forum <privatheit>
selbstbestimmtes_leben_in_der_digitalen_welt

FORUM PRIVATHEIT UND SELBSTBESTIMMTES LEBEN IN DER DIGITALEN WELT

White Paper

DATENSCHUTZ IN DER BLOCKCHAIN

Diskussion der Herausforderungen und Lösungsansätze auf Basis der Blockchain-Konsultation der Bundesregierung

White Paper

DATENSCHUTZ IN DER BLOCKCHAIN

Diskussion der Herausforderungen und Lösungsansätze auf Basis der Blockchain-Konsultation der Bundesregierung

Autoren:
Frank Ebbers[1], Murat Karaboga[1], Benjamin Bremert[2], Tamer Bile[3], Carsten Ochs[4], Yannic Meier[5], Severin Weiler[6]

(1) Fraunhofer-Institut für System- und Innovationsforschung ISI, Karlsruhe
(2) Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), Kiel
(3) Universität Kassel, Projektgruppe verfassungsverträgliche Technikgestaltung (provet)
(4) Universität Kassel, Fachgebiet Soziologische Theorie
(5) Universität Duisburg-Essen, Sozialpsychologie
(6) Universität München, Institut für Wirtschaftsinformatik und Neue Medien (WIM)

Herausgeber(-innen):
Michael Friedewald, Regina Ammicht Quinn, Marit Hansen, Jessica Heesen, Thomas Hess, Nicole Krämer, Jörn Lamla, Christian Matt, Alexander Roßnagel, Michael Waidner

Inhaltsverzeichnis

Kurzzusammenfassung 5

1 Einleitung 6

2 Ursprung und Kontext der Blockchain-Technologie 8
2.1 Entstehung und technischer Hintergrund 8
2.1.1 Technische Details der Blockchain-Technologie 9
2.1.2 Arten von Blockchains 10
2.2 Anwendungsbereiche der Blockchain-Technologie 11
2.3 Datenschutzrechtliche Herausforderungen der Blockchain-Technologie 13
2.3.1 Anwendbares Recht 13
2.3.2 Erlaubnistatbestände 15
2.3.3 Betroffenenrechte 16
2.3.4 Automatisierte Entscheidung im Einzelfall 17
2.4 Herausforderungen der Blockchain-Technologie jenseits des Datenschutzes 18

3 Datenschutz und Blockchain: Analyse des Diskurses im Rahmen der Blockchain-Konsultation 20
3.1 Methodik 20
3.2 Themenkomplex 1: Relevanz von Datenschutz in der Blockchain 21
3.3 Themenkomplex 2: Herausforderungen 23
3.4 Themenkomplex 3: Lösungsansätze 25
3.4.1 Bestehende technische Lösungen 26
3.4.2 Rechtliche Anpassung 27
3.4.3 Organisatorische Maßnahmen 28

4 Bewertung der Aussagen der Akteure 29
4.1.1 Betroffenenrechte: Löschung und Berichtigung 29
4.1.2 Betroffenenrechte: Datenübertragbarkeit 33
4.1.3 Bestimmbarkeit des Verantwortlichen 33
4.1.4 Verschlüsselung 33
4.1.5 Daten für alle Blockchain-Teilnehmer sichtbar und schreibbar 35
4.1.6 Pseudonymisierung und Depseudonymisierung 35
4.1.7 Anonymisierung 36
4.1.8 Speicherung außerhalb der EU 37
4.1.9 Sicherheit der gespeicherten Daten 38
4.1.10 Integrität und Qualität der zu speichernden Daten 38
4.1.11 Forderungen nach rechtlichen Anpassungen 39
4.1.12 Forderungen nach organisatorischen Maßnahmen 40
4.1.13 Technische Weiterentwicklungen und Standards 41

5 Zusammenfassung und Fazit 43

6 Literaturverzeichnis 46

7 Anhang 54
7.1 Zuweisung der Kategorisierung für Probleme 54
7.2 Zuweisung der Kategorisierung für Lösungsvorschläge 55
7.3 Probleme und deren Lösungsvorschläge in der Übersicht 56
7.4 Detaillierte Auswertungen: Lösungsansätze der Akteure pro Anwendungsbereich 57

Abbildungsverzeichnis

Abbildung 1: Beispielanwendung eines Smart Contracts im Bereich der Energiewirtschaft (eigene Darstellung) 12
Abbildung 2: Branchenzugehörigkeit aller Akteure 21
Abbildung 3: Relevanz von Datenschutz und Blockchain 22
Abbildung 4: Relevanz von Datenschutz und Blockchain 23
Abbildung 5: Seitens der Akteure identifizierte datenschutzrechtliche Herausforderungen 24
Abbildung 6: Seitens der Akteure identifizierte datenschutzrechtliche Herausforderungen 25
Abbildung 7: Seitens der Akteure vorgeschlagene Lösungen 26
Abbildung 8: Alle unter dem Punkt "Bestehende techn. Lösungen" subsumierte Lösungsvorschläge 27
Abbildung 9: Alle unter dem Punkt "Rechtliche Anpassung" subsumierten Vorschläge 27
Abbildung 10: Alle unter dem Punkt "Organisatorische Maßnahmen" subsumierten Vorschläge 28
Abbildung 11: Merkle-Tree Baumstruktur 30
Abbildung 12: Gruppierung der Problembeschreibungen 54
Abbildung 13: Gruppierung der Lösungsvorschläge 55
Abbildung 14: Übersicht über Datenschutzherausforderungen 56

Tabellenverzeichnis

Tabelle 1: Arten von Blockchains und deren datenschutzrelevanten Charakteristika 10
Tabelle 2: Lösungsansätze der Akteure pro Anwendungsbereich 57

Kurzzusammenfassung

Das Forum Privatheit nimmt den fortschreitenden Einsatz der Blockchain-Technologie und die Blockchain-Strategie der Bundesregierung zum Anlass, um die seitens der an der Blockchain-Konsultation der Bundesregierung beteiligten Akteure genannten datenschutzrelevanten Herausforderungen und Lösungen zu untersuchen. Als empirische Grundlage dienen die öffentlichen Antworten der am Konsultationsprozess beteiligten Akteure (1048-seitiges Dokument mit 6261 inhaltlichen Statements). Diese wurden nach datenschutzrelevanten Schlagworten durchsucht (537 relevante Statements) und anschließend nach Problembeschreibungen und Lösungsvorschlägen sowie allgemeinen Aussagen zum Datenschutz codiert.

Die Ergebnisse zeigen, dass ein Großteil der Akteure aufgrund der datenschutzrechtlichen Vorschriften ernsthafte Bedenken im Hinblick auf die Nutzbarkeit der Blockchain-Technologie äußert (81 %), diese Herausforderungen jedoch zugleich für bewältigbar hält (70 %). Hierzu wird insbesondere auf bestehende technische Lösungen verwiesen: Am häufigsten wurde auf die Off-Chain-Speicherung verwiesen (46 %), gefolgt von Verschlüsselung (39 %) und Pseudonymisierung (19 %). Daneben wurde auch der Verzicht auf die Speicherung personenbezogener Daten (40 %) und die Nutzung einer privaten oder halb-privaten Blockchain (31 %) befürwortet.

Unter Berücksichtigung des derzeitigen Stands der Technik halten wir die Off-Chain-Speicherung für die sinnvollste Lösung, für einen datenschutzkonformen Einsatz im Rahmen einer öffentlichen Blockchain. Zudem kann auch die Verschlüsselung zum datenschutzkonformen Einsatz beitragen. Ansonsten sollte auf die Speicherung personenbezogener Daten möglichst verzichtet werden oder auf die Nutzung einer privaten oder halb-privaten Blockchain gesetzt werden, da sich dadurch die datenschutzrechtlichen Herausforderungen – zu Lasten der mit Blockchains intendierten verbesserten Gewährleistung von Transparenz – vermeiden lassen. Insgesamt begrüßen wir die anhaltende intensive Debatte über den datenschutzkonformen Einsatz der Blockchain-Technologie und möchten anregen, dass weitere Anstrengungen auf diesem Gebiet unternommen werden, um die Potentiale dieser Technologie nutzbar zu machen, während ihre gesellschaftliche und rechtliche Verträglichkeit erhalten bleibt.

1 Einleitung

Seit dem weltweiten Erfolg der Bitcoin-Währung wird sowohl in Wirtschafts- als auch in Wissenschaftskreisen rege über die Potentiale der Blockchain diskutiert. Eine aktuelle Studie zeigt, dass für 53 % der befragten Unternehmen weltweit die Blockchain bei den strategischen Entscheidungen zu den Top Fünf gehört (Deloitte 2019). Nachdem viele Staaten zunächst zögerlich reagierten, war es die deutsche Bundesregierung, die dem Diskurs zu einem neuen Höhepunkt verhalf. Zunächst kündigte die aus CDU/CSU und SPD bestehende Regierungskoalition im Koalitionsvertrag Anfang 2018 die Entwicklung einer umfassenden Blockchain-Strategie an, „um das Potenzial der Blockchain-Technologie zu erschließen und Missbrauchsmöglichkeiten zu verhindern" (CDU/CSU und SPD 2018, S. 43–44). Zu diesem Zweck initiierten die zuständigen Ministerien für Wirtschaft und Energie sowie der Finanzen eine Online-Konsultation, in der zum einen nach den Potentialen der Blockchain-Technologie im Kontext verschiedener Anwendungsfelder und zum anderen nach den technologischen, ökonomischen, ökologischen und rechtlichen Herausforderungen gefragt wurde.

Die unter Hinzuziehung der eingereichten Stellungnahmen erarbeitete Blockchain-Strategie der Bundesregierung wurde schließlich im September 2019 veröffentlicht. Darin legte die Bundesregierung Rahmenbedingungen für die weitere Entwicklung der Technologie fest und kündigte mehrere Dutzend Maßnahmen auf fünf Handlungsfeldern (Finanzsektor, Förderung von Reallaboren, Schaffung verlässlicher Rahmenbedingungen, Einführung digitaler Verwaltungsdienstleistungen, Fortsetzung und Ausbau des Blockchain-Dialogs) an. Die darauffolgenden Reaktionen reichten von deutlicher Unterstützung (Sausen 2019) über skeptische Erleichterung (Brandenburg 2019; Cavus 2019) bis hin zu grundsätzlicher Kritik (Streim und Hansen 2019). Bemängelt wurde insbesondere das Fehlen einheitlicher Ziele und eines verbindlichen Zeitplans.[1]

Im Hinblick auf datenschutzrechtlichen Fragen im Zusammenhang mit Blockchain-Anwendungen teilte die Bundesregierung mit, dass kein Änderungsbedarf der DSGVO gesehen werde und dass die Adressierung der datenschutzrechtlichen Unsicherheiten von Entwicklern und Anwendern einerseits unter Rückgriff auf bestehende technische Lösungen (u. a. Verwendung von Hashwerten, Pseudonymisierung, Zero-Knowledge-Proof) und andererseits mittels der Durchführung eines „Runden Tischs" zum Thema Blockchain und Datenschutz erfolgen soll (Presse- und Informationsamt der Bundesregierung 2019).

Die Aufforderung zur Einreichung von Beiträgen stieß auf Seiten der Stakeholder auf großes Interesse. Insgesamt 158 Expertinnen und Experten bzw. Organisationen machten von der Möglichkeit Gebrauch. Ende September 2019 veröffentlichten die Ministerien schließlich alle eingegangenen und seitens der Ministerien zur Veröffentlichung freigegebenen Stellungnahmen in Form eines 1048-seitigen Dokuments.

Die Tatsache, dass zahlreiche private und öffentliche Stellen (Zhang et al. 2019; Kazan et al. 2015) trotz der bekannten Datenschutzrisiken bereits Blockchain-basierte Produkte und Dienste anbieten und viele weitere in Entwicklung sind, nimmt das Forum Privatheit zum Anlass, sich mit den datenschutzrechtlichen Herausforderungen und den

[1] Siehe für einen aktuellen Überblick des Umsetzungsstands der Ziele: https://www.bitkom.org/Themen/Technologien-Software/Blockchain/Bestandsaufnahme-Blockchain-Strategie-der-Bundesregierung (letzter Zugriff: 25.01.2021).

vorgeschlagenen Lösungsansätzen auseinanderzusetzen. Die vorliegende Studie hat das Ziel, eine fundierte Diskursanalyse auf Grundlage aller veröffentlichten Stellungnahmen des Konsultationsprozesses vorzunehmen. Von Interesse ist dabei zunächst zum einen, welche Herausforderungen im Zusammenhang mit Blockchain und Datenschutz gesehen werden und zum anderen, welche Lösungen zur Adressierung der genannten Herausforderungen als adäquat vorgeschlagen werden. Im Anschluss werden die Herausforderungen und Lösungsvorschläge gegenübergestellt und in ihren Wirkungen bewertet. Damit möchten wir einen Beitrag zu den datenschutzrechtlichen Aspekten der Blockchain-Debatte liefern und zur Klarstellung einiger datenschutzrechtlicher Probleme beitragen.

Die Studie beginnt mit einer kurzen Einführung in die Entstehung und grundlegende technische Funktionsweise der Blockchain-Technologie sowie mit der Vorstellung aktueller Anwendungsfelder. Daran schließt sich eine Diskussion der datenschutzrechtlichen Herausforderungen der Blockchain-Technologie sowie die Betrachtung grundsätzlicher Herausforderungen jenseits des Datenschutzrechts an. Es folgt eine Analyse der im Rahmen der Konsultation eingereichten Stellungnahmen. In Kapitel 4 folgt schließlich die Diskussion und Einordnung der Antworten.[2] Im letzten Kapitel fassen wir die Ergebnisse zusammen und ziehen ein Fazit.

[2] Für ausführliches und hilfreiches Feedback, insb. zur Bewertung der technischen Lösungsansätze, bedanken wir uns bei den Kollegen Dirk Achenbach und Jochen Rill vom FZI Forschungszentrum Informatik in Karlsruhe.

2 Ursprung und Kontext der Blockchain-Technologie

In diesem Kapitel gehen wir auf den Kontext der Blockchain-Technologie ein, der den Rahmen für die Blockchain-Konsultation der Bundesregierung bildet. Dazu widmen wir uns im Unterkapitel 2.1 der Entstehung und dem technischen Hintergrund und stellen im darauffolgenden Unterkapitel 2.2 bereits existierende und künftig potentiell mögliche Anwendungsfelder der Blockchain-Technologie dar. Daran schließt sich in Unterkapitel 2.3 die Diskussion der datenschutzrechtlichen Herausforderungen der Blockchain-Technologie sowie in Unterkapitel 2.4 die Betrachtung grundsätzlicher Herausforderungen jenseits des Datenschutzrechts an.

2.1 Entstehung und technischer Hintergrund

Blockchain (BC) ist ein Überbegriff für eine Technologie, die technisch gesehen eine verteilte Transaktionsdatenbank darstellt. Oft wird die Blockchain mit der *Distributed-Ledger-Technologie* (DLT) gleichgesetzt.[3] Dies ist jedoch nur bedingt korrekt. Vielmehr kann die Blockchain als eine Variante der DLT bezeichnet werden. Gemein haben beide Technologien, dass die Daten verteilt, also dezentral auf den Systemen jedes Teilnehmers (sog. „Nodes") (Nofer et al. 2017) gespeichert werden. Jedoch müssen diese bei DLT nicht zwingend in zusammengefassten Transaktions-Blöcken gespeichert sein, sondern können auch andere Formen der Speicherung aufweisen (Bashir 2018). Gemein haben sie außerdem, dass Daten mittels kryptographischer Hash-Funktionen ausschließlich an die vorhergehenden Daten angehängt werden können (append-only data structure) und sich deshalb nachträglich nicht ändern oder löschen lassen. Die Daten werden danach von anderen Teilnehmern (sog. „Minern") überprüft und an den vorherigen Block angehängt. Es kann jedoch passieren, dass mehrere Miner zeitgleich die Überprüfung abschließen. Dadurch entstehen kurzzeitig mehrere valide Blockchains im Netzwerk. Da es jedoch nur eine einzige valide Kette geben darf, wird nur die längste valide Kette im Netzwerk akzeptiert. Genauer gesagt jene Kette, für die die meiste Rechenleistung durch die Miner erbracht wurde (Schlatt et al. 2016; Zohar 2015). Schließlich wird diese Kette an alle Beteiligten in Netzwerk weitergegeben. Somit existieren – abhängig von der Zahl der Teilnehmer einer Blockchain – mehrere exakt gleiche Kopien der Datenbank. Eine solche Überprüfung ist jedoch nur bei Finanztransaktionen möglich, da bei ihr der Gesamtwert aller vorhandenen Werte (Münzen, „Coins") im System addiert wird. Somit können niemals mehr Münzen in den Transaktionen vorhanden sein als im Gesamtsystem möglich.

Eine hilfreiche Analogie für ein besseres Verständnis der Prozesse ist die eines besonderen Notizbuches: Alle Teilnehmer einer Blockchain teilen sich dasselbe miteinander vernetzte Notizbuch. Nimmt ein Teilnehmer eine Ergänzung am Notizbuch vor, taucht diese in den Notizbüchern aller anderen Teilnehmer ebenso auf, während eine nachträgliche Änderung der Notizen oder gar das Herausreißen einzelner Seiten unmöglich sind (Beispiel aus: Fridgen et al. 2019).

Das Ziel der Blockchain-Technologie besteht also darin, nicht manipulierbare Transaktionen im Internet zu ermöglichen und Konsens über den Inhalt und Korrektheit einer

[3] DLT gibt es nicht erst seitdem Kryptowährungen, allem voran Bitcoin, den Massenmarkt erreicht haben. Bereits 1991 stellten Haber und Stornetta eine Möglichkeit für das verkettete Signieren von Dokumenten auf Basis von Hash-Werten und Zeitstempeln vor.

Transaktion zu finden, ohne hierfür einem Intermediär, z. B. einer Bank, vertrauen zu müssen (Iansitit und Lakhani 2017). Somit wird der wesentliche Mehrwert einer Blockchain darin gesehen, Funktionalität und Sicherheit ohne eine zentrale Vertrauensstelle gewährleisten zu können. Diese neue Form der Vertrauensinfrastruktur spielte insbesondere beim Erfolg der Kryptowährung Bitcoin eine wichtige Rolle: Während Anleger in der Finanzkrise von 2008 das Vertrauen in Banken verloren, positionierte sich die Kryptowährung Bitcoin als eine neue, vertrauenswürdigere Alternative zu diesen und konnte u. a. dadurch enorme Wertsteigerungen erfahren (Skwarek 2019).

2.1.1 Technische Details der Blockchain-Technologie

Auf technischer Ebene ist eine Blockchain lediglich eine Datenbank. Die einzelnen Datenblöcke stehen dabei in Beziehung zu dem jeweils vorangehenden Block, indem jeder Block einen Hash des vorangehenden Blocks enthält. Bei einem Hash handelt es sich um eine Art digitalen Fingerabdruck. Dieser wird mittels einer mathematischen Hashfunktion für den konkreten Inhalt bzw. für die Daten des Vorgängerblockes errechnet. Ein Hash ist der Rückgabewert, der für gleiche Eingangsinformationen immer denselben eindeutigen Wert zurückgibt. Dieser Vorgang ist reproduzierbar, kann jedoch nicht rückgängig gemacht werden. Die Hash-Funktionen dürfen, damit sie für kryptografische Anwendungen nutzbar sind, nicht anfällig für Kollisionen sein[4], keinen Rückschluss auf die Ausgangsinformationen ermöglichen und müssen zufällig wirken[5]. Durch die Verknüpfung der Informationen enthält jeder Datenblock eine (fingerabdruckartige) Referenz auf den Vorgängerblock. Im Ergebnis führt dieses Prinzip dazu, dass der Inhalt eines Blocks nicht verändert werden kann, ohne zwangsläufig auch den Inhalt aller folgenden Blöcke verändern zu müssen. Ansonsten wären die – ohne großen Aufwand – überprüfbaren Hash-Werte der Einzelblöcke nicht mehr konsistent.

Der jeweilige Inhalt der Blöcke hängt dabei vom konkreten Einsatzzweck der Blockchain ab. Im Anwendungsfall „Bitcoin" enthalten die Blöcke Daten über Bitcoin-Transaktionen, die in ihrer Gesamtheit alle Zahlungen und das Guthaben der jeweiligen Nutzer abbilden. Gesichert sind diese Einzeldaten mit den kryptografischen Schlüsseln des jeweiligen Wallets, aus denen durch die Anwendung verschiedener Hash-Funktionen eine öffentliche Adresse abgeleitet wird. Diese Adressen sind sichtbar mit sämtlichen sie betreffenden Transaktionen verknüpft. Ebenso ist der öffentliche Schlüssel oder eine Ableitung dessen, mit dem die Transaktion eines Nutzers über durch ihn verfügte Wallets (von den Nodes im Netzwerk) verifiziert werden kann, verknüpft.

Die Verknüpfung der Blöcke stellt für sich genommen keine große Hürde dar. Um den kompletten Inhalt der Blockchain nicht einfach neu berechnen zu können, wird – gerade bei Kryptowährungen – ein weiterer Mechanismus implementiert, der „proof of work" heißt. Hierbei geht es darum, dass derjenige Teilnehmer, der einen neuen Block in die Blockchain geschrieben hat, dafür in einem gewissen Umfang Rechenleistung aufgewendet haben muss. Ursprünglich wurde hierin, unabhängig von Blockchain oder Bitcoin, eine Möglichkeit gesehen, um E-Mail-Spam zu begegnen, da der Absender (bzw. dessen Mailserver) für den Empfänger nachvollziehbar Rechenleistung für den Versand der E-Mail aufwenden musste (Dwork und Naor 1992). Dies sollte für den Versand einzelner E-Mails keine Hürde darstellen, den Massenversand für Spammer allerdings unattraktiv machen. Bei Bitcoin soll ein neuer Block lediglich alle zehn Minuten generiert werden können. Auf diese Weise soll auch dem Anstieg von Teilnehmer-

[4] Also der Fall, bei dem zwei verschiedene Eingabewerte denselben Hash-Wert erzeugen.

[5] Kleine Änderungen in den Ausgangsinformationen führen in der Regel zu erheblichen Unterschieden des Hash-Wertes.

zahlen und der damit zusammenhängenden Erhöhung der Rechenkapazität begegnet und somit verhindert werden, dass durch inflationäre Tokengenerierung ein Wertverfall einsetzt. Daher wird die Schwierigkeit alle 2016 Blöcke angepasst. Aus dem Schwierigkeitswert lassen sich verschiedene Informationen ableiten, mit denen die Lösung des „proof of work" überprüft werden kann: Einerseits die Anzahl von Nullen, die am Anfang des Hashes eines bestimmten Blocks stehen müssen, damit er als gültiges Ergebnis angesehen werden kann und andererseits der Wert, den dieser zu findende Hash des bestimmten Blockchain-Blocks unterschreiten muss (Schlatt et al. 2016). Der Anreiz, die dafür notwendige Rechenkapazität aufzuwenden ist der neu geschaffene Bitcoin, den der Miner erhält, wenn er einen Block mit validem Hash errechnet.

2.1.2 Arten von Blockchains

Grundsätzlich lassen sich Blockchains in drei verschiedene Arten unterteilen, die sich hauptsächlich durch die teilnehmenden Nutzer unterscheiden (Zheng et al. 2017) (siehe Tabelle 1). *Private Blockchains* werden von einer einzelnen Stelle kontrolliert. Sie sind somit zentralisiert und haben wenige Mitglieder. Die jeweilige Organisation bestimmt, wer Informationen lesen und Transaktionen übermitteln kann. Bei *öffentlichen Blockchains*, zu denen u. a. auch der Bitcoin gehört, gibt es keine zentrale Instanz. Hier kann jeder genehmigungsfrei teilnehmen. Im Gegensatz zu privaten Blockchains bleibt der Nutzer dabei anonym und kann alle Informationen lesen und Transaktionen tätigen. Als dritte Variante gibt es *halb-private,* auch *konsortiale genannte, Blockchains*. Diese Variante stellt einen Zwischenweg zwischen privaten und öffentlichen Blockchains dar. Weder wird die Blockchain von einer einzigen Stelle verwaltet, noch kann jeder an ihr teilnehmen. Stattdessen kontrolliert eine ausgewählte Gruppe (Konsortium) von Organisationen und/oder Einzelpersonen die Blockchain. Als Vorteil dieser Blockchain-Variante wird die Möglichkeit bewertet, durch Mehrheitsentscheidungen innerhalb der Gruppe betrügerische Aktivitäten oder Fehlentscheidungen zu verhindern (Zheng et al. 2017).

	Öffentlich	***Privat***	***halb-privat (konsortial)***
Zugang	Für alle zugänglich	Zulassungsbeschränkt	Zulassungsbeschränkt
Teilnehmer	Jeder möglich	Innerhalb einer Organisation (z. B. Unternehmen)	Zwischen Organisationen (z. B. Verbände)
Verantwortliche	Nicht vorhanden	Vorhanden	Vorhanden
Transparenz	Hoch, da Historie für alle Teilnehmer sichtbar	Nur für ausgewählten Teilnehmerkreis	Nur für ausgewählten Teilnehmerkreis
Löschbarkeit	Durch Architekturvorgabe nicht möglich	Möglich, da zentrale Instanz vorhanden	Möglich, z. B. durch Mehrheitsbeschluss
Änderbarkeit	Durch Architekturvorgabe nicht möglich	Möglich, da zentrale Instanz vorhanden	Möglich, z. B. durch Mehrheitsbeschluss
Änderungen an der Architektur	Kaum möglich	Möglich	Möglich
Bildung neuer Blöcke	Dezentral durch besondere Teilnehmer, so genannte Miner	Zentral durch einzelne Instanz	Unterschiedlich, je nach Ausgestaltung
Sicherheit, Manipulationsmöglichkeit	Kaum möglich, nur mittels 51%-Attacke	Durch die festgelegte, verantwortliche Instanz möglich	Unterschiedlich, je nach Ausgestaltung

Tabelle 1: Arten von Blockchains und deren datenschutzrelevanten Charakteristika

Strukturell hängt der Aufbau einer Blockchain von der konkreten Implementierung ab. Grundsätzlich kann zwischen verschiedenen Akteuren unterschieden werden:

- Teilnehmern, die lediglich auf Daten der Blockchain zugreifen,
- Teilnehmern, die Daten durch die konkrete Nutzung schreiben lassen,
- Nodes (die je nach konkreter Implementierung auch noch in unterschiedlichen Arten vorliegen können), also einem oder mehreren Knoten, die jeweils eine lokale Kopie der jeweiligen Blockchain enthalten, Daten mit anderen Nodes austauschen und Transaktionen überprüfen und
- Minern (die je nach konkreter Implementierung auch Nodes sein können), also Netzwerkteilnehmern, die neue Blöcke errechnen.

Im nächsten Unterkapitel stellen wir typische Anwendungsbereiche für die Blockchain vor, die über den Bereich der Kryptowährungen hinausgehen. Zudem geht das Kapitel darauf ein, wie mittels Smart Contracts Verhandlung und Abwicklung von Verträgen automatisiert vollzogen werden können.

2.2 Anwendungsbereiche der Blockchain-Technologie

Bisher sind Kryptowährungen der größte und bekannteste Anwendungsbereich für die Blockchain. Doch auch abseits der Finanzwelt werden Blockchains eingesetzt (Zheng et al. 2017). Auch die Bundesregierung erwähnt in der Konsultation verschiedene Anwendungsbereiche neben dem Finanzsektor, darunter Energie, Gesundheit/Pflege, Mobilität, Lieferketten/Logistik, Internet der Dinge, Identitäten-/Rechtemanagement, Verwaltung, Plattformökonomie (BMWi und BMF 2019). Grundsätzlich versprechen sich Unternehmen durch den Einsatz der Blockchain-Technologie eine Steigerung der Verlässlichkeit (PwC 2018). So könnten mithilfe von Smart Contracts und Decentralized Autonomous Organizations (DAO) Verträge, wie z. B. Minitransaktionen, völlig automatisiert ohne Eingriff eines Nutzers oder eines Intermediärs, geschlossen werden (Morabito 2017). Smart Contracts sind also kleine Computerprogramme, die automatisiert eine Entscheidung treffen, sobald eine oder mehrere Bedingungen erfüllt sind (Kõlvart et al. 2016).

Ein konkreter Anwendungsfall für eine Minitransaktion könnte z. B. im Bereich der Energiewirtschaft liegen (Abbildung 1): Haushalte, welche mittels Solarzellen Strom gewinnen und in das öffentliche Netz einspeisen, können mit Energiekonsumenten einen automatisierten Vertrag eingehen. Dieser handelt die Preise automatisch aus und überträgt den entsprechenden Betrag automatisiert auf das Konto des stromproduzierenden Haushalts (Ahl et al. 2019). Neben einem Wegfall der Nutzerinteraktion ergeben sich somit auch Zeitgewinne.

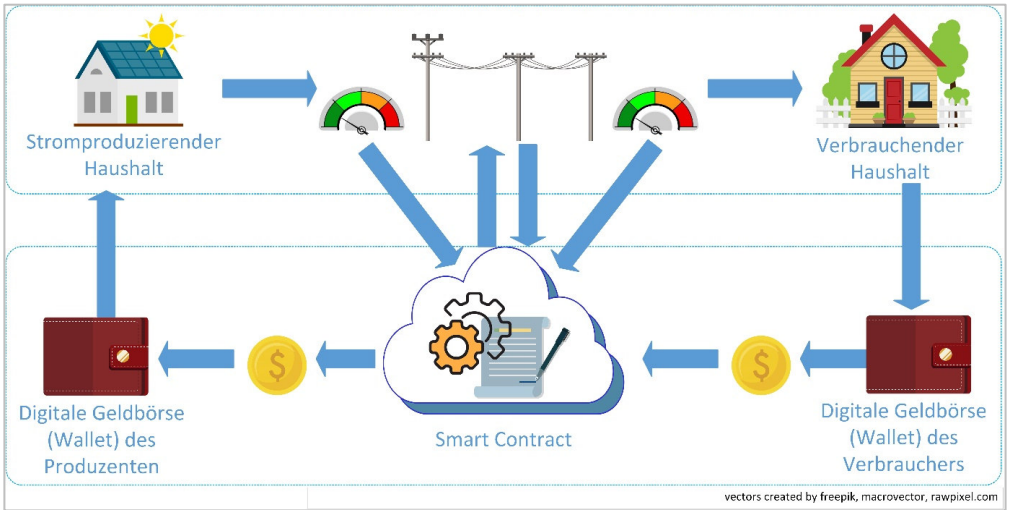


Abbildung 1: Beispielanwendung eines Smart Contracts im Bereich der Energiewirtschaft (eigene Darstellung)

Folglich versprechen sich insbesondere Akteure aus der Wirtschaft Vorteile durch den Einsatz einer Blockchain. Salviotti et al. (2018) identifizieren in ihrer Forschung neben Kryptowährungen vier weitere Anwendungsbereiche, auf die vor allem Wirtschaftsakteure setzen und die im Folgenden kurz vorgestellt werden sollen:

Demnach sollen mittels der Blockchain-Technologie neue Zahlungssysteme mit geringen Nutzungskosten angeboten werden können, wodurch positive wirtschaftliche Effekte. Bereits heute etablieren sich Anbieter, die mit Hilfe der Blockchain-Technologie grenzüberschreitenden Zahlungsverkehr zwischen Afrika und Europa ermöglichen. Durch Application Programming Interfaces (API) könnten Dienstleister zudem verschiedene weitere Leistungen anbieten (Kazan et al. 2015). Bereits im Jahr 2018 nutzten rund 90 % der führenden australischen, europäischen und nordamerikanischen Banken die Blockchain als Investitionsobjekt und/oder in ihren Produkten (Carson et al. 2018).

Hohes Potenzial wird dem Einsatz der Blockchain-Technologie darüber hinaus im Energiesektor zugesprochen, etwa im Hinblick auf die Senkung von Unternehmenskosten oder die Verbesserung der Transparenz bei der Gestaltung des Strompreises. Blockchain-Anwendungen spielen des weiteren eine wichtige Rolle beim „Smart-Grid". Dabei wird angestrebt, die Erzeugung, Speicherung und den Verbrauch von Energie zu kombinieren und ideal aufeinander abzustimmen. So könnten die einzelnen Systeme dezentral mittels Smart Contracts direkt untereinander Transaktionen von Gebühren sowie die Energielieferung durchführen (Agung und Handayani 2020). Denkbar ist, dass Energieverbraucher so variabel auf Angebots- und Nachfrageschwankungen reagieren können, indem sie ihren Stromverbrauch entsprechend anpassen. Die Entwicklung von Blockchain-Lösungen im Energiesektor befindet sich allerdings noch in einem vergleichsweisen frühen Stadium.

Darüber hinaus wird diskutiert, dass sich die Technologie zur Bekämpfung von Betrug eignet, da es in einer öffentlichen Blockchain unmöglich ist, vorhandene Daten zu verändern (Salviotti et al. 2018). Sofern die Input-Daten zuverlässig in eine Blockchain eingespeist werden, könne Betrug in Form von falschen Angaben bei der Beantragung von Krediten oder steuerlichen Angaben vorgebeugt werden (Cai und Zhu 2016; Hyvärinen et al. 2017). Obwohl es bereits Initiativen gibt, die Blockchain dafür einzusetzen, Betrug an Börsen in Lateinamerika zu verhindern, ist die Technologie in diesem Bereich ebenfalls noch wenig ausgereift (Mauri 2017).

Potentiale werden auch im digitalen Identitätsmanagement gesehen. Derzeit ist ein Verbraucher gezwungen, seine persönlichen Dokumente wie die Kopie des Reisepasses oder der Kreditkarte zur Identifizierung über das Internet an Dritte weiterzugeben. Diese Dokumente werden auf zentralen Servern gespeichert und sind somit anfällig für Cyber-Attacken (Salviotti et al. 2018). Blockchain-basierte Plattformen würden es dagegen ermöglichen, die Identität von Verbrauchern zu verifizieren, ohne einen zentralen Speicherort zu involvieren. Dabei würden die digitalen Identitäten nicht mehr von zentralen Institutionen kontrolliert, sondern von den Verbrauchern selbst (Schlegel et al. 2018). Obwohl das digitale Identitätsmanagement ein vielversprechender Anwendungsfall ist, sind viele Konzepte noch nicht marktreif (Carson et al. 2018). Während große Unternehmen (wie IBM) zum Zeitpunkt dieses White Papers noch an Lösungen in diesem Bereich arbeiten, sind einige kleinere Firmen und Startups bereits mit Lösungen auf dem Markt (MEDICI 2017). So bietet Civic Technologies (2020) einen auf der Blockchain basierenden Identity-Management Service an, der es Nutzern ermöglicht die Identität unveränderbar zu speichern, um damit Identitätsdiebstahl zu verhindern. Bitnation (2020) bietet als „Governance 2.0" aktuell einen digitalen Reisepass sowie digitale Heiratszertifikate an.

Schließlich werden Blockchain-Technologien Potentiale im Zusammenspiel mit anderen Technologien, wie dem Internet der Dinge (IoT) oder der Cloud-Speicherung, beigemessen. Ein vielversprechender Bereich sei die Nutzung von Blockchains zur Überwachung und Verfolgung von IoT-Informationen sowie zur Datensicherung (Korpela et al. 2017). Das Ziel dabei sei es, einerseits mit den im Zuge der Verbreitung des Internets der Dinge einhergehenden enormen Anstieg von Datenmengen (Balan et al. 2015) besser zu handhaben und andererseits die Herausforderungen einer zentralisierten IoT-Kommunikationsinfrastruktur anzugehen. Indem auf sog. fortgeschrittenes Tracking gesetzt wird, das auf einer Kombination von IoT-Technologien und herkömmlichen Tracking-Methoden basiert (Salviotti et al. 2018), könnten Millionen von vernetzen Geräten überwacht und so die Koordination der Geräte vereinfacht werden (Salviotti et al. 2018; Huh et al. 2017). Dadurch würde die Fehleranfälligkeit reduziert und betreiberseitige Kosten für die Instandhaltung von Datenzentren verringert, indem die Speicherkapazität zwischen den einzelnen Geräten verteilt wird (Salviotti et al. 2018).

Eine weitere Einsatzmöglichkeit für die Blockchain ist die dezentrale Cloud-Speicherung. Auf einer Blockchain-Plattform können Nutzer bereits heute überschüssige Speicherkapazität anbieten. Dokumente können so ohne den Einbezug eines Dritten mit Hilfe der verteilten Cloud-Speicherplattform gespeichert und genutzt werden (Nofer et al. 2017). Ein Beispiel für solch eine Plattform ist „Storj" (2020). Dabei handelt es sich um ein System, das es Menschen ermöglicht, ihren Festplattenspeicher an andere Benutzer auf der ganzen Welt zu vermieten, indem sie einen Kryptowährungstoken verwenden, mit dem die erbrachten Dienstleistungen bezahlt werden.

2.3 Datenschutzrechtliche Herausforderungen der Blockchain-Technologie

Der Einsatz von Blockchains, in denen personenbezogene Daten gespeichert werden, gilt in der öffentlichen Debatte und Fachliteratur weithin als nicht datenschutzkonform möglich. Deshalb legte die Bundesregierung in der Blockchain-Konsultation einen Schwerpunkt auf die Lösung der datenschutzrechtlichen Herausforderungen.

2.3.1 Anwendbares Recht

Der sachliche Anwendungsbereich der Datenschutz-Grundverordnung beschränkt sich nach Art. 2 Abs. 1 DSGVO auf die Verarbeitung personenbezogener Daten. Nach Art. 4 Nr. 1 DSGVO sind Daten personenbezogen, wenn sie sich auf eine identifizierte oder

identifizierbare Person beziehen. Identifizierbar ist eine Person, wenn sie direkt oder indirekt zu einer Kennung, Kennnummer, Standortdaten, Online-Kennung oder einem oder mehreren besonderen Merkmalen zugeordnet werden kann. Im Falle der Kryptowährung Bitcoin werden, wie in Kapitel 2 dargestellt, mit den jeweiligen Finanztransaktionen kryptografische Schlüssel gespeichert, mit denen einerseits der Nutzer, der die Transaktion durchführt, die Transaktion kryptografisch signiert und andererseits das Bitcoin-Netzwerk in Form der Netzknoten die Gültigkeit der Transaktionen überprüfen kann. Die Transaktionsdaten enthalten somit keine unmittelbaren Anhaltspunkte auf die Identität des jeweiligen Nutzers, sondern nur pseudonymisierte Daten. Diese Daten können allerdings durch andere Dienste (etwa Finanzmarktplätze, die den Tausch von Bitcoin zu konventioneller Währung erlauben oder Anbieter, die eine Zahlung von Waren oder Dienstleistungen mit Bitcoin ermöglichen) gegebenenfalls durch vorhandenes Zusatzwissen wieder einem Nutzer zugeordnet werden (Bechtolf und Vogt 2018).

Auch abseits der Bitcoin-Blockchain stellt sich die Frage, ob und wie personenbezogene Daten in der Kette gespeichert werden. So ist es möglich und in vielen Blockchain-Technologien üblich, dass zu jeder Transaktion Pseudonyme, wie der Public Key gespeichert werden (CNIL 2018), welcher ein personenbezogenes Datum darstellt (Finck 2017). Zudem könnte die IP-Adresse, welche für eine Transaktion eingesetzt wurde, durch Dritte identifiziert werden (Biryukov und Tikhomirov 2014). Vielfach ist auch davon die Rede, dass durch Hashing-Verfahren Anonymität zustande kommt und somit die DSGVO keine Anwendung findet. Dies ist jedoch nicht der Fall, da Hashing als Pseudonymisierung angesehen wird (Maxwell und Salmon 2017). Zu beachten ist auch, dass je nach Blockchain-Anwendung beliebig viele weitere personenbezogene Daten auf der Blockchain gespeichert werden können. Nach den Grundsätzen des EuGH (EuGH 2016) ist damit davon auszugehen, dass die Blockchain jedenfalls indirekt identifizierbare Daten enthält, da im Einzelfall rechtliche Möglichkeiten bestehen, diese Zusatzinformationen durch den jeweiligen Anbieter zu erlangen und dadurch einen konkreten Personenbezug herzustellen.

Der räumliche Anwendungsbereich der Datenschutz-Grundverordnung wird in Art. 3 DSGVO geregelt. Nach Abs. 1 ist die DSGVO räumlich anzuwenden auf alle Verarbeitungen im Rahmen der Tätigkeit einer Niederlassung eines Verantwortlichen in der EU. Zudem ist die DSGVO nach Abs. 2 anzuwenden auf die Verarbeitung von personenbezogenen Daten von Personen, die sich in der Union befinden, durch einen Verantwortlichen, der sich nicht in der EU befindet und dieser den betroffenen Personen Waren oder Dienstleistungen anbietet (Abs. 2 lit. a) oder der das Verhalten von betroffenen Personen in der EU beobachtet (Abs. 2 lit. b). Hierbei stellt sich die Frage nach dem Verantwortlichen in einer Blockchain. Nach Art. 4 Nr. 7 DSGVO ist ein Verantwortlicher jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. In der Blockchain sind dies alle Teilnehmer, welche nach Art. 26 DSGVO gemeinsam verantwortlich sind (Bäcker et al. 2018; Schrey und Thalhofer 2017). Problematisch ist in diesem Zusammenhang, dass der einzelne Nutzer nur einen kleinen Beitrag zur Verarbeitung leistet (Bechtolf und Vogt 2018) und die Aufgaben des Verantwortlichen (insb. die Gewährleistung der Löschung personenbezogener Daten, vgl. 2.3.3) regelmäßig nicht übernehmen können wird. Genauso treten Probleme bei der Umsetzung einer solchen Verantwortlichkeit sowie bei der Grenzziehung zwischen den einzelnen Verantwortlichen auf. Einen Sonderfall stellt die private oder konsortiale Blockchain dar, welche eine zentrale Zulassungsverwaltung vorweisen. In diesem Fall ist derjenige verantwortlich, der die Blockchain verwaltet. Alle anderen Beteiligten könnten aber ggf. Auftragsverarbeiter sein (Martini und Weinzierl 2017).

2.3.2 Erlaubnistatbestände

Die Speicherung der personenbezogenen Daten in einer Blockchain muss wie jede andere Verarbeitung auf einen der Erlaubnistatbestände aus Art. 6 Abs. 1 DSGVO gestützt werden können. Die Anwendbarkeit der einzelnen Rechtsgrundlagen sowie ihre Grenzen hängen allerdings von der konkreten Implementierung der Blockchain ab. Allein die rechtlichen Implikationen, die von der Nutzung der verschiedenen Arten möglicher Blockchains abhängen, also privater, öffentlicher oder konsortialer Blockchain, sind selbst ohne Berücksichtigung des eigentlichen Verarbeitungszweckes erheblich.

Möglich wäre eine Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO. Eine ausdrückliche informierte Einwilligung ist jedoch dann nicht anzunehmen, wenn, wie bei einer öffentlichen Blockchain, laufend neue Nodes hinzukommen und sich somit schon die maßgeblichen Verantwortlichen ständig ändern. Wenn die Verantwortlichen aber im Moment der Einwilligungserteilung nicht genau feststehen, kann die für eine wirksame Einwilligung erforderliche Transparenz über die anderen Teilnehmer der Blockchain nicht hergestellt werden (Schrey und Thalhofer 2017). Anders kann es dann zu werten sein, wenn es sich um eine private Blockchain handelt, alle Netzwerkknoten also feststehen und somit eine Einwilligung in Bezug auf alle Akteure erteilt werden kann. Eine Rechtfertigung nach Art. 6 Abs. 1 lit. a DSGVO dürfte aber in vielen Fällen ausgeschlossen sein.

Die zweite denkbare Möglichkeit wäre, die Verarbeitung auf die Erfüllung eines Vertrags nach Art. 6 Abs. 1 lit. b DSGVO zu stützen. Diese Möglichkeit ist je nach Zweck der Blockchain denkbar (Schrey und Thalhofer 2017). Jedenfalls bei einer öffentlichen Blockchain stellen sich ähnliche Probleme wie bei der Einwilligung, da die Vertragspartner zum Zeitpunkt des Vertragsschlusses feststehen müssen; sie sind *essentialia negotii*, also unverzichtbare Bestandteile eines wirksamen Vertrags. Problematisch bei einer öffentlichen Blockchain ist, dass die Teilnehmer der Transaktionsräume zu keinem Zeitpunkt in unmittelbarem Kontakt zu Blockchain-Registrars treten. Die Transaktionsdaten werden an keinen bestimmten Registrar kommuniziert, sondern an das Netzwerk übermittelt, wo sie im Rahmen der dezentralen Koordination in die Rechenoperation aller an der Validierung beteiligten Teilnehmer einfließen (Hofert 2017). Aus diesem Grund lässt sich ein rechtsgeschäftsähnliches Schuldverhältnis kaum konstruieren, weil sich dieses dadurch auszeichnet, dass die Parteien einander zu Rücksichtnahme und Vertrauen verpflichtet sind, wie dies üblicherweise in Vertragsverhandlungen oder Vertragsanbahnungen im bilateralen Verhältnis der Fall ist. Die dezentrale Ausgestaltung der öffentlichen Blockchain läuft jedoch einer solchen Einordnung der Rechtsbeziehung zwischen Registrars und Nutzern der Blockchain zuwider (Hofert 2017).

In Betracht kommt zudem die Möglichkeit, die Datenverarbeitung auf berechtigte Interessen zu stützen, also Art. 6 Abs. 1 lit. f DSGVO. Damit die Interessenabwägung zu Gunsten des bzw. der Verantwortlichen ausfiele, dürften die Interessen der betroffenen Person dagegen nicht überwiegen. Gerade in den Fällen, in denen eine öffentliche Blockchain zum Einsatz kommt, dürfte die Interessenabwägung regelmäßig zu Gunsten der betroffenen Person ausfallen, da nicht ersichtlich ist, wieso sie es hinnehmen müsste, dass ihre personenbezogenen Daten bei einer unbestimmten Anzahl an Verantwortlichen verarbeitet wird (Schrey und Thalhofer 2017). Anders könnte es zu werten sein, wenn die betroffene Person ein eigenes Interesse an der konkreten, verteilten (und dadurch besonders gefahrengeneigten) Form der Datenverarbeitung hätte. Im Falle von privaten Blockchains dürfte die Abwägung regelmäßig anders ausfallen, da hier in der Regel nur eine begrenzte Anzahl an Netzwerkknoten agieren. Maßgeblich käme es bei der Frage der Interessenabwägung somit auf die konkreten personenbezogenen Daten (Robrahn und Bremert 2018), die innerhalb der Blockchain gespeichert würden, sowie auf die konkrete technische Ausgestaltung der Blockchain an. Die Datenverarbeitung

auf Art. 6 Abs. 1 lit. f DSGVO zu stützen, dürfte demnach erheblichen rechtlichen Zweifeln begegnen.

2.3.3 Betroffenenrechte

Wie bei jeder Datenverarbeitung, die in den Anwendungsbereich des Datenschutzrechts fällt, muss auch bei Blockchain-Anwendungen die Ausübung der Betroffenenrechte gewährleistet sein. Sie umfassen die Informationsrechte nach Art. 13 und 14 DSGVO, das Auskunftsrecht nach Art. 15 DSGVO, das Berichtigungsrecht nach Art. 16 DSGVO, das Löschungsrecht nach Art. 17 DSGVO, das Einschränkungsrecht nach Art. 18 DSGVO, das Recht auf Datenübertragbarkeit nach Art. 20 DSGVO sowie bei einer auf Art. 6 Abs. 1 lit. e oder f DSGVO gestützten Datenverarbeitung das Widerspruchsrecht nach Art. 21 DSGVO. Die Betroffenenrechte sind von dem Verantwortlichen oder den gemeinsamen Verantwortlichen umzusetzen. Wie dargelegt, sind bei einer Blockchain alle Teilnehmer gemeinsam verantwortlich. Das bedeutet, dass sich betroffene Personen zur Geltendmachung ihrer Betroffenenrechte an jeden Teilnehmer der Blockchain wenden können müssen. Die Details sind auch hier abhängig von dem zugrundeliegenden Anwendungsfall. Informationsrechte der betroffenen Person aus Art. 13 und 14 DSGVO sollen sicherstellen, dass die betroffene Person umfassend beispielsweise über die Art und Weise der Datenerhebung, den Zweck, die Dauer, die Rechtsgrundlagen und Empfänger der Daten informiert wird. Im Falle der Speicherung personenbezogener Daten auf einer öffentlichen Blockchain, könnte jeder beliebige Teilnehmer dieser Blockchain die Auskunfts- und Informationsrechte theoretisch umsetzen. Das Problem der Bestimmung aller Teilnehmer bliebe dabei weiterhin erhalten. Schwieriger umzusetzen wären Auskunfts- und Informationsrechte hingegen im Falle einer öffentlichen Blockchain dann, wenn personenbezogene Daten Off-Chain gespeichert würden, dies aber von den dafür Verantwortlichen nicht transparent gemacht würde. In diesem Fall wären weder die Teilnehmer noch die Off-Chain gespeicherten Daten bekannt. Für das Recht auf Auskunft sind die Voraussetzungen des Art. 15 DSGVO zu erfüllen. Die betroffene Person muss also beispielsweise über die Verarbeitungszwecke, die verarbeiteten Kategorien personenbezogener Daten, die Empfänger der Daten und weitere Vorgaben informiert werden. Sofern sich diese Parameter automatisiert darstellen lassen, könnte das Auskunftsrecht nach Art. 15 DSGVO mittels einer entsprechenden technischen Gestaltung umgesetzt werden. Die betroffene Person würde dann einen entsprechenden Abruf starten und alle Informationen automatisiert erhalten.

Das Recht auf Löschung aus Art. 17 DSGVO und auf Berichtigung aus Art. 16 DSGVO stehen im Konflikt mit dem maßgeblichen Kriterium einer Blockchain, dem Grundsatz der Unveränderlichkeit der dort gespeicherten Daten. Der Art. 16 DSGVO ist im Gegensatz zu Art. 17 DSGVO voraussetzungslos, d. h., dass unrichtige Daten unverzüglich zu berichtigen sind (Schrey und Thalhofer 2017). Die Berichtigung wäre vergleichbar mit einer Löschung und der erneuten, korrekten Speicherung eines Datums. Zur Lösung dieses Konflikts werden mehrere technische Ansätze zur Veränderbarkeit von Blockchain-Einträgen diskutiert. Zu nennen sind hierbei bspw. das sog. „Forking", also die Abspaltung von den vorgegebenen Regeln einer Blockchain und der Aufbau einer neuen Kette (Fridgen et al. 2019), die „51%-Attacke" (Bechtolf und Vogt 2018) und das „Pruning", also das Löschen von Transaktionsdaten aus dem Transaktionsteil eines Blocks (Martini und Weinzierl 2017), was allerdings nur bei „alten" unwichtigen Daten möglich ist (vgl. die Diskussion in Unterkapitel 4.1.1).

Das Recht auf Löschung nach Art. 17 DSGVO ist an bestimmte Voraussetzungen gebunden. So besteht das Recht nur, wenn einer der in lit. a bis f genannten Gründe zutrifft (z. B. Widerruf der Einwilligung, Zweckfortfall, fehlende Rechtsgrundlage oder Widerspruch). Wurden die personenbezogenen Daten einer betroffenen Person von dem Verantwortlichen öffentlich gemacht, so hat dieser nach Abs. 2 angemessene Maßnahmen zu treffen, um alle Empfänger dieser Daten zu informieren, dass die be-

troffene Person ihr Recht auf Löschung geltend macht. Im Fall der Blockchain ist fraglich, ob die Daten öffentlich gemacht werden, denn alle Teilnehmer der Blockchain sind Empfänger der Daten und gleichzeitig verantwortlich für die Datenverarbeitung.

Nach Abs. 3 kann das Recht auf Löschung von der betroffenen Person nicht in Anspruch genommen werden, wenn z. B. Daten zur Erfüllung einer rechtlichen Verpflichtung oder zur Geltendmachung von Rechtsansprüchen notwendig sind. Abhängig von dem Zweck der Blockchain ist diese Ausnahme essenziell, z. B. bei Smart Contracts oder digitalen Registern, wobei nach Vertragserfüllung die Ausnahme des Abs. 3 wegfällt. Das Problem der Unveränderlichkeit der in der Blockchain gespeicherten Daten könnte in Bezug auf das Recht auf Löschung dahingehend gelöst werden, „dass es unionsrechtlich zulässig sei, keine physische Löschung der Daten vornehmen zu müssen, sondern dass es ausreiche, personenbezogene Daten in der Blockchain unkenntlich zu machen“ (Bundesnetzagentur 2019, S. 22).

Dieselbe Problematik wie bei dem Recht auf Löschung besteht bei dem Recht auf Einschränkung der Verarbeitung nach Art. 18 DSGVO, jedoch kann dieses Recht nur nach den dort genannten Voraussetzungen, beispielsweise bei Bestreiten der Richtigkeit der personenbezogenen Daten durch die betroffene Person oder bei erhobenem Widerspruch gegen die Verarbeitung der Daten, geltend gemacht werden. Eine Sperrung der Daten als milderes Mittel des Löschens war nach § 35 Abs. 3 BDSG a. F. zulässig (Schrey und Thalhofer 2017), die DSGVO sieht dies jedoch nicht vor.

Das Recht auf Datenübertragbarkeit aus Art. 20 DSGVO verpflichtet den Verantwortlichen, die personenbezogenen Daten, die ihm bereitgestellt wurden, in einem strukturierten, gängigen und maschinenlesbaren Format der betroffenen Person zugänglich zu machen. Die betroffene Person hat weiterhin das Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu übermitteln. Die Daten aus einer Blockchain wären leicht übertragbar, wenn sie im selben Format gespeichert wären. Wie bei vielen anderen Informationssystemen auch, gibt es bei den Blockchains jedoch eine große Heterogenität.

Es reicht nicht aus, wenn Änderungen oder Löschungen von Daten an einer Stelle erfolgen. Vielmehr müssten verbindliche Regeln existieren, die zu einer sicheren Propagierung dieser Änderungen im Netzwerk führen würden. Die dafür notwendigen technischen Änderungen dürften bei bestehenden (öffentlichen) Blockchain-Implementierungen kaum durchführbar sein, ohne nicht auch die Abwärtskompatibilität des Netzwerkes opfern zu müssen.

2.3.4 Automatisierte Entscheidung im Einzelfall

Wenn die Anwendung einer Blockchain zu einer automatisierten Einzelentscheidung führt, bspw. im Rahmen eines Smart Contracts, findet Art. 22 DSGVO Anwendung. In Abs. 1 des Artikels ist ein grundsätzliches Verbot einer automatisierten Einzelentscheidung festgelegt. Dieses Verbot gilt nicht, wenn die Entscheidung für den Abschluss eines Vertrags erforderlich ist (Art. 22 Abs. 2 lit. a DSGVO) oder eine Einwilligung vorliegt (Art. 22 Abs. 2 lit. c DSGVO). Für diese Rückausnahmen gilt das bereits für die Rechtsgrundlagen gesagte, insbesondere die Einschränkungen hinsichtlich der Erteilung von Einwilligungen und für den Schluss von Verträgen. Darüber hinaus wäre eine Zulässigkeit aufgrund von Rechtsvorschriften der Union oder des Mitgliedstaates (Art. 22 Abs. 2 lit. b DSGVO) möglich. Denkbar wäre dies im Rahmen von regulatorischen Gestaltungsvorschlägen, z. B. für öffentliche Register.

2.4 Herausforderungen der Blockchain-Technologie jenseits des Datenschutzes

Während die Blockchain-Literatur tendenziell von der Darstellung von Potenzialen der Technologie dominiert wird, werden grundsätzliche Kritikpunkte im Hinblick auf die Idee der Blockchain als alternative Vertrauensinfrastruktur, die nicht in den Bereich des Datenschutzes fallen, seltener formuliert. Dieses Unterkapitel greift daher einige dieser Kritikpunkte auf und stellt sie kurz vor.

Blockchain gilt mitunter als Technologie, die Vertrauen überflüssig macht, da Transaktionen hier transparent und dezentral dokumentiert werden. Eine solche Sicht übersieht in naiver Weise die grundsätzlich soziale Einbettung jedweder Technologie. Eben diese Einbettung lässt eher eine durch Blockchain hervorgerufene *Verschiebung*, als eine *Abschaffung* von Vertrauen erwarten. Dies lässt sich anhand verschiedener Problemstellungen verdeutlichen, die wir im Folgenden kurz skizzieren möchten:

- ***Transparenz & Irreversibilität***: Sozialformationen verfügen nicht nur über Kulturtechniken des Speicherns, sondern auch des Löschens – Kontextabhängig kann Reversibilität genauso vertrauensfördernd wirken (z. B. Recht auf Vergessen), wie Irreversibilität (z. B. Nachvollziehbarkeit von Geldströmen). Die Einführung einer Technologie, die erbarmungslos Löschbarkeit unterminiert – somit also dauerhafte, totale Transparenz und damit auch Kontrolle generiert – dürfte in bestimmten Bereichen Vertrauen eher zerstören. Zu denken ist hierbei etwa an die Mitteilung von Krankheitsgeschichten, politische Äußerungen oder die Überwachung am Arbeitsplatz, wenn alle Arbeitsschritte aufgezeichnet werden.
- ***Das Garbage in-/Garbage out-Problem***: Damit in engem Zusammenhang steht die Frage, welche Instanzen eigentlich kontrollieren können sollen, welche Inhalte in die Blockchain geschrieben werden. Denn sind die fehlerhaften Daten einmal gespeichert, so kann man diese nicht mehr löschen. Vertrauensvorschüsse werden also lediglich verschoben: Nur wenn der eintragenden Instanz vertraut wird, wird der dahinterliegenden Technologie vertraut – denn der Technologie selbst werden nur einige wenige Expert*innen trauen. Und es ist kaum zu erwarten, dass viele Menschen in der Lage sein werden, das für den Vertrauenserwerb notwendige Fachwissen zu erwerben. Dieses Problem vervielfacht sich schließlich im Falle öffentlicher Blockchains, in denen keinerlei Zugangskontrolle vorgesehen ist.
- ***Technischer Dezentralitätsmythos***: Damit stellt sich auch gleich die Frage, inwiefern die Blockchain das Versprechen der Dezentralität einzuhalten vermag, wenn sie erst einmal sozial verankert ist. An dieser Stelle ist unbedingt vor Fehlschlüssen von technischer Strukturierung auf soziale Institutionalisierung zu warnen: Internet und World Wide Web wurden lange Zeit aufgrund ihrer technisch dezentralen Struktur als quasi-automatische Dezentralisierungsagenturen verstanden, in der Hoffnung, dass sie das zentralistische Broadcasting-Schema traditioneller Medien durch eine demokratisierende Netzwerkstruktur ersetzen würden. Aktuell sind vielfach rezentralisierende sozio-technische Vorgänge zu beobachten, von Netzwerk- und Lock-In-Effekten über Monopolisierung bis hin zum „nationalen Internet“, wie es in Teilen der Welt längst praktiziert wird. All dies ist nicht besonders vertrauenerweckend und lässt vermuten, dass auch die Blockchain nicht einfach Intermediäre ausschalten wird: Gesellschaften werden auch zukünftig auf vertrauensschaffende Instanzen und Vermittler, auf institutionelle Intermediäre angewiesen sein.

- ***Technokratisches Vertrauen***: Doch selbst wenn gesellschaftliche Akteure der Blockchain durchweg „vertrauten", würde dabei Vertrauen doch eher durch technokratisches Kalkül ersetzt: An die Stelle der sozialen Produktion von allgemeinverbindlichen Vertrauensnormen träte dann das garantierte Wissen um die Erfüllung der eigenen Erwartungen. Dem Gegenüber muss gar nicht mehr vertraut werden, weil die Technik die Einhaltung der Regeln erzwingt. Dies mag in manchen gesellschaftlichen Bereichen wünschenswert erscheinen, dürfte sich aber in anderen Bereichen eher nachteilig auswirken. Überspitzt formuliert: Wenn alle Akteure immer und überall regelkonform handelten, bloß, weil sie sich dazu technisch gezwungen sehen, würde die gesellschaftliche Reproduktion allgemeinverbindlicher Spielregeln verlernt. Dass dieses Szenario eintritt, ist eher unwahrscheinlich, zu erwarten wäre eher, dass Vertrauen sich auch in dieser Hinsicht eher verschiebt, als verschwindet.

Damit weist auch dieses Szenario darauf hin, dass demokratische Gesellschaften auf Vertrauen angewiesen sind und dies auch zukünftig bleiben werden. Das Blockchain-Versprechen einer Abschaffung von – gesellschaftlich stets auszuhandelndem – Vertrauen, erweist sich somit als Chimäre. Die Blockchain scheint deshalb bloß in jenem engen Anwendungsbereich einsetzbar, in dem maximale Transparenz und technische Zuverlässigkeit Vertrauen flankieren müssen – nicht umsonst wird in der Debatte immer wieder das Beispiel des Grundbuchs genannt. Hierfür und im Falle ähnlich gelagerter Anwendungsbereiche, wie beispielsweise Geburtenregister, scheint der Einsatz der Blockchain denkbar – in vielen anderen Gesellschaftsbereichen dagegen keineswegs.

3 Datenschutz und Blockchain: Analyse des Diskurses im Rahmen der Blockchain-Konsultation

Dieses Kapitel widmet sich der Analyse des Blockchain-Diskurses anhand der im Rahmen der Blockchain-Konsultation eingegebenen Antworten der Stakeholder. Nach einer kurzen Einführung in die Methodik (3.1), widmen wir uns zunächst der Frage nach, wie wichtig den Stakeholdern die datenschutzrechtlichen Herausforderungen sind (0). Im Anschluss wird untersucht, welche Herausforderungen (3.3) für die Antwortenden wichtig waren und welche möglichen Lösungsansätze (3.4) sie sehen.

Grundlage der Analyse war das von den zuständigen Ministerien veröffentlichte Dokument, das alle zur Veröffentlichung freigegebenen Antworten enthält (BMWi und BMF 2019).[6]

3.1 Methodik

Das initiale Dokument hat 1048 Seiten und umfasst insgesamt 6261 inhaltliche Statements. Diese wurden in ein maschinenlesbares Tabellen-Format überführt. Im Anschluss wurden mittels einer Schlagwortsuche[7] die datenschutzrelevanten Statements extrahiert, sodass 537 inhaltliche Statements von insgesamt 94 Akteuren (72 %) analysiert werden konnten. Im nächsten Schritt wurde Branchenzugehörigkeit der 94 Akteure, die sich zum Datenschutz geäußert haben, erfasst (vgl. Abbildung 2). Eine Vielzahl der Akteure stammt aus der IT-Branche (38 %), gefolgt von den Bereichen Forschung (18 %) und Finanzen (13 %).

[6] Weil in dem Dokument nur jene Stellungnahmen veröffentlicht wurden, die von den Autoren bzw. den Ministerien freigegeben wurden, sind darin 130 der 158 Stellungnahmen doukumentiert.

[7] Diese beinhaltete die Suchbegriffe „Datenschutz“, „Privatsphäre“, „personenbezogen“, „persönliche Daten“, „private Daten“, „Privacy“, „DSGVO“, „DS-GVO“ und „GDPR“ (groß/kleinschreibungsunabhängig, inkl. Teilworte).

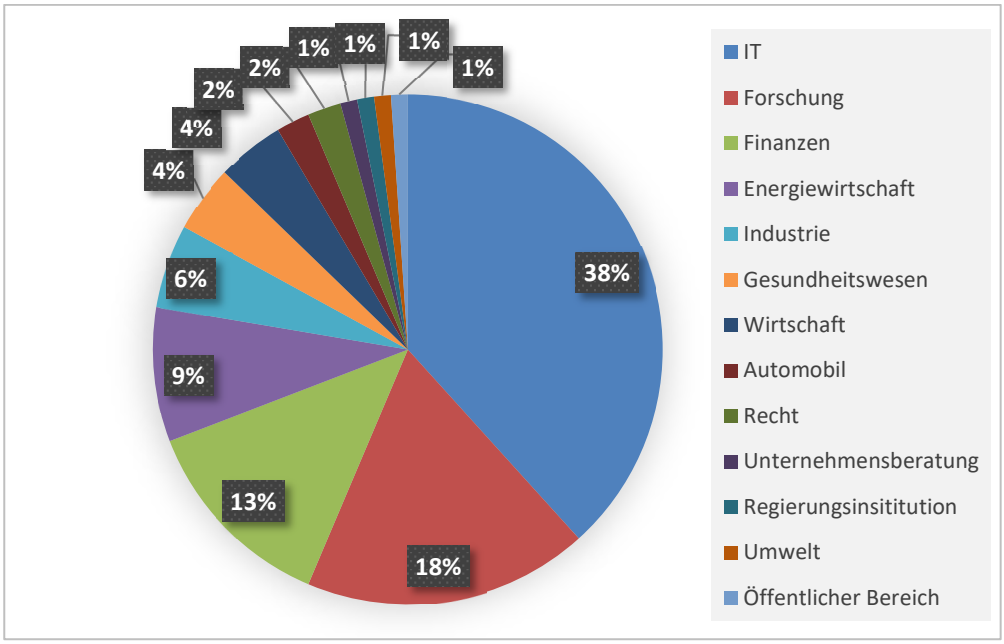


Abbildung 2: Branchenzugehörigkeit aller Akteure, die sich zum Datenschutz geäußert haben (eigene Auswertung)

Die datenschutzrelevanten Statements wurden im Hinblick auf drei Themenkomplexe codiert. *Erstens* interessierte die Frage, für wie relevant das Thema Datenschutz und Blockchain im Allgemeinen befunden wird; *zweitens* interessierte die Frage, welche spezifischen Herausforderungen seitens der Akteure genannt wurden; und *drittens*, welche Lösungen zur Adressierung der genannten Herausforderungen vorgeschlagen wurden. Diese Themenkomplexe wurden selbst wieder in verschiedene Argumente und Aussagen unterteilt. Außerdem wurde stets mitcodiert, ob ein Akteur die Antwort abhängig von einem vorgegebenen Anwendungsfeld[8] in einer Frage oder allgemein gegeben hat, z. B.:

Beispiel - Anwendungsfeld „Gesundheit/Pflege“: „Wie könnten datenschutzrechtskonforme Lösungen zur Anwendung von Blockchain aussehen, vor dem Hintergrund der besonderen Anforderungen im Umgang mit Gesundheitsdaten?“

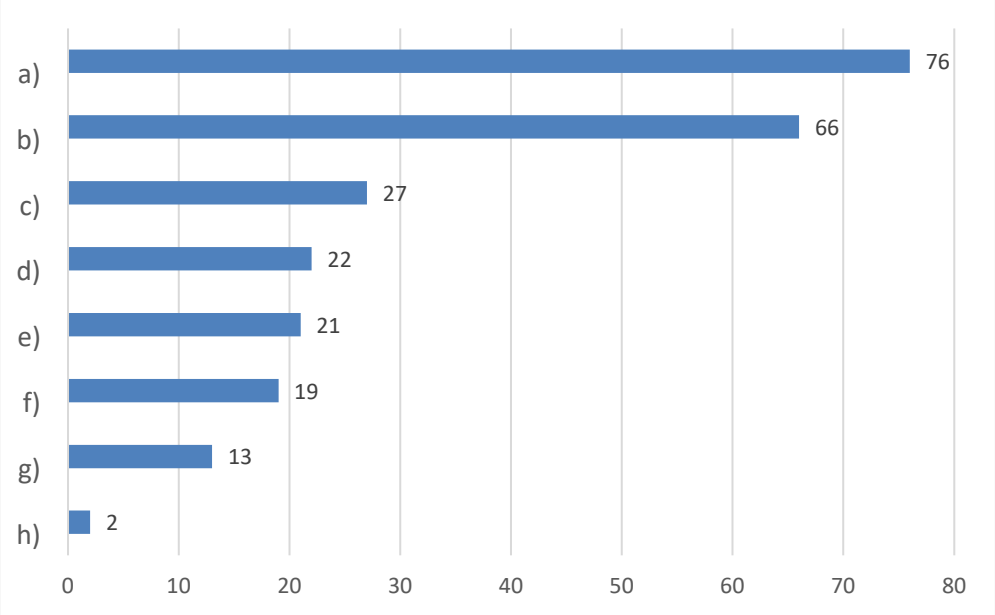
Beispiel - Allgemein: „Welche Governance-Aspekte sind bei internationalen Blockchain-Anwendungen mit öffentlicher Beteiligung zu beachten?“

3.2 Themenkomplex 1: Relevanz von Datenschutz in der Blockchain

Zur Auswertung der Relevanz von Blockchain und Datenschutz im Allgemeinen, wurden die Statements der Akteure den in Abbildung 3 aufgelisteten Kategorien zugeordnet. So waren 76 der 94 Akteure (a, 81 %) der Meinung, dass die Gewährleistung des Datenschutzes bei Blockchain-Anwendung eine Herausforderung darstellt, die es zu

[8] Diese sind: Finanzsektor, Energie, Gesundheit/Pflege, Mobilität, Lieferketten/Logistik, Internet der Dinge, Identitäten-/Rechtemanagement, Verwaltung, Plattformökonomie (BMWi und BMF 2019).

lösen gilt. Davon gaben 66 Akteure (b, 70 %) an, dass sie die Lösung der datenschutzrechtlichen Herausforderungen für möglich halten, während 21 Akteure (e, 22 %) der Meinung waren, dass der Datenschutz überhaupt keine Herausforderung darstelle. Insgesamt 19 Akteure (f) bewerteten die datenschutzrechtlichen Probleme hingegen als dermaßen schwerwiegend, dass sie diese für einen „Show Stopper" hielten. Das bedeutet, dass die Nutzung der Blockchain aufgrund der Datenschutzbestimmungen unmöglich sei, falls keine technischen und/oder organisatorischen Maßnahmen getroffen werden. Einige Akteure (d, 22 bzw. 23%) waren der Ansicht, dass jedes Problem und jede Lösung im Einzelfall zu prüfen sei und Pauschalaussagen schwer zu treffen seien. 13 Akteure (g, 14 %) äußerten sich dahingehend, dass die Lösung der datenschutzrechtlichen Herausforderungen nur auf Kosten von Funktionalität bzw. Nutzen möglich wäre. 27 Akteure (c, 29 %) waren hingegen der Meinung, dass mittels des Einsatzes von Blockchain-Technologien sogar eine Verbesserung des Datenschutzes möglich sei. Hier führten sieben Akteure (7 %) vor allem das Konstrukt der „Self-Sovereign Identity" an, womit Nutzende festlegen und nachvollziehen können sollen, wie ihre Daten verwendet werden dürfen (Laurence 2019; Stokkink und Pouwelse 2018). Nur zwei Akteure (h) vertraten die Meinung, dass die anzutreffenden Datenschutz-Herausforderungen Unternehmen davon abschrecken, auf Blockchain-Lösungen zurückzugreifen.



a) Datenschutz stellt eine Herausforderung dar
b) Lösung der Herausforderung ist möglich
c) Blockchain kann zur Stärkung des Datenschutzes beitragen
d) Muss im Einzelfall geprüft werden
e) Datenschutz stellt keine Herausforderung dar
f) Datenschutzrechtliche Herausforderungen stellen einen Show Stopper dar
g) Nur mit Kompromissen möglich
h) Datenschutzrechtliche Herausforderungen schrecken Unternehmen ab

Abbildung 3: Relevanz von Datenschutz und Blockchain (eigenen Auswertung, Mehrfach-Codierung möglich)

Eine Auswertung der Relevanz anhand der in der Konsultationsvorlage vorgegebenen Anwendungsfelder (Abbildung 4) zeigt eine ungefähr gleichmäßige Verteilung von Problemanerkennung, Lösungsmöglichkeiten und Show Stopper-Effekten.

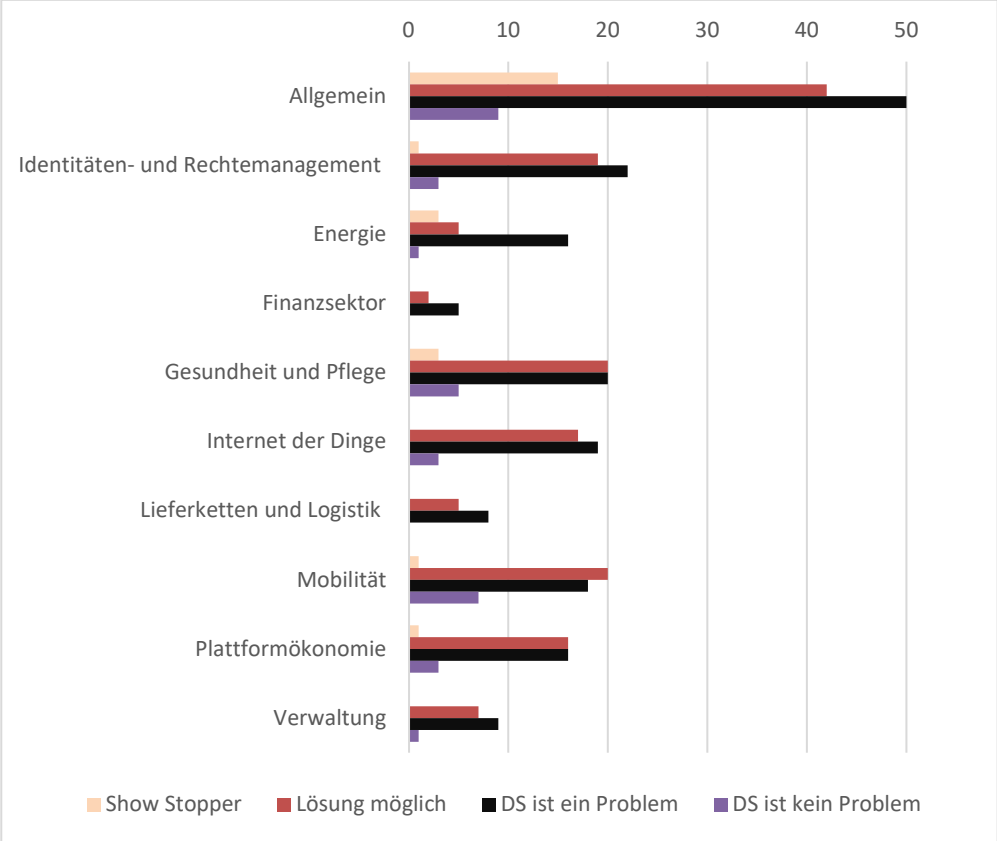


Abbildung 4: Relevanz von Datenschutz und Blockchain, gruppiert nach den in der Konsultation vorgegebenen Anwendungsfeldern (eigene Auswertung, Mehrfach-Codierung möglich).

Im Allgemeinen zeigen die Ergebnisse dieses Untersuchungsschritts, dass zwar eine Mehrzahl der Akteure erhebliche Herausforderungen im Zusammenhang mit der datenschutz-kompatiblen Nutzung von Blockchain-Anwendungen erkennt. Zugleich demonstrieren die Ergebnisse, dass eine fast ebenso große Mehrzahl der Akteure der Ansicht ist, dass eine Lösung der datenschutzrechtlichen Herausforderungen möglich ist.

3.3 Themenkomplex 2: Herausforderungen

Zur Frage von Herausforderungen im Kontext der Blockchain-Technologie nannten 53 Akteure die Gewährleistung der Betroffenenrechte (gruppiert)[9]. Von diesen bezeichneten 50 die Löschung als Hauptproblem, Berichtigung wurde von 38 und Datenübertragbarkeit von sechs Akteuren genannt. Die am zweithäufigsten (43-mal) genannte Herausforderung bildet die Sichtbarkeit der in einer Blockchain gespeicherten personenbezogenen Daten für alle Teilnehmer. Schließlich wurde das Problem der Bestimmbarkeit eines Verantwortlichen am dritthäufigsten (31-mal) genannt. Außerdem verwie-

[9] Diese Kategorie umfasst Löschung, Berichtigung, Betroffenenrechte (allgemein) und Datenübertragbarkeit,

sen sieben Akteure auf das Problem einer möglichen Speicherung der personenbezogenen Daten außerhalb der EU. Sieben Akteure bemängelten die unklare rechtliche Situation sowohl im Hinblick auf weltweit divergierende Rechtsrahmen, die die Nutzung einer globalen Blockchain erschwerten, als auch im Hinblick auf die aus ihrer Perspektive unklare Rechtslage in der EU.

Von weiterem Interesse sind die Herausforderungen, die mit vorgeschlagenen Lösungen einhergehen (siehe hierzu das Unterkapitel „Themenkomplex 3: Lösungsansätze" ab Seite 25). So äußerten sich 15 Akteure kritisch gegenüber aktuell eingesetzten Verschlüsselungstechnologien für personenbezogene Daten auf der Blockchain. 14 Akteure zweifelten die effektive Umsetzbarkeit der Pseudonymisierung an und betonten daher das Problem, dass Daten de-pseudonymisiert werden können (De-Pseudonymisierung). Sieben Akteure bemängelten die Sicherheit der Speicherung, die vor allem bei einer möglichen Off-Chain-Speicherung oder bei der Speicherung der zur Verschlüsselung benötigten Schlüssel zum Tragen komme. Vier Akteure äußerten Bedenken hinsichtlich der Integrität bzw. der Qualität des Inputs. Sie gaben an, dass es schwierig sei, die Korrektheit von Daten zu überprüfen, die sich auf Objekte der physischen Welt beziehen (Beispielsweise: Wie kann man sicher sein, dass Person A das Haus, welches sie als Besitzer in die Blockchain einträgt, wirklich besitzt? Es gibt keine Instanz die den tatsächlichen besitz bezeugen kann). Schließlich kritisierten jeweils drei Akteure die für eine wirksame Nutzung von Zero-Knowledge-Proofs (ZKP, siehe hierzu die detaillierte Erklärung dieser Methode auf Seite 30) benötigte Rechenleistung bzw. die effektive Umsetzbarkeit der Anonymisierung personenbezogener Daten.

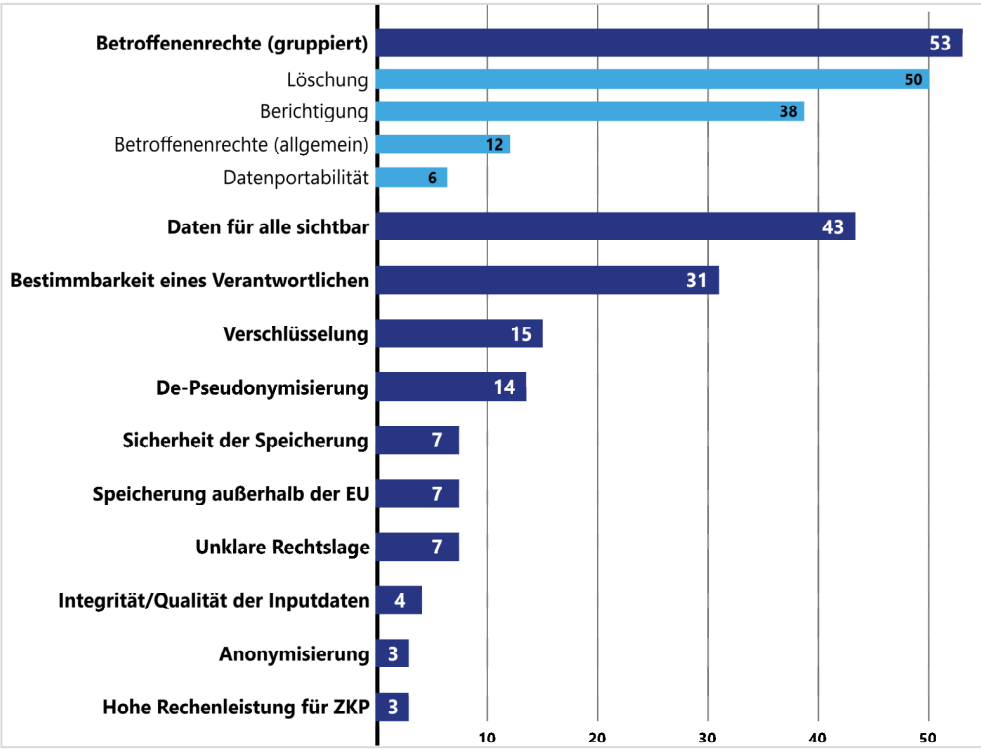


Abbildung 5: Seitens der Akteure identifizierte datenschutzrechtliche Herausforderungen im Zusammenhang mit Blockchain (eigene Auswertung, Mehrfach-Codierung möglich).

Eine Analyse der Herausforderungen anhand der in der Konsultation vorgegebenen Anwendungsfelder zeigt, dass es in den Feldern weitgehend ähnliche Herausforderungen gibt (Abbildung 6). Eine grundsätzliche Häufung findet sich jedoch im Allgemeinen. Jedoch gibt es Besonderheiten in manchen Anwendungsfeldern. Für den Bereich

Gesundheit und Pflege (39 verschied. Nennungen) sowie für das Identitätsmanagement (40 verschied. Nennungen) zeigen sich besonders viele verschiedene Herausforderungen. Beinahe jede Art von Herausforderung zeigt sich beim Einsatz der Blockchain für die Plattformökonomie. Weiter zeigt sich, dass die Akteure Herausforderungen im Finanzsektor vor allen im Bereich der Betroffenenrechte sehen. In der öffentlichen Verwaltung stellen die Betroffenenrechte, die Sichtbarkeit der Daten dar. Zudem wurde erwähnt, dass die rechtliche Situation unklar sei, da z.B. Standards oder Empfehlungen von Datenschutzbehörden fehlen.

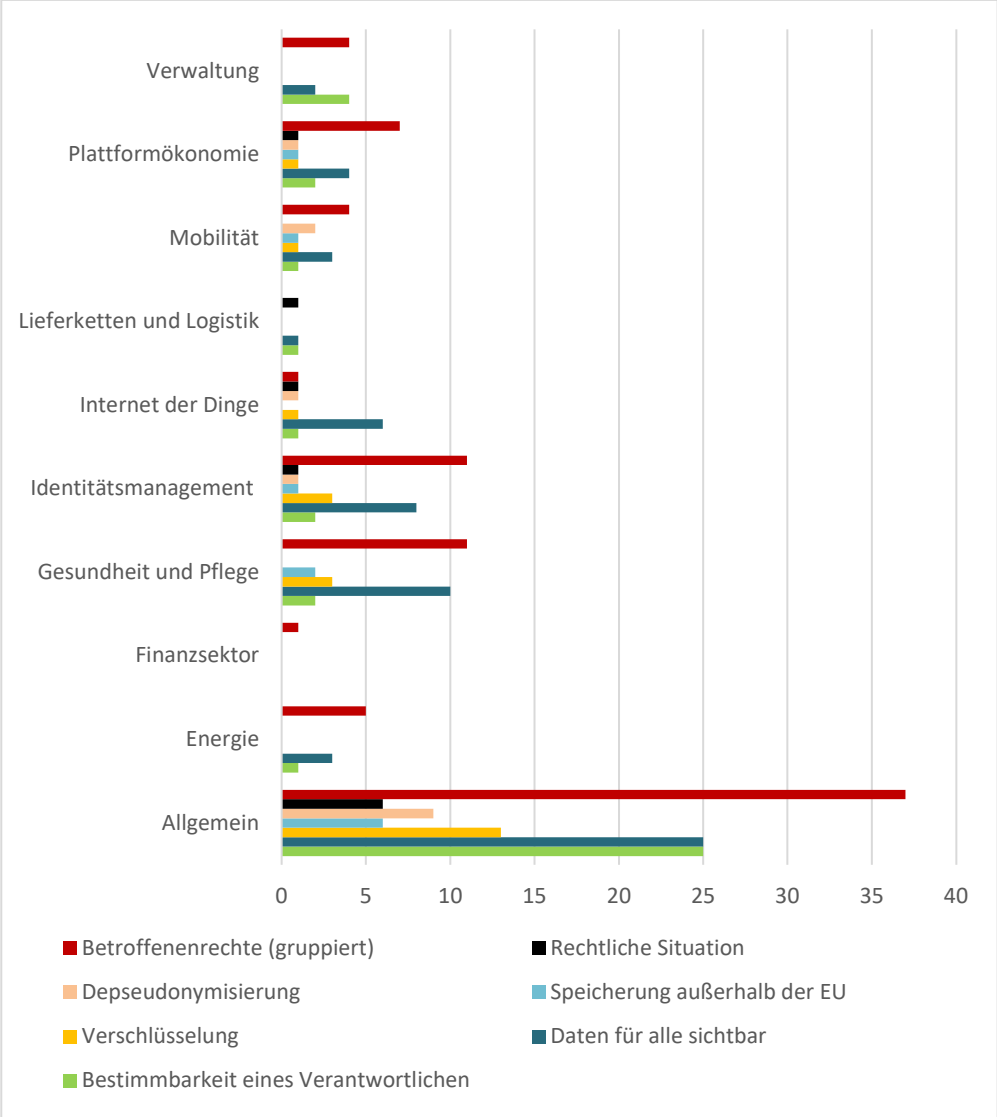


Abbildung 6: Seitens der Akteure identifizierte datenschutzrechtliche Herausforderungen im Zusammenhang mit der Blockchain, nach Anwendungsfeldern gruppiert (eigene Auswertung, Mehrfach-Codierung möglich)

3.4 Themenkomplex 3: Lösungsansätze

Wie bereits in Abbildung 3 gezeigt, war die Mehrheit der an der Konsultation beteiligten Akteure der Ansicht, dass eine Lösung der datenschutzrechtlichen Herausforderungen grundsätzlich möglich sei. Im Folgenden stellen wir kurz vor, welche Lösungsvorschläge seitens der Akteure genannt wurden.

Abbildung 7 zeigt, dass die Mehrzahl der beteiligten Akteure (62 bzw. 66 %) der Ansicht war, dass eine Lösung der datenschutzrechtlichen Herausforderungen bereits unter Rückgriff auf bestehende technische Verfahren möglich wäre. Der am zweithäufigsten genannte Vorschlag, den 38 Akteure (40 %) nannten, war, auf die Speicherung personenbezogener Daten in einer Blockchain schlicht zu verzichten. Daneben befürworteten 31 Akteure (33 %) eine Zugriffsbeschränkung in Form der Nutzung einer privaten oder halb-privaten Blockchain. 29 Akteure (31 %) sprachen sich für eine Anpassung der rechtlichen Grundlagen aus. Darunter fallen, wie in Abbildung 9 ersichtlich, die Konkretisierung und ggf. die Änderung der DSGVO, die Schaffung weltweit geltender Rechtsgrundlagen sowie die Zusammenarbeit mit anderen Ländern. Gleichzeitig waren 29 Akteure (31 %) der Meinung, dass technische Weiterentwicklungen und Standards erforderlich seien, um Blockchains datenschutzkonform betreiben zu können. Mithilfe von organisatorischen Maßnahmen, wie z. B. Nutzerrollen oder Datenaggregation, könne laut 17 Akteuren (18 %) eine Lösung für Datenschutzprobleme gefunden werden.

Eine detaillierte Auswertung der genannten Lösungsansätze pro Anwendungsbereich findet sich im Anhang in Tabelle 2 auf Seite 57. Hier zeigt sich, dass ein Großteil der durch die Akteure vorgeschlagenen Ansätze für den allgemeinen Einsatz der Technik, sowie im Identitätsmanagements und der Mobilität erwähnt werden.

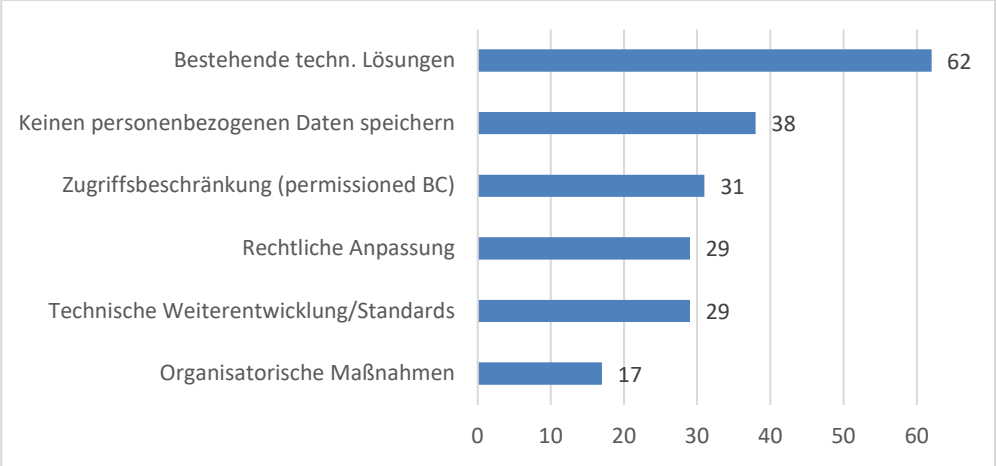


Abbildung 7: Seitens der Akteure vorgeschlagene Lösungen für datenschutzrechtliche Herausforderungen (eigene Auswertung, Mehrfachcodierung möglich)

3.4.1 Bestehende technische Lösungen

Wie bereits erwähnt, war eine Mehrheit der Akteure der Ansicht, dass bestehende technische Lösungen bzw. der aktuelle Stand der Technik ausreiche, um die datenschutzrechtlichen Herausforderungen der Blockchain auf angemessene Weise zu adressieren. Im Folgenden stellen wir alle unter dem Punkt "Bestehende technische Lösungen" subsumierte Lösungsvorschläge vor (Abbildung 8).

Mit großer Mehrheit führten die Akteure die Off-Chain-Speicherung (43, bzw. 46 %) an erster Stelle auf. Dicht gefolgt wird diese von Verschlüsselungstechniken (37, bzw. 39 %). 18 Akteure (19 %) betrachteten Methoden zur Pseudonymisierung als einen sinnvollen Lösungsansatz. Der Einsatz von Zero-Knowledge-Proofs (ZKP) stellte für 13 Akteure (14 %) eine mögliche Lösung dar. Zwölf Akteure (13 %) waren der Meinung, dass Löschmöglichkeiten in der Blockchain bereits grundsätzlich existierten. Darunter fällt z. B. das sog. Pruning, also das „Abschneiden" von alten Hash-Verkettungen. Der Rückgriff auf bestehende Anonymisierungstechniken wurde von elf Akteuren (12 %) erwähnt.

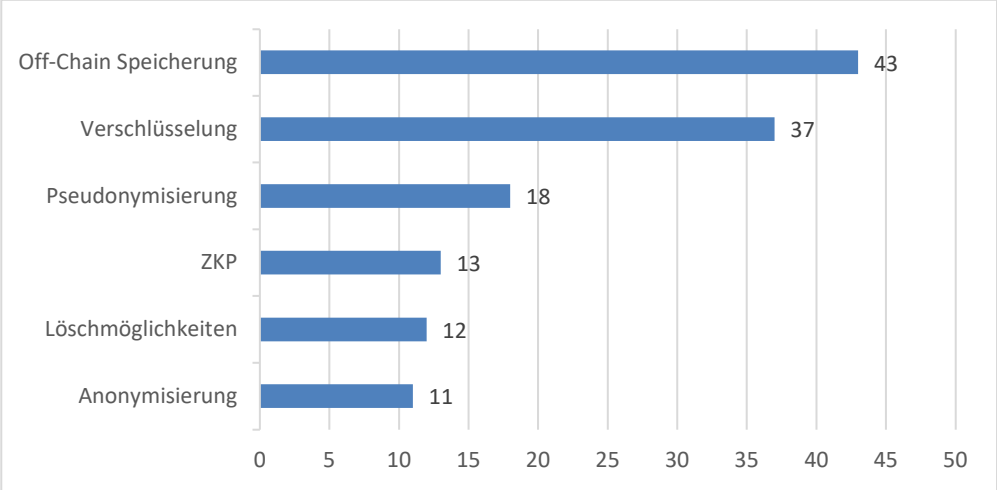


Abbildung 8: Alle unter dem Punkt "Bestehende techn. Lösungen" subsumierte Lösungsvorschläge (eigene Auswertung, Mehrfachcodierung möglich)

3.4.2 Rechtliche Anpassung

Da sich ein knappes Drittel der Akteure für eine rechtliche Anpassung aussprach, wird in diesem Absatz kurz dargelegt, worauf sich diese Forderung im Einzelnen bezogen hat (Abbildung 9). So hielten fast alle Akteure, die sich zu rechtlichen Anpassungen äußerten (27 von insgesamt 29 Akteuren bzw. 30 % aller beteiligten Akteure), eine Konkretisierung und ggf. auch Anpassung der DGSVO-Vorgaben für zielführend und nötig. Die Schaffung weltweit geltender Regeln (4 Akteure, 4 %), bzw. der Ausbau der Zusammenarbeit mit anderen Ländern (2 Akteure, 2 %) wurde hingegen von einer sehr geringen Anzahl von Akteuren befürwortet.

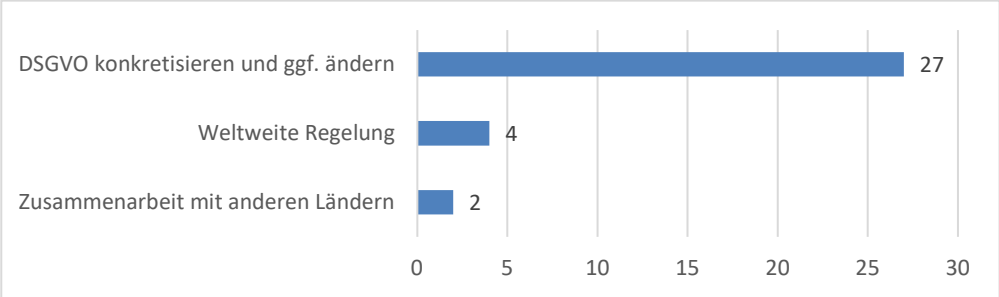


Abbildung 9: Alle unter dem Punkt "Rechtliche Anpassung" subsumierten Vorschläge (eigene Auswertung, Mehrfachcodierung möglich)

3.4.3 Organisatorische Maßnahmen

18 Prozent der Akteure äußerten sich dahingehend, dass sie organisatorische Maßnahmen für eine gangbare Lösung halten. Abbildung 10 zeigt die darunter subsumierten Vorschläge. So sprachen sich neun Akteure (10 %) für Nutzerrollen und -rechte innerhalb einer Blockchain Anwendung aus, sodass nicht jeder beliebige Anwender alle Daten einsehen kann. Die Zuweisung von verschiedene Schutzniveaus für verschiedene Arten von Daten, z. B. für Medizindaten, wurde von acht Akteuren (9 %) als Lösung angesehen. Zudem wurde die ausschließliche Speicherung von Datenaggregaten (3 Akteure, 3 %) genannt.

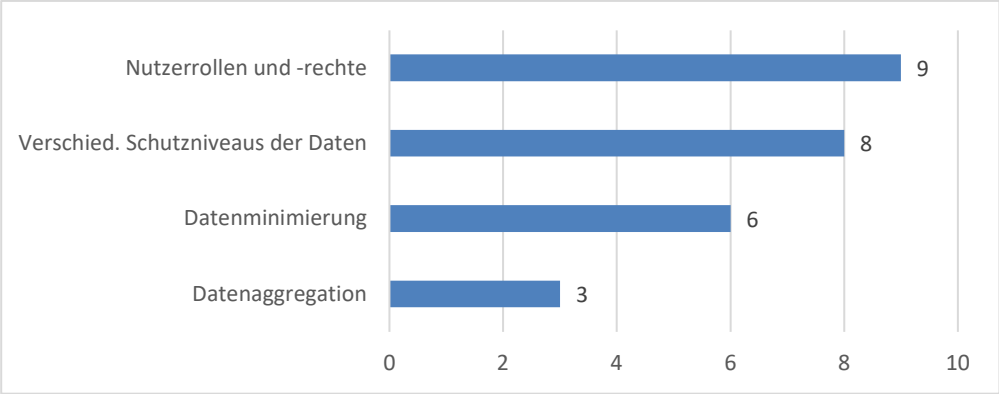


Abbildung 10: Alle unter dem Punkt "Organisatorische Maßnahmen" subsumierten Vorschläge (eigene Auswertung, Mehrfachcodierung möglich)

4
Bewertung der Aussagen der Akteure

In diesem Kapitel möchten wir erörtern, wie die Aussagen der Akteure einzuordnen sind. Wir nehmen Bezug zu einzelnen Aussagen und bewerten die festgestellten Probleme, als auch die vorgeschlagenen Lösungen anhand der Fachliteratur. Des Weiteren erläutern wir diese Probleme und Lösungen anhand von einigen Beispielen. Zudem gehen wir an einigen Stellen auf weitere, für den datenschutzrechtlichen Blockchain-Diskurs relevante Argumente und Aspekte ein, die im öffentlichen Diskurs sowie in der Fachliteratur diskutiert werden, jedoch von den an der Konsultationsphase beteiligten Akteuren nicht beachtet wurden. In Abbildung 14 (im Anhang auf Seite 55) geben wir eine Übersicht über alle genannten Probleme und zeigen, welche Lösungsansätze die Akteure in der Konsultation genannt haben und welche weiteren in der Fachliteratur vorgeschlagen werden.

Grundsätzlich zeigte die Auswertung der Akteursaussagen, dass Datenschutz in der Blockchain für die Mehrheit der Beteiligten (81 %) eine ernstzunehmende Herausforderung darstellt. Dies deckt sich z. B. mit den Ergebnissen einer großangelegten Umfrage von BITKOM überein, in der 66 % der befragten 1077 Unternehmen Datenschutz als Herausforderung bewerteten (Gentemann 2019, S. 39). Unsere Auswertung des Diskurses zur Blockchain-Konsultation zeigt darüber hinaus, dass 70 % der beteiligten Akteure die Herausforderungen zugleich als bewältigbar einstufen. Dies ist in der BITKOM-Umfrage nur für sehr wenige Teilnehmer (4 von 16 Experten) der Fall.

Somit zeigt unsere Auswertung auch, dass die Akteure grundsätzlich zwei Meinungsbilder zur Datenschutzthematik in der Blockchain haben. Während viele Akteure als Befürworter der Blockchain-Technologie angesehen werden können, stehen andere der Technologie eher kritisch gegenüber oder können keine allgemeingültige Aussage treffen. Auf die einzelnen Aussagen und deren Bewertung möchten wir im Folgenden eingehen.

4.1.1 Betroffenenrechte: Löschung und Berichtigung

Problembeschreibung
Das mit Abstand am häufigsten genannte Problem bezieht sich auf die Gewährleistung der Betroffenenrechte. Im Speziellen bezogen sich die Akteure auf Lösch- und Berichtigungsmöglichkeiten. Dass die Blockchain-Architektur auf die Unveränderbarkeit der darin gespeicherten Transaktionen ausgelegt ist und somit zunächst grundsätzlich nicht DSGVO-konform einsetzbar ist, stellt somit die zentrale Herausforderung dar.

Vorgeschlagene Lösungsansätze und Bewertung
Um dieses Problem zu umgehen, erwähnt eine Mehrheit der Akteure die sog. ***Off-Chain-Speicherung*** (auch als „Anchoring" bezeichnet), also das Speichern der Daten außerhalb der Blockchain. Der Speicherort könnte dabei ein normaler Server sein, auf welchem Daten auch gelöscht werden können. In der Blockchain selbst wird dann nur eine Referenz (ähnlich einem Link im Internet) auf die Datei gespeichert. Diese Referenzierung kann z. B. über einen Hashwert realisiert werden (siehe hierzu Kapitel 2). Da dieser Wert für jede Datei eindeutig ist, könnten Manipulationen an den Off-Chain gespeicherten Daten schnell erkannt werden, da die Referenzierung dann nicht mehr gültig wäre. Wenn die Datei gelöscht wird, würde zwar der Link weiterhin in der Blockchain stehen, jedoch würde dieser dann auf eine gelöschte Datei verweisen. Der entsprechende „Transaktionsblock kann aber weiterhin verifiziert werden und die Integrität der übrigen Transaktionen und der Blockchain als Ganzes bleibt erhalten" (BSI 2019, S. 63). Die problematische Speicherung personenbezogener Daten auf der

Blockchain würde also dadurch umgangen, dass diese außerhalb der Blockchain, d. h. Off-Chain gespeichert werden. Die Off-Chain-Speicherung würde somit die Löschung von Daten im Kontext der Blockchain ermöglichen. Hierfür gibt es bereits Lösungsansätze, um insbesondere große Datenmengen und Rechenoperationen, welche durch Smart Contracts ausgeführt werden, zu speichern und durchzuführen (Eberhardt und Tai 2017).

Wie bereits erwähnt, liegen die Daten bei der Off-Chain Speicherung nicht direkt in der Blockchain, sondern nur die Referenz zu Daten auf externen Servern. Somit muss, im Gegensatz zur eigentlichen Idee der Blockchain, dem Serverbetreiber vertraut werden, da dieser gespeicherte Daten nachträglich ändern könnte (mehr hierzu im Absatz zu Chamäleon-Hashfunktionen auf Seite 31). Der Einsatz von Hashwerten ist jedoch auch mit Herausforderungen verbunden. Zwar kann mittels Hash eine Originaldatei nicht „zurückgerechnet" werden. Jedoch kann bei einem kleinen Suchraum ein Hashwert relativ einfach einem konkreten Datensatz zugeordnet werden, z. B. indem viele Datensätze erneut gehashed und dann miteinander verglichen werden. Bei einem kleinen Suchraum ist diese „Trial and Error"-Herangehensweise vielversprechender als bei vielen möglichen Daten (Kohn und Tamm 2019; Niemzik 2019). Um dieses Problem zu umgehen, muss der zu hashenden Datei ein sog. „Secret" oder „Salt", also eine Zufallszahl, angefügt werden (LeBlanc und Howard 2002). Da diese Zufallszahl jedoch nur der Ersteller der Datei kennt, kann das mit dem Einsatz einer Blockchain verfolgte Ziel der Herstellung voller Transparenz nicht mehr gewährleistet werden. Selbst wenn die Zufallszahl an eine andere Stelle weitergegeben wird, wäre die Übermittlung nicht sicher, da diese nicht im Rahmen der Blockchain erfolgen würde. Eine mögliche Lösung für dieses Problem sind sog. „***Merkle-Trees***", welche auch von einigen Akteuren vorgeschlagen wurden. Dabei wird für jeden Datenpunkt ein eigenes „Salt" verwendet und die gehashten Dateien werden in einer Baumstruktur angeordnet. Schließlich wird nur dessen oberer Wert (Roothash oder Top-Hash) in der Blockchain gespeichert (Karame und Androulaki 2016). Abbildung 11 zeigt diese Baumstruktur.

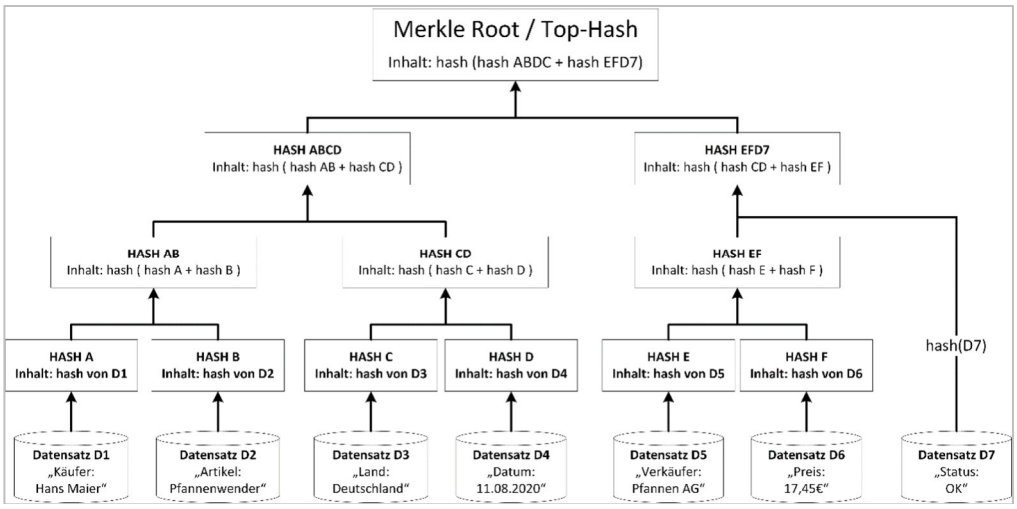


Abbildung 11: Merkle-Tree Baumstruktur (eigene Darstellung)

Eine weitere Lösung, welche sogar auf die Freigabe des „Salt" verzichtet, stellen die ***Zero-Knowledge-Proofs (ZKP)*** dar. Diese Lösung nannten 13 der an der Blockchain-Konsultation beteiligten Akteure. Bei ZKPs werden keine wirklichen Daten (kein „Wissen") einer Person benutzt, sondern vielmehr ein Beweis, dass das Datum existiert oder korrekt ist. ZKPs ermöglichen es somit, Antworten auf bestimmte Fragen zu erhalten, ohne dass die dahinterliegenden Daten bekannt werden. Wenn beispielsweise abgefragt wird, ob eine Person volljährig ist, erhält die fragende Stelle nur eine Ja-/Nein-

Antwort. Das Geburtsdatum bleibt aber weiterhin unbekannt. Diese Methode wird auch bei den Attribute Based Credentials (ABC) verwendet (Rannenberg et al. 2015). Doch auch hier gibt es Nachteile. Zum einen ermöglicht es potentiellen Angreifern den Hash-Wert zu erraten, da kein Secret mehr gebraucht wird. Es könnten also alle möglichen Werte (z. B. Geburtsdatum einer Person) als Input ausprobiert werden bis ein Beweis („Proof") verifiziert ist. Des Weiteren wird für ZKP eine erhebliche Rechenleistung benötigt (Morais et al. 2019; Bootle et al. 2016), was auch drei Akteure (3 %) kritisch anführten.

Bewertung der Aussagen der Akteure

Als weitere Löschmethoden nannten die Akteure „***Tombstones***" und „***Data Revocation Keys***". Beide Methoden zielen darauf ab, Daten als ungültig zu markieren, sodass diese nicht weiterverbreitet werden, obwohl es sich nicht um Löschung im klassischen Sinne handelt.

Zudem scheint das „***Forking***" auf den ersten Blick eine Lösung zu sein. Hierbei handelt es sich um eine irreversible Abspaltung von den vorgegebenen Regeln einer Blockchain und somit den Aufbau einer neuen Kette bzw. die Fortführung von zwei inkompatiblen Ketten (Fridgen et al. 2019). Ein Fork kommt beispielsweise dann vor, wenn in der Programmierung ein Fehler gefunden wurde, und dieser durch ein Update behoben werden muss. Da die neue Programmierung nicht mehr mit der alten Kette kompatibel wäre, kommt es zu einer Abspaltung (Orcutt 2018). Grundsätzlich löst dies das Problem der Unveränderlichkeit nicht. Denn es können keine Daten gezielt nachträglich entfernt werden. Lediglich der Aufbau einer neuen Kette und die komplette Löschung der alten Kette wäre hier eine Möglichkeit. Ob sich dies praktisch (bei einer unbestimmten Zahl an Teilnehmern) durchsetzen lässt, ist jedoch fraglich. Datenänderungen und Löschungen können sehr häufig vorkommen, sodass die Kette sehr oft aufgespalten werden müsste. Dies widerspricht der grundlegenden Blockchain-Idee, da bei sehr kurzen Ketten ggf. keine ausreichende Transparenz mehr gegeben ist. Einen ganz anderen Ansatz könnte in diesem Kontext die ***Verschlüsselung*** darstellen, welche von 37 Akteuren (39 %) vorgeschlagen wurde. Die Akteure argumentieren, dass damit eine Löschung von Daten nicht nötig sei, weil die verschlüsselten Daten nur von den Personen gelesen werden könnten, die dazu berechtigt sind. Dies ist jedoch in vielerlei Hinsicht kritisch zu bewerten (vgl. hierzu Unterkapitel in 4.1.4).

Grundsätzlich bauen die bislang diskutierten Methoden (Off-Chain-Speicherung, Merkle-Trees, Zero-Knowledge-Proofs) darauf, die Speicherung personenbezogener Daten in der Blockchain zu vermeiden. Im Folgenden sollen nun Methoden diskutiert werden, die eine tatsächliche und physische Löschung der in der Blockchain gespeicherten Daten zum Ziel haben. Derartige Löschmöglichkeiten werden in der Fachdebatte nicht nur im Kontext der DSGVO-Konformität diskutiert, sondern auch zur Verhinderung der Speicherung illegaler Inhalte in Blockchains (Deuber et al. 2019). Einige wenige am Blockchain-Konsultationsprozess beteiligte Akteure verwiesen auf das Konzept der „***Redactable Blockchain***". Dabei können mithilfe von sog. ***Chamäleon-Hashfunktionen*** Daten nachträglich aus einer Blockchain gelöscht werden (Ateniese et al. 2017). Hierbei werden die Datenblöcke, wie bereits oben beschrieben, miteinander verkettet. Jedoch lässt sich durch einen Kollisions-Algorithmus die Verbindung aufheben, um einen neuen Block einzufügen. Es wäre somit nicht nötig, alle Blöcke, die nach dem entnommenen Block in der Kette sind, neu zu berechnen. Dies wäre mit einer physischen Löschung gleichzusetzen. Danach kann ein neuer Block an dessen Stelle eingefügt werden. Dies wird durch eine sog. „Narbe" (Lumb et al. 2016) sichtbar gemacht, um eine gewisse Art von Transparenz zu schaffen. Jedoch müssen sich (verantwortliche) Stellen darüber einig werden, ob der Block entfernt wird. Somit käme diese Lösung hauptsächlich in einer zulassungsbeschränkten, also privaten Blockchain infrage (Lumb et al. 2016). Eine Partei alleine kann dies nicht veranlassen (Marnau 2017). Daher schlagen einige Forscher vor, auf einen Abstimmungsmechanismus zu setzen (Matzutt et al. 2018). In einer privaten Blockchain (s. u.) könnte eine festgelegte

Bewertung der Aussagen der Akteure

Person oder Gruppe über eine Löschung entscheiden, in einer öffentlichen Blockchain müsste dieser Abstimmungsmechanismus „so unter den Teilnehmern verteilt sein, dass nur eine Mehrheit ihn gemeinsam einsetzen könnte“ (Marnau 2017, S. 1030). Zudem stellt sich die Frage, wie oft solche Blockersetzungen durchgeführt werden. Auch die Entwickler der Redactable Blockchain gehen davon aus, dass die Möglichkeit nur in Ausnahmefällen eingesetzt würde (Ateniese et al. 2017). Da Lösch- und Änderungsanfragen jedoch – abhängig vom Kontext – möglicherweise häufiger auftreten, löst diese Herangehensweise das Problem der Betroffenenrechte nicht auf zufriedenstellende Weise. Und selbst wenn diese Änderungen – beispielsweise durch organisatorische Maßnahmen – häufiger durchgeführt werden könnten, wäre es abhängig vom Kontext weiterhin möglich, Rückschlüsse auf eine Person zu ziehen. So wären beispielsweise im Medizinumfeld allein durch die Anzahl von neuen Einträgen Rückschlüsse auf die Häufigkeit von Arztbesuchen möglich. Zudem unterscheidet sich diese Speichervariante kaum noch von herkömmlichen Lösungen zur verteilten Speicherung, weil die Besonderheit der Nutzung einer unveränderlichen Blockchain nicht mehr gegeben ist (Wust und Gervais 2018).

Eine bereits in der Bitcoin-Blockchain verwendete Löschmethode ist das sog. „***Pruning***“. Hierbei werden alte und somit nicht mehr benötigte Teile der Kette entfernt, um Speicherplatz zu sparen, während die Integrität der ganzen Kette erhalten bleibt. Problematisch ist jedoch, dass sich auf diese Weise nur Transaktionen löschen lassen, deren Wert bereits aufgebraucht ist, also bereits in anderen Transaktionen ausgegeben wurde. Dieses Vorgehen ist wieder nur auf monetäre Transaktionsdaten einer Kryptowährung beschränkt. Ein personenbezogenes Datum, wie eine Adresse, stellt keinen monetären Wert da, und kann somit nie als „verbraucht“ oder „ausgegeben“ angehsehen werden. Zudem speichert der Bitcoin-Pruning-Algorithmus immer Informationen zur jeweils letzten Transaktion eines Coins (Farshid et al. 2019). Darüber hinaus gibt es weitere Vorschläge und Prototypen, welche eine Löschbarkeit mittels Pruning ermöglichen wollen (vgl. Farshid et al. (2019), Buterin (2015)). Diese sind aber noch nicht praxistauglich.

Eine komplett andere Lösungsmethode, die von den Akteuren genannt wurde, setzt auf den Einsatz einer ***privaten oder konsortialen Blockchain***. Dabei gibt es einen oder mehrere klare Verantwortliche, welche das Privileg haben, Transaktionen zu löschen oder nachträglich zu verändern. Auf diese Idee setzt auch der Lösungsvorschlag von Lumb et al. (2016). Jedoch widerspricht diese Lösung der Idee der Schaffung möglichst weitreichender Transparenz in der Blockchain.

Abschließend lässt sich feststellen, dass im Feld der Gewährleistung von Löschmöglichkeiten bei gleichzeitiger Erhaltung von Transparenz aktuell intensiv Forschung betrieben wird und verschiedenste Ansätze verfolgt werden. Während manche Ansätze (***Redactable Blockchains, Pruning und ZKP***) die Architektur der Blockchain ändern (Farshid et al. 2019) oder auf private Blockchain-Lösungen mit klar adressierbaren Verantwortlichen setzen (Lumb et al. 2016), schlägt beispielsweise Florian et al. (2019) Lösungen zum Löschen auf lokaler Ebene beim Endanwender vor. Viele dieser Ideen beziehen sich allerdings auf den Bereich der Kryptowährungen und sind nur bedingt auf andere Anwendungsfelder übertragbar. Es zeigt sich jedoch, dass es auch im Bereich der Kryptowährungen bisher keine zufriedenstellende Lösung gibt. Zur Gewährleistung der in Art. 17 DSGVO vorgeschriebenen Löschpflicht scheint der Ansatz der Off-Chain-Speicherung somit aktuell der einzig gangbare Weg zu sein.

4.1.2 Betroffenenrechte: Datenübertragbarkeit

Bewertung der Aussagen der Akteure

Problembeschreibung

Möchte eine Person den Anbieter wechseln, so muss es ihr gemäß Art. 20 DSGVO möglich sein, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten und diese zum neuen Anbieter zu übertragen. Acht Akteure (9 %) wiesen in diesem Zusammenhang darauf hin, dass die Übertragung von Daten, die in einer Blockchain gespeichert sind, nur schwierig umsetzbar sei. So fehle ein „Austauschformat für Daten in Blockchains" (Bitkom e. V.) oder die „Akzeptanz einer einheitlichen Datenbasis" (Das Blockchain-Institut). Daher könnte die Bereitstellung der Daten in einem strukturierten und gängigen Format, wie sie die DSGVO vorschreibt, problematisch sein. Zudem stellt das BSI (2019, S. 64) fest, dass „nicht unbedingt von allen Personen, von denen eventuell Daten in der Blockchain gespeichert sind, erwartet werden [kann], dass sie die sie betreffenden Daten selbst aus der Blockchain extrahieren können. Auch die Fachliteratur bezeichnet fehlende Standards als ein Problem (Isler und Michael 2017; Jaikaran 2018). Die Akteure erwähnen jedoch nicht, dass selbst wenn die Daten in einem standardisierten Format vorliegen würden, kein Verantwortlicher vorhanden wäre, an den sich Betroffene für den Export und Import der Daten wenden könnten (siehe hierzu Punkt 4.1.3). Des Weiteren schließt das Recht auf Datenübertragbarkeit eine Löschung beim alten Anbieter ein. Wie bereits in 4.1.1. erörtert, ist dies aber schwierig.

Vorgeschlagene Lösungsansätze und Bewertung

Abgesehen vom Fehlen einer verantwortlichen Stelle und der Löschmöglichkeit, könnte das Recht auf Datenübertragbarkeit durch ***standardisierte Speichermodelle und Strukturen*** relativ einfach gelöst werden. Jedoch gehen die aktuellen Entwicklungen eher in Richtung einer Vielzahl separater Blockchain-Technologien, sodass kaum davon ausgegangen werden kann, dass für die Bereitstellung der Daten in einem strukturierten, gängigen und maschinenlesbaren Format zeitnah ein weltweit gültiger Standard verabschiedet wird.

4.1.3 Bestimmbarkeit des Verantwortlichen

Problembeschreibung

31 Akteure (33 %) merkten an, dass aufgrund der verteilen Datenspeicherung keine verantwortliche Stelle ausgemacht werden könne. Aus technischer Sicht könnten mehrere Parteien als Verantwortlicher in Frage kommen: Der Programmierer der Blockchain, die Stelle, welche die Blockchain aufsetzt und administriert, die Nodes oder die Nutzer, welche Transaktionen durchführen (Fridgen et al. 2019).

Vorgeschlagene Lösungsansätze und Bewertung

Auch hier wäre die einzig mögliche Lösung die Nutzung einer ***privaten oder konsortialen Blockchain***, da nur hier detaillierte Informationen, wie zum Beispiel Kontaktdaten über die Nutzer, vorliegen. Gleichzeitig führt dies die Grundidee von Transparenz und einer verteilten Verantwortung ad absurdum.

4.1.4 Verschlüsselung

Problembeschreibung

Seitens der Akteure wurde häufig darauf verwiesen (37 Akteure bzw. 39 %), dass sich viele Datenschutzprobleme in der Blockchain durch ***Verschlüsselung*** lösen ließen. „Zusammenfassend ist nur Verschlüsselung die richtige Antwort auf Datenschutz", formulierte beispielsweise die Achelos GmbH. Bitkom e.V. führte zudem an, dass es technisch möglich sei, Daten „mit Encryption- und Decryption-Keys zu erstellen und im Falle der Löschung den Decryption-Key zu löschen" (Bitkom e.V. 2017, S. 18). Die Deutsche Bank AG schlug zudem vor, dass Smart Contracts eingesetzt werden könnten

Bewertung der Aussagen der Akteure

um „bestimmte Daten nach Ablauf einer festgelegten Zeit automatisch wieder [zu] verschlüsseln und damit unzugänglich [zu] machen". Auch in der Fachliteratur wird die Verschlüsselung als Lösung angesehen, bspw. in Tönnissen und Teuteberg (2020). Gleichzeitig merken sie jedoch an, dass durch die Weiterentwicklungen der Verschlüsselungsmechanismen die „Komplexität nur noch von wenigen Programmierern wirklich beherrscht werden kann. Damit bietet die Komplexität eine zunehmende Angriffsfläche für betrügerische Aktivitäten" (Tönnissen und Teuteberg 2020, S. 327).

Die hinter diesen Vorschlägen liegende Idee ist, dass mittels Verschlüsselung eigentlich personenbezogene Daten auf eine Weise in einer Blockchain gespeichert werden, bei der es nur einzelnen Akteuren, die über den Zugangsschlüssel verfügen, möglich wäre, auf die personenbezogenen Daten zuzugreifen. Somit würden diese Daten nur für jene Akteure als personenbezogene Daten gelten, die über den Schlüssel verfügen. Diese wären zugleich Verantwortliche und sie könnten durch Löschen des Schlüssels gewährleisten, dass – abgesehen von Entschlüsselungsverfahren – niemand mehr Zugriff auf die Daten hat, sodass die Löschpflicht als erfüllt angesehen werden könnte (Fridgen et al. 2019).

Problematisch ist bei diesem Vorschlag, dass Verschlüsselungskonzepte keine physische Löschung von Daten ermöglichen, sondern vielmehr eine Unkenntlichmachung. Insofern besteht die größte Herausforderung darin, dass aktuelle Verschlüsselungsverfahren in Zukunft z. B. unter Rückgriff auf Quantencomputing-Verfahren geknackt werden könnten (Fridgen et al. 2019), was zur Folge hätte, dass die Daten als personenbezogen gelten würden (Kirsch und Chow 2015). Diese Befürchtung wurde auch von einem Teil der Akteure (15 Akteure bzw. 16 %) vertreten.

Vorgeschlagene Lösungsansätze und Bewertung:
Die Argumentation, dass Verschlüsselungen zukünftig geknackt werden können ist zwar theoretisch korrekt, jedoch praktisch relativ unwahrscheinlich, da viele weitverbreitete Verfahren, wie z. B. AES-256 und RSA-2048 und höher von der Fachliteratur noch über die nächsten Dekaden als sicher angesehen werden (Lenstra 2004; Isa et al. 2012; Dent 2010). Ebenso gibt es bereits Verschlüsselungsverfahren, welche resistent gegen Angriffe mittels Quantencomputern sind (Bernstein und Lange 2017). Dennoch ist hierbei anzumerken, dass mittels Blockchain eine unveränderliche Technologie angestrebt wird, deren Architektur auf kryptographische Verfahren (Signaturen) aufbaut. Diese kann nach der Implementierung einer bestimmten Blockchain-Anwendung nicht mehr geändert werden. Sofern deren Sicherheit künftig gebrochen werden kann, würde die komplette Architektur der Implementierung unbrauchbar.

Einschränkend ist zu erwähnen, dass verschlüsselte Daten nicht als anonym anzusehen sind. Die rechtliche Betrachtung dieser Argumentation hat dies bereits in Unterkapitel 2.3.1 ausgeführt und basiert auf der Rechtsprechung des EUGH zur Anonymität von IP-Adressen (EuGH 2016). Ebenso wenig sieht die Artikel-29-Datenschutzgruppe Verschlüsselung als eine Methode zur Anonymisierung an und bestätigt, dass mehrere Studien und Forschungsartikel belegen, dass eine wahre Anonymisierung extrem schwierig ist (Article 29 Data Protection Working Party 2014, S. 3).

Der Rückgriff auf Verschlüsselung ist somit hilfreich, um das Problem der Verantwortlichkeit im Falle der Speicherung personenbezogener Daten in Blockchains zu adressieren, da nur jene Stelle als Verantwortliche im Sinne der DSGVO angesehen werden kann, die über den entsprechenden Schlüssel verfügt. Eine Befreiung von den Pflichten, denen Verantwortliche unterliegen, geht mit der Verschlüsselung nicht einher.

4.1.5 Daten für alle Blockchain-Teilnehmer sichtbar und schreibbar

Bewertung der Aussagen der Akteure

Problembeschreibung
Alle Nutzer einer Blockchain können grundsätzlich alle darin gespeicherten Daten einsehen. Zeitgleich können Nutzer aber auch alle möglichen Daten einspeichern – und somit auch personenbezogene Daten von sich oder anderen. Während Nodes Bitcoin-Transaktionsdaten überprüfen, bevor sie diese in die Blockchain schreiben, ist nicht klar, wie dieser „Proof" bei Daten, die keine Kryptowährungs-Transaktionsdaten darstellen, umgesetzt werden kann. Doch auch die Überprüfung von Bitcoin-Transaktionen lässt sich mit vielerlei Methoden umgehen, um somit auch „falsche" Transaktionen zu speichern (Orcutt 2018).

Hier entsteht ein Dilemma: Während die Sichtbarkeit aller Daten die Transparenz fördert, führt diese Sichtbarkeit und die Schreibmöglichkeit zu erheblichen Datenschutzbedenken.

Vorgeschlagene Lösungsansätze und Bewertung
Eine von 31 Akteuren (33 %) vorgeschlagene Lösung ist der Einsatz von zugriffsbeschränkten, also ***privaten Blockchains***. Der Betreiber einer solchen privaten Blockchain könnte diese so konfigurieren, dass die Daten nicht für jeden einsehbar sind. Dies würde die datenschutzrechtlichen Herausforderungen zwar lösen, jedoch zugleich der mit dem Einsatz einer Blockchain im Regelfall verfolgten Intention der Gewährleistung möglichst weitreichender Transparenz entgegenlaufen.

Ein weiterer Lösungsvorschlag, der von 30 Akteuren (32 %) vertreten wurde, setzt zur Vermeidung des Personenbezugs auf die ***Speicherung von pseudonymisierten Daten*** in einer Blockchain. Dass eine Depseudonymisierung in vielen Fällen dennoch möglich ist, beschreiben wir in im folgenden Unterkapitel (4.1.6).

Eine recht pragmatische und einfache Methode schlagen 75 Akteure (80 %) vor: Schlicht ***keine personenbezogenen Daten zu speichern***. Dies lässt sich durch technische oder organisatorische Maßnahmen jedoch nicht gänzlich bewerkstelligen. Denn durch „immer bessere maschinelle Lerntechniken wird zudem die Unterscheidung zwischen personenbezogenen und nicht personenbezogenen Daten mit der Zeit verschwinden, da eine Identifizierung einer natürlichen Person auch durch nicht personenbezogene Daten möglich wird" (Tönnissen und Teuteberg 2020, S. 327). Zudem könnten Inhaltsfilter von versierten Nutzern schnell umgangen werden (Matzutt et al. 2018). Des Weiteren beziehen sich diese Filter nur auf den medialen Inhalt und nicht explizit auf personenbezogene Daten. Auch das Ausschließen von Nutzern, welche mehrfach unerwünschte Inhalte speichern, ist nicht möglich, da Nutzer ihre (Bitcoin-) Adresse beliebig oft ändern können (Matzutt et al. 2018). Da es bereits für Menschen schwer sein kann, festzustellen, was ein personenbezogenes Datum ist und was nicht, stellt dies technisch eine noch viel größere Herausforderung dar, sodass fraglich bleibt, wie sich die Speicherung personenbezogener Daten in einer öffentlichen Blockchain seitens der Nodes effektiv verhindern lässt.

4.1.6 Pseudonymisierung und Depseudonymisierung

Problembeschreibung
Bei der Pseudonymisierung wird ein personenbezogener Identifier durch ein Pseudonym, beispielsweise eine Zeichenfolge aus Buchstaben und Zahlen, ersetzt. Die Zuordnung von Originaldatensatz und Pseudonym wird dann in einer externen Tabelle gesichert. Nur wer Zugriff auf diese Tabelle hat, kann die Daten nachträglich depseudonymisieren. Wird die Tabelle gelöscht, ist eine Depseudonymisierung zumindest theoretisch nicht mehr möglich. In der Blockchain-Konsultation vertraten 30 Akteure die Ansicht, dass die Pseudonymisierung eine effektive Methode zur Umgehung des Personenbezugs sei (vgl. Abs. 4.1.5). Die neuesten Entwicklungen in der Datenverarbei-

Bewertung der Aussagen der Akteure

tung (Big Data, Künstliche Intelligenz) zeigen jedoch, dass es relativ einfach ist, Daten nachträglich wieder zuzuordnen, obwohl die Zuordnungstabelle unbekannt ist (Kohn und Tamm 2019; Niemzik 2019). Wie bereits im Zusammenhang mit Hashwerten beschrieben (vgl. Abs. 4.1.1), muss dazu der Suchraum nur klein genug sein. Das bedeutet, dass in der Blockchain gespeicherte pseudonyme Daten, potentiell jetzt oder in Zukunft zuordenbar sein werden.

Das Problem ist die grundsätzliche Architektur der Blockchain, Transaktionen öffentlich zu dokumentieren. So sind den Netzwerkknoten die jeweiligen IP-Adressen bekannt und es besteht die Gefahr, dass einzelne Transaktionen einem konkreten Netzwerkknoten zugeordnet werden können (Biryukov und Tikhomirov 2014). Inwieweit die Speicherung der Identitäten der Netzwerkknoten vorgesehen ist, hängt von der konkreten Implementierung ab. Daher lässt sich nicht pauschal sagen, ob je nach Anwendungsfall weitere personenbezogene Daten in der Blockchain gespeichert werden.

Dieses Problem wurde von 14 Akteuren (15 %) angeführt. So gab ein Akteur an, dass auch Protokolldaten von Industriemaschinen Rückschlüsse auf den Bediener ermöglichten. Grundsätzlich stellte die Hochschule für Angewandte Wissenschaften Hamburg fest, dass „über Tracing auf einer Blockchain immer ein Aktivitätsprofil erstellt werden kann".

Auch die IP-Adresse, die dem Nutzer während der Durchführung einer Transaktion zugeordnet war, bietet Potenziale zur Depseudonymisierung. Die IP-Adresse wird (je nach Anwendung) zwar technisch gesehen nicht in der Kette gespeichert, jedoch gibt es Möglichkeiten, die IP-Adresse aus einer Transaktion herauszufinden. In einer Studie aus dem Jahr 2014 über die Deanonymisierung von IP-Adressen in einer Bitcoin-Blockchain lag die Erfolgsrate zwischen 10 % und 60 % (Biryukov und Tikhomirov 2014). Im Jahr 2019 arbeitete dasselbe Forscherteam an einer ähnlichen Studie. Sie nutzen dabei ein sog. „adjusted anonymity degree" (Biryukov und Tikhomirov 2019) zur Berechnung der Anonymität (0 = ein Angreifer kann alle Daten deanonymisieren, 1= volle Anonymität). Die Ergebnisse zeigten Werte zwischen 0,63 und 0,88. Eine weitere Methode zur Deanonymisierung besteht schließlich im Aufbau eines eigenen Nutzer- und Transaktionsnetzwerks (Reid und Harrigan 2013).

Vorgeschlagene Lösungsansätze und Bewertung
Eine allgemeine Lösung für das Problem der Depseudonymisierung wurde von den Akteuren nicht identifiziert und auch die Fachliteratur bietet keine grundsätzliche Lösung. Lediglich für gewisse Anwendungsfelder gibt es Lösungen, z. B. für Bitcoin. Für den Fall der Identifizierung mittels der Public Keys werden sog. ***Bitcoin-Mixer*** oder das ***Wechseln von Adressen*** als mögliche Lösung diskutiert (Schneider 2019). Im Fall der Identifizierung über die IP-Adresse wäre es möglich, dass der Client über Anonymisierungstools wie The Onion Router (TOR) Transaktionen durchführt (The Tor Project 2020). Neueste Forschungen zeigen jedoch, dass auch TOR-Nutzer durch Bitcoin-Transaktionen identifiziert werden können (Jawaheri et al. 2020).

4.1.7 Anonymisierung

Problembeschreibung
Drei Akteure (3 %) merkten an, dass eine Anonymisierung von Daten sowohl rechtlich als auch technisch nicht umsetzbar sei. So sei laut msg systems AG „Verschlüsselung oder Aggregation […] keine Anonymisierung gem. DSGVO". Der Krankenhaus-Kommunikations-Centrum KKC e. V. merkte an, dass „je nach Sicherheitsstandards zusätzliche Performance, Rechenleistung und damit Zeit" nötig sei. Zudem haben viele Forscher gezeigt, dass vor allem Bitcoin-Transaktionen einer Person zugeordnet werden können und somit nicht anonym sind (Meiklejohn et al. 2013; Herrera-Joancomartí 2015; Reid und Harrigan 2013).

Bewertung der Aussagen der Akteure

Vorgeschlagene Lösungsansätze und Bewertung

Mögliche Lösungen wurden bereits in Unterkapitel 4.1.6 diskutiert. Wir greifen diese hier erneut als problematische Lösung auf, da ein Wechseln der Adresse oder die Nutzung von Bitcoin-Mixer unserer Meinung nach eher als Lösung für das Pseudonymisierungsproblem steht und nicht für Anonymität. Einen anderen Weg geht die Währung Monero. Hier wird für jede Transaktion ein neues Konto angelegt, auf das nur der Zahlungsempfänger Zugriff hat und somit keine Adresse vergeben oder gespeichert wird (sog. Stealth-Adressen) (Braun-Dubler et al. 2020; Wijaya et al. 2019). Zusätzlich wird der Betrag jeder Transaktion verschleiert, indem mehrere Transaktionen zusammen ausgeführt werden (Farshid et al. 2019). Einen ähnlichen Ansatz verfolgt bspw. ein „deterministic wallet". Mithilfe dieser „Geldbörse" kann eine unendliche Anzahl von öffentlichen Adressen generiert werden. Somit lassen sich nicht direkt Rückschlüsse auf das dahinterliegende Wallet ziehen (Braun-Dubler et al. 2020). Jedoch zielen all diese Lösungen direkt auf Kryptowährungen ab und lassen andere Anwendungsfelder unberücksichtigt. Zudem hat sich gezeigt, dass auch diese Lösungen fehleranfällig sind. Beispielsweise wurde 2018 klar, dass Nutzer bei Monero doch identifiziert werden können (Möser et al. 2018). Aufgrund von Implementationsfehlern ist es außerdem möglich, dass die Algorithmen, welche Bitcoin-Adressen „mixen", fehlerhaft sein können (Farshid et al. 2019).

4.1.8 Speicherung außerhalb der EU

Problembeschreibung

Eine weitere Herausforderung zur Einhaltung der datenschutzrechtlichen Bestimmungen im Zusammenhang mit Blockchains ergibt sich aus den Anforderungen der DSGVO an die Übermittlung personenbezogener Daten in Drittländer in den Artikeln 44 - 50 DSGVO. Denn in einer öffentlichen Blockchain können Personen von jedem beliebigen Standort aus teilnehmen. Daher kann nicht bestimmt werden, wo genau Daten gespeichert werden. Aufgrund dieser Unbestimmtheit ist davon auszugehen, dass durch die verteilte Datenstruktur der Blockchain Daten auch außerhalb der Europäischen Union gespeichert werden. Da im Falle einer öffentlichen Blockchain auch die Bestimmung des Verantwortlichen nicht möglich ist, kollidiert dies mit den DSGVO-Vorgaben.

Vorgeschlagene Lösungsansätze und Bewertung

Auch im Hinblick auf diese Herausforderung wurde seitens der Akteure auf die Nutzung einer ***privaten oder konsortialen Blockchain*** verwiesen. Auch hier gilt, dass dadurch die datenschutzrechtlichen Herausforderungen zwar gelöst, jedoch zugleich die mit dem Einsatz einer Blockchain im Regelfall verfolgte Absicht der Gewährleistung möglichst weitreichender Transparenz durchkreuzt würde.

Eine weitere Lösung, welche jedoch nicht von den Akteuren erwähnt wurde, besteht in der Einführung von ***Geoblocking*** für Blockchain-Technologien. Dadurch könnten Nutzer ausgesperrt werden, die mit einer außereuropäischen IP-Adresse auf die Blockchain zugreifen möchten. Seit 2018 ist solch eine Technik in Europa allerdings verboten, um den digitalen Binnenmarkt zu fördern (Kops 2017; Committee on Industry, Research and Energy 2016; European Parliament 2018). Zudem kann Geoblocking relativ einfach mittels virtuellen privaten Netzwerken (VPN) umgangen werden.

Der Betrieb einer öffentlichen Blockchain unter Einhaltung der DSGVO-Vorgaben an die Übermittlung personenbezogener Daten an Drittländer erscheint somit derzeit nicht möglich.

Bewertung der Aussagen der Akteure

4.1.9 Sicherheit der gespeicherten Daten

Problembeschreibung

Von sechs Akteuren (6 %) wurden Probleme in Bezug zur Sicherheit der gespeicherten Daten erwähnt. So stellt beispielsweise der Bitkom e. V. fest, dass „kryptografische Schlüssel verloren gehen/gestohlen werden" können. Grundsätzlich verfolgt die Informationssicherheit drei Schutzziele: Vertraulichkeit, Integrität und Verfügbarkeit (Hanschke 2020). Während die Verfügbarkeit bei verteilten Systemen und die Integrität aufgrund der Nichteditierbarkeit i.d.R. gegeben ist, stellt die Vertraulichkeit („confidentiality") ein Problem dar, da potentiell jeder die Daten sehen kann (Mani 2017; Gupta 2018). Anders sieht es jedoch aus, wenn die Daten Off-Chain gespeichert werden. Hier kommen wieder alle drei Schutzziele als Problem in Frage: (1) Vertraulichkeit, da jeder die Daten einsehen kann. (2) Integrität, da die Off-Chain gespeicherten Daten editiert[10] oder gelöscht werden können. Und (3) Verfügbarkeit, da nicht sicher davon ausgegangen werden kann, dass alle Daten jedem Nutzer rund um die Uhr zugänglich sind und die Speichersysteme nicht ausfallen können. Auch das BSI stellt fest, dass keine Aussage über die Gesamtsicherheit des Systems gemacht werden kann, da die Sicherheit „abhängig von der Komposition der einzelnen Mechanismen und ihrer Integration in das Gesamtsystem" ist (BSI 2019, S. 40).

Vorgeschlagene Lösungsansätze und Bewertung

Zur Lösung dieser Probleme machte keiner der Akteure einen konkreten Vorschlag. Lediglich die achelos GmbH merkte an, dass „nur ***Verschlüsselung*** die richtige Antwort auf Datenschutz" sein könne. Dem gegenüber steht jedoch, dass Verschlüsselung nur gegen externe Angriffe hilfreich sein kann. Sie kann aber nicht interne Fehler, wie eine fehlerhafte Konfiguration oder Missbrauch seitens des Verantwortlichen verhindern (Gupta 2018). Selbst die Nutzung einer privaten Blockchain sei kein adäquates Mittel für die Datensicherheit. So stellte der Softwareentwickler MaibornWolff GmbH die Frage „was passiert, wenn jemand in die Infrastruktur einbricht und den Ledger (Datenbestand) der Blockchain kopiert? Dies kann nie zu 100 % ausgeschlossen werden und daher gehört dieser Schutz auf Anwendungsdatenebene zu einer guten Sicherheitsarchitektur der Gesamtanwendung". Allumfassende Lösungsvorschläge liefert auch die wissenschaftliche Literatur nicht.

4.1.10 Integrität und Qualität der zu speichernden Daten

Problembeschreibung

Auch hier lässt sich wieder Bezug nehmen zu den oben angesprochenen drei Schutzzielen der Informationssicherheit. Das hierbei von den Akteuren angesprochene Problem bezieht sich auf die Tatsache, dass es schwierig zu gewährleisten ist, dass die in die Blockchain eingetragenen Daten auch korrekt sind. Die Verifikation von monetären Transaktionsdaten innerhalb einer Blockchain ist sehr einfach, da der maximale Gesamtwert aller Beträge bekannt ist. Fraglich, bzw. aktuell unmöglich, ist hingegen die Verifikation von nicht-monetären Daten, wie z. B. eines Geburtsdatums. Somit ist die Verifizierbarkeit nicht per se eine Eigenschaft der Blockchain, sondern vielmehr der von Kryptowährungen. Etwas plakativer ausgedrückt: Wie kann sichergestellt werden, dass Person A ein Haus wirklich besitzt, bevor sie den Besitz in die Blockchain einträgt? Gleiches gilt für die Qualität der Daten, die in die Blockchain eingetragen werden. So merkte der Gesamtverband der Deutschen Versicherungswirtschaft an, dass „ohne qualitativ hochwertige, richtige und vollständige Daten […] kein mehrwertstiftender Einsatz einer

[10] Unabhängig davon, dass die Verlinkung in der Blockchain ungültig wird, da sich bei der Änderung des Datensatzes auch der damit verbundene Hashwert ändert.

Blockchain“ möglich sei. Auch in der Fachliteratur wird diskutiert, dass die Blockchain-Technologie die Datenqualität weder sicherstellt noch verbessert (Piscini et al. 2017).

Bewertung der Aussagen der Akteure

In diesem Kontext besteht ein weiteres, von den Akteuren jedoch unbeachtetes Problem darin, dass in einer öffentlichen Blockchain grundsätzlich alle Teilnehmer personenbezogene Daten in die Blockchain eintragen können.

Vorgeschlagene Lösungsansätze und Bewertung
Weder die Akteure noch die Literatur haben eine Lösung für die Qualitätsproblematik. Möglichkeiten zur Verhinderung der Speicherung von personenbezogenen Daten wurden bereits im letzten Absatz des Unterkapitels 4.1.5 beschrieben.

4.1.11 Forderungen nach rechtlichen Anpassungen

Problembeschreibung
Angesichts der Herausforderungen eines datenschutzkonformen Blockchain-Einsatzes forderte etwas weniger als ein Drittel (30 %), der an der Blockchain-Konsultation beteiligten Akteure, die Konkretisierung und ggf. die Änderung der DSGVO. Zudem nahmen einige wenige Akteure Bezug auf das Problem des potentiell grenzüberschreitenden Transfers personenbezogener Daten im Rahmen der Nutzung öffentlicher Blockchains.

Vorgeschlagene Lösungsansätze und Bewertung
Im Hinblick auf die Konkretisierung der DSGVO empfahlen die Akteure in der Regel, dass Leitlinien und Empfehlungen seitens staatlicher Stellen, beispielsweise seitens des Europäischen Datenschutzausschusses, herausgegeben werden. Konkrete inhaltliche Forderungen wurden allerdings keine benannt. Die Veröffentlichung von Leitlinien und Empfehlungen stellt durchaus eine realistische Handlungsoption dar. Denkbar wären vor allem Empfehlungen, etwa, dass der datenschutzkonforme Einsatz einer Blockchain, auf der personenbezogene Daten gespeichert werden, unter den derzeit gegebenen technischen Möglichkeiten nicht möglich ist und stattdessen eher auf die Off-Chain-Speicherung in öffentlichen Blockchains oder auf private Blockchains verwiesen wird.

Etwas konkreter waren hingegen die Vorschläge zur Änderung der DSGVO. Der eco-Verband für Internetwirtschaft e. V. forderte beispielsweise, die DSGVO-Vorgaben so zu interpretieren, dass die verifizierte Vernichtung des Schlüssels verschlüsselter Daten als ausreichende Anonymisierung gelten sollte. Zudem kritisierte eco, dass pseudonyme Daten als personenbezogen gelten. Da ohne die Kenntnis der Zuordnungsregeln eine Identifikation „in der Regel“ nicht möglich sei, wurde die Flexibilisierung des Rechtsrahmens gefordert, indem Löschungs- und Korrekturrechte nur in Abhängigkeit von einer Identifizierbarkeit geltend gemacht werden können sollten. Vorgeschlagen wurde auch, dass Node-Betreiber nicht als Verantwortliche klassifiziert werden. Gefordert wurde auch, unter anderem von der MACH AG, dass sog. „hoheitliche Daten“ (personenbezogene Daten aus einem Identitätsregister wie Geburtsdatum oder über (Grundstücks-)Besitzverhältnisse) aus dem Anwendungsbereich des Datenschutzrechts ausgenommen sein sollten, da derartige Daten nicht dem Bürger, sondern dem Staat gehören würden. Derartige Versuche der Flexibilisierung des Datenschutzrahmens wurden bereits während der Aushandlung der DSGVO unternommen, sie konnten sich jedoch nicht durchsetzen. Der Vorschlag, die Geltendmachung von Betroffenenrechten von der Identifizierbarkeit abhängig zu machen, entspricht bereits ohnehin der geltenden Rechtslage. So ist eine Stelle nur dann in der Verantwortung zur Gewährleistung von Betroffenenrechten, wenn diese Stelle über die Mittel zur Depseudonymisierung verfügt. Eine solche Stelle kann beispielsweise ein Finanzmarktplatz sein, der den Tausch von Bitcoin zu konventioneller Währung erlaubt. Der Vorschlag zur Einführung einer neuen Kategorie personenbezogener Daten in Form von so genannten hoheitlichen Daten ist grundsätzlich als schwierig zu bewerten. So stellen Geburtsdatum und Anga-

Bewertung der Aussagen der Akteure

ben zum Grundstücksbesitz personenbezogene Daten dar, deren Verarbeitung sich auf eine der Rechtsgrundlagen der DSGVO stützen muss. Ihre Verarbeitung ist unter den gegebenen rechtlichen Rahmenbedingungen also möglich. Der Datenschutz dient dabei zur Gewährleistung einer ordnungsgemäßen Verarbeitung, die keine negativen Auswirkungen auf die Rechte und Freiheiten des Einzelnen zur Folge hat. Die Herausnahme derartiger Daten aus dem Anwendungsbereich der Datenschutzgesetze würde dem Missbrauch derartiger Daten Vorschub leisten und kann nicht als zielführend im Hinblick auf den datenschutzkonformen Betrieb von Blockchains bewertet werden. Aktuell zeigt sich, dass eine Änderung der DSGVO in naher Zukunft ohnehin eher unwahrscheinlich ist (European Commission 24.06.2020) . Denkbar ist eher der verstärkte Rückgriff auf Leitlinien und Empfehlungen des Europäischen Datenschutzausschusses.

Im Hinblick auf die Übermittlung personenbezogener Daten in nicht-sichere Drittländer (European Commission 2017) wurde zudem auf die Verabschiedung von Standarddatenschutzklauseln oder unternehmensinterne Verhaltensregeln verwiesen. Im Falle einer zugangsbeschränkten Blockchain kann dieser Vorschlag nützlich sein. Weniger sinnvoll ist der Vorschlag hingegen im Kontext öffentlicher Blockchains. Wenn nicht klar ist, wer die Teilnehmer einer Blockchain sind, kann nicht bestimmt werden, welche Akteure Verhaltensregeln oder Standarddatenschutzklauseln verabschieden müssen.

Zur Lösung der Herausforderung inkompatibler internationaler Gesetzesrahmen wurde die Schaffung weltweiter Regeln und die Intensivierung der internationalen Kooperation vorgeschlagen, die einzelnen Vorschläge blieben jedoch unkonkret im Hinblick auf die Zielerreichung. Die Schaffung eines internationalen Rechtsrahmens würde die internationale Angleichung der Datenschutzgesetze erforderlich machen. Die DSGVO ist in der Tat dabei, sich als internationaler Datenschutzstandard durchzusetzen (Greenleaf 2019). Allerdings kann auch dieser Vorschlag die Probleme der Löschung einerseits und der Bestimmung der Verantwortlichkeit in öffentlichen Blockchains andererseits nicht lösen. Die Verabschiedung eines neuen internationalen Rechtsrahmens, in dem die Vorgaben zu Bestimmung des Verantwortlichen und zur Löschung ausgehebelt werden, ist hingegen angesichts in Kraft befindlicher internationaler Datenschutzvereinbarungen wie den OECD-Datenschutz-Richtlinien, der Datenschutz-Konvention des Europarats oder der EU-Grundrechtecharta als sehr unwahrscheinlich zu bewerten.

4.1.12 Forderungen nach organisatorischen Maßnahmen

Problembeschreibung

Für einige Akteure (18 %) scheinen die oben genannten technischen oder rechtlichen Lösungen nicht ausreichend, sodass sie organisatorische Maßnahmen vorschlugen. Diese drei Maßnahmen waren die (1) Einführung von Nutzerrollen- und rechten, (2) die Zuweisung von verschiedene Schutzniveaus für verschiedene Arten von Daten, z. B. für Medizindaten sowie (3) die ausschließliche Speicherung von Datenaggregaten. Sie haben das gemeinsame Ziel, einen geänderten Umgang mit den Daten zu erzielen. All diese Vorschläge sind in der allgemeinen Computer-Literatur seit langem bekannt und werden auch unabhängig der Blockchain-Technologie thematisiert (Sandhu et al. 1996).

Vorgeschlagene Lösungsansätze und Bewertung

Der Begriff der organisatorischen Maßnahmen ist in Art. 32 DSGVO zu finden und war bereits im BDSG (alt) verankert. Somit kommen diese auch regelmäßig im Kontext der Blockchain-Architektur zum Tragen. Im Falle einer privaten (und damit zulassungsbeschränkten) Blockchain sind ***Nutzerrollen und -rechte*** leicht umzusetzen (Fridgen et al. 2019). Eine zuvor festgelegte Stelle könnte neue Nutzer zulassen und gleichzeitig Rollen vergeben. Diese Rollen könnten bspw. festlegen, welche Daten ein Nutzer lesen darf (Fridgen et al. 2019). Solche Bedingungen ließen sich auch sehr gut in Form von Smart Contracts direkt in der Blockchain speichern. Kaum möglich ist dies jedoch bei

öffentlichen Blockchains, da potentiell jedes Individuum anonym teilnehmen kann und die Teilnahme von keiner zentralen Stelle kontrolliert wird.

Bewertung der Aussagen der Akteure

Damit Nutzer nur auf gewisse Daten zugreifen können, kann es ratsam sein, anhand der „Risiken […], die mit der Verarbeitung verbunden sind" (Bauer et al. 2018, S. 152), ***verschiedene Schutzniveaus für Daten festzulegen***. So könnte beispielsweise Medizindaten einen höheren Schutz beigemessen werden, wie es mit der HIPAA-Verordnung in den USA der Fall ist (CDC 2018). Technisch könnten den in der Blockchain gespeicherten Daten Kategorien zugewiesen werden, welche Nutzungs- oder Verarbeitungsbedingungen festlegen oder der Kreis der Rezipienten durch den Endnutzer festgelegt werden (De Filippi 2016; Finck 2017; Zyskind et al. 2015). Jedoch muss dabei darauf geachtet werden, dass die verwendeten Metadaten ebenfalls personenbezogen sein können (Finck 2017). Eine weitere Idee wäre, dass Serviceanbieter die Datenverarbeitung direkt im Netzwerk des Nutzers durchführen, also nie Zugang zu den Rohdaten erhalten (Zyskind et al. 2015). Diese Idee resultiert in Daten-Souveränität und bezieht sich meist auf die Möglichkeit, die eigene digitale Identität zu speichern, um sich damit zu authentifizieren. Mit dem „Enigma Project" hat das Massachusetts Institute of Technology ein System entwickelt, das die feinkörnige Preisgabe von bestimmten personenbezogenen Daten für ein festgelegtes Publikum erlaubt (MIT Media Lab 2020).

Zusätzlich schlugen drei Akteure (3 %) die ausschließliche Sicherung von ***Datenaggregaten*** vor. Dabei werden Daten von verschiedenen Personen zusammengeführt und gruppiert, sodass einige individuelle Informationen bewusst verloren gehen (Horster und Fox 2013). Möchte man beispielsweise wissen, wie viele Kunden in einer Stadt (z. B. Karlsruhe) anwesend sind, müssten nicht alle Kunden mit Adresse übermittelt oder gespeichert werden. Stattdessen würde eine einfache Gruppierung der Stadt und die anschließende Suche nach „Karlsruhe" ausreichen, um diese Information zu nutzen. Dieses Vorgehen ist aber nicht mit Pseudonymisierung oder gar Anonymisierung gleichzusetzen. Denn nur in wenigen Fällen ist es möglich, dass nach der Aggregation tatsächlich kein Personenbezug mehr vorhanden ist. Mit den im Unterkapitel 4.1.6 beschriebenen Techniken lassen Datenanalysen Rückschlüsse auf die einzelnen Personen zu. Nichtsdestotrotz entwickelten Forscher verschiedene Möglichkeiten, um Datenaggregationen mit Fokus auf Datenschutz zu ermöglichen. So beschäftigten sich bereits Yao und Wen (2008) damit, verschiedene „Privatheitslevel" für die Datenaggregation festzulegen – basierend auf der Anzahl der Datensätze in einer Gruppe. Weitere Forschung gab es in Anwendungsbereichen wie Sensordaten (Shi et al. 2010) oder Internet der Dinge (Lu et al. 2017). Die Weiterentwicklungen der Datenanalyse, vor allem im Hinblick auf Big Data und Künstliche Intelligenz, werden es allerdings künftig weiter erschweren, Datenaggregate ohne die Möglichkeit eines Personenbezugs zu erstellen.

4.1.13 Technische Weiterentwicklungen und Standards

Problembeschreibung

29 Akteure (31 %) waren der Meinung, dass technische Weiterentwicklungen erforderlich seien, um Blockchains datenschutzkonform betreiben zu können. Bestehende Lösungen seien nicht in der Lage, die Vorteile der Blockchain mit den Anforderungen des Datenschutzes auf zufriedenstellende Weise zu verbinden. Aktuell gebe es nur „tradeoffs zwischen Security, Datenschutz, Effizienz, Flexibilität, Plattformkomplexität und Benutzerfreundlichkeit für Entwickler", so die DB Systel GmbH. Auch die Ergebnisse der Diskussion der Hindernisse und Lösungen in den vorangegangenen Kapiteln unterstreichen diese Aussage. So scheint es aktuell kaum möglich, eine öffentliche Blockchain datenschutzkonform einzusetzen. Daher sind weitere Entwicklungen und Forschung an unterschiedlichen Funktionen und Eigenschaften der Blockchain nötig.

Bewertung der Aussagen der Akteure

Vorgeschlagene Lösungsansätze und Bewertung

Die in diese Richtung formulierten Lösungsansätze bezogen sich in aller Regel auf allgemeine Hinweise zur Weiterentwicklung, da sich die Blockchain-Technologie noch immer in einem sehr frühen Stadium befinde und mit fortschreitender Technologie-Reife auch die datenschutzrechtlichen Herausforderungen aus dem Weg geräumt werden könnten. Viele der Akteure, die für technische Weiterentwicklungen eintraten, sprachen sich für die Förderung von Standardisierungsvorhaben aus, da sich auf diese Weise die systematischen Herausforderungen hinsichtlich der Löschung von Daten oder zur Gewährleistung der Datenübertragbarkeit auf nachhaltigste Weise lösen ließen. Im Hinblick auf das Thema Standardisierung und Löschung wurden keine konkreten Vorschläge formuliert, im Hinblick auf die Datenübertragbarkeit wurde dagegen die Verbesserung der Interoperabilität zwischen unterschiedlichen Blockchains gefordert. Dem pflichtet auch die Literatur bei, die besagt, dass die Voraussetzungen für eine erfolgreiche Forschung in diesem Bereich bereits geschaffen seien und nun eine Vielzahl neuer Anwendungsfälle aufkommen werde (Belchior et al. 2020).

5
Zusammenfassung und Fazit

Die datenschutzrechtliche Beurteilung des Einsatzes der Blockchain-Technologie hängt maßgeblich von der konkreten Ausgestaltung der Blockchain-Anwendung und der konkreten Verarbeitungszwecke ab. Daher muss sich jeder Verantwortliche vor Inbetriebnahme seiner Datenverarbeitungsverfahren die Frage stellen, inwieweit die Implementierung in seinem konkreten Fall einen Mehrwert bietet. Dies gilt insbesondere für Fälle, in denen eine öffentliche Blockchain genutzt wird und ist abhängig von den jeweiligen personenbezogenen Daten, die in dieser Blockchain gespeichert werden sollen. Ein solcher, gefahrengeneigter Einsatz kann den Einsatz der Technologie nicht nur der Technologie halber begründen. Die Berücksichtigung der Betroffenenrechte, wie sie die DSGVO vorsieht, kann nur dann gelingen, wenn Datenschutzaspekte von Anfang an berücksichtigt werden. Die laufenden Debatten und die Blockchain-Konsultation stellen somit einen wichtigen Eckpfeiler bei der Gewährleistung von Datenschutz durch Technikgestaltung („Data Protection by Design“) dar. Dies ist aus unserer Perspektive eindeutig zu begrüßen und mit der vorliegenden Analyse des Diskurses zur Blockchain-Konsultation der Bundesregierung leisten wir gerne einen konstruktiven Beitrag zur Debatte.

Im Rahmen dieses White Papers haben wir die Äußerungen der an der Blockchain-Konsultation der Bundesregierung beteiligten Akteure zum Datenschutz empirisch untersucht. Von besonderem Interesse war für uns dabei, welche Herausforderungen gesehen werden, ob und welche Lösungsansätze zur Bewältigung dieser vorgeschlagen werden und wie diese zu einzuschätzen sind.

Deutlich wurde, dass es insbesondere im Hinblick auf die Nutzung öffentlicher Blockchains noch viele Herausforderungen und ungelöste Probleme gibt. So stellt die grundsätzliche Idee der Architektur, die Unveränderlichkeit und Sichtbarkeit aller Daten, die größten Herausforderungen für den datenschutzkonformen Einsatz von öffentlichen Blockchains dar. Daneben wird die Einhaltung des Datenschutzrechts dadurch erschwert, dass in einer öffentlichen Blockchain keine Gewissheit über die Teilnehmer und somit über die Verantwortlichen besteht.

Im Rahmen der Diskursanalyse zeigte sich, dass ein Großteil der Akteure, die sich zum Thema Datenschutz und Blockchain äußerten, die Meinung vertrat, dass die Gewährleistung des Datenschutzes bei Blockchain-Anwendungen eine Herausforderung darstellt, die es zu lösen gilt. Zugleich gaben viele Akteure aber auch an, dass sie die Herausforderungen für bewältigbar halten. Einige vertraten dabei die Überzeugung, dass eine Lösung bereits unter Rückgriff auf bestehende technische Verfahren möglich wäre. Am häufigsten wurde dabei auf die Off-Chain-Speicherung verwiesen, gefolgt von Verschlüsselung und Pseudonymisierung. Daneben wurde auch empfohlen, auf die Speicherung personenbezogener Daten in einer Blockchain zu verzichten oder auf die Nutzung einer privaten oder halb-privaten Blockchain zu setzen. Einige Akteure sprachen sich für rechtliche Anpassungen, etwa die Konkretisierung der DSGVO oder die Verabschiedung weltweit geltender Rechtsgrundlagen aus.

Unsere Diskussion zeigte, dass bestehende technische Lösungen oftmals keine zufriedenstellende Lösungsmöglichkeit bieten. So können beispielsweise mittels Pruning nicht beliebige Daten gelöscht werden. Chamäleon-Hashfunktionen, welche eine tatsächlich physische Lösung ermöglichen, aber dennoch einen Hinweis über eine Löschung hinterlassen, benötigen einen Konsens, welcher durch die Beteiligten ermöglicht werden muss. Auch die oft genannte Verschlüsselung oder Löschmarkierungen mittels Tombstones, stellen keine physische Löschung dar. Trotz verstärkter Forschung

in den letzten Jahren sind die meisten derartigen Ideen noch nicht über ein Proof-of-Concept-Stadium hinaus und meist auf den Einsatz im Kontext von Kryptowährungen beschränkt (Hughes et al. 2019). Unabhängig davon wären alle Bemühungen, Daten in der Blockchain löschbar zu machen ein fundamentaler Bruch mit den Ideen und Prinzipien der Architektur der Blockchain. Das Forum Privatheit sieht die Tatsache, dass eine Löschung nur mittels Konsensverfahren mehrerer Teilnehmer möglich ist, als einzigen Vorteil gegenüber traditionellen Speicherarten.

Weiterhin ist das Problem, dass alle Daten für jeden Teilnehmer sichtbar sind, technisch nur bedingt lösbar. Wie auch außerhalb der Blockchain-Thematik bereits diskutiert, sind Pseudonymisierung und Anonymisierung durch Fortschritte in Datenanalysen oder Fehlern in Pseudonymisierungs- bzw. Anonymisierungsalgorithmen angreifbar. Für vergleichsweise sinnvoll halten wir die von 37 Akteuren befürwortete Verschlüsslung der Daten. Durch den Rückgriff auf Verschlüsselung wird es möglich, dass nur der jeweils über den Zugriffsschlüssel verfügende Akteur als Verantwortlicher im Sinne des Datenschutzrechts angesehen werden kann.

Die von 38 Akteuren befürwortete Lösung, schlicht keine personenbezogenen Daten zu speichern, wäre nur mit einem außerordentlich hohen und komplexen Programmier- bzw. Organisationsaufwand möglich. Es müsste für jeden Kontext vollkommen sichergestellt werden können, dass kein Eintrag tatsächlich personenbezogen ist. Obwohl diese Lösung sehr viele der in Kapitel 4 genannten Probleme lösen könnte, halten wir sie auch in der nahen Zukunft für nicht realisierbar. Auch die Gewährleistung weiterer Betroffenenrechte ist technisch nicht oder nur sehr schwer möglich. So erschweren fehlende Standards die Datenübertragbarkeit. Zudem existieren weiterhin keine praktikablen Lösungsvorschläge mittels derer in einer öffentlichen Blockchain eine verantwortliche Person ausgemacht werden könnte, an welche Betroffenenrechte adressiert werden können.

Darüber hinaus ist aufgrund der verteilten Speicherung unklar, an welchem geografischen Ort die Daten gespeichert sind. Für die Speicherung außerhalb der Europäischen Union stellt die DSGVO sehr hohe Anforderungen. Technisch gesehen wären diese zumindest theoretisch leicht einzuhalten, wenn für die Blockchain-Anwendung Geofilter eingesetzt würden. Mittels virtueller privater Netzwerke (VPN) ließe sich diese Sperre allerdings leicht umgehen, sodass die Praxistauglichkeit dieses Ansatzes zu bezweifeln ist. Solange das Problem der Bestimmbarkeit der Verantwortlichen in öffentlichen Blockchains ungelöst ist, können zudem auch internationale Vereinbarungen, Verhaltensregeln usw. diesbezüglich keine Abhilfe schaffen, weil keine Klarheit über die Vertragsparteien bestehen kann.

Wie bei jedem Informationssystem muss auch bei Blockchain-Anwendungen die Datensicherheit betrachtet werden: Während die Verfügbarkeit bei verteilten Systemen und die Integrität aufgrund der Nichteditierbarkeit gegeben ist, stellt die Vertraulichkeit ein Problem dar, da potentiell jede Person an einer öffentlichen Blockchain teilnehmen und die dort gespeicherten Daten sehen, bzw. selbst personenbezogene Daten eintragen kann. Letztendlich kann somit durch die Blockchain die Datenqualität weder verbessert noch sichergestellt werden.

Das Gesamturteil im Hinblick auf die datenschutzkonforme Nutzung der Blockchain-Technologie fällt entsprechend ernüchternd aus. Eine allumfassende technische Lösung der datenschutzrechtlichen Herausforderungen existiert derzeit nicht. Jeder Lösungsvorschlag bringt Vor- aber auch neue Nachteile mit sich. Einige klingen in der Theorie durchaus vielversprechend, dürften sich in der Praxis jedoch als äußert schwierig umsetzbar erweisen.

Abschließend bleibt festzuhalten, dass bei einer Betrachtung der vorgeschlagenen Lösungsansätze und Bewertung drei dominante Ansätze – mit all ihren in Kapitel 4 beschriebenen Vor- und Nachteilen – hervorstechen:

- die Off-Chain-Speicherung personenbezogener Daten im Falle der Nutzung einer öffentlichen Blockchain zur Adressierung der Herausforderung der Lösch- und Berichtigungspflichten,
- die Verschlüsselung On-Chain gespeicherter personenbezogener Daten im Falle der Nutzung einer öffentlichen Blockchain zur Adressierung der Herausforderung der Verantwortlichkeit sowie
- der Einsatz einer privaten Blockchain, welche das Löschen von Daten ermöglicht und das Problem der Verantwortlichkeit löst – allerdings sei noch einmal daran erinnert, dass dieser Lösungsvorschlag dem mit Blockchains verfolgten Ziel der besseren Gewährleistung von Transparenz widerspricht.

Bemerkenswert ist, dass von den 66 Akteuren, die eine Lösung der datenschutzrechtlichen Herausforderung für möglich hielten, eine Mehrheit von 43 Akteuren die Nutzung der Off-Chain-Speicherung befürwortet hat. Somit scheint diese Möglichkeit zur Umgehung von Lösch- und Berichtigungsbeschränkungen bei den Akteuren einen hohen Stellenwert einzunehmen. Ebenso wurde der Rückgriff auf Verschlüsselung von einer Mehrheit von 37 Akteuren und der Einsatz einer zugriffsbeschränkten privaten oder halb-privaten Blockchain von 31 Akteuren befürwortet.

In der Blockchain-Strategie der Bundesregierung wird ebenfalls positiv auf die Off-Chain-Speicherung verwiesen. Die Nutzung von Verschlüsselung oder einer privaten bzw. halb-privaten Blockchain zur Adressierung der datenschutzrechtlichen Herausforderungen wird dagegen an keiner Stelle empfohlen. Positiv nimmt die Blockchain-Strategie hingegen auf die aus unserer Sicht weniger zielführenden Vorschläge Pseudonymisierung und Zero-Knowledge-Proofs Bezug. Nichtsdestotrotz sind wir der Ansicht, dass Forschungsaktivitäten auch auf diesen Feldern vorangetrieben werden sollten, um die Sicherheit von Pseudonymisierung zu erhöhen und die Nutzbarkeit von Zero-Knowledge-Proofs zu verbessern. Wir begrüßen zudem, dass keine Änderung der DSGVO aus Sicht der Blockchain-Technologie für erforderlich gehalten wird und stattdessen der datenschutzkonforme Einsatz der Blockchain-Technologie mittels bestehender und zu entwickelnder technischer Lösungen nach dem Ansatz des Datenschutzes durch Technikgestaltung befürwortet wird (Presse- und Informationsamt der Bundesregierung 2019, S. 12).

Die Frage, ob konventionelle verteilte Datenbanken die, aus Datenschutzsicht, bessere Alternative ist, möchten wir bewusst unbeantwortet lassen. Mögliche Vorteile könnten im Detail stecken, etwa die Möglichkeit des „kollektiven Löschens" mittels Chamäleon-Hashfunktionen. Auf diese Weise könnte die mit dem Einsatz einer Blockchain angestrebte Transparenz zum einen durch die Speicherung der Daten in der Blockchain und zum anderen durch die Festlegung von Löschinstanzen mit kollektiver Löscherlaubnis gewahrt werden. Abschließend bleibt jedoch anzumerken, dass die Off-Chain Speicherung gegen die Grundidee der Blockchain spricht und für die grundsätzliche Diskussion über den Einsatz von Blockchain kaum Vorteile bringt. Die wirkliche Vereinbarkeit der Grundidee einer unveränderlichen Blockchain mit datenschutzrechtlichen Vorgaben, die eine Veränderbarkeit vorschreiben, halten wir somit für unwahrscheinlich. Dies bedeutet aber nicht, dass nicht weiterhin an technischen Lösungsansätzen geforscht werden sollte.

6 Literaturverzeichnis

Agung, Anak Agung Gde; Handayani, Rini (2020): Blockchain for smart grid. In: *Journal of King Saud University - Computer and Information Sciences*. DOI: 10.1016/j.jksuci.2020.01.002.

Ahl, Amanda; Yarime, Masaru; Tanaka, Kenji; Sagawa, Daishi (2019): Review of blockchain-based distributed energy: Implications for institutional development. In: *Renewable and Sustainable Energy Reviews* 107, S. 200–211. DOI: 10.1016/j.rser.2019.03.002.

Article 29 Data Protection Working Party (Hg.) (2014): Opinion 05/2014 on Anonymisation Techniques. Online verfügbar unter https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf, zuletzt geprüft am 09.07.2020.

Ateniese, Giuseppe; Magri, Bernardo; Venturi, Daniele; Andrade, Ewerton (2017): Redactable Blockchain – or – Rewriting History in Bitcoin and Friends. In: IEEE European Symposium on Security and Privacy (EuroS&P). IEEE EuroS&P. Paris. Piscataway, NJ: IEEE, S. 111–126.

Bäcker, Matthias; Bergt, Matthias; Boehm, Franziska; Caspar, Johannes; Dix, Alexander (2018): Datenschutz-Grundverordnung/BDSG. Kommentar. 2. Auflage. Hg. v. Jürgen Kühling und Benedikt Buchner. München: C.H. Beck.

Balan, S.; Otto, J.; Ganesan, R.; Ganesan, N.; Sundararajan, L. (2015): Internet of Things: Evolution and its Applications. In: Twenty-third Americas Conference on Information Systems. (AMCIS).

Bashir, Imran (2018): Mastering Blockchain. Distributed ledger technology, decentralization, and smart contracts explained. 2nd ed. Birmingham: Packt Publishing. Online verfügbar unter https://ebookcentral.proquest.com/lib/gbv/detail.action?docID=5340530.

Bauer, Christoph; Eickmeier, Frank; Eckard, Michael (Hg.) (2018): E-Health: Datenschutz und Datensicherheit. Herausforderungen und Lösungen im IoT-Zeitalter. Unter Mitarbeit von Kerstin Kafke, Daniela Klette und Astrid Schwaner. Wiesbaden: Springer Gabler.

Bechtolf, Hans; Vogt, Niklas (2018): Datenschutz in der Blockchain – Eine Frage der Technik. Technologische Hürden und konzeptionelle Chancen. In: *ZEITSCHRIFT FÜR DATENSCHUTZ* (2), S. 66–70. Online verfügbar unter https://www.beck-shop.de/zd-zeitschrift-datenschutz/product/9002683, zuletzt geprüft am 28.04.2020.

Belchior, Rafael; Vasconcelos, André; Guerreiro, Sérgio; Correia, Miguel (2020): A Survey on Blockchain Interoperability: Past, Present, and Future Trends.

Bernstein, Daniel J.; Lange, Tanja (2017): Post-quantum cryptography. In: *Nature* 549 (7671), S. 188–194. DOI: 10.1038/nature23461.

Biryukov, Alex; Tikhomirov, Sergei (2014): Deanonymization and linkability of cryptocurrencytransactions based on network analysis.

Biryukov, Alex; Tikhomirov, Sergei (2019): Deanonymization and Linkability of Cryptocurrency Transactions Based on Network Analysis. In: Proceedings of the 4th IEEE EuroS&P. Proceedings of the 4th IEEE EuroS&P. Stockholm, Sweden: IEEE, S. 172–184.

Bitkom e.V. (2017): Faktenpapier Blockchain und Datenschutz. Hg. v. Bitkom e.V. Online verfügbar unter https://www.bitkom.org/Bitkom/Publikationen/Faktenpapier-Blockchain-und-Datenschutz.html, zuletzt geprüft am 03.09.2019.

Bitnation (2020): The Internet of Sovereignty. MyBitnation. Online verfügbar unter https://tse.bitnation.co/, zuletzt aktualisiert am 03.12.2019, zuletzt geprüft am 19.06.2020.

BMWi; BMF (2019): Online-Konsultation zur Erarbeitung der Blockchain-Strategie der Bundesregierung. Hg. v. Bundesministerium für Wirtschaft und Energie, Bundesministerium der Finanzen. Online verfügbar unter https://www.bmwi.de/Redaktion/DE/Downloads/Stellungnahmen/Stellungnahmen-Blockchain/stellungnahmen.pdf.

Bootle, Jonathan; Cerulli, Andrea; Chaidos, Pyrros; Groth, Jens (2016): Efficient Zero-Knowledge Proof Systems. In: Alessandro Aldini, Javier Lopez und Fabio Martinelli (Hg.): Foundations of security analysis and design VIII. FOSAD 2014/2015/2016 tutorial lectures. Switzerland: Springer (Tutorial, 9808), S. 1–31.

Brandenburg, Mario (2019): Die Blockchain-Strategie der Bundesregierung – ein überfälliges Positionspapier. In: *BTC-ECHO* 2019, 08.10.2019. Online verfügbar unter https://www.btc-echo.de/die-blockchain-strategie-der-bundesregierung-ein-ueberfaelliges-positionspapier/, zuletzt geprüft am 11.04.2020.

Braun-Dubler, Nils; Gier, Hans-Peter; Bulatnikova, Tetiana; Langhart, Manuel; Merki, Manuela; Roth, Florian et al. (2020): Blockchain: Capabilities, Economic Viability, and the Socio-Technical Environment: vdf Hochschulverlag AG an der ETH Zürich.

BSI (2019): Blockchain sicher gestalten. Konzepte, Anforderungen, Bewertungen.

Bundesnetzagentur (2019): Die Blockchain-Technologie – Potenziale und Herausforderungen in den Netzsektoren Energie und Telekommunikation. Bonn. Online verfügbar unter https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Allgemeines/Bundesnetzagentur/Publikationen/Berichte/2019/DiskussionspapierBlockchain.html, zuletzt geprüft am 28.04.2020.

Buterin, Vitalik (2015): State Tree Pruning. Hg. v. Ethereum Foundation. Online verfügbar unter https://blog.ethereum.org/2015/06/26/state-tree-pruning/, zuletzt geprüft am 13.02.2020.

Cai, Y.; Zhu, D. (2016): Fraud detections for online businesses. A perspective from blockchain technology. In: *Financial Innovation* 2 (20), S. 1–10.

Carson, B.; Romanelli, G.; Walsh, P.; Zhumaev, A. (2018): Blockchain beyond the hype. What is the strategic business value. McKinsey & Company. Online verfügbar unter https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value, zuletzt geprüft am 07.08.2019.

Cavus, Mustafa (2019): Blockchain-Strategie der Bundesregierung. Status Projektsammlung. In: *COMPUTERWOCHE* 2019, 07.10.2019. Online verfügbar unter https://www.computerwoche.de/a/status-projektsammlung,3547799, zuletzt geprüft am 11.04.2020.

CDC (2018): Health Insurance Portability and Accountability Act of 1996 (HIPAA). Hg. v. U.S. Department of Health & Human Services. Online verfügbar unter https://www.cdc.gov/phlp/publications/topic/hipaa.html, zuletzt aktualisiert am 01.01.2019, zuletzt geprüft am 22.06.2020.

CDU/CSU; SPD (2018): Ein neuer Aufbruch für Europa. Eine neue Dynamik für Deutschland. Ein neuer Zusammenhalt für unser Land. Koalitionsvertrag zwischen CDU, CSU und SPD. 19. Legislaturperiode. CDU Deutschlands, CSU Landesleitung, SPD Deutschlands. Online verfügbar unter https://www.spdfraktion.de/system/files/documents/koalitionsvertrag_2018-2021_bund.pdf, zuletzt geprüft am 25.082020.

Civic Technologies (2020): Civic Wallet - digital wallet for money and cryptocurrency. Online verfügbar unter https://www.civic.com/, zuletzt geprüft am 19.06.2020.

CNIL (2018): Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data. Hg. v. CNIL. Online verfügbar unter https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data, zuletzt geprüft am 07.02.2020.

Committee on Industry, Research and Energy (2016): REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. Document 52016PC0289. Hg. v. European Parliament. Brussels. Online verfügbar unter https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016PC0289, zuletzt geprüft am 12.02.2020.

De Filippi, Primavera (2016): The Interplay between Decentralization and Privacy: The Case of Blockchain Technologies. In: *Journal of Peer Production* (7), S. 1–19. Online verfügbar unter https://ssrn.com/abstract=2852689, zuletzt geprüft am 11.08.2020.

Deloitte (2019): Deloitte's 2019 Global Blockchain Survey. Blockchain gets down to business. Deloitte Development LLC. Online verfügbar unter https://www2.deloitte.com/content/dam/insights/us/articles/2019-global-blockchain-survey/DI_2019-global-blockchain-survey.pdf, zuletzt geprüft am 07.02.2020.

Dent, Alexander W. (2010): Choosing key sizes for cryptography. In: *Information Security Technical Report* 15 (1), S. 21–27. DOI: 10.1016/j.istr.2010.10.006.

Deuber, Dominic; Magri, Bernardo; Thyagarajan, Sri Aravinda Krishnan (2019): Redactable Blockchain in the Permissionless Setting. In: 2019 IEEE Symposium on Security and Privacy. 2019 IEEE Symposium on Security and Privacy (SP). San Francisco, CA, USA, 5/19/2019 - 5/23/2019. Los Alamitos, CA: IEEE Computer Society, S. 124–138.

Dwork, Cynthia; Naor, Moni (1992): Pricing via Processing or Combatting Junk Mail. In: Ernest F. Brickell (Hg.): Proceedings of the 12th Annual International Cryptology Conference CRYPTO '92, Bd. 740. Proceedings of the 12th Annual International Cryptology Conference CRYPTO '92. Santa Barbara, California, USA,. Berlin: Springer (Lecture Notes in Computer Science, 740), S. 139–147.

Eberhardt, Jacob; Tai, Stefan (2017): On or Off the Blockchain? Insights on Off-Chaining Computation and Data. In: Flavio de Paoli, Stefan Schulte und Einar Broch Johnsen (Hg.): Service-Oriented and Cloud Computing. 6th IFIP WG 2.14 European Conference, ESOCC 2017, Oslo, Norway, September 27-29, 2017, Proceedings, Bd. 10465. Cham: Springer International Publishing (Lecture Notes in Computer Science, 10465), S. 3–15.

EuGH (2016): Relativer Personenbezug dynamischer IP-Adressen. C-582/14. Online verfügbar unter http://curia.europa.eu/juris/document/document.jsf?docid=184668&doclang=DE, zuletzt aktualisiert am 19.10.2016.

European Commission (2017): Adequacy decisions. How the EU determines if a non-EU country has an adequate level of data protection. Online verfügbar unter https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en, zuletzt aktualisiert am 23.06.2020, zuletzt geprüft am 24.06.2020.

European Commission (24.06.2020): Commission report: EU data protection rules empower citizens and are fit for the digital age. Online verfügbar unter https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1163, zuletzt geprüft am 03.08.2020.

European Parliament (Hg.) (2018): Distributed ledger technologies and blockchains: building trust with disintermediation. Online verfügbar unter http://www.europarl.europa.eu/doceo/document/TA-8-2018-0373_EN.html, zuletzt geprüft am 12.02.2020.

Farshid, Simon; Reitz, Andreas; Roßbach, Peter (2019): Design of a Forgetting Blockchain: A Possible Way to Accomplish GDPR Compatibility. In: 52nd Hawaii International Conference on System Sciences.

Finck, Michhle (2017): Blockchains and Data Protection in the European Union. In: *SSRN Journal*. DOI: 10.2139/ssrn.3080322.

Florian, Martin; Henningsen, Sebastian; Beaucamp, Sophie; Scheuermann, Bjorn (2019): Erasing Data from Blockchain Nodes. In: 2019 IEEE European Symposium on

Security and Privacy Workshops (EuroS&PW). Stockholm, Sweden, 6/17/2019 - 6/19/2019: IEEE, S. 367–376.

Fridgen, Gilbert; Guggenberger, Nikolas; Hoeren, Thomas; Prinz, Wolfgang; Urbach, Nils (2019): Chancen und Herausforderungen von DLT (Blockchain) in Mobilität und Logistik. Hg. v. Bundesministerium für Verkehr und digitale Infrastruktur. Fraunhofer-Institut für Angewandte Informationstechnik FIT. Berlin. Online verfügbar unter https://www.bmvi.de/SharedDocs/DE/Anlage/DG/blockchain-gutachten.pdf, zuletzt geprüft am 10.04.2020.

Gentemann, Lukas (2019): Blockchain in Deutschland – Einsatz, Potenziale, Herausforderungen. Studienbericht 2019. Hg. v. Bitkom e.V. Berlin. Online verfügbar unter https://www.bitkom.org/sites/default/files/2019-06/190613_bitkom_studie_blockchain_2019_0.pdf, zuletzt geprüft am 07.02.2020.

Greenleaf, Graham (2019): Global Data Privacy Laws 2019: New Eras for International Standards. In: *Social Science Research Network*. Online verfügbar unter https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3384012, zuletzt geprüft am 24.06.2020.

Gupta, Rajneesh (2018): Hands-on cybersecurity with Blockchain. Implement DDoS protection, PKI-based identity, 2FA, and DNS security using Blockchain. Birmingham, UK: Packt Publishing. Online verfügbar unter http://proquest.tech.safaribooksonline.de/9781788990189.

Haber, Stuart; Stornetta, W. Scott (1991): How to time-stamp a digital document. In: *Journal of Cryptology* 3 (2), S. 99–111. DOI: 10.1007/BF00196791.

Hanschke, Inge (2020): Informationssicherheit und Datenschutz - einfach & effektiv. Integriertes Managementinstrumentarium systematisch aufbauen und verankern.

Herrera-Joancomartí, Jordi (2015): Research and Challenges on Bitcoin Anonymity. In: Joaquin Garcia-Alfaro (Hg.): Data privacy management, autonomous spontaneous security, and security assurance, Bd. 8872. Cham: Springer (Lecture Notes in Computer Science, 8872), S. 3–16.

Hofert, Eduard (2017): Blockchain-Profiling. Verarbeitung von Blockchain-Daten innerhalb und außerhalb der Netzwerke. In: *ZEITSCHRIFT FÜR DATENSCHUTZ*, S. 161–166.

Horster, P.; Fox, D. (2013): Datenschutz und Datensicherheit: Konzepte, Realisierungen, Rechtliche Aspekte, Anwendungen: Vieweg+Teubner Verlag.

Hughes, Laurie; Dwivedi, Yogesh K.; Misra, Santosh K.; Rana, Nripendra P.; Raghavan, Vishnupriya; Akella, Viswanadh (2019): Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda. In: *IJIM* 49, S. 114–129. DOI: 10.1016/j.ijinfomgt.2019.02.005.

Huh, S.; Cho, S.; Kimet, S. (2017): Managing IoT devices using blockchain platform. In: Proceedings of the 19th International Conference on Advanced Communications Technology: Phoenix Park, Pyeongchang, Korea (South), Feb, S. 19–22.

Hyvärinen, H.; Risius, M.; Friis, G. (2017): A blockchain-based approach towards overcoming financial fraud in public sector services. In: *Business & Information Systems Engineering* 59 (6), S. 441–456.

Iansitit, Marco; Lakhani, Karim R. (2017): The truth about blockchain. In: *Harvard business review : HBR* 95 (1), S. 118–127. Online verfügbar unter https://hbr.org/2017/01/the-truth-about-blockchain, zuletzt geprüft am 03.09.2019.

Isa, Herman; Bahari, Iskandar; Sufian, Hasibah; Z'aba, Muhammad Reza (2012): AES: Current security and efficiency analysis of its alternatives. In: IEEE (Hg.): 2011 7th International Conference on Information Assurance and Security. 2011 7th International Conference on Information Assurance and Security (IAS). Melacca, Malaysia, 12/5/2011 - 12/8/2011. IEEE: IEEE, S. 267–274.

Isler; Michael (2017): Datenschutz auf der Blockchain. In: *Jusletter*. Online verfügbar unter https://www.walderwyss.com/user_assets/publications/2231.pdf, zuletzt geprüft am 14.02.2020.

Jaikaran, Chris (2018): Blockchain: Background and Policy Issues. Hg. v. Congressional Research Service. Congressional Research Service.

Jawaheri, Husam Al; Sabah, Mashael Al; Boshmaf, Yazan; Erbad, Aiman (2020): Deanonymizing Tor hidden service users through Bitcoin transactions analysis. In: *Computers & Security* 89 (101684). DOI: 10.1016/j.cose.2019.101684.

Karame, G. O.; Androulaki, E. (2016): Bitcoin and Blockchain Security: Artech House Publishers.

Kazan, E.; Tan, C. W.; Lim, E. T. (2015): Value Creation in Cryptocurrency Networks. Towards A Taxonomy of Digital Business Models for Bitcoin Companies. In: Proceedings of the Pacific Asia Conference on Information Systems. (PACIS).

Kirsch, Zach; Chow, Ming (2015): Quantum Computing: The Risk to Existing Encryption Methods, S. 1–15. Online verfügbar unter http://www.cs.tufts.edu/comp/116/archive/fall2015/zkirsch.pdf, zuletzt geprüft am 10.02.2020.

Kohn, W.; Tamm, U. (2019): Mathematik für Wirtschaftsinformatiker: Grundlagen und Anwendungen: Springer Berlin Heidelberg.

Kõlvart, Merit; Poola, Margus; Rull, Addi (2016): Smart Contracts. In: Tanel Kerikmäe und Addi Rull (Hg.): The Future of Law and eTechnologies. 1st ed. 2016. Cham: Springer International Publishing, S. 133–147.

Kops, max (2017): EU möchte Geoblocking bei digitalen Währungen regulieren. Hg. v. BTC-ECHO. Online verfügbar unter https://www.btc-echo.de/geoblocking-digitale-waehrungen/, zuletzt geprüft am 12.02.2020.

Korpela, K.; Hallikas, J.; Dahlberg, T. (2017): Digital supply chain transformation toward blockchain integration. In: Proceedings of the 50th Hawaii International Conference on System Sciences.

Laurence, T. (2019): Introduction to Blockchain Technology: Van Haren Publishing.

LeBlanc, D.; Howard, M. (2002): Writing Secure Code: Pearson Education.

Lenstra, Arjen K. (2004): Key Lengths. Contribution to The Handbook of Information Security. Mendham, NJ.

Lu, Rongxing; Heung, Kevin; Lashkari, Arash Habibi; Ghorbani, Ali A. (2017): A Lightweight Privacy-Preserving Data Aggregation Scheme for Fog Computing-Enhanced IoT. In: *IEEE* 5, S. 3302–3312. DOI: 10.1109/ACCESS.2017.2677520.

Lumb, Richard; Treat, David; Jelf, Owen (2016): Editing the uneditable Blockchain. Why distributed ledger technology must adapt to an imperfect world. Online verfügbar unter https://www.accenture.com/_acnmedia/pdf-33/accenture-editing-uneditable-blockchain.pdf, zuletzt geprüft am 13.02.2020.

Mani, Vimal (2017): A View of Blockchain Technology From the Information Security Radar. In: Information Systems Audit and Control Association (Hg.): ISACA JOURNAL. Rolling Meadows, Illinois (4), S. 1–8. Online verfügbar unter https://www.isaca.org/resources/isaca-journal/issues/2017/volume-4/a-view-of-blockchain-technology-from-the-information-security-radar, zuletzt geprüft am 12.02.2020.

Marnau, Ninja (2017): Die Blockchain im Spannungsfeld der Grundsätze der Datenschutzgrundverordnung.

Martini, Mario; Weinzierl, Quirin (2017): Die Blockchain-Technologie und das Recht auf Vergessenwerden. Zum Dilemma zwischen Nicht-Vergessen-Können und Vergessen-Müssen. München. Online verfügbar unter https://dopus.uni-speyer.de/frontdoor/index/index/year/2017/docId/2487.

Matzutt, Roman; Henze, Martin; Ziegeldorf, Jan Henrik; Hiller, Jens; Wehrle, Klaus (2018): Thwarting Unwanted Blockchain Content Insertion. In: Abhishek Chandra (Hg.): 2018 IEEE IC2E. 2018 IEEE IC2E. Orlando, FL, 4/17/2018 - 4/20/2018. Piscataway, NJ: IEEE, S. 364–370.

Mauri, Ross (2017): Blockchain for fraud prevention: Industry use cases. IBM's Blockchain in Finance Service. Online verfügbar unter

https://www.ibm.com/blogs/blockchain/2017/07/blockchain-for-fraud-prevention-industry-use-cases/, zuletzt geprüft am 07.08.2019.
Maxwell, Winston; Salmon, John (2017): A guide to blockchain and data protection. Hg. v. Hogan Lovells.
MEDICI (2017): 21 Companies Leveraging Blockchain for Identity Management and Authentication. Hg. v. medium.com. Online verfügbar unter https://medium.com/@gomedici/21-companies-leveraging-blockchain-for-identity-management-and-authentication-d09d88e3a4bf, zuletzt geprüft am 19.06.2020.
Meiklejohn, Sarah; Pomarole, Marjori; Jordan, Grant; Levchenko, Kirill; McCoy, Damon; Voelker, Geoffrey M.; Savage, Stefan (2013): A fistful of bitcoins. In: Konstantina (Dina) Papagiannaki, Krishna Gummadi und Craig Partridge (Hg.): Proceedings of the 2013 conference on Internet measurement conference - IMC '13. the 2013 conference. Barcelona, Spain, 23.10.2013 - 25.10.2013. New York, New York, USA: ACM Press, S. 127–140.
MIT Media Lab (2020): Enigma - Securing the Decentralized Web. Online verfügbar unter https://www.enigma.co/, zuletzt aktualisiert am 17.06.2020, zuletzt geprüft am 22.06.2020.
Morabito, Vincenzo (2017): Business innovation through blockchain. The B3 perspective. Cham: Springer International Publishing. Online verfügbar unter https://ebookcentral.proquest.com/lib/gbv/detail.action?docID=4793398.
Morais, Eduardo; Koens, Tommy; van Wijk, Cees; Koren, Aleksei (2019): A survey on zero knowledge range proofs and applications. In: *SN Appl. Sci.* 1 (8), S. 319. DOI: 10.1007/s42452-019-0989-z.
Möser, Malte; Soska, Kyle; Heilman, Ethan; Lee, Kevin; Heffan, Henry; Srivastava, Shashvat et al. (2018): An Empirical Analysis of Traceability in the Monero Blockchain. In: *Proc. of PoPETs* (3). DOI: 10.1515/popets-2018-0025.
Niemzik, Maximilian (2019): Blockchain und DSGVO müssen kein Widerspruch sein. Online verfügbar unter https://m.heise.de/developer/artikel/Blockchain-und-DSGVO-muessen-kein-Widerspruch-sein-4337924.html?seite=all, zuletzt aktualisiert am 07.02.2020, zuletzt geprüft am 10.02.2020.
Nofer, Michael; Gomber, Peter; Hinz, Oliver; Schiereck, Dirk (2017): Blockchain. In: *Business & Information Systems Engineering* 59 (3), S. 183–187. DOI: 10.1007/s12599-017-0467-3.
Orcutt, Mike (2018): How secure is blockchain really? It turns out "secure" is a funny word to pin down. In: *MIT Technology Review*. Online verfügbar unter https://www.technologyreview.com/2018/04/25/143246/how-secure-is-blockchain-really/, zuletzt geprüft am 20.05.2020.
Piscini, Eric; Dalton, David; Kehoe, Lory (2017): Blockchain & Cyber Security. Hg. v. Deloitte Ireland LLP. Online verfügbar unter https://www2.deloitte.com/ie/en/pages/technology/articles/Blockchain_Cybersecurity.html, zuletzt geprüft am 12.02.2020.
Presse- und Informationsamt der Bundesregierung (Hg.) (2019): Blockchain-Strategie. Online verfügbar unter https://www.bundesregierung.de/breg-de/themen/digital-made-in-de/blockchain-strategie-1546662, zuletzt geprüft am 03.09.2019.
PwC (2018): Global Blockchain Survey 2018. PricewaterhouseCoopers. Online verfügbar unter https://www.pwc.de/de/digitale-transformation/global-blockchain-survey-2018.html, zuletzt geprüft am 03.09.2019.
Rannenberg, Kai; Camenisch, Jan; Sabouri, Ahmad (2015): Attribute-based Credentials for Trust. Cham: Springer International Publishing.
Reid, Fergal; Harrigan, Martin (2013): An Analysis of Anonymity in the Bitcoin System. In: Yaniv Altshuler, Yuval Elovici, Armin B. Cremers, Nadav Aharony und Alex Pentland (Hg.): Security and Privacy in Social Networks, Bd. 26. New York, NY: Springer New York, S. 197–223.

Robrahn, Rasmus; Bremert, Benjamin (2018): Interessenskonflikte im Datenschutzrecht - Die Rechtfertigung der Verarbeitung personenbezogener Daten über eine Abwägung nach Art. 6 Abs. 1 lit. f DSGVO. In: *ZEITSCHRIFT FÜR DATENSCHUTZ* (07), S. 291–300, zuletzt geprüft am 28.04.2020.

Salviotti, Gianluca; Rossi, Leonardo Maria de; Abbatemarco, Nico (2018): A structured framework to assess the business application landscape of blockchain technologies. In: Tung Bui (Hg.): HICSS-51 2018.

Sandhu, R. S.; Coyne, E. J.; Feinstein, H. L.; Youman, C. E. (1996): Role-based access control models. In: *Computer* 29 (2), S. 38–47. DOI: 10.1109/2.485845.

Sausen, Tim (2019): BVDW lobt Blockchain-Strategie der Bundesregierung. Hg. v. Bundesverband Digitale Wirtschaft (BVDW) e.V. Online verfügbar unter https://www.bvdw.org/der-bvdw/news/detail/artikel/bvdw-lobt-blockchain-strategie-der-bundesregierung/, zuletzt geprüft am 10.04.2020.

Schlatt, Vincent; Schweizer, André; Urbach, Nils; Fridgen, Gilbert (2016): Blockchain: Grundlagen, Anwendungen und Potenziale. Hg. v. Fraunhofer-Institut für Angewandte Informationstechnik FIT. Online verfügbar unter https://www.fit.fraunhofer.de/content/dam/fit/de/documents/Blockchain_WhitePaper_Grundlagen-Anwendungen-Potentiale.pdf, zuletzt geprüft am 09.09.2020.

Schlegel, M.; Zavolokina, L.; Schwabe, G. (2018): Blockchain Technologies from the Consumers' Perspective. What Is There and Why Should Who Care? In: Proceedings of the 51st Hawaii International Conference on System Sciences. (HICSS).

Schneider, David (2019): Ein kurzer Guide zu mehr Anonymität im Bitcoin-Netzwerk. Hg. v. BTC-ECHO. Online verfügbar unter https://www.btc-echo.de/ein-kurzer-guide-zu-mehr-anonymitaet-im-bitcoin-netzwerk/, zuletzt geprüft am 12.02.2020.

Schrey, Joachim; Thalhofer, Thomas (2017): Rechtliche Aspekte der Blockchain. In: *Neue juristische Wochenschrift* 70 (20), S. 1431–1436.

Shi, Jing; Zhang, Rui; Liu, Yunzhong; Zhang, Yanchao (2010): PriSense: Privacy-Preserving Data Aggregation in People-Centric Urban Sensing Systems. In: INFOCOM - IEEE Conference on Computer Communications workshops. Piscataway, NJ: IEEE, S. 1–9.

Skwarek, Volker (2019): Eine kurze Geschichte der Blockchain. In: *Informatik Spektrum* 42 (3), S. 161–165. DOI: 10.1007/s00287-019-01175-0.

Stokkink, Quinten; Pouwelse, Johan (2018): Deployment of a Blockchain-Based Self-Sovereign Identity. In: IEEE International Conference on iThings, GreenCom, CPSCom and SmartData. Halifax, NS, Canada: IEEE, S. 1336–1342.

Storj (2020): Decentralized Cloud Storage. Online verfügbar unter https://storj.io/, zuletzt geprüft am 19.06.2020.

Streim, Andreas; Hansen, Patrick (2019): Bitkom: Blockchain-Strategie gibt Aufbruchsignal. Bitkom e.V. Online verfügbar unter https://www.bitkom.org/Presse/Presseinformation/Bitkom-Blockchain-Strategie-gibt-Aufbruchsignal, zuletzt aktualisiert am 27.11.2019, zuletzt geprüft am 11.04.2020.

The Tor Project (2020): Privacy & Freedom Online. Online verfügbar unter https://www.torproject.org/, zuletzt aktualisiert am 14.04.2020, zuletzt geprüft am 28.04.2020.

Tönnissen, Stefan; Teuteberg, Frank (2020): DSGVO und die Blockchain. In: *Datenschutz und Datensicherheit* 44 (5), S. 322–327. DOI: 10.1007/s11623-020-1276-2.

Wijaya, Dimaz Ankaa; Liu, Joseph; Steinfeld, Ron; Liu, Dongxi; Yuen, Tsz Hon (2019): Anonymity Reduction Attacks to Monero. In: Fuchun Guo, Xinyi Huang und Moti Yung (Hg.): Information Security and Cryptology. 14th International Conference, Inscrypt 2018, Fuzhou, China, December 14-17, 2018, Revised Selected Papers. Cham, 2019. Cham: Springer International Publishing (Security and Cryptology), S. 86–100.

Wust, Karl; Gervais, Arthur (2018): Do you Need a Blockchain? In: 2018 Crypto Valley Conference on Blockchain Technology. Unter Mitarbeit von Emin Gün Sirer, Arthur

Gervais und Alexander Denzler. 2018 Crypto Valley Conference on Blockchain Technology (CVCBT). Zug, 6/20/2018 - 6/22/2018. Piscataway, NJ: IEEE, S. 45–54.

Yao, Jianbo; Wen, Guangjun (2008): Protecting Classification Privacy Data Aggregation in Wireless Sensor Networks. In: 4th International Conference on Wireless Communications, Networking and Mobile Computing. Dalian, China, 10/12/2008 - 10/14/2008. IEEE. Piscataway, NJ, S. 1–5.

Zhang, X.; Grannis, J.; Baggili, I.; Beebe, N. L. (2019): Frameup. An incriminatory attack on Storj: A peer to peer blockchain enabled distributed storage system. In: *Digital Investigation* 29, S. 28–42.

Zheng, Zibin; Xie, Shaoan; Dai, Hongning; Chen, Xiangping; Wang, Huaimin (2017): An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In: George Karypis und Jia Zhang (Hg.): 2017 IEEE International Congress on Big Data - BigData Congress 2017. 2017 IEEE International Congress on Big Data (BigData Congress). Honolulu, HI, USA, 6/25/2017 - 6/30/2017. Piscataway, NJ: IEEE, S. 557–564.

Zohar, Aviv (2015): Bitcoin: Under the Hood. In: *Commun. ACM* 58 (9), S. 104–113. DOI: 10.1145/2701411.

Zyskind, Guy; Nathan, Oz; Pentland, Alex Sandy (2015): Decentralizing Privacy: Using Blockchain to Protect Personal Data. In: 2015 IEEE Security and Privacy Workshops (SPW). 2015 IEEE Security and Privacy Workshops (SPW). San Jose, CA, 5/21/2015 - 5/22/2015. Piscataway, NJ: IEEE, S. 180–184.

7 Anhang

7.1 Zuweisung der Kategorisierung für Probleme

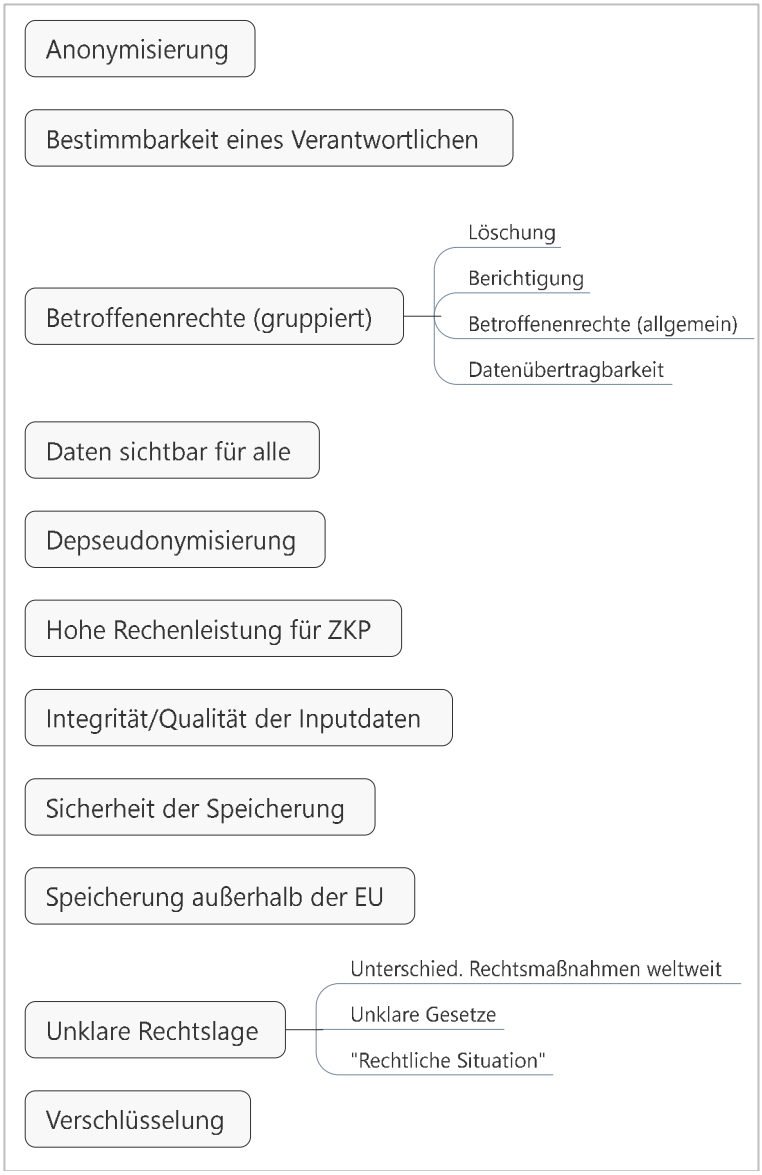


Abbildung 12: Gruppierung der Problembeschreibungen

7.2 Zuweisung der Kategorisierung für Lösungsvorschläge

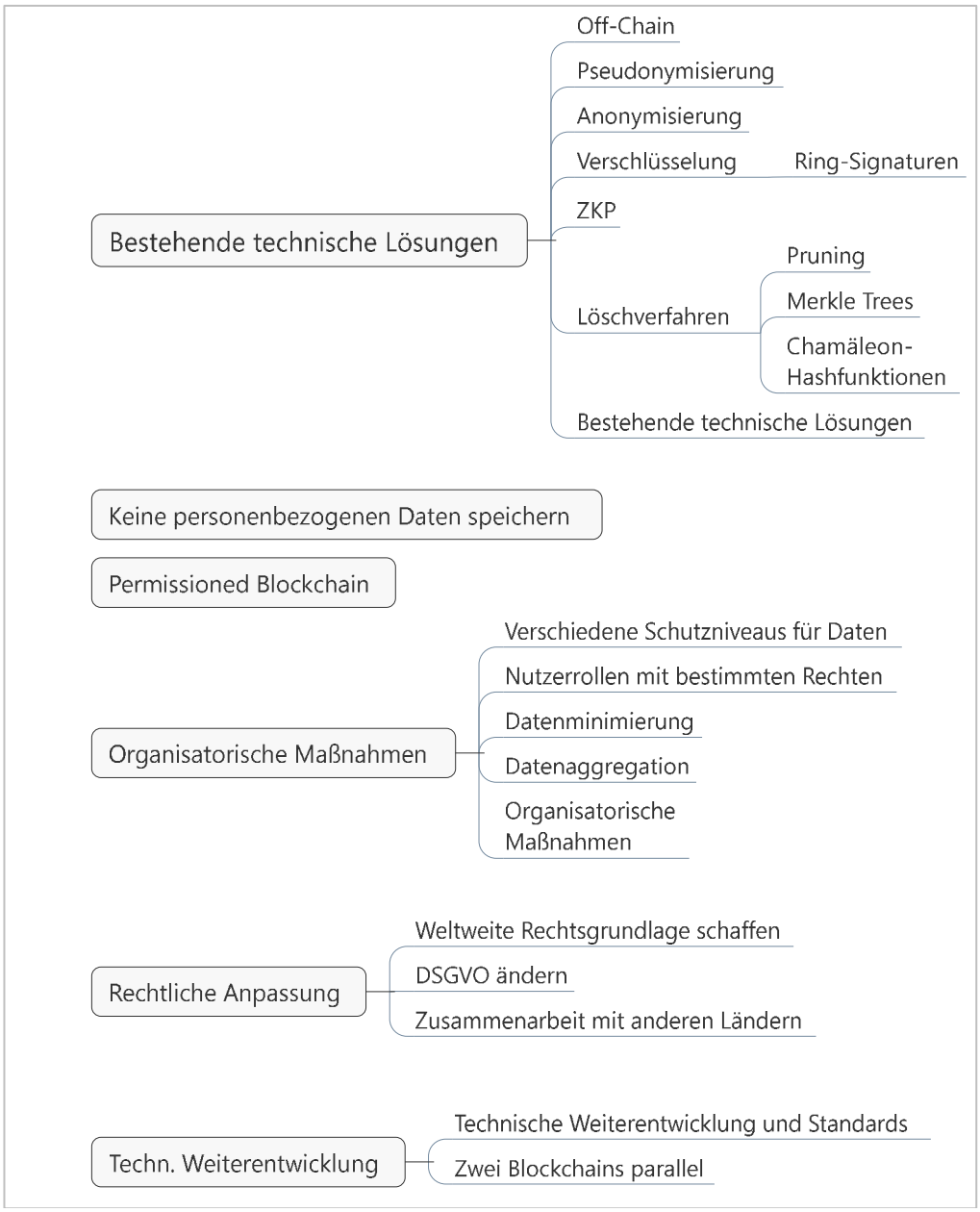


Abbildung 13: Gruppierung der Lösungsvorschläge

7.3 Probleme und deren Lösungsvorschläge in der Übersicht

Diese Abbildung zeigt alle genannten Probleme (Rauten-Form) sowie Lösungsvorschläge der Akteure (helles Rechteck) und weitere Lösungen in der Literatur (dunkles Rechteck).

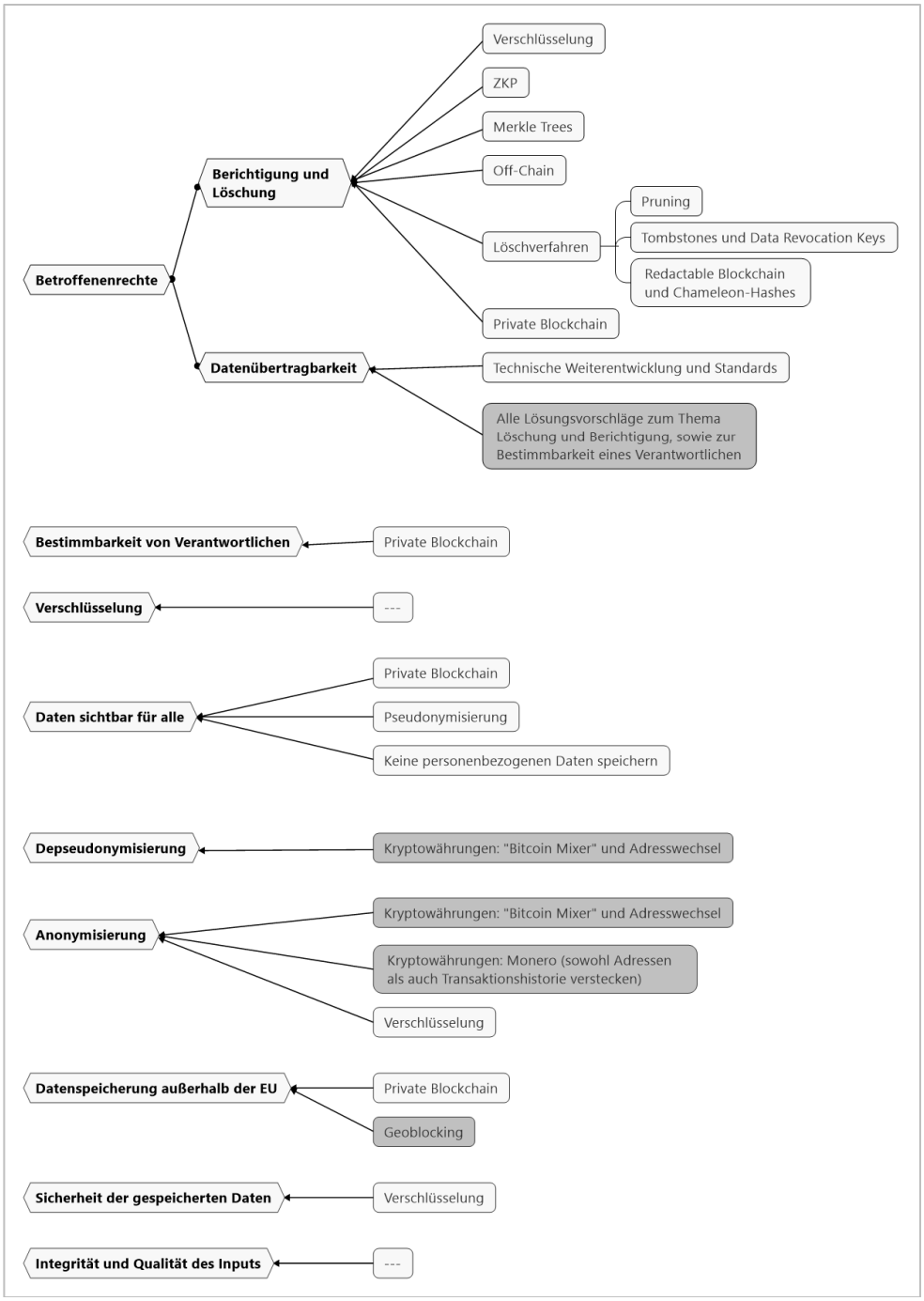


Abbildung 14: Übersicht über Datenschutzherausforderungen (Rauten-Form) und vorgeschlagene Lösungen von den Akteuren (helles Rechteck) und Literatur (dunkles Rechteck)

7.4 Detaillierte Auswertungen: Lösungsansätze der Akteure pro Anwendungsbereich

	Bestehende tech. Lösungen	***Technische Weiterentwicklung***	***Rechtliche Anpassung***	***Zugriffsbeschränkung (private BC)***	***Organisatorische Maßnahmen***	***Löschverfahren***	***Keinen personenbezogenen Daten speichern***	***Nutzerrollen und Rechte***
Allgemein	40	19	22	14	10	2	23	7
Energie	2	3	3	1	0	0	1	0
Finanzsektor	1	0	1	1	1	0	1	0
Gesundheit und Pflege	22	4	1	5	6	0	9	2
Identitätsmanagement	23	4	6	5	5	1	10	0
Internet der Dinge	18	3	0	3	0	0	9	0
Lieferketten und Logistik	2	1	3	2	0	0	0	0
Mobilität	20	1	5	5	1	0	8	1
Plattformökonomie	18	3	3	7	2	0	9	1
Verwaltung	8	1	0	3	0	0	5	0
Summe	***69***	***29***	***29***	***31***	***17***	***2***	***38***	***9***

Tabelle 2: Lösungsansätze der Akteure pro Anwendungsbereich[11]

[11] Anmerkung: Mehrfachnennungen der Akteure wurden in dieser Tabelle aufgenommen. Die Summenspalte zeigt jedoch nur Einfachnennungen der Akteure.

IMPRESSUM

Presse und Kommunikation:
Barbara Ferrarese, M.A.
Fraunhofer-Institut für System- und Innovationsforschung ISI
Breslauer Straße 48
76139 Karlsruhe

Telefon +49 721 6809-678
E-Mail presse@forum-privatheit.de

Projektkoordination:
Michael Friedewald
Fraunhofer-Institut für System- und Innovationsforschung ISI
Breslauer Straße 48
76139 Karlsruhe

Telefon +49 721 6809-146
Fax +49 721 6809-315
E-Mail info@forum-privatheit.de

www.isi.fraunhofer.de
www.forum-privatheit.de

Schriftenreihe:
Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt
ISSN-Print 2199-8906
ISSN-Internet 2199-8914

1. Auflage
Januar 2021

Zitiervorschlag:
Ebbers et al. (2020): White Paper Datenschutz in der Blockchain. Diskussion der Herausforderungen und Lösungsansätze auf Basis der Blockchain-Konsultation der Bundesregierung. Hrsg.: Michael Friedewald et al., Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt, Karlsruhe: Fraunhofer ISI.

forum <privatheit>
selbstbestimmtes_leben_in_der_digitalen_welt

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

PROJEKTPARTNER

Fraunhofer

Natur Technik Kultur Gesellschaft
UNIKASSEL VERSITÄT

provet
Projektgruppe verfassungsverträgliche Technikgestaltung

UNIVERSITÄT DUISBURG ESSEN
Offen im Denken

EBERHARD KARLS UNIVERSITÄT TÜBINGEN
INTERNATIONALES ZENTRUM FÜR ETHIK IN DEN WISSENSCHAFTEN

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein