentlichten, dh öffentlich einsehbaren, Blockchain verarbeiten. Hat der Verantwortliche diesen den Zugriff auf Daten ermöglicht, muss er Maßnahmen in die Wege leiten, um diejenigen Empfänger, welche die Daten auf Grund seiner Veröffentlichung verarbeiten, über eine Löschung zu unterrichten.[43] Die Informationspflicht greift insoweit unabhängig von der Verantwortlichen-Struktur und einer Zulassungsbeschränkung. Denn auch zulassungsbeschränkte Blockchains können so konstruiert sein, dass beliebige Personen von den Daten Kenntnis nehmen.[44] Legt der Verantwortliche Daten gegenüber *bekannten* Empfängern offen, greift hingegen die allgemeine (subsidiäre) Mitteilungspflicht des Art. 19 S. 1 DSGVO.[45]

---

[39] Beide formen gemeinsam das „Recht auf Vergessenwerden". Das ergibt sich aus der Überschrift sowie ErwGrd 66 DSGVO.

[40] Vgl. zu den dabei bereits generell bestehenden technischen Problemen *Kalabis/Selzer*, DuD 2012, 671 (671 f.); *Greveler/Wegener*, DuD 2010, 467 (467 f.).

[41] *Härting,* Datenschutz-Grundverordnung, 2016, Rn. 723; so auch *Paal,* in *Paal/Pauly,* DS-GVO, 2016, Art. 17 Rn. 33; die Begrenzung auf „known controler" (Rat, 7978/1/15 REV 1, 11, 39) hat keine Aufnahme in die DSGVO gefunden.

[42] ErwGrd 66 S. 1 DSGVO.

[43] Vgl. *Kamlah,* in *Plath,* BDSG/DSGVO, 2. Aufl. (2016), Art. 17 DSGVO Rn. 15.

[44] Diesen Umstand übersehen *Schrey/Thalhofer*, NJW 2017, 1431 (1435).

[45] Tatbestandlich ist die Mitteilungspflicht des Art. 19 DSGVO auch bei der Offenlegung einzelner Daten an *unbestimmte* Empfänger grds. einschlägig. Art. 17 II DSGVO ist insoweit jedoch Lex spezialis. In *zulassungsbeschränkten* Blockchains trifft die Pflicht des Art. 19 DSGVO den zentralen Verantwortlichen gegenüber den Teilnehmern, die er ausgewählt hat. In *zulassungsfreien* Blockchains unterliegt ihr jeder *Node*, der als Verantwortlicher aktiv Informationen an andere *Nodes* ausgesandt hat. Im Ergebnis besteht so in jedem Fall für offengelegte Informationen eine Informations- oder Mitteilungspflicht.

III. Umsetzbarkeit des Rechts auf Vergessenwerden in der Bitcoin-Blockchain

Kommt der Verantwortliche dem Löschungsverlangen eines Betroffenen nach, reißt das womöglich eine empfindliche Lücke in die Datenkette.[46] Die Daten einzelner Transaktionen sind für die Nachvollziehbarkeit der Transaktionshistorie und damit die Vertrauenswürdigkeit der Blockchain – mithin ihre Funktionalität – grds. unbegrenzt lange notwendig.

Für die Funktionsfähigkeit der Kette gilt dies jedoch nicht in gleicher Weise: Manche Transaktionsdaten lassen sich nachträglich entfernen, ohne dass die Blockchain technisch zerbricht. Darin liegt womöglich ein Schlüssel zur Lösung des datenschutzrechtlichen Konflikts.

1. Technische Umsetzbarkeit der Löschungs- und Informationspflicht

a) Ausweg aus dem Dogma der Unabänderlichkeit.

Die Blockchain-Architektur lässt es zu, *obsolete Transaktionen* in älteren Blöcken zu entfernen, deren Ergebnis bereits ihrerseits Ausgangspunkt einer neuen Transaktion geworden ist (sog. *Pruning*)[47]. Denn sie sind dann nicht mehr notwendig, um eine aktuelle Berechtigung nachzuweisen und damit die Kette fortzuschreiben. Soweit Bestandteile einer (obsoleten) Transaktion einzeln im Transaktionsteil eines Blocks verhasht und damit „Blätter" eines Hash-Baumes sind,[48] lassen sie sich gleichsam einzeln zurückstutzen. Je nach Gestaltung der Hash-Baum-Architektur wäre dann bspw. weiterhin öffentlich bekannt, dass in der Vergangenheit bestimmte Gesundheitsdaten erhoben wurden oder ein Zwangsversteigerungsverfahren stattgefunden hat – die personenbezogenen Daten der Beteiligten hingegen wären gelöscht.

b) Möglichkeiten der Information (Art. 17 II DSGVO) und Mitteilung (Art. 19 DSGVO).

Die Löschung bei *einem Node* bedingt nicht auch automatisch die Löschung bei allen weiteren *Nodes* des P2P-Netzwerks. Zwar kommunizieren die Knoten neue Transaktionen und Blöcke untereinander – nicht jedoch die bestehende Kette selbst. Vielmehr lebt das Netzwerk gerade davon, dass jeder *Node* seine Version der Blockchain autonom fortschreibt und sich

---

[46] Da vielfältige Ausgestaltungen der Blockchain-Technologie denkbar sind, dient als technische Referenz im Weiteren allein die Bitcoin-Blockchain.

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

[48] Für die technische Funktionalität der Kette ist alleine der Kopf des Blocks (sog. *Block Header*) relevant. Das *Pruning* findet hingegen alleine in dem Teil statt, in dem die einzelnen Transaktionen sowie deren *Hashes* liegen. Dort wird aus jeweils zwei *Hashes* ein neuer *Hash* gebildet – so lange, bis nur noch ein *Hash* übrig bleibt. Auf diese Weise entsteht ein so genannter *Hash*-Baum (auch *Merkle-Tree*), an dessen Spitze der so genannte *Merkle-Hash* (auch *Root Hash*) steht. Im *Block Header* findet sich nur dieser *Merkle-Hash*. Da der nachfolgende Block alleine auf den *Header* des vorhergehenden Blocks verweist, muss nur der *Header* dauerhaft erhalten bleiben, damit jeder Block seine Existenz auf einen früheren zurückführen kann und die Kette nicht zerbricht.

Änderungen in einer Kette gerade nicht auf die anderen auswirken. Ein „Vergessen“ des Datums setzt also eine gesonderte Löschung bei jedem einzelnen *Node* voraus.

Wie sich der Löschungshinweis sowohl an die (anderen) *Nodes* des Netzwerkes als auch an die Netzwerköffentlichkeit technisch gewährleisten lässt, den Art. 17 II bzw. 19 DSGVO normativ gebieten, liegt bislang im Dunkeln. Die Bitcoin-Blockchain enthält jedenfalls kein Konstruktionselement, das einen Löschungshinweis zwischen *Nodes* ermöglicht. Dies gilt umso mehr für einen Hinweis an die Allgemeinheit bei öffentlich einsehbaren Blockchains. Die Architektur des Internets, das regelmäßig als Grundlage der Kommunikation im P2P-Netzwerk einer Blockchain dient, kennt ebenfalls keine Mittel, um eine derartige breit gestreute Information vorzunehmen: Es stellt keinen Rückkanal zu demjenigen bereit, der Informationen abruft.[49] Zwar ließe sich die IP-Adresse des Abrufenden zum Zweck der späteren Identifikation und Information automatisch speichern. Dies ist aber bei zumeist dynamischen IP-Adressen weder praktikabel noch ohne Weiteres rechtmäßig möglich[50].

2. Durchsetzungsmöglichkeiten und –schwierigkeiten

Zu den technischen Schwierigkeiten eines wirksamen Vergessens gesellen sich auch praktische Herausforderungen bei der Durchsetzung des Rechts auf Vergessenwerden.

a) Zulassungsfreie Blockchain: dezentrale Verantwortlichkeit.

Agieren *Nodes* als selbständige, dezentrale Verantwortliche in einer zulassungsfreien Blockchain, sehen sich *Betroffene* angesichts der mitunter kaum überschaubaren Anzahl an *Nodes*, ihrer territorialen Entgrenzung und dem dynamischen personellen Wandel des Netzwerks bei dem Versuch, ihre Löschungsansprüche einzufordern, schnell einem hoffnungslosen Unterfangen ausgesetzt.[51]

Vor denselben Hindernissen stehen auch die *Aufsichtsbehörden* bei dem Ansinnen, aufsichtsrechtliche Maßnahmen zu ergreifen. Ein dezentrales Verantwortungssystem fordert nicht zuletzt die Zuständigkeitsordnung der Aufsichtsbehörden heraus: Das Verfahren der Zusammenarbeit unter einer federführenden Aufsichtsbehörde,[52] welches die interne Koordinierung sicherstellen soll (Art. 56 I, 60 ff. DSGVO), knüpft an die Aufgabenteilung zwischen einer Hauptniederlassung und weiteren Niederlassungen *eines* Verantwortlichen an. Das Peer-to-Peer-Netzwerk einer zulassungsfreien Blockchain kennt jedoch nicht einen, sondern mehrere (ggf. gemeinsam) Verantwortliche. Der unionsrechtlich verankerte Abstimmungsmechanismus läuft damit ins Leere.

---

[49] Vgl. instruktiv *Hornung/Hofmann*, JZ 2013, 163 (167 ff.); *Jandt/Kieselmann/Wacker*, DuD 2013, 235 (238 ff.).
[50] Vgl. etwa BGH, Urt. v. 16.5.2017 – VI ZR 135/13.
[51] Bei der Bitcoin-Blockchain operieren aktuell ca. 1400 deutsche u. weitere ca. 1700 europäische Nodes, vgl. https://bitnodes.21.co/. Zur Löschung in „open systems” *Druschel/Backes/Tirtea,* The right to be forgotten – between expectations and practice, 2012, 13 ff.
[52] Bzw. § 19 I 1 BDSG nF für die innerdeutsche Koordinierung.

b) Zulassungsbeschränkte Blockchain: zentrale Verantwortlichkeit.

In einer zulassungsbeschränkten Blockchain lässt sich die Durchsetzung des Rechts auf Vergessenwerden auf den ersten Blick einfacher als in einer zulassungsfreien bewerkstelligen. Nutzt bspw. ein Ministerium eine Gesundheitsdaten-Blockchain, kann ein Betroffener sich an dieses als zentralen Verantwortlichen halten.

Dem zentralen Verantwortlichen fehlen jedoch regelmäßig die – eigentlich notwendigen – Einflussmöglichkeiten auf die *Nodes*, um einem Löschungsverlangen nachzukommen. Denn er hat keinen tatsächlichen Einfluss auf die Datenverarbeitung der *Nodes* im Rahmen des eingerichteten Netzwerks; er kann auf deren Version der Datenkette nicht einwirken.

Um dem Recht auf Vergessenwerden zum Erfolg zu verhelfen, ist also erforderlich, dass der zentrale Verantwortliche einer zulassungsbeschränkten Blockchain die rechtliche Einflussmacht auf die *Nodes* erhält und sich entsprechend vorbehält.

IV. Anpassungsmöglichkeiten

In Blockchain-Anwendungen lassen sich obsolete Transaktionen zwar im Wege des *Pruning* funktionswahrend aus der Datenkette löschen. Die Nachvollziehbarkeit und Fälschungssicherheit, aus der die Blockchain ihre besondere Vertrauenswürdigkeit schöpft, kann dies jedoch empfindlich einschränken. Auch die Umsetzung der Informations- und Mitteilungspflicht aus Art. 17 II, 19 DSGVO gelingt nicht bruchfrei. Überdies stehen Anspruchsinhaber vor der Schwierigkeit, die *Nodes* zu ermitteln.

Um dieser unbefriedigenden Ausgangslage abzuhelfen, ist eine technische Abwandlung der Funktionsweise der Blockchain am wirksamsten. Ein solcher Schutz der Daten durch *Privacy by Design* (Art. 25 I DSGVO) entspricht auch der unionsrechtlich verankerten Systemverantwortung des Verantwortlichen für die von ihm eingesetzten Mittel der Datenverarbeitung.[53]

1. Anpassungen der Blockchain-Technologie hinsichtlich der Löschung

a) Einsatz von *Zero-knowledge-proof*-Verfahren

Als technischer Kompromiss zwischen Funktionalität und Persönlichkeitsschutz sind sog. *Zero-knowledge-proof* (*ZKP*)-Verfahren denkbar.[54] Sie erlauben es, Transaktionsreihen in verschlüsselter Form vorzunehmen, und versuchen dadurch die Identifizierbarkeit der handelnden Akteure auszuschließen. In der Datenkette ist dann nur sichtbar, *dass* eine

[53] Vgl. *Kamlah,* in *Plath,* BDSG/DSGVO, 2. Aufl. (2016), § 35 BDSG Rn. 21.
[54] Vgl. *Samman,* The Trend Towards Blockchain Privacy: Zero Knowledge Proofs, http://www.coindesk.com/trend-towards-blockchain-privacy-zero-knowledge-proofs/.

Transaktion stattgefunden hat – nicht aber, welcher öffentliche Schlüssel als Sender welchen Wert an welchen öffentlichen Schlüssel als Empfänger transferiert hat.

Für die staatliche Nutzung bergen solche Lösungen freilich den Nachteil, der verantwortlichen öffentlichen Stelle bereits im Moment der Transaktion keine Einsicht mehr in die Vorgänge zu eröffnen. Setzt der Staat Blockchains ein, um Leistungen zu transferieren oder Register zu führen, muss er wissen, wem er bspw. welche Sozialleistungen zuerkennt oder wessen Grundstück er versteigert. Auch bei einer zulassungsfreien Blockchain entfalten sich die Transparenzvorteile der Blockchain-Technologie nur bei einer für alle (Teilnehmer) nachvollziehbaren Datenspeicherung. Alleine dann, wenn Vertraulichkeit unabdingbar ist, können *ZKP*-Verfahren also pro futuro hilfreich sein – ansonsten schießen sie über das Ziel hinaus.

b) (Nachträgliche) Anonymisierung durch Löschung der Zuordnungsdaten.

Ein gangbarer Weg, die Datenverarbeitung in einer zulassungsbeschränkten Blockchain mit der Löschungspflicht zu versöhnen, kann darin bestehen, anstelle der Blockchain-Transaktionsdaten selbst (lediglich) die – außerhalb davon hinterlegten – Zuordnungsdaten öffentlicher Schlüssel zu löschen bzw. die Zuordnung zu kappen. Derjenigen Stelle, welche die Zulassung erteilt, ist dann eine Identifizierung verwehrt. Eine (nachträgliche) Anonymisierung der in der Blockchain gespeicherten Daten scheint so herstellbar (vgl. § 3 I BDSG bzw. ErwGrd 26, S. 5, 6 DSGVO).

Eine Zuordnung lässt sich zum einen bereits *ex ante* (dh bei der Zuteilung eines öffentlichen Schlüssels) erschweren bzw. verunmöglichen. Bei einer Gesundheitsdaten-Blockchain könnte die Zuteilung des öffentlichen Schlüssels bspw. in einem zweistufigen Verfahren erfolgen: Eine staatliche Stelle nimmt die Identifizierung vor (etwa über die eID des neuen Personalausweises) und erteilt eine pseudonyme Berechtigung. Der (private oder organisatorisch getrennte staatliche) Blockchain-Betreiber vergibt auf diese Berechtigung hin den öffentlichen Schlüssel. Ein Problem aber bleibt: Bei staatlichen Nutzungen verträgt sich eine Ex-ante-Löschung nicht mit dem zwingenden Bedürfnis, die Personenzuordnung zu ermöglichen[55].

Denkbar ist zum anderen, die (beim zentralen Verantwortlichen aufbewahrte) Zuordnungsinformation zu einem öffentlichen Schlüssel *ex post* (dh nachträglich, etwa auf Antrag) zu löschen. Ein solches Vorgehen stößt jedoch an Sinngrenzen: Regelmäßig hat der mit den Zuordnungsdaten verknüpfte öffentliche Schlüssel nicht nur für eine einzige Transaktion Verwendung gefunden. Die Verbindung lässt sich dann nicht lediglich partiell für bestimmte Transaktionen kappen. Um dieses Problem zu umschiffen, müssten für jede

[55] Dazu bereits für *ZKP*-Verfahren oben IV. 1. a).

Transaktion eigene Zuordnungsdaten vergeben werden – ein im Zweifel wenig praktikables Vorgehen.

Stets bleibt ein entscheidender Einwand gegen derartige Verfahren bestehen: Sie sind nicht in der Lage, alle denkbaren Identifizierungswege aufzuheben. Vielmehr schließen sie regelmäßig nur eine „direkte Identifizierung" aus.[56] Bspw. bleibt die Herstellung eines Personenbezuges via Big-Data-Verfahren möglich. Deshalb ist bereits zweifelhaft, ob sich mit der Kappung der Verbindung zu den Zuordnungsdaten überhaupt Anonymität und damit ein (vollständiges) Vergessenwerden erzielen lässt.[57] Die in der Blockchain hinterlegten öffentlichen Schlüssel bleiben vielmehr regelmäßig weiterhin lediglich Pseudonyme identifizierbarer Personen.

2. Anpassung der Blockchain hinsichtlich der Durchsetzbarkeit der Löschung

a) Gatekeeper: Beschränkung der Lese- und Schreibrechte einer Blockchain.

Ein pragmatischer Lösungsweg, den rechtlich verbürgten Löschungsanspruch durchzusetzen, kann darin bestehen, den Kreis der *Nodes* wesentlich enger zu ziehen. Statt einer zulassungsbeschränkten Blockchain, bei der alle in der Sache Beteiligten auch als *Nodes* fungieren, ließe sich die Blockchain als besondere Speicherungsform zentral verwalteter Informationen nutzen. Der Verantwortliche führt dann etwa eine Grundbuch-Blockchain alleine auf seinem eigenen Rechnernetz. Er könnte dort Löschungen ungehindert selbst vornehmen. Die Blockchain wäre auch nicht öffentlich einsehbar. Alle Personen, die ein Interesse am Inhalt haben, sind dann auf einen (bspw. durch eine Homepage) vermittelten Zugang zu Einzelinformationen angewiesen – der Betreiber avanciert dadurch zum Gatekeeper der Blockchain. Ein unkontrolliertes Kopieren und damit unkontrollierbares zeitloses Aufbewahren der Informationen durch Dritte wäre ausgeschlossen.

Bei einer Gatekeeper-Blockchain käme die Dezentralität des Systems und damit die Abschaffung Vertrauen beanspruchender Intermediäre, mithin die Peer-to-Peer-Struktur zwischen den eigentlich Betroffenen, jedoch abhanden. Die innovativen Vorteile der Blockchain wären damit in weiten Teilen unterminiert. Der Verantwortliche ist uU besser beraten, eine klassische Serverlösung mit Administratorrechten zu wählen, bei er sich auch nicht den Skalierbarkeitsschranken der Blockchain-Technologie ausgesetzt sieht.

b) Technische Implementierung einer nachträglichen Änderungsmöglichkeit.

Als Ausweg aus dem Löschungsdilemma sind neben einem partiellen Entfernen einzelner Transaktionen aus den Blöcken (*Pruning*) Blockchain-Varianten denkbar, die von vorneherein

---

[56] Vgl. *Artikel-29-Datenschutzgruppe,* Stellungnahme 5/2014 zu Anonymisierungstechniken, WP 216, 2014, 10 f.; aA *Dammann,* in *Simitis,* BDSG, 8. Aufl. (2014), § 3 Rn. 179.
[57] Vgl. *Hofmann/Johannes*, ZD 2017, 221 225 m. Fn. 76.

darauf ausgelegt sind, *nachträglich verändert* werden zu können (zB durch Nutzung eines wandlungsfähigen sog. *Chameleon-Hashes*).[58]

Die Besonderheit eines *Chameleon-Hashes* liegt darin, auch Änderungen an bereits in der Kette eingebetteten Blöcken zuzulassen – nicht alleine Einschreibungen pro futuro. Nur eine derartige nachträgliche Entfernung einzelner Informationen wird der Löschungspflicht gerecht. Sie setzt zugleich aber logisch voraus, dass eine zentrale Instanz für die nachträgliche Änderung der Blockchain nach festen Regeln zuständig ist.[59] In der Sache impliziert dies eine technische Hoheitsschnittstelle in der Blockchain, über die sich Entscheidungen einer für die Konfliktlösung vorgesehenen Instanz in die dezentrale Datenkette einspeisen lassen.[60]

Von ihrem Reiz der Dezentralität und auf technischer Autonomie beruhenden Vertrauenswürdigkeit büßt die Technologie dann jedoch ebenso wie im Falle einer Gatekeeper-Blockchain viel ein: Selbst wenn Änderungen nachvollziehbar sind, steht die gesamte Anwendung unter dem Damoklesschwert der Angreifbarkeit unter Ausnutzung der Hoheitsschnittstelle. Denn wer in der Lage ist, den Änderungsbefehl auszutauschen oder zu fälschen, hält das Schicksal der gesamten Blockchain in seinen Händen. Die in der Dezentralität wurzelnde Angriffsresilienz ist in ihren Grundfesten bedroht.

c) Einräumung einer Löschungsanordnungsbefugnis bei zentraler Verantwortlichkeit.

Ist die Verantwortlichkeit für eine Blockchain in einer Hand zentralisiert, lässt sich eine Löschung im Rahmen des bestehenden Auftragsverhältnisses rechtlich konstruieren. Der zentrale Verantwortliche bedarf hierzu einer Löschungsanordnungsbefugnis gegenüber den einzelnen *Nodes*. Abbilden lässt sich dies als Teil der Weisungsbindung des Auftragsverarbeiters (vgl. Art. 28 III 1 aE, 29 DSGVO). Die *Nodes* unterliegen danach der Pflicht, eine Löschung (in Form des *Prunings*) in ihrer Blockchain vorzunehmen, sobald sie eine entsprechende Anweisung des Verantwortlichen erhalten.

Dafür bedürfte es einer in der Blockchain integrierten technischen Struktur,[61] die im Idealfall eine Löschung automatisch auslöst, sobald sie einen dahin gehenden Befehl erhält, der über das P2P-Netzwerk versandt und durch jeden *Node* lokal verifiziert wird. In der Sache entspricht dies einer Hoheitsschnittstelle in der Blockchain.

3. Anpassungen zur Umsetzung der Informations- und Mitteilungspflicht

Wie sich die Informationspflicht des Art. 17 II DSGVO im Rahmen einer (öffentlich einsehbaren) Blockchain erfüllen lässt, zeichnet sich nur schemenhaft ab. Denkbar ist die

---

[58] Vgl. *Accenture,* Why distributed ledger technology must adapt to an imperfect world, 2016, 7.
[59] Vgl. *Accenture* (o. Fußn. 59), 7.
[60] Vgl. *Kolain*, in: *Hill/Kugelmann/Martini,* Die Blockchain als „vollkommenes Gesetzbuch"?, 2017, S. 147 ff. (158). Eine Justiz-Schnittstelle anreißend *Kaulartz/Heckmann*, CR 2016, 618 (624).
[61] Vgl. speziell die Betonung in Art. 28 I DSGVO.

Kennzeichnung zu löschender bzw. gelöschter Informationen (bspw. durch Übernahme von bei Webseiten praktizierten Mechanismen wie dem *robots.txt*) oder ähnliche allgemein in Bezug auf die Veröffentlichung im Internet diskutierte Verfahren.[62]

Die Pflicht zur Mitteilung innerhalb der Blockchain (Art. 19 DSGVO) lässt sich ggf. durch eine Anpassung des *Clients* erreichen: Er müsste dem einzelne *Node* die Möglichkeit eröffnen, einen Löschungshinweis auf demselben Weg an das Netzwerk zu entsenden, auf dem dieses auch Transaktionsdaten verteilt. Jeder *Node* kann dann auf den Hinweis hin seine Löschungspflicht autonom prüfen. Eine solche Automatisierungslösung hätte den Charme, an der Dezentralität der Blockchain selbst nicht zu rütteln. Technisch verfügbar ist sie aber noch nicht. Sowohl Art. 17 II als auch Art. 19 DSGVO verlangen dem Verantwortlichen normativ aber auch nur das technisch Mögliche und Zumutbare ab.

4. Zwischenergebnis

Ein tieferer Blick in den Maschinenraum der Blockchain fördert technische Gestaltungsmöglichkeiten zutage, die einem Recht auf Löschung in ihrer faktischen Wirkung bereits nahekommen (zB *ZKP*, Löschung der Zuordnungsdaten). Sie wahren auch das funktionale Unveränderlichkeitsdogma der Datenkette. Gleichwohl begegnen sie verschiedenen Bedenken: Einerseits können sie die Schaffung einer Hoheitsschnittstelle erfordern, andererseits gewährleisten sie keine vollständige Anonymisierung. Ansätze, welche die Durchsetzung der Löschung vereinfachen sollen (zB *Chameleon-Hash*, Löschungsanordnungsbefugnis), begegnen ebenfalls Bedenken: Sie knüpfen stets an die Existenz einer zentralen Instanz an.

Darin offenbart sich ein Grundkonflikt: Erforderliche Modifikationen führen die Innovationsvorteile der Blockchain-Technologie –Dezentralität, Autonomie und Vertrauenswürdigkeit – mitunter auf ein Minimum zurück. Von dem technischen Mehrwert der Bitcoin-Blockchain bleibt bei solchen Anwendungen nicht mehr viel übrig. Sie verhelfen mitunter sogar zentralen Vertrauensinstanzen (wie Staaten und Banken), welche die Technologie gerade abschütteln *will*, zur Renaissance.

Anders verhält es sich alleine bei Anpassungen, welche die akzessorische Informations- und Mitteilungspflicht umsetzen sollen. Sie lassen sich – im Rahmen der allgemein im Internet bestehenden Grenzen – in die bestehende Blockchain-Struktur implementieren, ohne ihre Funktionalität zu tangieren.

V. Regulatorische Lösungsansätze

Nimmt man das Recht auf Löschung in seiner gegenwärtigen Ausformung ernst, ist der Einsatz der Blockchain-Technologie in weiten Bereichen nur in einer Weise vorstellbar, die an

---

[62] Vgl. *Hornung/Hofmann*, JZ 2013, 163 (168 f.).

ihren Grundsäulen rüttelt. Einschränkungen ihrer Transparenz, Vollständigkeit und technischen Autonomie lassen sich zwar als Preis des persönlichkeitsrechtlichen Löschungsanspruchs verstehen. Er ist jedoch unangemessen hoch. Denn er torpediert im Ergebnis den gewinnbringenden Einsatz der Technologie. Ein absolut verstandenes Recht auf Vergessenwerden schießt im Fall der Blockchain-Technologie über seine eigene Zielsetzung hinaus: [63] Konzipiert ist das Recht auf Löschung (gerade im Internet) für Persönlichkeitsgefährdungen durch Veröffentlichungen des Klarnamens, etwa in Zeitungsberichten im Falle einer früheren Insolvenz oder Straftat.[64] Die Blockchain speichert und veröffentlicht indes keine Klarnamen, sondern kryptographische *Hashes* und öffentliche Schlüssel – und damit Pseudonyme. Beziehen sich Daten lediglich auf eine *bestimmbare* Person, können auch technische Umfeldmaßnahmen, die eine Re-Identifizierung wesentlich erschweren, den Interessen des Betroffenen genügen.

Für pseudonymisierte Daten sollte das unionale Datenschutzrecht daher das Recht auf Löschung de lege ferenda beschränken, wenn sich kein praktikabler technischer Weg findet, die Blockchain-Technologie mit ihm zu versöhnen. Dies entspricht auch der Grundtendenz der DSGVO, bereits in der Pseudonymisierung selbst einen weitgehenden Persönlichkeitsschutz zu sehen (vgl. ErwGrd 28 u. 29, Art. 32 Abs. 1 lit. a DSGVO).

Die DSGVO gestattet den Mitgliedstaaten de lege lata bereits, das Löschungsrecht unter Rückgriff auf die Schutzziele ihres Art. 23 I zurückzustutzen. Art. 23 I lit. e iVm ErwGrd 73 DSGVO gesteht ihnen insbes. das Recht zu, für „das Führen öffentlicher Register aus Gründen des allgemeinen öffentlichen Interesses“ Abweichungen von den Betroffenenrechten zuzulassen. Diese Öffnungsklausel lässt sich für viele *staatliche Blockchain-Anwendungen* nutzbar machen. Denn im Vergleich zu klassischen Serverlösungen eröffnet eine Blockchain im Grundsatz ein merklich höheres Potenzial, manipulative Eingriffe in die Datenstruktur zu verhindern. Sie kann überdies Verwaltungsprozesse beschleunigen und durch den Wegfall von Schnittstellen Kosten einsparen. Sofern der so erzielbare Nutzen die berührten Persönlichkeitsinteressen überwiegt, kann das eine mitgliedstaatliche Beschränkung des Löschungsrechts rechtfertigen. Für Blockchain-Anwendungen *Privater* liegt die Sache jedoch anders: Ein gesamtwirtschaftliches Interesse, die Innovationskraft der Blockchain-Technologie nutzbar zu machen, genügt den hohen normativen Anforderungen des Art. 23 I DSGVO nicht ohne Weiteres.[65] Regulatorische Spielräume der Mitgliedstaaten bestehen hier nicht – vielmehr ist der Unionsgesetzgeber gefragt. Die grundrechtlichen Verbürgungen sowohl des Art. 16 I AEUV als auch des Art. 8 GrCh lassen ihm dafür hinreichenden Raum.

Als Minus zum vollständigen Verzicht auf eine Löschung kommt daneben eine *Sperrung* der Daten in Betracht. Die DSGVO normiert zwar bereits ein solches Recht auf Sperrung

---

[63] Vgl. die grds. Bedenken des GA Jääskinen, BeckRS 2013, 81374 (Rn. 30, 79).
[64] Vgl. EuGH, EuZW 2014, 541 (543, Rn. 36 f.; 545, Rn. 62; 546, Rn. 80): Suche „anhand des Namens“.
[65] Insbes. Art. 23 I lit. e DSGVO umfasst nicht das Ziel der allgemeinen Wirtschaftsförderung, vgl. bereits ErwGrd 112.

(„Einschränkung der Verarbeitung“ – Art. 18 DSGVO).[66] Es greift aber nur unter sehr engen Voraussetzungen.[67] Den Mitgliedstaaten verbleibt nur das limitierte Abweichungsrecht aus Art. 23 DSGVO.[68] In der Sache dürfte dadurch jedoch wenig zu gewinnen sein. Denn in Blockchain-Anwendungen lässt sich eine Sperrung faktisch wohl ebenso wenig wie eine Löschung umsetzen: Eine automatisch angestoßene Zugriffsverweigerung auf bestimmte Transaktionsdaten oder deren Verschlüsselung griffe in gleicher Weise wie eine Löschung tief in die Blockchain-Architektur und damit die Vertrauenswürdigkeit ein.

Von der Möglichkeit, das Löschungsrecht normativ zurückstutzen, sollte der Normgeber daher (ggf. in Gestalt einer Experimentierklausel) Gebrauch machen. Nicht zuletzt die langsam aus dem Dornröschenschlaf erwachende Start-up-Szene wird es ihm danken, wenn er das datenschutzrechtliche Gerüst an neue Formen der automatisierten und autonomen Datenverarbeitung in komplexen dezentralen Systemen anpasst. Deren Eigenheiten zu erfassen und in geeignete rechtliche Kategorien zu gießen, ist freilich alles andere als ein regulatorisches Kinderspiel.

VI. Fazit

Die Blockchain-Technologie und das Recht auf Vergessenwerden sind Antagonisten. Zwar lässt sich eine bestehende Löschungspflicht bei abgeschlossenen Transaktionen an sich funktionswahrend umsetzen (sog. *Pruning*). Der Betroffene hat jedoch wenig Aussicht, sein Recht auch effektiv durchzusetzen. Denn in zulassungsfreien Blockchains mit dezentraler Verantwortlichkeit können weder er noch die Aufsichtsbehörden der Gesamtheit aller *Nodes* zuverlässig habhaft werden, um Daten wirksam aus dem Netzwerk zu verbannen. In zulassungsbeschränkten Anwendungen ist der zentrale Verantwortliche auf besondere rechtliche Mittel angewiesen, um seine Pflicht zur Löschung bei den *Nodes* durchzusetzen.

Technische Anpassungen der Blockchain-Technologie versprechen zwar – ebenso wie eine Hoheitsschnittstelle bei *private Blockchains* – Abhilfe. Von ihrer eigentlichen Idee bleibt bei solchen Anwendungen jedoch nicht mehr viel übrig: Gestaltungen, die es ermöglichen, Daten nachträglich zu löschen, schränken die besondere Vertrauenswürdigkeit und Vollständigkeit der via Blockchain abgewickelten Transaktionen empfindlich ein. Dies gilt insbes. dann, wenn einer zentralen Einrichtung das Recht zuwächst, (zB iRe Löschungsanordnungsbefugnis) auf den Inhalt der bei den *Nodes* gespeicherten Datenketten einzuwirken. Auf das Dilemma zwischen Vergessen-Müssen und Nicht-Vergessen-Können müssen Einsatzszenarien eine Antwort finden – reibungslos auflösen lassen wird es sich wohl nicht.

---

[66] So auch die Regelung des § 35 BDSG nF bzw. §§ 20 III Nr. 3, 35 III Nr. 3 BDSG.
[67] In wenigen Fällen hilft Art. 18 I lit. c DSGVO: Soweit die in einer Blockchain gespeicherten personenbezogenen Daten nicht mehr zur Verarbeitung, sondern nur noch zur Geltendmachung, Ausübung o. Verteidigung v. Rechtsansprüchen des Betroffenen erforderlich sind, zeichnet die DSGVO den Weg der Sperrung normativ vor.
[68] Das systematische Verhältnis zwischen Löschung und Sperrung bestimmt die DSGVO zwar selbst und unmittelbar. Von diesen Regeln lässt Art. 23 DSGVO aber gerade Ausnahmen zu. Das schließt auch eine Reduzierung der Löschung auf eine Sperrung ein.

Um das Innovationspotenzial der Blockchain-Technologie nicht zu gefährden, ist es dem Gesetzgeber deshalb anzuraten, das Recht auf Löschung für komplexe dezentral organisierte IT-Architekturen zugunsten eines Rechts auf hinreichende Schutzmaßnahmen, insbes. Pseudonymisierung, zu reduzieren.

Sich als Gesellschaft die technischen Möglichkeiten des digitalen Wandels wegen eines absolut verstandenen Persönlichkeitsschutzes zu versagen, wäre ein Irrweg.[69] In vorauseilendem Gehorsam schon den Versuch zu unterlassen, den vielversprechenden Einsatz der Blockchain-Technologie durch die Schaffung legislativer Rahmenbedingungen zu flankieren, hieße gesellschaftliches Innovationspotenzial am ausgestreckten Arm verhungern zu lassen.

Glossar

Blockchain:	Konzept einer digitalen Datenbank, basierend auf den Elementen „Dezentralität", „kryptographische Verkettung von Blöcken" (mittels Hash↗) und „Verifikation durch öffentlich-private Schlüsselpaare".
open/closed Blockchain:	Blockchain↗, die beliebige Interessierte/ nur die *Nodes*↗ einsehen können (auch: öffentlich einsehbar/nicht öffentlich einsehbare Blockchain).
public/private Blockchain:	Blockchain↗, bei der jedermann zum *Node*↗ werden kann/ die nur bestimmte Personen als *Node* zulässt (auch: zulassungsfreie/zulassungsbeschränkte Blockchain).
Block:	Untergliederung der Blockchain↗, bestehend aus einem *Block Header*↗ und einem Transaktionsteil.
Block Header:	Teil des Blocks↗, in dem der *Previous Hash*↗, *Merkle-Hash*↗, *Time Stamp* (Fn. 3) und *Nonce*↗ gespeichert sind.
Client:	Benutzungssoftware, mit deren Hilfe die aktuelle Version einer Blockchain↗ heruntergeladen werden kann. Sie ermöglicht damit die Teilnahme am P2P-Netzwerk↗ (insbesondere öffentliche und private Schlüssel zu generieren und zu verwalten sowie Transaktionen an das P2P-Netzwerk auszusenden).
Chameleon-Hash:	besondere Hashfunktion zur Berechnung des *Previous Hash*↗, die es einer hierzu berechtigten Instanz erlaubt,

[69] Das widerspräche auch ErwGrd 4 DSGVO, vgl. *Hofmann/Johannes*, ZD 2017, 221 (225).

	den vorhergehenden Block↗ zu verändern, ohne dass der folgende *Block Header*↗ mit geändert werden muss.
Hash:	Ergebnis einer Hashfunktion (auch: Hashalgorithmus), die aus einer Zeichenfolge beliebiger Länge (zB Transaktionsdaten, pdf-Dateien) eine Zeichenfolge mit fester Länge (zB 256 Bit) errechnet. Bei Blockchains↗ findet dabei eine sog. kryptographische Hashfunktion Verwendung, die es ausschließt, aus einem *Hash* auf den Ausgangsinhalt rückzuschließen.
Hash-Baum, Merkle-Hash:	Bestandteil des Transaktionsteils eines Blocks↗: Er entsteht, indem aus einer Transaktion ein *Hash*↗ und aus jeweils zwei *Hashes* ein neuer gebildet wird – so lange, bis nur noch ein *Hash* (der sog. *Merkle-Hash)* übrig bleibt, der gleichsam den Wipfel des Hash-Baums bildet.
Miner:	derjenige *Node*↗, der durch *Mining*↗ einen neuen Block↗ errechnet hat.
Mining:	Berechnen neuer Blöcke↗ aus an das Netzwerk ausgesandten Transaktionen nach Prüfung anhand der bestehenden Blockchain↗.
Node:	Teilnehmer (*Peer*) des Blockchain-P2P-Netzwerks↗.
Nonce:	Bestandteil des *Block Headers*↗: Beim *Mining*↗ gefundener Arbeitsbeweis.
P2P/Peer-to-Peer-Netzwerk:	Netzwerk unter gleichberechtigten Computern, dessen Teilnehmer (*Peers*) unmittelbar ohne zentrale Instanz miteinander interagieren.
Previous Hash:	Bestandteil des *Block Headers*↗: Er enthält den *Hash*↗ des *Block-Headers* (*nicht* des gesamten Blocks↗ bzw. des Transaktionsteils) des vorangehenden Blocks.
Pruning:	Löschen von Transaktionsdaten aus dem Transaktionsteil eines Blocks↗.