Rainer Böhme, Paulina Pesch

Technische Grundlagen und datenschutzrechtliche Fragen der Blockchain-Technologie

Die Blockchain-Technologie beflügelt derzeit wie kaum eine andere Phantasien von einer transparenteren Informationsgesellschaft. Ihr Verhältnis zum Datenschutz ist allerdings kompliziert. Der Beitrag skizziert die Grundzüge der Problematik.

1 Problemaufriss

Der Erfolg von Bitcoin lenkt zunehmend Aufmerksamkeit auf die dieser virtuellen Kryptowährung zugrunde liegenden Technologie.[1] Während ihre kryptographischen Komponenten als hinreichend verstanden erscheinen, ist deren Kombination zum Zweck der Integritätssicherung einer verteilten, öffentlichen Datenbank neu. Zwei wesentliche Eigenschaften dieses auch als *Distributed Ledger* (engl. für verteiltes Register) bezeichneten Datenbanktyps sind, dass erstens lediglich Einträge hinzugefügt und nicht mehr verändert oder gelöscht werden können und diese zweitens in einem Konsensmechanismus als gültig befunden werden. Bei den Einträgen handelt es sich in der Regel um strukturierte Daten, deren Gültigkeit sich formal beschreiben und mit Bezug auf alle bisherigen Einträge effizient feststellen lässt. Durch diesen Prozess entsteht eine öffentlich einsehbare Aufzeichnung aller historischen Einträge in einer zeitlichen Ordnung. Der Begriff Blockchain[2] beschreibt eine spezielle technische Realisierung der Integritätssicherung, bei der Einträge in Blöcke zusammengefasst und durch kryptographische Hash-Funktionen zu einer praktisch unveränderlichen Folge verkettet werden.[3] Die Datenstruktur einer typischen Blockchain ist im folgenden Abschnitt skizziert und erläutert.

Besonders im Finanzsektor[4] wird der Blockchain-Technologie ein transformatives Potenzial zugesprochen, welches sich aus Erwartungen an die folgenden Eigenschaften speist:[5]

- Nachträgliche Unveränderlichkeit von Daten (engl. *Immutability*)
- Kein Vertrauen in eine zentrale Partei (engl. *Trustlessness*[6])
- Widerstandsfähigkeit (engl. *Resilience*) durch Vermeidung von kritischen Einzelkomponenten (engl. *Single Points of Failure*)
- Transparenz

Gerade die in der Öffentlichkeit der Daten begründete Transparenz legt eine kritische Betrachtung der neuen Technologie aus dem Blickwinkel des Datenschutzes nahe. Schließlich lassen Finanzdaten Rückschlüsse auf Gewohnheiten und Lebensumstände von Personen zu. Mögliche Einsatzgebiete beschränken sich jedoch nicht auf den Finanzsektor, sondern umfassen eine Vielzahl von Anwendungen, bei denen nicht weniger aufschlussreiche Daten anfallen, so z. B. die Überwachung von Medienkon-

1 Zu Bitcoin allgemein siehe *Sorge/Krohn-Grimberghe*, DuD 2012, 479 ff.; *Zohar*, CACM 09/2015, 104 ff.; *Böhme/Christin/Edelman/Moore*, Journal of Economic Perspectives, Vol. 29 (2015), 213 ff.

Prof. Dr. Rainer Böhme

ist Inhaber des Lehrstuhls für Security and Privacy am Institut für Informatik der Universität Innsbruck. Forschungsschwerpunkte: Digitale Forensik, virtuelle Währungen, Privacy-enhancing technologies (PET), ökonomische Aspekte von Informationssicherheit und Privatheit, Cybercrime.
E-Mail: rainer.boehme@uibk.ac.at

Dr. Paulina Pesch

ist wissenschaftliche Mitarbeiterin des Zentrums für Angewandte Rechtswissenschaft (ZAR) am Karlsruher Institut für Technologie (KIT). Foschungsschwerpunkte: Dezentrale virtuelle Währungen, Internet- und IT-Recht.
E-Mail: paulina.pesch@kit.edu

2 Obwohl Blockchains nur eine Form der Realisierung eines Distributed Ledgers darstellen, wird der Begriff stellvertretend für die durch die Bitcoin-Blockchain inspirierte Technologie verwendet.

3 Alternative Datenstrukturen wurden vorgeschlagen, z. B. *Lewenberg/Sompolinsky/Zohar*, in: *Böhme/Okamoto*, Financial Cryptography and Data Security, 19th International Conference, FC 2015, S. 528 ff., und sind teilweise im Einsatz. Ihnen ist gemeinsam, dass eine zeitliche Ordnung der Einträge entsteht und alte Einträge nicht ohne erheblichen Aufwand verändert werden können.

4 *Pinna/Ruttenberg*, ECB Occasional Paper Series, No 172 / April 2016, abrufbar unter https://www.ecb.europa.eu/pub/pdf/scpops/ecbop172.en.pdf (letzter Abruf: 17.3.2017).

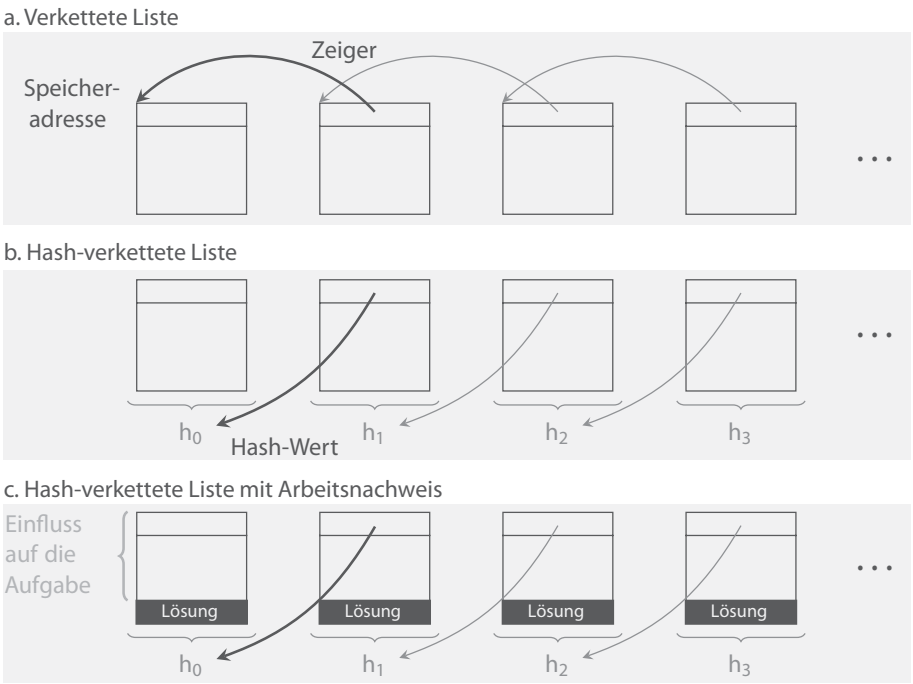
5 *Walch*, Open Source Operational Risk: Should Public Blockchains Serve as Financial Market Infrastructures?, Draft, S. 3 abrufbar unter https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2879239 (letzter Abruf: 17.3.2017).

6 Der englische Begriff ist dahingehend missverständlich, dass dennoch Vertrauen in das Verhalten einer abstrakten Nutzergemeinschaft sowie in die Gültigkeit von mathematischen und physikalischen Annahmen erforderlich ist.

sum[7], Telemetrie im Zusammenhang mit dem Internet der Dinge[8] oder eine Initiative der UNICEF, digitale Geburtsurkunden mithilfe der Blockchain-Technologie[9] zu realisieren. Wie diese Beispiele andeuten, ist das Thema Blockchain-Technologien gekennzeichnet durch sehr dynamische technische Fortschritte bei gleichzeitig unklaren Geschäftsmodellen sowie einer Vielzahl offener Rechtsfragen, die oft Rechtsgebiete und Rechtsräume übergreifen. Dies führt zu einem schwer systematisierbaren Geflecht aus Interessen und Informationen.

Ziel dieses Beitrags ist es, die namensgebende Datenstruktur (Abschnitt 2) und technische Architektur (Abschnitt 3) der Blockchain-Technologie verallgemeinernd vorzustellen, um darauf basierend grundsätzliche Fragen des Datenschutzrechts aufzuwerfen und soweit möglich zu beantworten (Abschnitt 4). Schließlich werden Lösungsansätze und sich ergebende Forschungsfragen skizziert (Abschnitt 5). Der Beitrag behandelt primär Blockchains mit öffentlichem Lesezugriff.[10] Auf private Blockchains, eine von der Blockchain-Technologie inspirierte Art der Integritätssicherung in Datenbanksystemen, wird nur eingegangen, wo sie sich in Funktionsweise und datenschutzrechtlicher Behandlung von herkömmlichen Datenbanksystemen unterscheiden.

Abb. 1 | Von der verketteten Liste zur Blockchain



2 Die authentifizierte Datenstruktur von Blockchains

Die als Blockchain bezeichnete authentifizierte Datenstruktur[11] lässt sich als Weiterentwicklung der verketten Liste betrachten. Abbildung 1 veranschaulicht die entscheidenden Ergänzungen.

Von einer (einfach) *verketteten Liste* spricht man, wenn jedes Listenelement einen Zeiger enthält, der die Adresse der ersten Speicherzelle des vorhergehenden Elements aufnimmt.[12] Diese Datenstruktur lässt sich sequenziell durchlaufen. Neue Elemente können ohne Änderung von bestehenden Elementen angehängt und durch Änderung *eines* Elements eingefügt bzw. gelöscht werden. Speicheradressen sind allerdings lokal und flüchtig. Sie müssen durch andere Kennungen ersetzt werden, wenn die verkettete Liste verteilt gespeichert oder verarbeitet werden soll.

Eine korrespondierende *authentifizierte Datenstruktur* erhält man, indem Zeiger durch Hash-Werte der vorhergehenden Elemente ersetzt werden. Hash-Werte sind eine Art Prüfsumme, in deren Berechnung alle in einem Element vorhandenen Daten eingehen. Bei der Verwendung von kryptographischen Hash-Funktionen sind Referenzen auf durch ihre Hash-Werte identifizierte Elemente mit überwältigend hoher Wahrscheinlichkeit eindeutig. Dies vereinfacht die Verteilung von Daten in Rechnernetzen, wo Zeiger mangels einheitlichen Adressraums ungeeignet sind.[13] Genau wie einfach-verkettete Listen können Hash-verkettete Listen ohne Änderung bestehender Elemente fortgeschrieben werden. Das Löschen, Einfügen und Ändern von Elementen erfordert jedoch eine Änderung *aller* nachfolgenden Elemente, denn die Referenz geht – anders als bei Zeigern – jeweils in die Berechnung des Hash-Werts ein. Somit pflanzt sich eine Modifikation bis zum letzten Element der Liste fort.

Im Prinzip lässt sich bei Hash-Verkettung eine Modifikation von Inhalten durch Vergleich des letzten Elements (bzw. dessen Hash-Werts) mit einem Vergleichswert – aus vertrauenswürdiger Quelle – erkennen. Allerdings kann in dezentralen Systemen nicht von der Existenz eines allgemein akzeptierten Vergleichswerts für das zu jedem Zeitpunkt letzte Element ausgegangen werden. Um die nachträgliche Modifikation großer Teile

7 Z. B. *Ascribe*, Homepage abrufbar unter https://www.ascribe.io (letzter Abruf: 17.3.2017).

8 *IBM Institute for Business Value* (2015), Empowering the edge: Practical insights on a decentralized Internet of Things, abrufbar unter http://www-935.ibm.com/services/multimedia/GBE03662USEN.pdf (letzter Abruf: 17.3.2017).

9 *UNICEF* (2016), UNICEF is funding blockchain and health tech to solve the world's biggest problems, abrufbar unter http://unicefstories.org/2016/11/15/unicef-is-funding-blockchain-and-health-tech-to-solve-the-worlds-biggest-problems/ (letzter Abruf: 17.3.2017).

10 Eine Differenzierung nach Schreibberechtigung („permissioned" vs „permissionless") wird in der Literatur vorgenommen, z. B. *European Securities and Markets Authority* (2017), The Distributed Ledger Technology Applied to Security Markets, Report ESMA50-1121423017-285, S. 4; *Mills* et al. (2016), Finance and Economics Discussion Series 2016-095, Board of the Governors of the Federal Reserve System, Washington, S. 12, hier aber nicht weiter vertieft.

11 Authentifizierte Datenstrukturen sind Gegenstand der Grundlagenforschung in der Informatik, vgl. z. B. *Tamassia,* in: Battista/Zwick, Algorithms – ESA 2003, S. 2 ff.; *Miller/Hicks/Katz/Shi* (2014), in: Proceedings of the ACM Conference on Principles of Programming Languages (POPL), S. 411 ff.

12 Statt auf Vorgänger zu verweisen, ist es auch möglich, Zeiger auf das nachfolgende Element zu verwenden. Die hier gewählte Konvention vereinfacht den Übergang zur Blockchain.

13 Vgl. *Balakrishnan/Kaashoek/Krager/Morris/Stoica*, CACM 2/2003, S. 43 ff.

der Datenstruktur für einen Angreifer impraktikabel aufwändig zu machen, kann als Konvention vereinbart werden, dass gültige Elemente die Lösung für eine algorithmisch schwierige, aber effizient überprüfbare Aufgabe enthalten müssen, deren genaue Aufgabenstellung (d. h. die Instanz des Problems) von allen anderen Daten in diesem Element abhängt. Dies schließt insbesondere den Hash-Wert des Vorgängers mit ein. Damit muss – stark vereinfacht – ein die Integrität kompromittierender Angreifer ähnlich viel Rechenleistung aufbringen, wie alle Verteidiger zusammen in die Erstellung der Datenstruktur investiert haben. Tatsächlich ist der Aufwand zur Änderung weit zurück liegender Elemente höher als kürzlich hinzugefügter. Deshalb hat sich bspw. bei Bitcoin die Konvention etabliert, sechs „Bestätigungen" (Elemente) abzuwarten, bevor eine Transaktion als endgültig angesehen wird.[14] Diese Datenstruktur kann als *Hash-verkettete Liste mit Arbeitsnachweis* bezeichnet werden und wird als Idealtyp für eine Blockchain verstanden. Listenelemente sind dabei Blöcke, die als Nutzdaten eine Liste von Einträgen (z. B. Transaktionen bei Bitcoin) enthalten.

3 Architekturprinzipien öffentlicher Blockchains

Zur Erklärung der Blockchain-Technologie bieten sich drei Wege an. Am ausführlichsten ist der Zugang über die Schichtarchitektur. Er setzt lediglich Informatik-Grundwissen und das Verständnis asymmetrischer Kryptographie voraus. Wer mit Netzwerkprotokollen vertraut ist, findet bei der Einordnung nach Dauerhaftigkeit des Zustands eine alternative Abgrenzung (Abschnitt 3.2). Leser, die Bitcoin kennen, haben den kürzesten Weg. Sie finden eine Verallgemeinerung in Abschnitt 3.3.

3.1 Zugang über die Schichtarchitektur

Ein allgemeiner Zugang zur Blockchain-Technologie beginnt mit der Vergegenwärtigung eines Grundprinzips der Informatik, in Schichten zu abstrahieren. Niedrige Schichten verstecken Details der Implementierung und damit Entwurfskomplexität vor höheren Schichten, denen sie wohldefinierte Funktionen über Schnittstellen anbieten. Abbildung 2 zeigt oben eine typische Schichtarchitektur eines Einzelplatzrechners. Die Lücke zwischen Anwendung und Betriebssystem füllt sich beim Übergang zu vernetzten Rechnern (Abb. 2 unten). Jeder Netzteilnehmer betreibt seinen eigenen Rechner, der alle Schichten implementiert und für Anwendungen (z. B. Webbrowser) das Internet als eine gemeinsame Kommunikationsplattform bereitstellt[15], über die Daten (z. B. Inhalte) ausgetauscht werden können. In der Regel besteht eine Zuordnung zwischen einem physischen Endgerät und seinem Besitzer, dessen Identität durch Teilnehmerkennungen (Benutzername, IP-Adresse) technisch definiert ist. Jedes Endgerät verfügt über einen lokalen Zustand, den es nach eigenen Regeln unter Berücksichtigung der Eingaben des Teilnehmers und der vom Netz empfangenen Nachrichten fortschreibt. Teilnehmer A hat keine wirksame Möglichkeit, den Zustand eines sicheren Endgeräts von Teilnehmer B gegen dessen Willen zu beeinflussen.[16]

Zur Realisierung von dezentralen virtuellen Währungen ist diese Architektur nicht ausreichend, denn es gibt keinerlei Vorkehrungen, die einen konsistenten gemeinsamen Zustand zwischen allen Teilnehmern sichern. Dieser ist aber gerade notwendig, wenn es um die Verwaltung und Zuteilung von virtuellem Vermögen geht. Das Problem ließe sich umgehen, wenn alle Teilnehmer einem herausgehobenen Teilnehmer vertrauen und ihm die Verwaltung alleine überließen. Eine solche Rolle nehmen E-Geld-Institute nach 2000/46/EG ein. Sie stellen aber zentrale Parteien dar, die bei der Blockchain-Technologie vermieden werden sollen.

Abb. 2 | Schichtarchitekturen eines typischen Einplatz-Rechners (oben) und von Internet-Rechnern (unten)

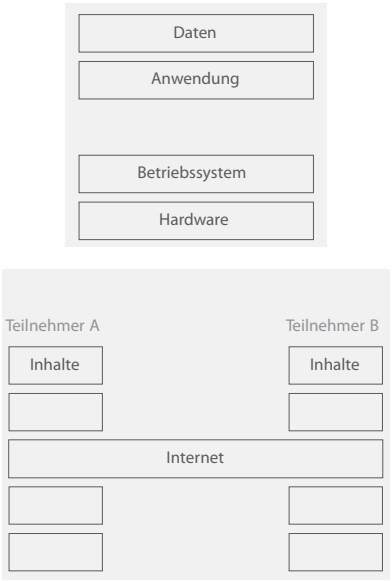


Abbildung 3 erweitert die Schichtarchitektur der Internet-Rechner zur Blockchain-Technologie. Gemeinsame Basis ist das Internet als weltweites Kommunikationsmedium. Neu und charakteristisch für die Blockchain-Technologie ist, dass alle höheren Schichten keinen direkten Bezug zum lokalen Endgerät haben. Die Technologie folgt vielmehr der Philosophie von *Peer-to-Peer*-Netzen, bei denen – im Folgenden als Knoten bezeichnete – Endgeräte zur Laufzeit beliebig dem Netzwerk beitreten und es wieder verlassen können.

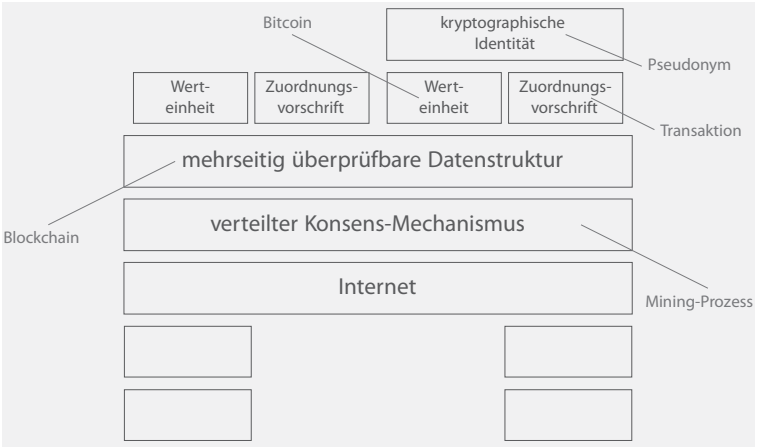
Auf der Anwendungsschicht läuft ein verteilter *Konsens-Mechanismus*, dessen Aufgabe es ist, die darüber liegende „Datenschicht" stets konsistent auf allen Knoten fortzuschreiben. Eventuell auftretende Konflikte, die durch Laufzeitunterschiede und damit verbundenen unterschiedlichen Sichten unvermeidbar sind, werden korrigiert und bleiben somit stets temporär. Eine darüber hinaus gehende Anforderung an den Konsens-Mechanismus ist seine Widerstandsfähigkeit gegen gezielte Manipulationen, die auch Angriffsszenarien vieler koordinierter Kno-

14 Bitcoin verwendet – wie die meisten Blockchain-Systeme – einen Regelkreis, der die Schwierigkeit der Aufgabe an die im Netz zur Verfügung stehende Rechenleistung anpasst. Damit kann Bitcoin die Blockrate bei durchschnittlich einem Block pro zehn Minuten stabil halten.

15 Diese vereinfachte Darstellung unterscheidet nicht zwischen Client und Server. Die Unterscheidung dieser Rollen ist bei typischer Internet-Nutzung sehr präsent.

16 Das DRM-Problem ist eine Ausprägung dieser generellen Schwierigkeit. Trusted Computing zielt darauf ab, dieses Problem durch den Einsatz von vertrauenswürdiger Hardware und Kryptographie zu lösen, siehe dazu *Böhme/Pfitzmann*, DuD 2008, 342 ff.

Abb. 3 | Schichtarchitektur der Blockchain-Technologie (mit Beispielen aus dem Bitcoin-System).



ten enthalten.[17] Der so genannte Mining-Prozess beim Hinzufügen neuer Blöcke zur Bitcoin-Blockchain löst dieses Problem mit der Suche nach Lösungen zu kryptographischen Puzzles. Die stochastische Zeitdauer zur Lösung kann als Mechanismus zur Stauauflösung betrachtet werden, ähnlich der Kollisionsauflösung im Ethernet, aber in einer strategiesicheren Variante: Endgeräte können die Zeit nicht eigenmächtig verkürzen. Dies folgt der Annahme, dass die verfügbare Rechenkapazität unter allen Teilnehmern gleichmäßiger verteilt ist als die Möglichkeit, Knoten hinzuzufügen (z. B. durch Virtualisierung). Inwieweit diese Annahme zutrifft, hängt maßgeblich von der Gestaltung der Puzzles ab. Neuere Blockchains verwenden in diesem Sinne „demokratischere" Aufgaben als die bei Bitcoin eingesetzte partielle Invertierung der SHA-256-Funktion.

Der Konsens-Mechanismus stellt eine alle Knoten umspannende (und in der Regel redundant gespeicherte) *mehrseitig überprüfbare Datenstruktur* bereit, welche die Schicht der Daten bzw. Inhalte in Abbildung 2 ersetzt. Mehrseitige Überprüfbarkeit bezieht sich dabei auf den Inhalt aller in der Regel zeitlich geordneten und im Klartext vorliegenden[18] Einträge, die sich von jedem Teilnehmer zu jedem Zeitpunkt auf ihre Vollständigkeit und formale Korrektheit überprüfen lassen. Die formale Korrektheit kann sich dabei stets nur auf Bezüge innerhalb dieser Datenstruktur beziehen. Ob die Daten valide sind, also Tatsachen außerhalb des Systems korrekt wiedergeben, erfordert lokales Zusatzwissen und ist daher nicht von jedem Knoten entscheidbar. In aller Regel ergibt sich die Korrektheit der Datenstruktur aus der Gültigkeit aller ihrer Einträge[19]. Dies zu fordern würde aber die Allgemeinheit unnötig einschränken. Eine Besonderheit dieser Datenstruktur ist ihre variable Persistenz. Zu jedem Zeitpunkt sind unterschiedliche Einträge unterschiedlich dauerhaft, wobei typischerweise die Wahrscheinlichkeit einer zukünftigen Änderung exponentiell mit dem Alter eines Eintrags abnimmt. Diese Eigenschaft folgt aus dem Konsens-Mechanismus, der lediglich probabilistische Konsistenz herstellt.[20]

Selbstverständlich können Knoten lokal persistente Kopien von temporären Zuständen der Datenstruktur erstellen. Diese finden sich allerdings nicht in dem von allen Knoten als verbindlich zu betrachtenden *gemeinsamen Zustand* wieder (vgl. Zugang über den Gültigkeitsbereich des Zustands in Abschnitt 3.2). Wegen des gemeinsamen Zustands kann ein Blockchain-System als eine einzige verteilte virtuelle Maschine begriffen werden, deren Ablauf jeder einzelne Knoten nur beeinflussen kann, indem er die Datenstruktur um gültige Einträge ergänzt. Zur Realisation der mehrseitig überprüfbaren Datenstruktur kommt oft eine Form der in Abschnitt 2 erklärten Hash-verketten Liste mit Arbeitsnachweis (kurz: Blockchain i.e.S.) zum Einsatz.

Den meisten Blockchain-Systemen ist gemeinsam, dass sie über der Datenschicht Informationen definieren, die man allgemein in *Werteinheiten* und *Zuordnungsvorschriften* unterteilen kann. Werteinheiten sind virtuelle Gutschriften, die im formal vorgegebenen Rahmen innerhalb des Netzes eingesetzt werden können und in der Regel von allen akzeptiert werden. Zwar ergeben sich hieraus allein keine Rechte, aber fast immer gibt es Märkte, auf denen diese Werteinheiten gegen andere Leistungen oder Geld getauscht werden können. Werteinheiten liegen meist nicht explizit in der Datenstruktur vor, sondern werden durch Zuordnungsvorschriften implizit definiert. Zuordnungsvorschriften sind in der Datenstruktur abgelegte formale Regeln, die festlegen, wie Werteinheiten übertragen werden können.[21] Auf diesem Weg können Guthaben an Werteinheiten abgebildet werden: Eine Zuordnungsvorschrift, die die Weitergabe einer Werteinheit ausschließlich an den Nachweis der Kenntnis eines zu einem öffentlichen Schlüssel gehörenden privaten Schlüssels fordert, gibt dem Inhaber des privaten Schlüssels[22] Verfügungsgewalt über diese Einheit. Sie „gehört" damit der *kryptographischen Identität* des betreffenden Schlüsselpaars und in aller Regel dessen Erzeuger. Da Schlüsselpaare in beliebiger Anzahl erzeugt werden können, fungieren sie als Pseudonyme, unter denen Personen im Blockchain-System auftreten.

Abbildung 3 und der Zugang über die Schichtarchitektur veranschaulichen, dass die Blockchain-Technologie virtuelle Parteien in Form von kryptographischen Identitäten von realen Parteien, d. h. von Besitzern oder Betreibern der Knoten sowie der sie verbindenden Netze, trennt. Sowohl Knoten als auch Pseudonyme sind schwache Identitäten. Sie können in nahezu beliebiger Anzahl erzeugt werden und das System zu gewählten Zeitpunkten betreten sowie weitgehend konsequenzlos wieder verlassen. Eine ökonomische Folge ist, dass diese Parteien keine Schulden machen oder negative Reputation erlangen können.[23] Deshalb gibt es in den meisten virtuellen Währungen nur Guthaben. Systeme, die kompliziertere Transaktionen zulassen wollen, müssen mit dieser Unvollständigkeit des Marktes leben oder auf anderem Wege eine nachhaltige Identifizierung von Parteien rea-

17 Vgl. *Douceur* (2002), The Sybil Attack, abrufbar unter https://www.freehaven.net/anonbib/cache/sybil.pdf (letzter Abruf: 17.3.2017).

18 Abschnitt 5.1 geht auf die Möglichkeit einer (Teil-)Verschlüsselung ein.

19 Bei Bitcoin werden Einträge als Transaktionen bezeichnet.

20 Vgl. *Wattenhofer*, The Science of the Blockchain (2016), S. 77 ff.

21 Unterschiedliche Blockchain-Systeme verwenden verschieden mächtige formale Sprachen zur Formulierung dieser Regeln. Bitcoin verfolgt bspw. eine eher vorsichtige Strategie während Ethereum eine Turing-vollständigen Sprache verspricht. Der Begriff *Smart Contract* hat sich für Zuordnungsvorschriften eingebürgert, deren Logik mehr als eine Bedingung evaluiert. Es handelt sich damit um spezielle Computerprogramme. Eine Assoziation mit Verträgen im rechtlichen Sinne ist irreführend, auch wenn den Zuordnungen vertragliche Regelungen zugrunde liegen können.

22 Jedem, der den privaten Schlüssel kennt.

23 Vgl. *Friedman/Resnick*, Journal of Economics & Management Strategy, Vol. 10 (2001), 173 ff.

lisieren. Dies bricht allerdings oft mit dem Ziel einer vollständigen Dezentralität.

3.2 Zugang über den Gültigkeitsbereich des Zustands

Für Netzwerk-Protokolle hat sich die Unterscheidung zwischen zustandslos (engl. *stateless*, z. B. bei HTTP oder der REST-Schnittstelle) und zustandsbehaftet (engl. *stateful*, z. B. durch Sitzungskennungen) etabliert. Der Zustand bezieht sich hierbei lediglich auf eine Instanz einer Kommunikationsbeziehung. Jede Instanz eines Protokollablaufs kann im Prinzip einen eigenen Zustand (*stateful*) oder bewusst keinen (*stateless*) einnehmen.

Diese Terminologie lässt sich erweitern, sodass ein Übergang zur Blockchain-Technologie entsteht. Statt jeder Instanz in ihrer Kommunikationsbeziehung „lokal" einen eigenen Zustand zu geben, bietet sich die Annahme eines gemeinsamen, globalen Zustands aller Teilnehmer an.[24] Dieser muss zunächst nicht vollständig öffentlich sein, sondern jeder Teilnehmer kennt eine definierte Projektion des globalen Zustandsraums. Die Sicht der einzelnen Teilnehmer ist auch nicht immer konsistent, denn der Zustand wird durch „lokale" Protokollläufe aktualisiert. Beispiel hierfür wäre die Weitergabe von digitalen Zertifikaten, die den Empfängern Kenntnis über die Beziehung von kryptographischen Schlüsseln und natürlichen oder juristischen Personen verschafft. Auch elektronische Zahlungssysteme, die auf der Weitergabe von kryptographischen Münzen[25] basieren, schreiben einen globalen Zustand (das Guthaben aller Beteiligten) fort, ohne dass jedem Einzelnen alle Guthaben bekannt sind. Trotzdem können Regelverletzungen (z. B. *Double Spending*) erkannt und sanktioniert werden.[26]

Bei der Blockchain-Technologie ist der globale Zustand bewusst öffentlich. Er wird in einer mehrseitig überprüfbaren Datenstruktur (siehe Abschnitt 2) abgelegt und unter Wahrung der im Protokoll definierten formalen Korrektheit durch Hinzufügen von Eingaben der Teilnehmer aktualisiert. Dies geschieht durch ein Mehrparteien-Protokoll, welches die Herstellung von Konsistenz unterstützt. Dieses Protokoll läuft in genau einer maßgeblichen Instanz.[27] Es realisiert ab dem Zeitpunkt der Initialisierung ohne Unterbrechung einen gemeinsamen, verteilten Zustandsautomat.

Um die Langlebigkeit zu sichern, ist das Protokoll so angelegt, dass es nicht von einzelnen Teilnehmern abhängt. Vielmehr können Teilnehmer jederzeit beitreten oder austreten. Weil ohne starke Identitäten Mehrfachteilnahme nicht effektiv ausgeschlossen werden kann, sind einzelne Teilnehmer für den Protokollverlauf nahezu bedeutungslos. Parteien treten stattdessen mit kryptographischen Identitäten (i.d.R. öffentliche Schlüssel) auf, die sich aus den in der Datenstruktur abgelegten Einträgen definieren.

3.3 Zugang über die Verallgemeinerung von Bitcoin

Bitcoin hat die Blockchain-Technologie eingeführt und populär gemacht. Grundsätzlich gibt es zwei Wege, die Technologie für andere Anwendungsgebiete als die Zahlungsabwicklung in einer virtuellen Kryptowährung zu öffnen.

Einerseits kann das Transaktionsformat und die darin verwendete Skriptsprache an neue Anwendungen angepasst werden. Dies impliziert eine Veränderung der im Programmcode festgelegten Regeln zur Überprüfung der Gültigkeit einer Transaktion. Auf diesem Weg entsteht eine spezielle Blockchain für die gewählte Anwendung. Da diese weitgehend unabhängig[28] von Bitcoin betrieben wird, können auch Parameter des Mining-Prozesses wie die Blockrate, Blockgröße oder die Wahl des Arbeitsnachweises modifiziert werden. Namecoin, ein dezentrales System zur Verwaltung von Namensräumen, ist ein Beispiel für so eine domänenspezifische Blockchain.

Andererseits können das Transaktionsformat und die Skriptsprache von Bitcoin so verallgemeinert werden, dass eine Plattform für verschiedene Anwendungen entsteht. Dies bedeutet regelmäßig die Aufgabe der Zerlegung von Zahlbeträgen in Inputs und Outputs, welche ermöglicht, dass die Beträge und Empfängeradressen zur Laufzeit – unter Wahrung der buchhalterischen Korrektheit – verändert werden können. Ethereum, eine Turingvollständige dezentrale virtuelle Maschine, ist ein Beispiel für so eine Plattform.

Im Prinzip lassen sich auf beiden Wegen Systeme entwerfen, die mit der ursprünglichen Anwendung der Zahlungsabwicklung nichts mehr zu tun haben. Allerdings ist es unwahrscheinlich, dass derartige Systeme dezentral fortbestehen können, ohne dass es irgendeine Art übertragbarer Werteinheit gibt.[29] Werteinheiten sind notwendig, um Anreize zum Fortschreiben der Blockchain zu setzen sowie den Schreibzugriff auf diese knappe Ressource zu rationieren.[30] Ohne Anreize zum Fortschreiben müsste eine Partei dies aus originär eigenem Interesse (oder Altruismus) tun. Das System wäre nicht mehr dezentral.[31] Ohne Rationierung müsste der Zugriff extern geregelt werden. Das System wäre nicht mehr offen, sondern eine „*permissioned*" Blockchain, die abhängig von der Verteilung der Berechtigungen möglicherweise nicht mehr dezentral kontrolliert würde.

4 Datenschutzrechtliche Fragestellungen

Blockchain-Systeme sind einerseits in besonderem Maße transparent, andererseits wird die Identität der Parteien durch Kryptographie verschleiert. Während die Nutzung herkömmlicher

24 Der globale Zustandsraum ist nicht das Kreuzprodukt aller lokalen Zustände, denn zwei Instanzen eines Protokolls zwischen den gleichen Kommunikationspartnern können bei globaler Betrachtung keinen unterschiedlichen Zustand einnehmen.

25 Vgl. *Chaum*, CACM, 10/1985, 1030 ff.

26 Die Erkennung erfordert i.d.R. zentrale Parteien, die Sanktionierung starke Identitäten.

27 Für Testzwecke steht bei vielen Systemen eine zweite, nicht als verbindlich angesehene Instanz zur Verfügung.

28 Es kann sinnvoll sein, eine einseitige Abhängigkeit von populäreren Blockchains zu erhalten: Techniken wie Side Chains und Merged Mining bieten Effizienz- und Sicherheitsgewinne.

29 Vgl. *Böhme*, Internet Protocol Adoption: Learning from Bitcoin, IAB Workshop on Internet Technology Adoption and Transition (ITAT) 2013, abrufbar unter https://www.iab.org/wp-content/IAB-uploads/2013/06/itat-2013_submission_17.pdf (letzter Abruf: 17.3.2017).

30 Vgl. *Möser/Böhme*, in: *Brenner/Christin/Johnson/Rohloff*, Financial Cryptography and Data Security (FC 2015), International Workshops, BITCOIN, Puerto Rico, S. 19 ff.

31 Aber ggf. trotzdem mehrseitig überprüfbar, vgl. *Danezis/Meiklejohn*, Network and Distributed System Security Symposium (NDSS) 2016, abrufbar unter http://www0.cs.ucl.ac.uk/staff/G.Danezis/papers/ndss16currencies.pdf (letzter Abruf: 17.3.2017).

Datenverarbeitungssysteme das Vertrauen in deren Anbieter erfordert und regelmäßig mit dem Risiko einer ungewollten Veröffentlichung von Daten verbunden ist, unterliegen Blockchain-Daten dezentraler Kontrolle und sind öffentlich zugänglich. Dementsprechend wirft die Blockchain-Technologie spezifische datenschutzrechtliche Fragen auf, die der vorliegende Beitrag skizziert. Der Fokus des Beitrags liegt auf den Daten, die in Blockchains gespeichert sind. Darüber hinaus entstehen in Blockchain-Systemen Verkehrsdaten der Netzkommunikation, die ebenfalls beobachtet und gespeichert werden können.[32] Um Blockchain-Systeme haben sich Ökosysteme von Intermediären gebildet, die solchen Nutzern Zugang verschaffen, die selbst nicht unmittelbar an den dezentralen Netzen teilnehmen.[33] Im Zusammenhang mit der Nutzung solcher Intermediäre fallen Daten an, die nur insofern Berücksichtigung finden, als sie sich auf die Blockchain beziehen.

4.1 Anwendbarkeit datenschutzrechtlicher Regelungen

Vorab stellt sich die Frage, ob datenschutzrechtliche Regelungen – und wenn ja, welche – Anwendung auf die Verarbeitung von Blockchain-Daten finden.

Sachliche Anwendbarkeit: Personenbeziehbarkeit
Das Datenschutzrecht betrifft nur die Verarbeitung personenbezogener Daten, § 1 Abs. 1 BDSG, Art. 1 Abs. 1 EU-Datenschutzrichtlinie[34] (im Folgenden: DS-RL), Art. 1 Abs. 1 Datenschutzgrundverordnung[35] (im Folgenden: DS-GVO). Dabei handelt es sich gemäß der einfachgesetzlichen Definition aus § 3 Abs. 1 BDSG um Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person.[36]

Blockchain-Daten, insb. die kryptographischen Identitäten, lassen sich potenziell auf natürliche Personen beziehen. Art. 2 lit. a Hs. 2 DS-RL und ebenso Art. 4 Nr. 1 Hs. 2 DS-GVO stellen klar, dass es einer direkten Identifizierbarkeit nicht bedarf.[37] Es kommt darauf an, ob aus Sicht des für die Datenverarbeitung Verantwortlichen die Identifizierung des Betroffenen mit Mitteln erreicht werden kann, die vernünftigerweise eingesetzt werden könnten, vgl. jeweils Erwägungsgrund 26 der DS-RL und der DS-GVO. Diese schließen Verknüpfungen mit Zusatzinformationen und die Hilfe Dritter ein.[38] Werden Blockchain-Daten verarbeitet, kommt es daher im Einzelfall darauf an, ob dem Verantwortlichen Möglichkeiten zur Erlangung der zur Identifizierung nötigen Zusatzinformationen eröffnet sind. Lässt sich die kryptographische Identität einer natürlichen Person mit öffentlichen Zusatzinformationen direkt zuordnen, kann von Personenbeziehbarkeit für jedermann – sowohl für die Teilnehmer des dezentralen Netzwerks als auch für Dritte – ausgegangen werden. Hieraus kann sich die Personenbeziehbarkeit weiterer kryptographischer Identitäten ergeben, insbesondere, wenn diese auf Grundlage spezieller Heuristiken[39] mit hoher Wahrscheinlichkeit derselben natürlichen Person zugeordnet werden können.

Anwendbares Datenschutzrecht
Angesichts der globalen Verteilung der Netzwerke weisen Blockchain-Anwendungen stets einen grenzüberschreitenden Bezug auf. Deshalb stellt sich die Frage, welche datenschutzrechtlichen Regelungen zur Anwendung kommen. Im Grundsatz gilt im deutschen Datenschutzrecht das Territorialitätsprinzip, demzufolge das Recht des Ortes anzuwenden ist, an dem die Daten erhoben, genutzt und verarbeitet werden,[40] vgl. § 1 Abs. 5 Satz 2 BDSG. Davon abweichend bestimmt § 1 Abs. 5 Satz 1 BDSG im Einklang mit Art. 4 Abs. 1 DS-RL, dass das BDSG keine Anwendung findet, wenn die verantwortliche Stelle ihren Sitz in einem anderen EU-Mitgliedstaat oder Vertragsstaat der EWR hat und nicht in Deutschland niedergelassen ist (Niederlassungsprinzip).[41] Das anwendbare Recht hängt also maßgeblich davon ab, wer als verantwortliche Stelle anzusehen ist.

Verantwortliche Stelle
§ 3 Abs. 7 BDSG definiert den Verantwortlichen als die Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.[42] Den Regelungen liegt die Vorstellung zugrunde, dass für jede Verarbeitung personenbezogener Daten mindestens eine Person oder Stelle ist verantwortlich ist.[43] Das Absenden eigener Daten an einen Blockchain-Knoten durch den Betroffenen selbst – mit dem Ziel, bspw. die Zuordnung von Werteinheiten, die einer eigenen kryptographischen Identität zugeordnet sind, zu ändern – liegt im eigenen Verantwortungsbereich. Die Knoten, die Daten an andere Knoten übermitteln und in die mehrseitig überprüfbare Datenstruktur eintragen, verarbeiten Daten i.S.v. § 3 Abs. 4 BDSG. Die Knoten sind allerdings nicht ohne weiteres lokalisier- und identifizierbar. Jeden Vorgang im dezentralen Netzwerk datenschutzrechtlich zu erfassen, erscheint insofern

32 Die Verkehrsdaten sind damit forensischer Aufklärung regelmäßig zugänglich. Zur Erhebung und Verarbeitung der Daten in der Blockchain *Pesch/Böhme*, DuD 2017, 93, 95 f.

33 *Pesch/Böhme*, DuD 2017, 93, 94.

34 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

35 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, gem. ihrem Art. 99 Abs. 2 anzuwenden ab Mai 2018.

36 Die Definition entspricht inhaltlich der in Art. 2 lit. a DS-RL. Der im Wortlaut von der DS-RL geringfügig abweichende Art. 4 Nr. 1 Hs. 1 DS-GVO geht nicht mit einer inhaltlichen Änderung des Begriffs einher, *Ernst*, in: Paal/Pauly, DS-GVO (1. Aufl. 2017), Art. 4, Rn. 3; *Kühling/Klar*, Anm. zu EuGH, Urt. v. 19.10,2016 – C-582/14, ZD 2017, 27, 28; *Richter*, Anm. zu EuGH, Urt. v. 19.10.2016 – C-582/14, EuZW 2016, 912, 913; *Mantz/Spittka*, Anm. zu EuGH, Urt. v. 19.10.2016 – C-582/14, NJW 2016, 3579, 3583.

37 Zu Art. 2 lit. a Hs. 2 DS-RL *EuGH*, Urt v. 19.10.2016 – C-582/14, Rn. 41, NJW 2016, 3582, 3581 = ZD 2017, 24, 25. Zur Personenbeziehbarkeit von Blockchain-Daten schon *Spindler/Bille*, WM 2004, 1357, 1368.

38 Näher dazu *EuGH*, Urt v. 19.10.2016 – C-582/14, Rn. 42 ff., NJW 2016, 3579, 3581 = ZD 2017, 24, 25 f.

39 Für Bitcoin vgl. *Meiklejohn/Pomarole/Jordan/Levchenko/McCoy/Voelker/Savage*, in: IMC '13 Proceedings of the 13th ACM IInternet Measurement Conference, 127 ff.; *Reid/Harrigan*, in: Altshuler/Elovici/Cremers/Aharony/Pentland, Security and Privacy in Social Networks (2013), S. 197 ff.

40 *Grapentin*, in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 2. Aufl. 2016, § 35, Rn. 20; *Simitis*, in: Simitis, BDSG, 8. Aufl. 2014, § 1, Rn. 8 ff.

41 Die DS-GVO erweitert den europäischen Datenschutz über das in Art. 3 Abs. 1 DS-GVO statuierte Niederlassungsprinzip hinaus um das Marktortprinzip, dazu (skeptisch) *Ernst*, in: Paal/Pauly, Datenschutz-Grundverordnung (1. Aufl. 2017), Art. 3, Rn. 13 f.

42 Die Vorschrift setzt Art. 2 lit. d DS-RL um, dem Art. 4 Nr. 7 DS-GVO entspricht.

43 *Dammann*, in: Simitis, BDSG, 8. Aufl. 2014, § 3, Rn. 224, 2. Vgl. auch Erwägungsgrd. 79 DS-GVO, demzufolge es einer klaren Zuteilung der Verantwortlichkeit bedürfe.

nicht zielführend, als der Einfluss einzelner, ggfs. identifizierbarer Knoten im dezentralen System so gering ist, dass ihre datenschutzrechtliche Inanspruchnahme keinen Erfolg verspricht.[44]

Das Konzept der DS-RL und des BDSG von der verantwortlichen Stelle wird im Kontext komplexer Datenverarbeitungssysteme zurecht kritisiert.[45] Die DS-GVO enthält mit Art. 26 zwar eine Regelung für gemeinsam Verantwortliche, schon die Anwendbarkeit der Vorschrift auf Blockchains ist aber zweifelhaft. Gem. Art. 26 Abs. 1 Satz 1 DS-GVO geht es um Personenmehrheiten, die Zwecke und Mittel der Verarbeitung gemeinsam festlegen.[46] Bei Blockchains steht es jedermann frei, das Ob und Wie der Teilnahme am System zu bestimmen. Welche Regeln gelten, ergibt sich nicht aus einer Einigung der Knoten, sondern letztlich bloß aus der Summe ihres unabhängigen Verhaltens. Selbst wenn man die Anwendbarkeit der Vorschrift bejaht, ließen sich in den dezentralen, pseudonymen Netzen weder der Abschluss einer gemeinsamen Datenschutzvereinbarung (Art. 26, Abs. 1, 2 DS-GVO) noch Betroffenenrechte gegenüber einzelnen Knoten (Art. 26, Abs. 3 DS-GVO) durchsetzen.

Die weiteren Ausführungen setzen bei vor- und nachgelagerten Vorgängen an: Einerseits können bestimmte Intermediäre Nutzern, die selbst nicht am verteilten System teilnehmen, Zugang verschaffen, etwa über kryptographische Identitäten des Intermediärs. Andererseits werden vielfach Daten aus existierenden Blockchains erhoben und verarbeitet. Zum Beispiel haben sich um das Bitcoin-System viele Intermediäre gebildet, die Blockchain-Daten aufbereiten[47] oder analysieren[48].

4.2 Anwendung zentraler Datenschutzgrundsätze

Soweit personenbezogene Daten Dritter an das dezentrale System übertragen oder Daten aus der Blockchain erhoben und verarbeitet werden, müssen diese Vorgänge datenschutzrechtlichen Vorgaben genügen.

Einwilligung, gesetzliche Erlaubnis und Zweckbindung

Das Datenschutzrecht sieht ein Verbot mit Erlaubnisvorbehalt vor: § 4 Abs. 1 BDSG bestimmt, dass die Erhebung, Verarbeitung und Nutzung personenbezogener Daten grundsätzlich verboten ist, es sei denn, eine Rechtsvorschrift gestattet dies[49] oder der Betroffene hat eingewilligt.[50] § 4a BDSG konkretisiert die Anforderungen an die Einwilligung. Insbesondere muss die Einwilligung gemäß § 4a Abs. 1 BDSG auf der freien Entscheidung des Betroffenen beruhen (Satz 1) und dieser auf den Zweck der Datenverarbeitung hingewiesen werden (Satz 2). Eine wirksame Einwilligung bedarf hinreichender Bestimmtheit der betroffenen Daten und der Bedingungen ihrer Verarbeitung.[51] Dem Betroffenen steht ein Recht zum Widerruf einer einmal erteilten Einwilligung zu, auf das nicht wirksam verzichtet werden kann.[52]

Fraglich ist, ob und inwieweit die Nutzer von Blockchain-Systemen in die Verarbeitung ihrer personenbezogenen Daten einwilligen. Selbst wenn man eine konkludente[53] Einwilligung in die Verbreitung und Verarbeitung der Daten in der Blockchain durch die Knoten[54] bejaht, lässt sich dem jedenfalls keine weitergehende Einwilligung auch in die Erhebung und Verarbeitung von Daten aus der Blockchain durch Dritte zu beliebigen Zwecken entnehmen. Die Zulässigkeit der Datenerhebung und -verarbeitung hängt damit von einem gesetzlichen Erlaubnistatbestand ab.

Das BDSG gestattet sowohl öffentlichen als auch nicht-öffentlichen Stellen unter bestimmten Voraussetzungen die Erhebung und Verarbeitung personenbezogener Daten.[55] § 28 Abs. 1 Satz 1 BDSG erlaubt nicht-öffentlichen Stellen das Erheben personenbezogener Daten zur Erfüllung eigener Geschäftszwecke, wenn ergänzend eine der Bedingungen der Nr. 1-3 erfüllt ist. Für Blockchain-Daten kann zunächst Nr. 1 Var. 2[56] einschlägig sein, wenn die Datenverarbeitung für die Durchführung eines rechtsgeschäftlichen Schuldverhältnisses erforderlich ist.[57] Dies wäre etwa der Fall, wenn der Verantwortliche einem Betroffenen zugeordnete Werteinheiten auf dessen Veranlassung einer Risikobewertung unterzieht.[58] Fraglich bleibt aber die Rechtfertigung der mit der Datenverarbeitung – wegen der Verweise in der Blockchain – zwangsläufig einhergehenden Verarbeitung der Daten Dritter, weil aus der Blockchain die zugrunde liegenden Rechtsbeziehungen nicht hervorgehen.[59]

Abseits von § 28 Abs. 1 Satz 1 Nr. 1 BDSG kann die Verarbeitung von Blockchain-Daten insbesondere durch § 28 Abs. 1 Satz 1 Nr. 3 Var. 1 BDSG gerechtfertigt sein, weil diese über das Internet durch jedermann abrufbar und damit allgemein zugänglich[60] sind, es sei denn, das schutzwürdige Interesse des Betroffenen überwiegt offensichtlich.

44 Dies gilt nicht für „permissioned" Blockchains, bei denen einzelne Knoten durch ihre Schreibberechtigung in einer herausgehobenen Position stehen.

45 *Dammann*, in: Simitis, BDSG, 8. Aufl. 2014, § 3, Rn. 2.

46 Zur Auslegung *Martiny*, in: Paal/Pauly, Datenschutz-Grundverordnung (1. Aufl. 2017), Art. 26, Rn. 19 ff.

47 Z. B. Blockchain.info, Homepage abrufbar unter https://blockchain.info/ (letzter Abruf: 17.3.2017). Vgl. zum automatischen Indexieren, Speichern und Zurverfügungstellen von Internetinhalten durch Suchmaschinen *EuGH*, Urt. v. 13.5.2014 – C-131/12, Rn. 25 ff., NJW 2014, 2257, 22258 f. = ZD 2014, 350, 352 f.

48 z. B. Elliptic, Homepage abrufbar unter https://www.elliptic.co/ (letzter Abruf: 17.3.2017).

49 Siehe im Kontext polizeilicher Ermittlungen *Pesch/Böhme*, DuD 2017, 93' 96.

50 Dies entspricht Art. 7 DS-RL sowie Art. 6 Abs. 1 DS-GVO.

51 *Gola/Klug/Dörfer*, in: Gola/Schomerus, Bundesdatenschutzgesetz (12. Aufl. 2015), § 4a, Rn. 26; *Kühling*, in: Wolff/Brink, BeckOK Datenschutzrecht (Std. 1.11.2016), § 4a BDSG, Rn. 44; *Simitis*, in: Simitis, BDSG, 8. Aufl. 2014, § 4a, Rn. 77.

52 *Kühling*, in: Wolff/Brink, BeckOK Datenschutzrecht (Std. 1.11.2016), § 4a BDSG, Rn. 57, 59; *Simitis*, in: Simitis, BDSG, 8. Aufl. 2014, § 4a, Rn. 94 f.; *Wegmann*, DuD 2007, 422 ff.

53 Die Zulässigkeit konkludenter Einwilligungen ist str.: Ablehnend *Helfrich*, in: Hoeren/Sieber, Handbuch Multimedia-Recht, Teil 16.1., Rn. 60; *Simitis*, in: Simitis, BDSG, 8. Aufl. 2014, § 4a, Rn. 44. Grds. bejahend *BGH*, Urt. v. 11.12.1991 – VIII ZR 4/91, NJW 1992, 737, 740; *Gola/Klug/Dörfer*, in: Gola/Schomerus, Bundesdatenschutzgesetz (12. Aufl. 2015), § 4a, Rn. 29a; *Kühling*, in: Wolff/Brink, BeckOK Datenschutzrecht (Std. 1.11.2016), § 4a BDSG, Rn. 44; (zurückhaltend) *OLG Frankfurt a.M.*, Urt. v. 13.12.2000 – 13 U 204/98, BeckRS 2000, 30149732. Die DS-GVO lässt eine konkludente Einwilligung zu, Art. 4 Nr. 11, *Ernst*, ZD 2017, 110,114; *Ernst*, in: Paal/Pauly, Datenschutz-Grundverordnung (1. Aufl. 2017), Art. 4, Rn. 88; *Schild*, in: Wolff/Brink, BeckOK Datenschutzrecht (Std. 1.11.2016), Art. 4 DS-GVO, Rn. 124.

54 Hierbei ergeben sich weitere Probleme, etwa, wie mit künftigen Regeländerungen des Netzwerks und der faktischen Unwiderruflichkeit wegen der nachträglichen Unveränderlichkeit der Blockchain umzugehen ist.

55 Die folgende Betrachtung beschränkt sich auf nicht-öffentliche Stellen.

56 Diese entspricht weitgehend Art. 7 lit b DS-RL sowie Art. 6 Abs. 1 lit. b DS-GVO.

57 Vgl. zu § 28 BDSG im Kontext von Blockchain-Daten auch *Spindler/Bille*, WM 2004, 1357, 1368.

58 Bei Bitcoins kann z. B. wegen des Herrührens aus kriminellen Transaktionen das Risiko bestehen, dass deren Handel an einer Börse vom Betreiber verweigert wird – sogar vorgeschrieben wäre dies bei einer Regulierung durch Sperrlisten, dazu *Pesch/Böhme*, DuD 2017, 93, 96 ff.

59 Vgl. *Simitis*, in: Simitis, BDSG, 8. Aufl. 2014, § 28, Rn. 63 f.

60 Vgl. *Gola/Klug/Dörfer*, in: Gola/Schomerus, Bundesdatenschutzgesetz (12. Aufl. 2015), § 28, Rn. 31; *Simitis*, in: Simitis, BDSG, 8. Aufl. 2014, § 28, Rn. 151 ff.; *Wolff*, in: Wolff/Brink, BeckOK Datenschutzrecht (Std. 1.8.2015), § 28 BDSG, Rn. 80 f.

Datensicherheit, Transparenz und Betroffenenrechte
Bei verbreiteten Blockchain-Systemen ist davon auszugehen, dass die Daten technisch bedingt transparent und sicher sind. Dies impliziert allerdings nicht, dass Eintragungen in die Blockchain oder die Erhebung und Verarbeitung von Daten aus der Blockchain ihrerseits transparent und sicher sind. Was den Umfang der nach § 9 BDSG[61] erforderlichen, d. h. verhältnismäßigen,[62] technischen und organisatorischen Datensicherheitsmaßnahmen anbetrifft, ergibt sich, dass hinsichtlich der ohnehin öffentlichen Blockchain-Daten ein geringes Schutzbedürfnis des Betroffenen besteht.[63] Anderes gilt bei einer abweichenden Aufbereitung der Daten oder der Kombination mit Zusatzinformationen. Dies folgt der Behandlung konventioneller Datenbanken.[64] Auch sonst sind bezüglich der Datensicherheitsanforderungen keine wesentlichen Besonderheiten bei der Verarbeitung von Blockchain-Daten ersichtlich.

Besonderheiten ergeben sich aber für das datenschutzrechtliche Transparenzgebot. Denn das Datenschutzrecht erfordert nicht nur Klarheit darüber, welche Daten betroffen sind. So bestimmt § 33 Abs. 1 Satz 1 BDSG für die Erhebung von Daten durch eine nicht-öffentliche Stelle ohne Kenntnis des Betroffenen,[65] dass dieser auch von der Zweckbestimmung der Datenverarbeitung und der Identität der verantwortlichen Stelle zu benachrichtigen ist.[66] Dies dient insbesondere dazu, den Betroffenen in die Lage zu versetzen, seine übrigen Rechte aus den §§ 33 ff. geltend zu machen.[67] Wegen der Pseudonymität von Blockchain-Daten sind Name und Anschrift des Betroffenen nicht bekannt. Angesichts dessen könnte erwogen werden, ob eine Pflicht zur Benachrichtigung – etwa nach § 33 Abs. 2 Nr. 7 lit. a) oder Nr. 8 – ausgeschlossen sein könnte, weil der Aufwand von Benachrichtigungen wegen der Vielzahl der Betroffenen als unverhältnismäßig anzusehen sein könnte.[68] Eine Identifizierung zum Zweck der Benachrichtigung liefe jedenfalls den Datenschutzinteressen der sich hinter den Pseudonymen verbergenden Betroffenen zuwider. Stattdessen wäre aber denkbar, pseudonyme Benachrichtigungen zum Abruf bereit zu halten, von denen Betroffene Kenntnis nehmen können.[69]

Im Kontext der Betroffenenrechte stellt sich die weiterhin die Frage, wie damit umzugehen ist, dass bestimmte Daten in der Blockchain nicht nachträglich geändert werden können. Dies führt dazu, dass sich etwaige Betroffenenrechte, insbesondere ein Recht auf Löschung (§ 35 Abs. 1, 2 BDSG; Art. 12 lit. b DS-RL; Art. 17 Abs. 1 DS-GVO), nicht im Wege einer Inanspruchnahme von zugangsvermittelnden Intermediären oder (einzelner) Knoten durchsetzen lassen. Stattdessen ließe sich erwägen, in Anlehnung an die EuGH-Entscheidung zum „Recht auf Vergessenwerden“[70] Intermediäre, die Blockchain-Daten aufbereiten[71] und so einem breiten Publikum erleichterten Zugang zu diesen verschaffen, dazu zu verpflichten, bestimmte Blockchain-Daten nicht anzuzeigen. Das Spannungsverhältnis zwischen Betroffenenrechten und Unveränderlichkeit betrifft im Übrigen auch private Blockchains.

Datenvermeidung und Datensparsamkeit
Dass das Löschen prinzipiell nicht möglich ist, dient der Gewährleistung der mehrseitigen Überprüfbarkeit. Dies wirkt sich darauf aus, in welchem Umfang personenbezogene Daten in der Blockchain gespeichert werden dürfen. § 3a Satz 1 BDSG bestimmt, dass so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen sind.[72] Die mehrseitige Überprüfbarkeit erfordert hinreichend bestimmte Informationen in unverschlüsselter Form.[73] Es liegt daher ein offensichtlicher Zielkonflikt mit dem Prinzip der Datensparsamkeit vor.

Dagegen entspricht die Pseudonymität von Blockchain-Systemen der in § 3a Satz 2 BDSG zum Ausdruck kommenden Vorstellung des Gesetzgebers, dass dem Grundsatz der Datenvermeidung und -sparsamkeit insbesondere durch Pseudonymsierung und Anonymisierung Rechnung getragen werden könne.[74]

Vor dem Hintergrund, dass sich die Vorgänge innerhalb der dezentralen Systeme durch die im BDSG vorherrschenden normativen Schutzvorschriften praktisch nicht greifen lassen,[75] erscheint eine verstärkte Fokussierung auf technisch implementierten Datenschutz unerlässlich.[76]

5 Ausblick auf technische Datenschutzlösungen

Lösungsansätze, die zukünftige Blockchain-Systeme mit dem Datenschutz besser vereinbar machen, lassen sich grob in drei Kategorien einteilen. Einerseits gibt es bereits in der Blockchain-Technologie Entwicklungen, die einen Kompromiss zwischen Öffentlichkeit und Überprüfbarkeit herstellen. Andererseits können vorliegende Erkenntnisse aus dem Technischen Datenschutz in die Blockchain-Technologie integriert werden. Schließlich kann das Datenschutzrecht auf die neuen Erfordernisse der Blockchain-Technologie hin weiterentwickelt werden.

5.1 Datenschutz-Overlays

Mit Zero-Knowledge-Verfahren und homomorpher Verschlüsselung stehen moderne kryptographische Verfahren zur Verfügung, die es erlauben, eine formale Korrektheitsprüfung durchzuführen, ohne den Inhalt der zu überprüfenden Information

61 Vgl. Art. 17 Abs. 1 DS-RL sowie Art. 24 Abs. 1, 2 DS-GVO.

62 *Gola/Klug/Dörfer*, in: Gola/Schomerus, Bundesdatenschutzgesetz (12. Aufl. 2015), § 9, Rn. 7; *Karg*, in: Wolff/Brink, in: BeckOK Datenschutzrecht (Std. 1.11.2016), § 9, Rn. 91; *Simitis*, in: Simitis, BDSG, 8. Aufl. 2014, § 9, Rn. 23.

63 Vgl. *Ernestus*, in: Simitis, BDSG, 8. Aufl. 2014, § 9, Rn. 42.

64 *Ernestus*, in: Simitis, BDSG, 8. Aufl. 2014, § 9, Rn. 42.

65 Angesichts der allgemeinen Zugänglichkeit von Blockchain-Daten darf eine Datenerhebung abweichend vom Grundsatz der Direkterhebung ohne Mitwirkung des Betroffenen erfolgen, vgl. *Bäcker*, in: BeckOK Datenschutzrecht (Std. 1.5.2016), § 4, Rn. 34.1; *Gola/Klug/Körffer*, in: Gola/Schomerus, Bundesdatenschutzgesetz (12. Aufl. 2015), § 4, Rn. 24.

66 So auch Art. 11 Abs. 1 lit a, b DS-RL sowie Art. 14 Abs. 1 lit. a, c DS-GVO.

67 Vgl. BT-Drs. 11/4306, S. 51.

68 Einen Ausschluss wegen unverhältnismäßigen Aufwands sehen auch Art. 11 Abs. 2 DS-RL sowie Art. 14 Abs. 5 lit. b DS-GVO vor.

69 Diese ließen sich mit dem öffentlichen Schlüssel des Betroffenen verschlüsseln, sodass nur der Betroffene nach Entschlüsselung mit seinem privaten Schlüssel vom Inhalt der Benachrichtigung Kenntnis nehmen könnte. Dazu näher unten unter 5.2.

70 *EuGH*, Urt. v. 13.3.2014 – C-131/12, Rn. 89 ff., NJW 2014, 2257, 2263 f. = ZD 2014, 350, 358 f.

71 S.o. Fn. 47.

72 Vgl. Art. 6 Abs. 1 lit. c DS-RL; Art. 5 Abs. 1 lit. c DS-GVO.

73 Im Bitcoin-System liegen etwa Kontostände, Referenzen auf Vorgängertransaktionen und Überweisungsbeträge offen, was die Finanzströme in hohem Maß nachvollziehbar macht.

74 Zur Blockchain-Technologie als Chance für Datenschutz *Guggenberger*, ZD 2017, 49 f.

75 S. o. 4.1.3.

76 Vgl. *Scholz*, in: Simitis, BDSG, 8. Aufl. 2014, § 3a, Rn.9 ff.

zu kennen. Dies löst den Konflikt zwischen Datensparsamkeit und der mehrseitigen Überprüfbarkeit.[77] Allerdings gelingt dies bislang nur für domänenspezifische Blockchains.[78] Praktische Beispiele dafür sind die virtuellen Kryptowährungen Monero, die die Herkunft eingehender Transaktionen verschleiert,[79] und Zcash, welche die Möglichkeit vollständig anonymisierter Transaktionen bietet. Auch die (kaum genutzten[80]) *Stealth*-Adressen zur Gewährung von Empfängeranonymität in Bitcoin können als ein frühes Beispiel für ein Datenschutz-Overlay angesehen werden.

Verbleibende Schwierigkeiten betreffen mangelndes Vertrauen in neuartige und wenig untersuchte kryptographische Verfahren, das erhebliche Datenschutzrisiko für den Fall kryptoanalytischer Erfolge oder der Kompromittierung von geheim zu haltenden Parametern und die Notwendigkeit, einen sozialen Konsens über den Grad an Transparenz in einem konkreten System zu finden.

5.2 Übertragung bekannter Konzepte aus dem Technischen Datenschutz

Mehr als 30 Jahre Forschung zu Technischem Datenschutz (engl. *Privacy Enhancing Technologies*, kurz PET) lassen vermuten, dass Erkenntnisse in die weitgehend unabhängig entwickelte Blockchain-Technologie übertragbar sind.[81] Ein erster Ansatzpunkt wären Konzepte, die für das datenschutz-fördernde Identitätsmanagement entwickelt wurden, wie Pseudonym-Relationen, partielle Identitäten und Identitätstreuhänder.[82] Letztere ermöglichen eine Identifizierung von hinter Pseudonymen stehenden Parteien unter (überprüfbaren) Bedingungen.

Ein konkreterer Vorschlag ergibt sich aus den Ausführungen in Abschnitt 4.2. Datenschutzrechtliche Einwilligungen und Benachrichtigungen könnten im System berücksichtigt und unter Ausnutzung der ohnehin vorhandenen kryptographischen Identitäten direkt in der Blockchain überprüfbar abgelegt werden.

Dies entspricht der Philosophie des Technischen Datenschutzes, einem Teilgebiet der Informatik, das Technik in Einklang mit den datenschutzrechtlichen Vorgaben erforscht und entwickelt. Im Gegensatz dazu stellt die dynamische Entwicklung der Blockchain-Technologie das Datenschutzrecht bzw. dessen Anwendung vor neue Herausforderungen. Insofern ist nicht auszuschließen, dass sich das Datenschutzrecht, behutsam und unter Wahrung seiner Grundsätze, an die Blockchain-Technologie anpassen wird.

Fazit

Komplexe, arbeitsteilige Datenverarbeitungssysteme entziehen sich dem geltenden Datenschutzrecht weitgehend. Dieses Defizit stellt sich für öffentliche Blockchains wegen deren Dezentralität und Pseudonymität als besonders gravierend heraus: Die verantwortlichen Stellen sind nicht ohne weiteres bestimmbar und oft praktisch nicht greifbar. Gleichzeitig werden regelmäßig Daten, die Rückschlüsse auf Gewohnheiten und Lebensumstände von Personen zulassen, praktisch unveränderbar in – aus Prinzip öffentlich einsehbaren – Datenstrukturen gespeichert. Im Vergleich zu konventionellen Datenbanken bedeutet dies eine erhebliche Verschlechterung des Datenschutzes. Deshalb sollten öffentliche Blockchains ausschließlich dann eingesetzt werden, wenn keine datenschutzfreundlichere Alternative zur Verfügung steht.

Damit Betroffenen beim Einsatz von Blockchain-Technologien nicht schon der Ansatzpunkt zur Durchsetzung des Schutzes ihrer personenbezogenen Daten entzogen ist, bedarf es neuer datenschutzrechtlicher Konzepte. Zu deren Entwicklung sind weitergehende datenschutzrechtliche Untersuchungen sowie die Erforschung und Erprobung spezifischer technischer Lösungsansätze notwendig. Mit dem vorliegenden Beitrag wurde ein erster Versuch unternommen, die Blockchain-Technologie und das geltende Datenschutzrecht zusammenzuführen. Er vermittelt Wissenschaft und Praxis ein grundlegendes Verständnis der Technologie und der datenschutzrechtlichen Herausforderungen und bietet Ansatzpunkte für die wissenschaftliche Aufklärung der offenen Fragen.

Danksagung

Die Autoren sind Prof. Dr. Franziska Boehm, Clemens Brunner, Michael Fröwis, Prof. Dr. Nikolas Guggenberger, Prof. Dr. Rüdiger Grimm, Martin Rost und Dr. Christian Sillaber zum Dank für wertvolle Hinweise verpflichtet.

77 *Meiklejohn/Orlandi*, in: Brenner/Christin/Johnson/Rohloff, Financial Cryptography and Data Security (FC 2015), International Workshops, BITCOIN, Puerto Rico, S. 127 ff.

78 Um Plattformen wie Ethereum datenschutzfreundlich zu realisieren, wären effiziente, *voll* homomorphe kryptographische Systeme notwendig. Deren Realisierung gilt als offenes Forschungsziel.

79 Die Erweiterung Confidential Transactions verschlüsselt darüber hinaus auch die Überweisungsbeträge, vgl. *Noether/Mackenzie*, Ledger Vol. 1 (2016), 1 ff.

80 *Möser/Böhme*, Anonymous Alone? Measuring Bitcoin's Second-Generation Anonymization Techniques (2017), in: IEEE Security & Privacy on the Blockchain (IEEE S&B), abrufbar unter http://informationsecurity.uibk.ac.at/pdfs/MB2017_AnonymousAlone.pdf (letzter Abruf: 12.6.2017).

81 Die Unabhängigkeit ist insofern eingeschränkt, als praktische Blockchain-Systeme oft über Anonymisierungsdienste betrieben werden, welche ein wesentliches Ergebnis der Forschung im Gebiet des Technischen Datenschutzes darstellen. Allerdings dient dies nicht immer hehren Datenschutzzielen, sondern oft der Vereitelung von Strafverfolgung. Zu den Grenzen der Ermittlungen *Pesch/Böhme*, DuD 2017, 93, 95 f.

82 Dazu *Hansen/Rost*, DuD 2003, 293, 294 f.