> CHRISTIAN PISKA / MARIE-CATHERINE WAGNER

ZUKUNFTSTECHNOLOGIE BLOCKCHAIN und wie man den Stolperstein DSGVO vermeiden kann*

The cost of the bankruptcy of Lehman Brothers in 2008 to the United States is estimated in trillions and triggered a chain of events that sent several countries into economic recession or depression. One contributor to the crisis was the centralized payment and monetary system based on clearinghouses that act as intermediaries. There is no need to rely on, or trust, a single organization, [however]. The blockchain allows services to be (completely) decentralized [and] promises to revolutionize the way we conduct business.**

I. Einleitung

Akkreditive – die Nachvollziehbarkeit von Lebensmittelketten – Grundbucheintragungen – das Management von Emissionsguthaben – elektronische Türschlösser – die Verwaltung von Gesundheitsdaten – internationale Versicherungspolizzen – die Betriebsbereitschaft von Leasing Fahrzeugen – weltweite Geldüberweisungen – Herkunftsnachweise von Diamanten – Zollerklärungen – die elektronische Gesundheitsakte – der Wertpapierhandel – die Transparenz einer pharmazeutische Kühlkette – Bankgarantien – die Produktionshistorie eines Produktes – Smart Grids – die Administration von Private Equity Funds – ...

Was haben diese Prozesse und (Trans)aktionen gemeinsam? Sie können automatisiert, sicher, transparent und unveränderbar auf Blockchains ablaufen und sind nur einige wenige Beispiele für die fast unendlichen Anwendungsmöglichkeiten einer Schlüsseltechnologie, die das Potential hat, die Weltwirtschaft zu verändern.[1]

II. The Method behind the Magic

Bei dieser derzeit die Wirtschaft revolutionierenden Technologie (einer speziellen Form der Distibuted Ledger Technology[2] bzw Sonderfall einer Distributed Data Base[3]) handelt es sich um eine beliebig erweiterbare Liste von Datensätzen (Blocks), die durch kryptographische Verfahren miteinander verbunden sind. Jedem dieser Blöcke (Datensätze) wird durch eine Hashfunktion eindeutig eine Zahl (Streuwert, Hash) bestimmter Länge zugeordnet. Bei jeder Veränderung der Daten enthält der Block sofort einen neuen Hash. Neben seinem eigenen Streuwert enthält ein Block auch den Streuwert des vorherigen Blocks. Durch diesen Algorithmus entsteht eine Datenstruktur (kryptographische Verkettung), in der jede Veränderung exakt und unlöschbar dokumentiert ist und bleibt, denn ändert sich bei einem Block der Hash, dann stimmt die Referenz beim Nachfolger nicht mehr. Ein Blockchain System ist ein Peer-to-Peer (P2P) Netzwerk, das ohne zentrale Serverinstanz alle Teilnehmer (Knoten, Nodes) gleichstellt und derart miteinander verbindet, dass sie direkt kommunizieren können. Diese verteilte, dezentrale Datenstruktur speichert Transaktionen transparent, chronologisch und unveränderbar auf jedem Rechner im Netzwerk. Wenn jemand dieser Transaktionsplattform beitritt, bekommt er eine vollständige Kopie der Blockchain und kann prüfen, ob sie in Ordnung ist. Jeder Teilnehmer erhält auch jeden neuen Block und validiert ihn (bzw die Transaktion) und bestätigt somit, dass er nicht manipuliert wurde. Alle Nutzer eines Netzwerkes einigen sich, welche Blöcke gültig sind und welche nicht (Consensus Protocol). Die Löschung eines einzelnen Blocks ist nicht möglich. Wird ein Block ohne Konsens der Mehrheit verändert, ist die gesamte Chain ungültig. Bei öffent-

* Unser herzlicher Dank gebührt dem BRZ für die tatkräftige Unterstützung beim Setup des vorliegenden Beitrags.

** *Ateniese/Magri/Venturi/Andrade*, Redactable Blockchain (2017), abrufbar unter <https://allquantor.at/blockchainbib/pdf/ateniese-2016redactable.pdf> (Stand 07.12.2018).

1 *Iansiti/Lakhani*, The Truth About Blockchain, abrufbar unter <https://hbr.org/2017/01/the-truth-about-blockchain> (Stand 07.12.2018).

2 *Meunier*, Blockchain technology – a very special kind of Distributed Database, abrufbar unter <https://medium.com/@sbmeunier/blockchain-technology-a-very-special-kind-of-distributed-database-e63d00781118> (Stand 07.12.2018).

3 *Catalini/Gans*, Some Simple Economics of the Blockchain (2017) und <https://www.youtube.com/watch?v=taG-1p-UNC0> (Stand 07.12.2018).

lichen, sogenannten public Blockchains – wie beispielsweise Bitcoin – kann jeder teilnehmen. Hier wird Konsens durch ein Mehrheitsvotum und einen sogenannten Proof of Work Mechanism erzielt, bei dem ein komplexes, ressourcenintensives kryptographisches Problem gelöst werden muss[4] und der eine missbräuchliche Verwendung verhindern soll.[5] In einer privaten (closed, permissioned[6]) Blockchain, die nur einem bestimmten Kreis von Berechtigten vorbehalten ist, entscheidet ein Netzwerkverantwortlicher bzw ein von ihm festgelegtes Regulativ über die Validität einer Transaktion, über die Vergabe von Lese- und Schreibrechten, etc.

III. Innovation meets Routine

Das Innovationspotential von Blockchains stützt sich im Wesentlichen auf zwei kryptographische Algorithmen: nämlich die digitale Signatur, die Sicherheit bietet, und Hashfunktionen mit speziellen Eigenschaften, die durch Transparenz und Unveränderbarkeit gegen nachträgliche Manipulation schützen.[7]

Optimale Einsatzbedingungen für diese Technologie ergeben sich überall dort, wo Daten von mehreren Stellen zusammengeführt, verarbeitet und für die Beteiligten nachvollziehbar und irreversibel dokumentiert werden müssen. Auch dann, wenn ein Abgleich in Echtzeit und die Automatisierung von Transaktionen sowie der direkte Zugriff aller daran Beteiligten ohne zentrale Instanz erwünscht ist, hat die Blockchain ihre Sternstunde. Sind alle Schritte eines Routineablaufs einmal festgelegt bzw vertragliche Vereinbarungen getroffen, werden die Ausführungsanweisungen für immer unveränderbar programmiert, so dass der mehrstufige Prozess automatisch und unmanipulierbar ablaufen kann. Sobald eine gewisse Bedingungen eintritt, wird automatisch eine bestimmte Aktion veranlasst.[8] Diese Blockchain-Architekturen, die Wenn-Dann-Aussagenverbindungen abbilden, und die insoweit automatisierte (Rechts-) Folgen bzw bestimmte Vorgänge herbeiführen, bezeichnet man als Smart Contracts.[9] Wird in einer herkömmlichen, dezentralen Datenbank die Software geändert, gibt es grundsätzlich keine Nachvollziehbarkeit mehr, wenn die Entwicklungsdokumentation verloren geht.[10] Bei Blockchains hingegen bleibt der Algorithmus unlöschbar gespeichert und ist somit für weitere Anwendungen jederzeit reproduzierbar.

IV. Ein Game Changer[11] für die Wirtschaft

Als in den 1970 Jahren durch die Entwicklung von Datenübertragungstechnologien verteilte Systeme zusammengeschlossen werden konnten, und die Einführung des TCP/IP Protokolls die Basis für das Internet legte[12], hatte wohl niemand eine Vorstellung, wie radikal diese neue Architektur einmal die Wirtschaft verändern würde. Zwanzig Jahre später ist das World Wide Web einer breiten Öffentlichkeit zugänglich und eine neue Generation von Unternehmen kann die Vorteile der niedrigen Übertragungskosten für innovative Geschäftsmodelle nützen.[13] Eine ähnliche Entwicklung wird der Blockchain, deren grundlegende Prinzipien bereits 1991 erstmals erwähnt werden,[14] in Bezug auf sichere Transaktionen prognostiziert. Durch ihre speziellen Eigenschaften wie Unlöschbarkeit, Transparenz und Sicherheit von Daten und Transaktionen ist auch die Blockchaintechnologie ein Game Changer par excellence. Sie hat das Potenzial, Businessmodelle und Geschäftsprozesse zu revolutionieren, Transaktionsaufwand und -kosten zu minimieren, Wertschöpfung zu steigern und neue Perspektiven für die Gestaltung von Produkten, Services und Prozessen zu eröffnen.[15] Durch den Verzicht auf eine zentrale Stelle können Prozesse verkürzt, Transaktionen beschleunigt und Kosten gesenkt werden.[16] Dabei spielt natürlich nicht nur die Technologie allein, sondern auch der darum stattfindende Hype eine Rolle, der den Entwicklungsprozess rund um die Blockchain gewaltig mit Eigendynamik befeuert.

Sehr viele Use Cases für Smart Contracts finden sich derzeit in der Automatisierung von Logistik, Workflow und Supply Chain Management. Man stelle sich beispielsweise die Vielzahl von Personen, Unternehmen, Institutionen, Dokumenten, Prozessschritten und Aktionen vor, die an einem weltweiten Waren-

4 *Jayachandran*, The diffenrence between public and private blockchain, abrufbar unter <https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain> (Stand 07.12.2018)
5 *Catalini/Gans*, Blockchain (FN 5) und <https://www.youtube.com/watch?v=taG-1p-UNC0> (Stand 07.12.2018).
6 *Hileman/Rauchs*, Global Blockchain Benchmarking Study (2017) 11.
7 *Narayanan/Bonneau/Felten/Miller/Goldfeder*, Bitcoin and Cryptocurrency Technologies (2016).
8 *Buchleitner/Rabl*, Blockchain and Smart Contracts, ecolex 2017, 4 (6).
9 *Eberhardt/Tai*, On or Off the Blockchain? (2017) 3.
10 *Liebig/Flik/Rechenberg/Reinefeld/Mössenböck*, Das Ingenieurwissen: Technische Informatik (2014) 167f.
11 Anwendung und Potentiale der Blockchain-Technologie, siehe dazu <https://gi.de/blockchain/> (Stand 07.12.2018).
12 Siehe dazu <http://web.mit.edu/6.02/www/f2006/handouts/net_L7.pdf> (Stand 07.12.2018).
13 *Iansiti/Lakhani*, Blockchain (FN 3).
14 *Konst*, Sichere Log-Dateien auf Grundlage kryptographisch verketteter Einträge (Diplomarbeit).
15 <http://smartblockchain.at/> (Stand 07.12.2018).
16 <https://www.ibm.com/blockchain/use-cases/> (Stand 07.12.2018).

versand beteiligt sind. So müssen etwa Verträge mit dem Käufer, dem Logistikunternehmen und Export/Import Brokern, Terminvereinbarungen sowie Bankgarantien eingehalten und Ein- und Ausfuhrgenehmigungen, Zollerklärungen und Zahlungsaufträge gesetzeskonform durchgeführt werden. All diese und viele andere Aktionen im Supply-Chain-Prozess erfordern einen großen Aufwand an Verwaltungsarbeit und sind zeitintensiv. Bei einer Automatisierung mittels Smart Contracts haben alle Beteiligten direkten Zugriff auf die Blockchain. Datenabgleich und -verarbeitung erfolgen in Echtzeit und die Speicherung ist transparent und fälschungssicher. Auch in einigen Produktionsbetrieben kommen Smart Contracts bei der Automatisierung von Erzeugungs- und Wartungsprozessen sowie bei der Dokumentation der einzelnen Schritte der Wertschöpfungskette bereits zum Einsatz.

Im Bereich Handel planen große, internationale Nahrungsmittelhersteller gemeinsame Blockchains zu betreiben, die allen am Prozess Beteiligten – Erzeuger, Lieferanten, Verarbeitungsbetrieben, Groß- und Einzelhändlern sowie den Konsumenten – Zugriffsrechte zu Informationen über Produkte in der Lebensmittelkette gewähren. Der Ursprung der Waren soll damit zurück verfolgbar und die Produkthistorie dokumentiert werden. Durch diese Nachvollziehbarkeit lassen sich im Falle einer Verunreinigung Gesundheitsrisiken schnell erkennen und sofort reduzieren. Damit kann vor allem auf Verbraucherseite ein bisher unerreichbarer Level of Trust geschaffen werden, zum Beispiel auch im Fall von immer beliebteren Bio-Produkten.

Ein breites Anwendungsportfolio liegt auch im Finanzsektor. So lassen sich unter anderem Auslandsüberweisungen, Smart Payment, Wertpapierhandel, Trade Financing und die rechnungslose Finanztransaktion (Paperless Trade) auf Blockchains effizient und kostengünstig abwickeln. Smart Contracts speichern die Vertragsinhalte, lösen automatisch Finanztransaktionen aus und überwachen den gesamten Prozess der Vertragsausführung. Für das Geschäftsmodell der Kryptowährungen ist die für jeden und jederzeit sichtbare genaue Protokollierung der Veränderungen bzw die systemimmanente Eigenschaft der Unlöschbarkeit eine unverzichtbare Basis. Der wirtschaftliche Erfolg dieser Produkte ist damit untrennbar verbunden.

Ganz besondere Vorteile bieten Blockchains für Archivierungsaufgaben und verlässliche, exakt nachvollziehbare, transparente Dokumentationen. So archiviert eine internationale Handelskette Daten aus der Kassa mittels Blockchain und wertet sie auch gleich aus.

Potentielle Anwendungsbereiche in der öffentlichen Verwaltung sind das Grund- und Firmenbuch sowie Patentverzeichnisse. Auch im Gesundheitswesen, in der Finanzverwaltung so wie bei der Polizei, Justiz (zB feste Geschäftsverteilungen) und Landesverteidigung eröffnen Blockchains eine Vielfalt von Optimierungsmöglichkeiten. Selbst der Einsatz für fälschungssichere Wahlen wird überlegt.[17] Zeitstempel, die beweisen, wann bestimmte Informationen bereits existiert haben, können durch Blockchains mittels Hashes fälschungssicher vergeben werden. Eine offizielle Instanz, die den Stempel bereitstellt, ist nicht mehr nötig.

Großbritannien versucht bereits die Auszahlung von Sozialleistungen über Blockchains zu verwalten[18] und die US-Regierung hat ähnliche Überlegungen für Gesundheitsdaten.[19] Auch die UNO will Blockchains zur Effizienzsteigerung bei der Verteilung von Hilfsgütern einsetzen.[20]

Große Erwartungen an die Blockchain hat man bei der Vernetzung von physischen und virtuellen Dingen im Internet of Things.[21] So sollen Smart Contracts effiziente Rahmenbedingungen für das Zusammenspiel von Dienstleistungen und Ressourcen schaffen. Zeitaufwendige Workflows können auf diese Weise automatisiert werden.[22] Im Weiteren kann auch die Sicherheit von Internet-Connected-Devices, die grundsätzlich in Bezug auf Cyberattacken sehr verletzlich sind, durch Hochladen von Updates auf eine Blockchain stark verbessert werden.[23]

V. Blocking the Blockchain?

Diesem enormen Entwicklungspotential an der Schnittstelle von Technologie und Wirtschaft stehen mit der DSGVO datenschutzrechtliche Herausforderungen in Bezug auf die Verarbeitung personenbezogener Daten gegenüber.

17 *Iansiti/Lakhani*, Blockchain (FN 3).

18 Vgl *Cellan-Jones*, Blockchain and benefits – a dangerous mix?, abrufbar unter <http://www.bbc.com/news/technology-36785872> (Stand 07.12.2018).

19 Vgl Office of the National Coordinator for Health Information Technology (ONC), ONC announces Blockchain challengewinners, Pressemitteilung vom 01.09.2016.

20 Vgl World Food Program, What is 'Blockchain' and How is it Connected to Fighting Hunger?, abrufbar unter <https://insight.wfp.org/what-is-blockchain-and-how-is-it-connected-to-fighting-hunger-7f1b42da9fe> (Stand 07.12.2018).

21 *Catalini/Gans*, Blockchain (FN 5) und <https://www.youtube.com/watch?v=taG-1p-UNC0> (Stand 07.12.2018).

22 *Christidis/Devetsikiotis*, Blockchains and Smart Constracts for the Internet of Things, abrufbar unter <https://mycourses.aalto.fi/pluginfile.php/378344/mod_resource/content/1/Christidis%20and%20Devetsikiotis.pdf> (Stand 07.12.2018).

23 <https://www.scientificamerican.com/article/using-blockchain-to-secure-the-internet-of-things/> (Stand 07.12.2018).

A. Personenbezogene Daten

Die DSGVO schützt personenbezogene Daten natürlicher Personen und schränkt deren Verarbeitung ein. Als personenbezogene Daten gelten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche (keine juristische) Person (sogenannte „betroffene Person") beziehen (Art 4 Z 1 DSGVO). Das Abgrenzungskriterium der Identifizierbarkeit wird vom EuGH[24] sehr weit gesehen. Schon die Möglichkeit des Verarbeiters oder eines Dritten, beispielsweise eine IP-Adresse mit zusätzlichen Informationen zu verknüpfen, kann ein Mittel zur Bestimmung einer Person darstellen. Ein personenbezogenes Datum liegt nicht vor, wenn die Mittel zur Identifizierung gesetzlich verboten oder nahezu unmöglich sind. Nahezu unmöglich ist die Identifikation, wenn sie nur mit einem unverhältnismäßig hohen Aufwand erreichbar ist. Der EuGH hat in seinem Urteil festgehalten, dass es sich sogar bei dynamischen IP-Adressen um personenbezogene Daten handelt.

Anonyme Daten lassen eine Identifizierung der betroffenen Person nicht zu. Sie sind von der Anwendung der Verordnung ausgenommen.[25] Davon zu unterscheiden ist der Prozess der Pseudonymisierung. Dabei müssen Informationen von personenbezogenen Daten, die zur Identifikation einer natürlichen Person notwendig sind, gesondert aufbewahrt werden und technische und organisatorische Maßnahmen ergriffen werden, die eine Zuordnung ohne diese Informationen verhindern. Durch die Pseudonymisierung von Daten wird deren Verarbeitung in einigen Bereichen der DSGVO privilegiert.

Bei Kryptowährungen beispielsweise können scheinbar unabhängige Informationen so zusammengeführt und analysiert werden, dass die IP-Adresse und damit die Identität von Nutzern ermittelt werden kann. Es handelt sich daher um personenbezogene Daten. Wenn aber alle zur Identifikation notwendigen Informationen ausreichend gesichert getrennt von den anderen Daten verwahrt werden, kann man von einer Pseudonymisierung sprechen.[26]

B. Rechtmäßigkeit der Verarbeitung

Bei Verarbeitung iSd DSGVO handelt es sich um jeden Vorgang – wie beispielsweise das Erheben, Erfassen, die Organisation, das Ordnen oder das Speichern – im Zusammenhang mit personenbezogenen Daten. Im Allgemeinen ist eine Verarbeitung verboten, außer es liegt eine Rechtsgrundlage im Sinne des Art 6 DSGVO vor: Diese ist unter anderem bei freiwilliger Einwilligung, der Erfüllung eines Vertrages oder einer rechtlichen Verpflichtung gegeben. Von einer rechtmäßigen Verarbeitung kann auch ausgegangen werden, wenn lebenswichtige Interessen geschützt oder Aufgaben im öffentlichen Interesse wahrgenommen werden. Als weitere Möglichkeit führt die DSGVO in Art 6 Z 1 lit f überwiegend berechtigte Interessen des Verantwortlichen oder eines Dritten an. Es wird im Einzelfall zu prüfen sein, auf welche Rechtsgrundlage sich eine Verarbeitung stützt; dabei sind Einwilligung und Vertragserfüllung für Unternehmen von besonderer Bedeutung.

Die Einwilligung der betroffenen Person muss freiwillig, unmissverständlich und zweckbezogen sein und in Form einer Erklärung oder eindeutigen Handlung erfolgen – Schweigen gilt nicht als Zustimmung. Freiwilligkeit ist nur dann gegeben, wenn die betroffene Person die Einwilligung verweigern oder zurückziehen kann, ohne dass ihr dadurch Nachteile entstehen. Dabei ist wichtig, dass die betroffene Person den Zweck der Verarbeitung kennt. Weiters muss ihr derjenige bekannt sein, der über Zweck und Mittel der Verarbeitung entscheidet (der sog. Verantwortliche – Art 4 Z 7 DSGVO). Die betroffene Person kann ihre Einwilligung jederzeit widerrufen (Art 7 DSGVO).

Bei einer öffentlichen Blockchain ist eine Einwilligung schon deshalb nicht denkbar, weil ein Verantwortlicher nicht eindeutig festgestellt werden kann. Bei einer privaten Blockchain allerdings wird jeder Nutzer von einer zentralen Stelle eingeladen. Diese zentrale Stelle kann grundsätzlich als Verantwortlicher im Sinne der DSGVO angesehen werden. Auf Einzelheiten den Verantwortlichen betreffend wird im Folgenden noch eingegangen. In der Praxis ist es für Unternehmer in vielen Fällen wahrscheinlich einfacher, sich bei der Verarbeitung auf die Rechtsgrundlage der Vertragserfüllung zu stützen: Eine Verarbeitung ist nämlich dann rechtmäßig, wenn sie für die Erfüllung oder den geplanten Abschluss eines Vertrags erforderlich ist.[27]

Gemäß Artikel 3 DSGVO bezieht sich die DSGVO grundsätzlich auf die Verarbeitung personenbezogener Daten innerhalb der EU, jedoch kann sie auch außerhalb der EU niedergelassene Verantwortliche bzw Auftragsverarbeiter betreffen. Voraussetzung dabei ist, dass sich die betroffene Person in der Union befindet, und die Datenverarbeitung im Zusammenhang damit steht, dieser Waren oder Dienstleistungen anzubieten. Es ist dabei nicht relevant, ob von der betroffenen Person eine Zahlung zu leisten ist. Allfällige Verträge sind

24 EuGH 19.10.2016, C-582/14, *Breyer*, ECLI:EU:C:2016:779, Rz 31 ff.
25 ErwGr 26 DSGVO.
26 Art 4 Z 5 DSGVO.
27 Art 6 Abs 1 lit b sowie ErwGr 44 DSGVO.

DSGVO konform zu verfassen, und die österreichische Datenschutzbehörde muss als zuständige Behörde anerkannt werden.

C. „Der" Verantwortliche

Für die Durchsetzung der Rechte auf Wahrung des Grundrechts auf Datenschutz muss ein für die Datenverarbeitung Verantwortlicher festgestellt werden. Dabei kann es sich gemäß Art 4 DSGVO um eine natürliche bzw juristische Person oder um eine andere Stelle handeln, die Entscheidungskompetenz über Zweck und Mittel der Verarbeitung der personenbezogenen Daten hat. Es kann auch mehrere gemeinsam Verantwortliche geben (Art 26 DSGVO).

Bei Blockchains ist aufgrund der dezentralen, verteilten Peer-to-Peer Technologie eine eindeutige Zuordnung der Verantwortung schwierig. Grundsätzlich könnte man erwägen, bei einer public Blockchain – wie beispielsweise Bitcoin – die einzelnen Nutzer, die direkt miteinander interagieren, als Verantwortliche zu sehen. Dies führe jedoch zu massiven Inkonsistenzen, da keiner der Beteiligten allein Einfluss auf das Gesamtsystem hat und auch keine konzertierte Abstimmung von Handlungen unter den Beteiligten im Ganzen erfolgt.[28] Anders ist es, wenn Plattformen wie Bitcoin-Geldbörse-Dienste zwischengeschaltet sind. In so einem Fall können diese dann als Verantwortliche im Sinne des Art 4 Z 7 DSGVO gesehen werden.[29] Bei private Blockchains ist derjenige verantwortlich, der den Zugang zur Blockchain festlegt. Er hat die Entscheidungskompetenz über Zweck und Mittel der Verarbeitung der personenbezogenen Daten. Der Verantwortliche hat eine Rechenschafts- und Auskunftspflicht gegenüber den betroffenen Personen. Er muss außerdem Pflichten wie Berichtigung und Löschung von Daten erfüllen. Verstöße gegen diese Bestimmungen werden mit drakonischen Strafen geahndet – diese betragen bis zu 4 % des (vorangegangenen) Jahresumsatzes bzw EUR 20 Mio.

D. Berichtigung und Löschung – „Das Recht auf Vergessenwerden"[30]

Personenbezogene Daten dürfen nur so lange gespeichert werden, wie dies für die festgelegten Verarbeitungszwecke erforderlich ist. Fällt die Rechtsgrundlage für die rechtmäßige Verarbeitung der Daten weg, müssen die Daten grundsätzlich gelöscht werden (Art 17 Abs 1 DSGVO). Wie bereits erwähnt, sind anonyme Daten von der Anwendung der DSGVO nicht betroffen. Daher stellt sich die Frage, ob man Daten tatsächlich löschen muss oder ob es reicht, sie zu anonymisieren. Daten gelten als anonymisiert, wenn die Bestimmbarkeit einer natürlichen Person unmöglich gemacht wurde.[31] Es darf keine Möglichkeit mehr bestehen, eine Verbindung zwischen den sich in den Daten befindlichen Informationen und der betroffenen Person herzustellen.

Das 2014 vom EuGH entwickelte „Recht auf Vergessenwerden"[32] findet sich in der DSGVO wieder. Unrichtige Daten sind auf Wunsch der betroffenen Person zu berichtigen bzw. zu löschen. Auch unvollständige Daten müssen vervollständigt werden. Das Recht auf Löschung kann gemäß Art 17 Abs 3 DSGVO verwehrt werden, wenn die Verarbeitung zur Ausübung des Rechts auf freie Meinungsäußerung, Erfüllung einer rechtlichen Verpflichtung, Geltendmachung von Rechtsansprüchen oder zur Durchsetzung öffentlicher Interessen erforderlich ist. Ein solcher Grund ist der betroffenen Person umgehend mitzuteilen.

Das „Recht auf Vergessenwerden"[33] stellt eine gewisse Hürde für Blockchains dar, da diese Technologie auf den Grundsätzen der Transparenz und Unlöschbarkeit basiert. Dieses Spannungsverhältnis gilt es durch den Einsatz geeigneter IT-Technologien aufzulösen. Zwar besteht die Möglichkeit, in einem neuen Block Informationen bzw Transaktionen älterer Blöcke für ungültig zu erklären, die alten, zu löschenden Informationen bleiben aber vorhanden und für alle Teilnehmer lesbar, was nicht datenschutzrechtlichen Anforderungen entspricht. Es gibt aber auch schon sogenannte „Redactable Blockchains". Sie ermöglichen eine nachträgliche Änderung alter Blöcke mittels eines kryptographischen Schlüssels. Der zu ändernde Block kann durch einen neuen ersetzt werden, ohne dass alle nachfolgenden Blöcke ihre Gültigkeit verlieren und neu berechnet werden müssen. Solche Redactable Blockchains ermöglichen, dass speziell ermächtigte Administratoren – unter definierten Voraussetzungen – ausnahmsweise Veränderungen vornehmen, die zB durch die DSGVO vorgeschrieben sind (zB Recht auf Löschung). Derartige Modelle lassen die kryptografischen Schlüsselelemente der Blockchain unangetastet. Die nachträgliche Veränderung eines Blocks in der Kette, kann durch eine „Narbe" erkennbar bleiben[34].

28 Daher muss dieser Punkt einer gesonderten Untersuchung vorbehalten bleiben.

29 *Erbguth/Fasching*, Wer ist Verantwortlicher einer Bitcoin-Transaktion, ZD 2017, 560 (565).

30 EuGH 13.05.2014, C-131/12, *Google Spain und Google*, ECLI:EU:C:2014:317.

31 ErwGr 26 DSGVO.

32 EuGH 13.05.2014, C-131/12, *Google Spain und Google*, ECLI:EU:C:2014:317.

33 EuGH 13.05.2014, C-131/12, *Google Spain und Google*, ECLI:EU:C:2014:317.

34 *Marnau*, Die Blockchain im Spannungsfeld der Grundsätze der

Durch Editierbarkeit soll, so der Anbieter Accenture, die Blockchain pragmatischer werden und in einer nicht perfekten Welt bestehen können.

Diese Lösung ist vor allem für private Blockchains eine Option, die von zentralen Aufsichtsinstanzen verwaltet werden, da es dort einen Verantwortlichen gibt, der auch die Löschungskompetenz übernehmen kann. Für public Blockchains ist diese Modifikation ungeeignet, da sie durch derartige Eingriffe in den meisten Fällen unglaubwürdig erscheinen und damit ihre Trust-Building Function verlieren würde. Es gibt zwar von den Entwicklern Überlegungen, wie man die Schlüssel unter den Nutzern verteilen könnte,[35] jedoch ist das in der Praxis wohl kaum anwendbar und würde auch dem Peer-to-Peer Prinzip widersprechen.

Im Zusammenhang mit Blockchains ist das Recht auf Löschung der eigenen (personenbezogenen) Daten des Nutzers grundsätzlich zu hinterfragen, da der Nutzer seine Daten in Kenntnis der Eigenschaften dieser Technologie bewusst veröffentlicht. Art 17 Abs 3 DSGVO zählt die Verwehrungsgründe der Löschung taxativ auf, eine Ausnahme in Bezug auf selbst veröffentlichte Informationen findet sich nicht. Die Ausnahme für „offensichtlich öffentlich gemachte" Daten in Art 9 DSGVO gilt nach einer systematischen Interpretation nur für sensible Daten: Die Verarbeitung von sensiblen Daten ist grundsätzlich ausgeschlossen, außer es liegt eine der in Absatz 2 taxativ aufgezählten Ausnahmen vor. Die Verarbeitungsvoraussetzungen des Artikel 6 für personenbezogene Daten bleiben auch bei sensiblen Daten anwendbar.[36] Durch das „offensichtlich öffentlich" Machen von sensiblen Daten unterliegen diese dann nur mehr den allgemeinen Voraussetzungen der DSGVO. Sensible Daten sind personenbezogene Daten aus denen sich sensible Informationen, wie beispielsweise die rassische oder ethnische Herkunft, die sexuelle Ausrichtung oder gesundheitsbezogene Informationen ableiten lassen (Artikel 9 DSGVO)[37]. Die Voraussetzungen für die Verarbeitung solcher Daten sind noch strenger. Daher wäre auch die Erwähnung einer gewissen Eigenverantwortung der betroffenen Personen in Bezug auf ihre eigenen personenbezogenen Daten in der Verordnung wahrscheinlich wünschenswert, da der Nutzer seine Informationen ja freiwillig und in Kenntnis der Charakteristika einer Blockchain preisgibt.

Die Unveränderbarkeit der Blockchain ist ihr größter USP und die Ursache für ihre vielfältigen Anwendungsfelder. Manche auf Blockchains basierende Geschäftsmodelle wie beispielsweise Kryptowährungen oder auf Smart Contracts basierende Transaktionen könnten ohne diese Eigenschaft nicht existieren. Die unveränderbare Speicherung der Originalblöcke und die daraus folgende immerwährende Nachvollziehbarkeit sind elementare Bestandteile der Wertschöpfung von standardisierten, selbstabwickelnden Verträgen. Ein Löschen einzelner Blöcke würde das ganze Modell so verändern, dass finanzielle Ansprüche nicht mehr nachvollziehbar wären bzw Forderungen vielfach nicht mehr gestellt werden könnten, und die Geltendmachung zukünftiger Rechtsansprüche nicht gesichert wäre. Wird ein konkretes, auf einer Blockchain programmiertes Angebot angenommen, kommt ein rechtsgültiger Vertrag zustande. Auf diese Weise könnten beispielsweise gewisse Tätigkeiten eines Notars ersetzt oder Immobilienkäufe und Mietverträge abgewickelt werden.

VI. Privacy by Design

Blockchain ist eine Technologie, die viele Branchen grundlegend verändern kann. Die Vorteile der Blockchain Technologie sind die dezentrale Speicherung (bessere Sicherheit vor Hackerangriffen als bei einer zentralen Datenbank) und die Unveränderbarkeit der einzelnen „Blöcke".[38] Somit ist eine transparente und lückenlos nachvollziehbare Dokumentation jedes Arbeitsschritts gewährleistet. Unternehmen müssen in Zukunft sehr genau unterscheiden, welche Art von Daten sie im Einzelfall verarbeiten. Während Blockchains für nichtpersonenbezogene Daten fast uneingeschränkte Einsatzmöglichkeiten bieten und noch enormes Entwicklungspotential in der Anwendung haben, ist die Situation für personenbezogenen Daten für den Einzelfall zu evaluieren. Eine Möglichkeit, dem Datenschutz gerecht zu werden, ist Privacy by Design. So wird die Softwarearchitektur im Zusammenhang mit der Blockchain Technologie auf den jeweiligen Anwendungsfall anzupassen sein. Das Spektrum reicht dabei von der public Blockchain, an welcher jeder Schreib- und Leserechte haben kann und den Source Code kennt bis zur privaten Redactable Blockchain mit sehr restriktiven Schreib- und Leserechten, die sich nur mehr wenig von einer zentralen Datenbank im herkömmlichen Sinne unterscheidet.[39] Für Unternehmen mit geschlossenen Blockchains gibt es eine Viel-

Datenschutzgrundverordnung (2017) und *Ateniese/Magri/Venturi/Andrade*, Redactable Blockchain (FN 2).

35 *Ateniese/Magri/Venturi/Andrade*, Redactable Blockchain (FN 2).

36 ErwGr 51 DSGVO.

37 Siehe auch ErwGr 51 DSGVO.

38 Siehe dazu jedoch oben die Überlegungen zu Blockchain Varianten, wie die redactable Blockchain.

39 *Catalini/Gans*, Blockchain (FN 5) und <https://www.youtube.com/watch?v=taG-1p-UNC0> (Stand 07.12.2018).

zahl von Möglichkeiten, diese Technologie DSGVO-konform zu verwenden, wenn ausreichend Kontrolle durch den Verantwortlichen gegeben ist. Vordringlich ist, sobald personenbezogene Daten verwendet werden, bei der Programmierung auf Löschbarkeit zu achten.

Besondere Vorteile in Bezug auf den Schutz personenbezogener Daten bieten editierbare (redactable) Varianten von permissioned Blockchains.[40] Während die Blockchain Technologie grundsätzlich darauf beruht, dass kein Hash (Zeichenfolge) mehr als einmal zugeordnet wird (Kollisionsfreiheit), ist es bei editierbaren Blockchains (durch die Programmierung von sogenannten Chameleon Hashes) möglich, den gleichen Hash für den selben Block mittels private Key öfter zu vergeben. Der alte Hash wird entsperrt und dann wieder durch dieselbe Zeichenfolge ersetzt.

Eine interessante Option bildet auch die Datenspeicherung und -verarbeitung außerhalb der Blockchain in einer Weise, dass die Sicherheit erhalten bleibt, die Daten und Prozesse jedoch löschbar und nicht öffentlich sichtbar sind.[41] Ein Speicherverfahren, das einen direkten Zugriff auf einzelne Objekte ermöglicht und gleichzeitig die Unveränderbarkeit der gespeicherten Information im Allgemeinen gewährleistet, ist Content Addressed Storage. Außerhalb der Blockchain gespeicherte Daten können dabei mittels Smart Contracts über in der Blockchain gespeicherte Referenzen aufgefunden werden.[42] Durch Delegated Computational Systems[43] ist es auch möglich, Verarbeitungsprozesse off-Blockchain so durchzuführen, dass die wesentlichen Blockchain Vorteile nicht verloren gehen, eine Löschbarkeit aber gegeben ist. Dabei werden mittels eines kryptographischen Zero-Knowledge Protokolls (zkSNARKs)[44] Inhalte und Verarbeitungen verifiziert, ohne dass sie tatsächlich bekannt sind. Inwieweit eine bestimmte Softwarearchitektur für einen speziellen Use Case sinnvoll ist, wird jeweils individuell unter Berücksichtigung von Best Practices zu entscheiden sein.

Ob diese Verfahren jedoch immer allen Ansprüchen in Bezug auf Datenschutz gerecht werden, ist nicht garantiert, da beispielsweise oft ein Personenbezug über Big Data hergestellt wird.[45]

VII. Fazit

Klar ist: Blockchain und DSGVO schließen einander keineswegs zwingend aus. Sie können zu einem friedlichen Miteinander finden, wenn man im jeweiligen Anwendungsfall unter sorgfältiger Beachtung rechtlicher Notwendigkeiten die passenden Rahmenbedingungen schafft. Man kann rechtliche Gestaltungsmöglichkeiten nutzen, um sich der Blockchain zu bedienen oder das System IT-seitig anpassen – die Blockchain-Technologie ist ja nicht in Stein gemeißelt. Letztlich gilt: It's all about design.

> DR. CHRISTIAN M. PISKA

Ao. Univ.-Prof. für öffentliches Recht am Juridicum Wien,
Schottenbastei 10-16, 1010 Wien.
E-Mail: christian.piska@univie.ac.at,
Web: staatsrecht.univie.ac.at.

> MAG. MARIE-CATHERINE WAGNER

Projektmitarbeiterin am Institut für Innovation und Digitalisierung im Recht an der Universität Wien,
Schenkenstraße 4, 1010 Wien.
E-Mail: marie-catherine.wagner@univie.ac.at,
Web: id.univie.ac.at.

40 Siehe dazu bereits oben.
41 *Eberhardt/Tai*, Blockchain (FN 11) 4.
42 *Eberhardt/Tai*, Blockchain (FN 11) 8.
43 *Eberhardt/Tai*, Blockchain (FN 11) 10.
44 *Wu/Zheng/Chiesa/Popa/Stoica*, A Distributed Zero-Knowledge Proof System (2018) 5.
45 *Martini/Weinzierl*, Die Blockchain-Technologie und das Recht auf Vergessenwerden (2017) 1252.