Blockchain und Datenschutz

Faktenpapier

www.bitkom.org

bitkom

Herausgeber

Bitkom e.V.
Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
Albrechtstraße 10 | 10117 Berlin | Tel.: 030 27576-0 | bitkom@bitkom.org | www.bitkom.org

Ansprechpartner

Marco Liesenjohann | Referent Bitkom Think! & Blockchain
T 030 27576-207 | m.liesenjohann@bitkom.org

Autoren

Elke Kunde | IBM
Dr. Markus Kaulartz | CMS Hasche Sigle
Med Ridha Ben Naceur | GFT Technologies
Samater Liban | Blockchain Helix
Matthias Kunz | syracom
Prof. Dr.-Ing. Volker Skwarek | HAW-Hamburg
Prof. Dr.-Ing. Katarina Adam | HTW Berlin
Rebekka Weiß | Bitkom
Marco Liesenjohann | Bitkom

Satz & Layout

Katrin Krause | Bitkom e.V.

Blockchain und Datenschutz

Faktenpapier

Inhaltsverzeichnis

Tabellenverzeichnis

Abbildungsverzeichnis

1 Motivation

1 Motivation

Die Datenschutz-Grundverordnung (DS-GVO) setzt das Prinzip der Datensparsamkeit konkreter und konsequenter um, als das die bisherigen Bestimmungen des Bundesdatenschutzgesetzes (BDSG) getan haben. Der Ansatz ist, den Nutzer über das Erheben von personenbezogenen Daten vollständiger zu informieren und diese Informationen transparenter als bisher zur Verfügung zu stellen. Welche Technologien besonders geeignet sind, um als Basis für Lösungen zu dienen, die diesen Anforderungen genügen können, wird auf absehbare Zeit Gegenstand der Diskussion sein.

Blockchain und Distributed Ledger-Technologien[1] rücken im Zuge des allgemeinen Interesses auch verstärkt in den Anwärterkreis von Technologieplattformen, die für Datenschutz und Datensicherheit neue Perspektiven aufzeigen. Denn Blockchain-Systeme verbinden Datenspeicherung, Datenvermittlung und Datensicherung mit neuen Zugangs- und Prüfverfahren, die es erlauben, neue Lösungen für die steigenden Anforderungen im Zeitalter der Datenökonomie zu entwickeln.

Öffentliche Blockchains stehen zurzeit unter kritischer Beobachtung durch die Datenschutzseite. Das Kennzeichen öffentlicher Blockchains ist, dass sie eine für jedermann transparente und nachvollziehbare Speicherung von Datensätzen ermöglicht.[2] Das bekannteste Beispiel ist das 2009 gestartete Bitcoin-Netzwerk zur Übertragung digitaler Werttoken – Bitcoin als erste virtuelle Währung auf Basis der Blockchain-Technologie. Jeder Nutzer dieses Systems hinterlässt seine Historie von Finanztransaktionen als nachverfolgbare Spur in der Blockchain. Dieses Technologiedesign erlaubt es, sich über Daten, die auch personenbezogen sein können, vollständig zu informieren. Daneben sieht das System keinen zentralen Mittler vor und die Manipulation von Datensätzen durch Dritte ist praktisch ausgeschlossen. Viele Nutzer sehen darin eine Umsetzung des Prinzips der informationellen Selbstbestimmung. Ein Leitbild, das auch die DS-GVO hat.

Mit den Errungenschaften der Basistechnologie öffentlicher Blockchains gehen viele Herausforderungen aus datenschutzrechtlicher Sicht einher. Denn Nutzer bewegen sich im rechtlichen Sinne der DS-GVO nicht anonym auf der Blockchain. Die Nachvollziehbarkeit aller jemals durchgeführten Transaktionen lässt Nutzer immer nur pseudonymisiert am System teilhaben. Bekannte Verfahren zur Erhöhung der Anonymität im Sinne des Datenschutzes beispielsweise durch Aggregation von Pseudonymgruppen oder die Verwendung von sich modifizierenden Pseudonymen sind nicht Teil des Grundentwurfs.

Außerdem stehen weitere inhärente Merkmale einer öffentlichen Blockchain im augenscheinlichen Widerspruch zu Vorgaben der DS-GVO. Die Begrenzung der Speicherdauer von personenbezogenen Daten, wie in der DS-GVO vorgesehen, ist nicht mit der Unveränderlichkeit der Anordnung der Blöcke öffentlicher Blockchains in Einklang zu bringen.

Private und konsortiale Blockchains, die Bruchstellen öffentlicher Blockchains mit Datenschutzanforderungen an vielen Stellen zu heilen vermögen, stellen Anwender und Hersteller vor nicht weniger drängende Fragen. Denn erste Erfahrungen zeigen, dass ein Erfolg von Projekten dann

1 Eine Abgrenzung der beiden Technologien wird im Abschnitt ↗Blockchain abgegrenzt zum Distributed Ledger vorgenommen.

2 Dies findet sich etwa in der Analyse »How blockchain technology could change our lives« des European Parliamentary Research Service zu Fragen der Sichtbarkeit personenbezogener Daten in Blockchain-Systemen: ↗http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_EN.pdf.

wahrscheinlicher wird, wenn eine unternehmensweite Innovationsstrategie die Implementierung von Lösungen auf Blockchain-Basis begleitet. Das heißt, erfolgreiche Blockchain Use-Cases sind nicht nur Kopien bestehender Prozesse und Produkte, sondern sie betreten oft Neuland. Unsicherheit in Datenschutzfragen sind hier unvermeidbar. Insbesondere Anwendungsfälle in stark regulierten Branchen mögen in diesem Licht anders bewertet werden als ähnliche Lösungen in weniger regulierten Branchen.

Die Blockchain-Technologie selbst ist für Datenschutz-sensible Anwendungen nur so gut wie die darauf aufbauenden Lösungen. Technologie ist kein Selbstzweck und bedarf einer feinen Austarierung mit den Anforderungen gesetzlicher Rahmenbedingungen. Bei mehr und mehr Unternehmen setzt sich diese Erkenntnis auch mit Blick auf Blockchain-Systeme durch: sie bewerten Blockchain als eine geeignete Technologieplattform, um Lösungen zu bauen, die einem fortschrittlichen und technologiegestützten Datenschutz dienen. So sollten auch Privacy-by-Design Blockchain-Konzepte oder digitales Identitätsmanagement auf Blockchain-Basis verstanden werden – sie sind zuerst lösungsorientiert und bedienen sich der Werkzeuge, die die Technologie-Plattform Blockchain bereitstellt.

Mit dieser Veröffentlichung verfolgen wir das Ziel, einige der aufgeworfenen Fragen und Herausforderungen näher zu beleuchten und sowohl Anwendern, die Orientierung aus datenschutzrechtlicher Sicht suchen, als auch Lösungsanbietern aus der ITK-Branche, die ein Mehr an Rechtssicherheit für ihre Produkte und Dienstleistungen erreichen wollen, einen Überblick zur Thematik zu geben.

2 Klassifizierung von Blockchain-Systemen

2 Klassifizierung von Blockchain-Systemen

Um der Ausdifferenzierung der Technologie und der rasanten Weiterentwicklung Rechnung zu tragen, sind verschiedene Einordnungen von Blockchain-Systemen gebräuchlich. Diese Klassifizierungsschemata greifen einzelne Merkmale heraus und entwickeln daraus schlüssige Abgrenzungskriterien für den gewählten Rahmen. So können Klassifizierungen unter anderem erfolgen nach

- Berechtigung der Teilnahme und Nutzung (allgemeiner Zugang, Wahrnehmung von Rollen im System)
- Eigenschaften als Datenbank, verteiltes System und kryptographischer Verfahren (Einordnung mit Blick auf Art der verteilten und dezentralen Datenbank, P2P-Netzwerke, Konsens-Protokoll, Transaktionsgeschwindigkeit, Energiekosten)
- Einsatzzweck (Systeme in Anwendungslandsschaft, Verwendungszweck)
- Anonymität (»Grad der Anonymität« der am System Beteiligten)
- Art der Prüfungs- und Schreibberechtigung (Konsensmechanismen, Prüfverfahren für Netzwerkregeln)
- Art des Tokens[3] (Wertaufbewahrungsmittel, Anteile an Projekten, Schnittstellen-Nutzungsrechte, Gutscheine für Leistungen, Zugangs- und Teilnahmeberechtigung am System)
- Umfang und wirtschaftliche Bedeutung der Transaktionen (Micropayments, Massentransaktionen, manuell oder automatisch initiierte Transaktionen)

2.1 Öffentliche, private und konsortiale Blockchain-Systeme

Nicht nur in der Finanzbranche sondern auch in anderen Wirtschaftszweigen von der Logistik bis hin zur Energiewirtschaft werden Proof-of-Concepts und erste Lösungen auf Basis von Blockchain-Technologie vorangetrieben. Und auch hier ist die Entwicklung facettenreich und sind die Entwicklungszyklen kurz. Der Bedarf, öffentliche und private Blockchains nicht nur intra- sondern auch interoperabel zu gestalten, wird zur Entwicklung von Blockchain-Hybrid-Netzwerken führen. Projekte, die sich mit dieser Herausforderung auseinandersetzen, sind unter anderen ↗Polkadot, ↗Cosmos oder ↗Hyperledger Quilt. Die in Tabelle 1 vorgestellte Unterscheidung soll ein grundsätzliches Verständnis zur Unterscheidung von öffentlichen Blockchains auf der einen und privaten Blockchains auf der anderen Seite ermöglichen.

Gemeinsamkeiten	Unterschiede
Sie laufen auf einem dezentralen Peer-to-Peer-Netzwerk.	Öffentliche Blockchains erlauben eine Teilnahme für jedermann.
Jeder Teilnehmer des Netzwerks hält eine Kopie des geteilten Ledgers.	Öffentliche Blockains sind auf einen Anreizmechanismus angewiesen, um Teilnehmer am Netzwerk für die Konsensus-Findung zu motivieren.

3 Eine Definition zu Token findet sich zu Beginn des Abschnitts ↗Einsatzzwecke von Blockchain-Systemen.

Gemeinsamkeiten	Unterschiede
Der Ledger erlaubt nur das Anhängen von Transaktionen.	Private Blockchains erlauben Implementierungen zur Korrektur von Transaktionen.
Die Transaktionen sind mittels digitaler Signatur verbunden.	Governance Modelle können bei privaten Blockchains individuell festgelegt werden.
Es existiert ein Konsensus-Protokoll zum Synchronisieren des geteilten Ledger.	
Sie weisen bestimmte Eigenschaften auf, die die Unveränderlichkeit des Ledgers garantieren.	

Tabelle 1: Gemeinsamkeiten und Unterschiede von öffentlichen und privaten Blockchains.[4]

Die historische Entwicklung der Begriffe öffentliche und private Blockchain ist durch die unterschiedlichen Zugangsberechtigungen zu den jeweiligen Systemen motiviert. Klassische öffentliche Blockchain-Systeme erlauben das Lesen, das Anhängen von Blöcken (Schreiben) und das Prüfen der Daten für jeden Teilnehmer. In einer öffentlichen Blockchain werden die Teilnehmer, die Prüfen, Validieren und damit neue Blöcke anhängen, als Miner bezeichnet. Die Teilnehmer, die die komplette Blockchain lokal speichern und keine Blöcke anhängen, werden als Full-Nodes bezeichnet. Sie sind die Kontrollinstanz einer öffentlichen Blockchain, da sie die Arbeit der Miner auf Übereinstimmung mit den Regeln des Netzwerkes bezeugen. Im Gegensatz zu den Minern sind sie nicht ökonomisch motiviert, sondern ausschließlich Bewahrer der im Blockchain-Protokoll hinterlegten Regeln.

Information

Zum einen wird nach der Verwaltung der Blockchain gefragt:

- Permissionless – jedermann kann teilnehmen und neue Blöcke in die Blockchain schreiben.
- Permissioned – nur zugelassene Rechner können Transaktionen überprüfen und neue Blöcke schreiben.

Zum anderen ist der Zugang maßgeblich. (Wer erhält überhaupt Zugriff auf das Netzwerk und ist zumindest zum Lesen der Blockchain berechtigt):

- Public – jedermann hat Zugriff.
- Private – der Zugriff ist beschränkt.

Bei privaten und konsortialen Blockchains ist die Aufgabe des Prüfens und Anhängens an eine qualifizierte und bekannte Partei oder Gruppe übertragen. Auf gleiche Weise ist die Teilnahme am Netzwerk nicht allgemein zugänglich. Beispielsweise ist die Teilnahme nur aus einem festgelegten IP-Adressraum oder mit Zugang zu einem VPN möglich.

4 In Anlehnung an ↗https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/ (Abruf 5. Oktober 2017) und erweitert.

Die Begriffe permissioned (zulassungsbeschränkt) und permissionless (zulassungsfrei) werden häufig synonym für die Beschreibung privater/konsortialer bzw. öffentlicher Blockchains genutzt. Konzeptionell sind etwa öffentliche und zulassungsbeschränkte Blockchain-Systeme denkbar. Es sind etwa all diejenigen, die ein Proof-of-Stake Konsensverfahren nutzen. Der Erwerb von Tokens von bereits existierenden Teilnehmern des Systems ist Voraussetzung, um eine Prüfleistung technisch überhaupt erbringen zu können. Gleichzeitig wird durch den Erwerb die Zulassung erteilt, um als Prüfer am System teilnehmen zu dürfen. Auch im Hinblick auf die Bewertung der Entwicklung neuer Governance-Modellen von Blockchain-Systemen kann diese Art der Kategorisierung nutzenstiftend sein.[5] Abbildung 1 stellt die wichtigsten Merkmale dieser Unterscheidung dar.

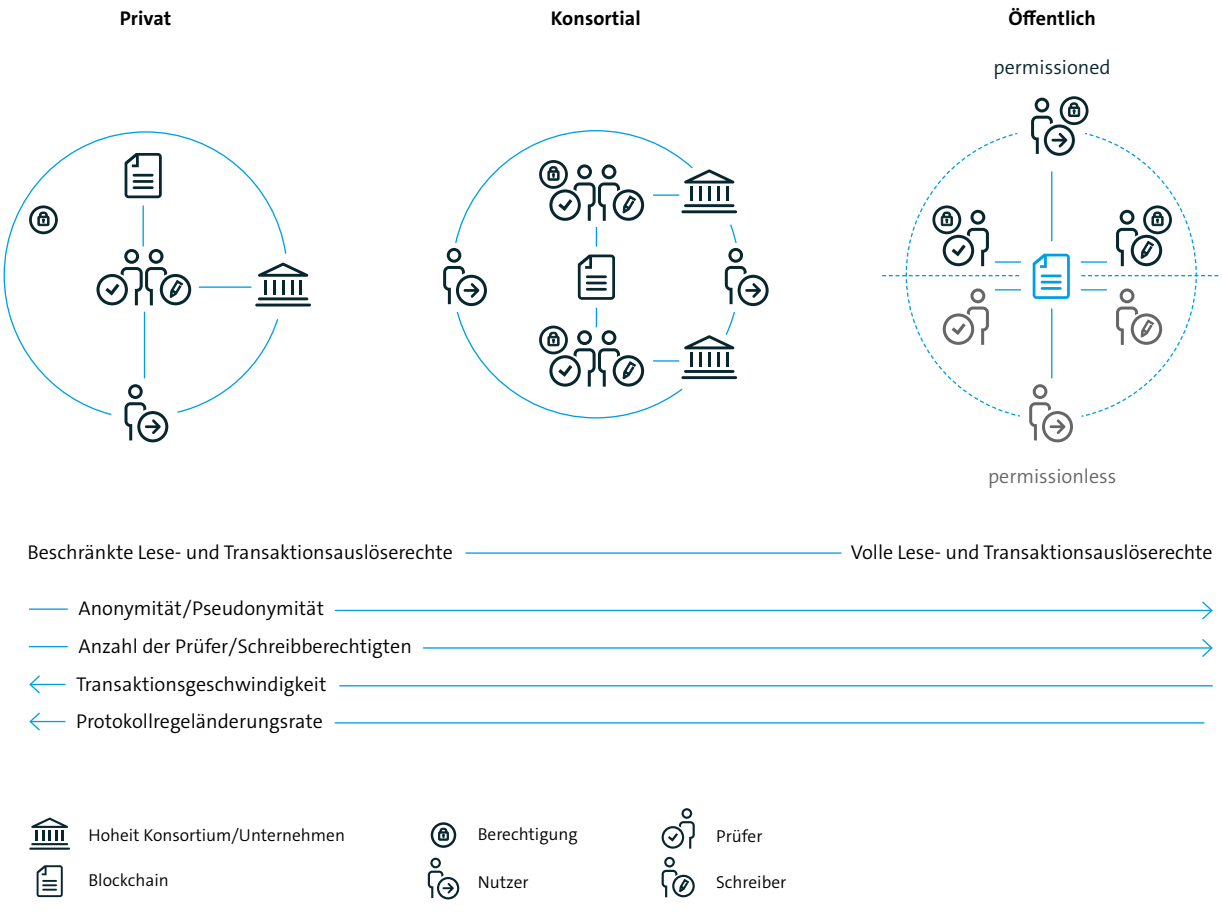

Abbildung 1: Ein Schema von Blockchain-Anwendungen mit Unterscheidung zwischen privatem (Nutzung durch ein Unternehmen/Organisation), konsortialem (Nutzung durch mehrere Unternehmen/Organisationen) und öffentlichem (grundsätzlich freie Teilnahme) System ist dargestellt. Außerdem werden fünf Eigenschaften in Bezug zu den drei Systemen gesetzt.

5 In einem Medium-Artikel zeigt Pavel Kravchenko Eigenschaftskombinationen für Blockchain-Systeme in einem Vier-Quadranten-Modell auf: ↗https://medium.com/@pavelkravchenko/ok-i-need-a-blockchain-but-which-one-ca75c1e2100 (Abruf 5. Oktober 2017).

2.2 Blockchain abgegrenzt zum Distributed Ledger

Distributed Ledger ist die Bezeichnung für eine Art von verteilter Datenbank. Die Datenbank ist mehrfach in Kopie lokal bei den Teilnehmern eines Netzwerks, den sogenannten Nodes, gespeichert. Der Austausch von Daten erfolgt in der Regel auf Basis einer Peer-to-Peer-Netzwerk-Architektur. Teil des Netzwerkprotokolls sind Konsensmechanismen die dafür sorgen, dass stets alle Kopien synchronisiert sind und nur ein einziger Zustand der Datenbank existiert.

Blockchains können als Untergruppe von Distributed Ledger-Systemen verstanden werden. Die Besonderheit von Blockchain-Systemen ist die Speicherung von Datensätzen mittels hash-verketteter Listen. Wie alle Distributed Ledger-Verfahren werden Informationen durch Verteilen abgesichert.[6]

In Tabelle 2 werden die generellen Unterschiede von Blockchains mit verteilten Datenbanken aufgeführt. Beim Einsatz von Blockchain-Systemen als Datenbank sind die Anforderungen der Anwendung in Bezug auf Skalierbarkeit, der Abfragbarkeit (Queryability) und der Operationalisierbarkeit besonders zu beachten.

Blockchain	Eigenschaften	Datenbank
Nur anhängen	**Operationen**	Einfügen, Aktualisieren, Löschen
Ja	**Redundanz**	Ja
Ja	**Hochverfügbarkeit**	Ja
Block (z.B. PoW)	**Konsenssystem**	Row, Replica Set
Immer	**Signaturen**	Manuell
Immer	**Datenprüfung**	Manuell
Smart Contracts	**Business Logic**	Gespeicherte Prozeduren
Ledger	**Primäre Verwendung**	Generisch

Tabelle 2: Vergleich der Eigenschaften einer Blockchain als Datenbank im Vergleich mit verteilten Datenbanken.

2.3 Einsatzzwecke von Blockchain-Systemen

Ein wichtiges Element von Blockchain-Systemen ist der sogenannte Token. Ein Token kann als fälschungssichere, digitale Entsprechung einer Urkunde mit inhärenter Übertragbarkeit definiert werden. In öffentlichen Blockchain-Systemen stellt er den sichtbaren Teil des im Protokoll kodifizierten Anreizmechanisums dar. Miner erhalten Token für das Anhängen von Blöcken mit regelkonformen Transaktionen, Nutzer zahlen Transaktionsgebühren in Token, um das Netzwerk zu

6 Vergleiche die Arbeit der ISO TC 307: ↗https://www.iso.org/committee/6266604.html.

nutzen. Token können darüber hinaus als Teilhabe an einem Projekt oder Anteil an einem Unternehmen, als Medium für Anwendungen im Web 3 oder als Zugangsrechte für Leistungen, Produkte oder Daten eines Netzwerkes verstanden werden. Token, deren einzige Funktion eine digitale Verkörperung von Wert ist, werden als Kryptowährungen oder virtuelle Währungen bezeichnet.

Öffentliche Blockchain-Systeme werden im Zuge dessen danach bewertet, welche Funktionalitäten sie in der Tokenökonomie darstellen.

2.4 Öffentliche Systeme

Der Token der klassischen Blockchain des Bitcoin-Netzwerks wird gemeinhin als Vertreter einer Kryptowährung verstanden – eher digitales Wertaufbewahrungsmittel, als digitales Zahlungsmittel. Bitcoin als alltägliches Zahlungsmittel z.B. im Onlinehandel konnte sich bisher nicht durchsetzen.[7] Verschiedene Erweiterungen des Bitcoin-Protokolls ab Mitte des Jahres 2017 verringern die technisch bedingten Einschränkungen im Hinblick auf diesen Einsatzzweck entfällt. Aufgrund der größten Marktkapitalisierung unter allen Blockchain-Token wird der Bitcoin als Referenzwert für alle anderen Token genutzt.

Die Skalierbarkeit von Blockchain-Systemen mit Blick auf den Durchsatz von Transaktionen ist eine weiterhin bestehende Entwicklungsaufgabe des Technologiefelds. Ein Ansatz um Anwendungen im Bereich des IoT zu ermöglichen, ist die Tangle-Architektur von IOTA. Das System ist als Infrastruktur für hohe Kommunikationsraten bei geringsten Transaktionsbeträgen ausgelegt. Der aktuelle Entwurf sieht keine Transaktionsgebühren, wie in klassischen Blockchain-Systemen vor und ist ein Distributed Ledger, keine Blockchain.

Ethereum ist die zurzeit vielversprechendste öffentliche Blockchain-Infrastruktur. Die Bereitstellung von Smart-Contracts, die ein Rahmenwerk für verteilten und automatisch ausführbaren Code darstellen und an Bedingungen geknüpfte Ausführung von Programmen erlauben, hat die Blockchain-Technologie-Entwicklung der letzten Jahre maßgeblich geprägt. Anwendungen sind dezentrale Apps (dApps), dezentrale autonome Organisationen und Anwendungen »ohne Mittelsmann«. Die Schaffung eines De-Facto-Standards für die Erzeugung neuer Token auf Basis von Smart-Contracts hat bedeutenden Anteil an der starken Zunahme von Token Generating Events (TGE)[8] in Form von Initial Coin Offerings (ICOs) im Jahr 2017. Die Anzahl der durchschnittlich aktiven Nodes (sie halten die Blockchain-Historie vor) ist mit einem Durchschnittswert von 22000 im Oktober 2017 etwa doppelt so groß als im Bitcoin-Netzwerk.[9]

7 Im Gespräch ist zurzeit die Einführung als Zahlungsmittel beim Onlinehändler Amazon: ↗http://www.businessinsider.de/geruecht-amazon-will-bitcoin-als-zahlungsmittel-zulassen-2017-10.

8 Das Bitkom Positionspapier »Token Generating Events als neue Säule der Wachstumsfinanzierung« gibt einen knappen Überblick zum Thema: ↗https://www.bitkom.org/Bitkom/Publikationen/Token-Generating-Events-als-neue-Saeule-der-Wachstumsfinanzierung.html.

9 Ethereum Netzwerk Statistik: ↗https://www.ethernodes.org/network/1; Bitcoin Netzwerk Statistik: ↗https://bitnodes.earn.com/

Andere Systeme die Blockchain-Technologie nutzen und ein dezentrales Zahlungssystem darstellen sind Monero und ZCash. Beide Systeme sind Antworten auf die Pseudonymität von Nutzern auf öffentlichen Blockchain-Systemen. Sie nutzen Verfahren zur Anonymisierung von Nutzern, Transaktionsdaten und zum Teil von Prüfern. Der Anspruch beider Systeme ist es tatsächliche Anonymität zu gewährleisten.

Monero setzt dabei zum einen auf eine Verschleierung der Transaktionsabfolge, in dem die Absenderadresse einer Transaktion versteckt wird. Die Absenderadresse wird Teil einer Gruppe möglicher Absenderadressen. Dieses Verfahren heißt »ring signatures«. Eine Analyse der Transaktionshistorie und Datenanalyse ist nur dann eine Möglichkeit zur Aufhebung der Verschleierung, wenn die Gruppe klein ist und die Auswahl nicht zufällig. Das bekannte Verfahren im technischen Datenschutz zur IP-Anonymisierung durch Aggregation setzt auf demselben Grundgedanken auf. Durch das »ring confidential transactions«-Verfahren ist es außerdem möglich den Betrag einer Transaktion zu verbergen. »Stealth Adresses« werden genutzt, um die Identität des Adressaten geheim zu halten.

ZCash nutzt das Konzept von »zero-knowledge proofs« auf Basis der »sk-SNARKs-Variante«. Die Geschichte eines »zero knowledge proofs« beginnt mit zwei Akteuren – der eine Akteur möchte den zweiten Akteur von Wissen über ein Geheimnis überzeugen, das er besitzt. Der zweite wird in die Lage versetzt, dieses Wissen über das Gehemnis zu bestätigen, ohne dass das Geheimnis ihm dabei bekannt wird. Dieses Verfahren wird eingesetzt, um sogenannte »shielded transactions« durchzuführen, die Sender, Empfänger und Transaktionsdaten verbergen. Zcash verfolgt damit einen technisch anderen Ansatz als Monero..

Eine Übersicht über öffentliche Blockchain- und Distributed Ledger-Systeme findet sich in Tabelle 3.

Name des Systems	Zweck	Handelbarer Token	Datenzugang	Protokoll	Weitere Merkmale
Bitcoin	Kryptowährung, Werttransfer ohne Intermediär	BTC, BCC	öffentliche Blockchain	Bitcoin-Protokoll	Proof-of-Work-Konsensmechanismus, Anzahl der Token ist fix
Monero	Kryptowährung, anonymer Werttransfer ohne Intermediär	XMR	öffentliche Blockchain	CryptoNote	Proof-of-Work-Konsensmechanismus, Anzahl der Token nimmt zu.
ZCash	Kryptowährung, anonymer Werttransfer ohne Intermediär	ZEC	öffentliche Blockchain	Zerocash	Proof-of-Work-Konsensmechanismus. Anzahl der Token ist fix.
Ethereum	Verteiltes System zur Bereitstellung von Rechenleistung	ETH	öffentliche Blockchain	Ethereum-Protokoll	Proof-of-Work-Konsensmechanismus; Smart Contract Funktionalität; Dezentrale Virtuelle Maschine; Plattform für dezentrale Apps (dApp); ERC-20-Standard für das Erzeugen von Tokens; Anzahl der Ethereum-Token nimmt zu.

Name des Systems	Zweck	Handelbarer Token	Datenzugang	Protokoll	Weitere Merkmale
IOTA	Infrastruktur für Transaktionen im IoT	MIOTA	öffentlich	Tangle-Protokoll	Tangle-Architektur (directed acyclic graph (DAG)); Distributed Ledger, keine Blockchain; Anzahl der Token ist fix.
Ripple	Infrastruktur für Interbanken-Transaktionen	XRP	öffentlich (ein Teil)	Interledger Protocol	Shared public database, keine Blockchain; Transaktionsinformationen sind öffentlich, Zahlungsinformationen nicht; Anzahl der Ripple-Token ist fix.

Tabelle 3: Übersicht zu einigen öffentlichen Blockchain und Distributed Ledger Systemen.

2.5 Beispiel-Use-Case Authentifizierung mittels öffentlichem Blockchain-System

Diese Authentifizierungslösung ist in Zusammenarbeit zwischen GFT Technologies SE und Auth0 entwickelt worden[10]. Das Ziel des Authentifizierungsverfahrens auf Blockchain-Basis ist, dass Ethereum-Nutzer fürs Login auf Webseiten von Drittanbietern lediglich ihre Ethereum-Adressen ohne Eingabe von weiteren für die jeweilige Webseite erforderlichen Benutzernamen oder Passwörtern nutzen.

Folgende Anforderungen wurden an die Umsetzung dieses neuen Authentifizierungsverfahrens gestellt:

- Die Webseite des Drittanbieters soll das Verfahren unterstützen, d.h. dieser ermöglicht den Zugang für Benutzer auf Basis ihrer Ethereum-Adresse (API-Anbindung ist vorhanden)
- Das Verfahren muss einfach konzipiert und benutzerfreundlich sein
- Die Sicherheit des Ethereum-Kontos darf nicht gefährdet werden. Der User muss in der Lage sein, sein Ethereum-Konto fürs Login zu nutzen, ohne jedes Mal seinen »private key« einzusetzen.
- Im Falle eins Verlustes müssen die Benutzer in die Lage versetzt werden, ihre Zugangsdaten wiederherzustellen
- Der Benutzer muss kein spezielles Wissen bezüglich Smart Contracts oder dem manuellen Aufruf von Smart Contracts in Ethereum haben
- Die Nutzung des Verfahrens soll kostenlos sein. Die Benutzer setzen keine Ether ein, wenn sie das Login zu Webseiten Dritter über deren Ethereum-Konto nutzen.

Um ein Verfahren zu entwickeln, das die oben genannten Anforderungen erfüllt, werden ein Authentifizierungsserver, eine mobile Application und das Ethereum-Netzwerk benötigt. Das Zusammenspiel dieser drei Komponenten ist in ↗Abbildung 2 dargestellt.

10 Weitergehende Informationen zur Registrierung für das Verfahren und detaillierte Beschreibung des Authentifizierungsprozesses bzw. Login-Prozesses können unter ↗https://auth0.com/blog/an-introduction-to-ethereum-and-smart-contracts-part-3/ eingesehen werden.

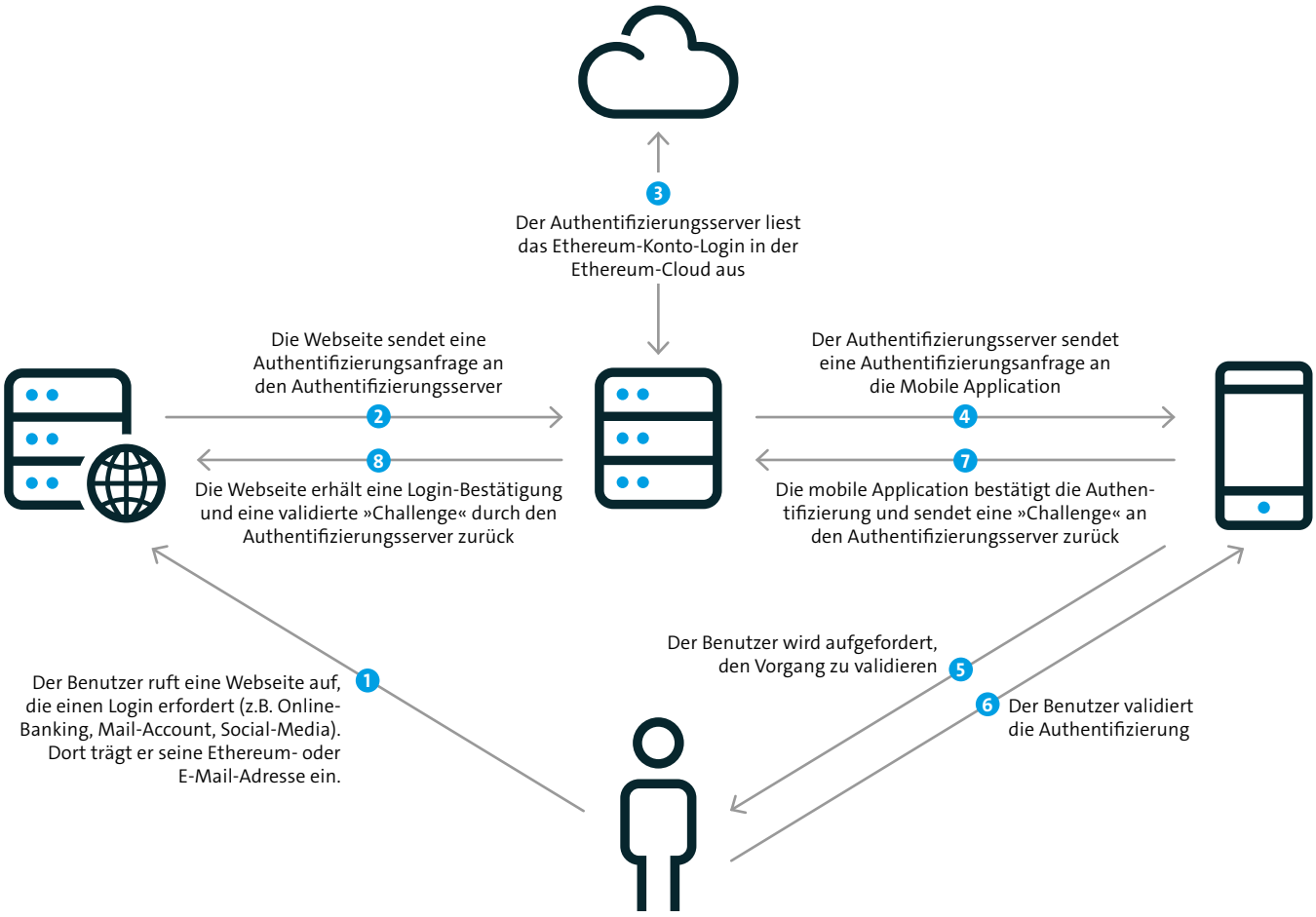

Abbildung 2: Schematische Darstellung eines Login-System mit Authentifizierung auf Basis eines Ethereum-Accounts (Uses-Case der Unternehmen GFT Technologies SE und Auth0).

Um der Sicherheit Rechnung zu tragen und die Ethereum-Adresse zu schützen, wird eine sogenannte Ethereum-Subadresse (login-only-Adresse) vom System generiert, welche ausschließlich für den Authentifizierungsprozess benutzt wird. Diese Subadresse wird mit der Ethereum-Hauptadresse durch einen Smart Contract gemappt. Dieser Smart Contract (der das Mapping abbildet) wird in der Ethereum-Blockchain gespeichert und hat folgende Funktionen:

- Mapping der 2 Ethereum-Adressen: Ethereum-Hauptadresse (the primary address) und Ethereum-Subadresse (login-only)
- Sicherstellung, dass nur der Besitzer der Hauptadresse das Mapping vornehmen kann
- Speicherung der Information in der öffentlichen Blockchain
- Anstoßen von Events, um Veränderungen der im Smart Contract gespeicherten Daten zu überwachen und darauf zu reagieren

2.6 Private und konsortiale Systeme

Hyperledger Fabric ist ein Open Source Blockchain Framework der Linux Foundation. Dort sind bewusst keine Token eingebaut, um eine »general purpose«-Blockchain zur Verfügung zu stellen. Diese bildet nicht notwendigerweise Zahlungsverkehrsanwendungen ab, sondern ist universell einsetzbar. Werden Token benötigt, werden diese im Datenmodell definiert.

Hyperledger Fabric bietet die optionale Rolle eines Regulators für den Einsatz in regulierten Industrien im Blockchain-Netzwerk. Teilnehmer können die Vertraulichkeit ihrer Transaktionen gegenüber anderen Teilnehmern wahren. Der Konsensmechanismus ist wählbar; aus Skalierungsgründen wird ein Quorum-basiertes Protokoll als Default verwendet. Proof-of-Work oder Proof-of-Stake können genauso verwendet werden. Das Haupteinsatzgebiet von Hyperledger Fabric sind private Blockchain-Netzwerke mit hohen Vertraulichkeitsanforderungen (z.B. private Kanäle/Untergruppen im Blockchain-Netzwerk).

Eine Übersicht über Blockchain- und Distributed Ledger-Systeme für den Einsatz in privaten oder konsortialen Netzwerken findet sich in Tabelle 4.

Name des Systems	Zweck	Handelbarer Token	Datenzugang	Protokoll	Weitere Merkmale
Hyperledger Fabric	Blockchain-Implementierung für Anwendungen und Lösungen »for business«	-	privat/ konsortial	Graduiertes Framework aus dem Hyperledger-Projekt der Linux Foundation	Konsensmechanismus ist austauschbar; Smart Contracts durch Chaincode-Funktionalität; optionale Funktionen für regulierte Industrien.
R3 Corda	Distributed Ledger-Plattform für Anwendungen der Finanzbranche	-	privat/ konsortial	Eigenentwicklung von R3CEV	Konsensmechanismus durch Notaries (RAFT, BFT, ...); Smart Contract Funktionalität, keine Blockchain.

Tabelle 4: Beispiele zu Blockchain und Distributed Ledger Systemen für private/konsortiale Einsatzszenarien.

2.7 Datenschutz in Blockchain-Systemen

Öffentliche und private bzw. konsortiale Blockchain-Systeme unterscheiden sich aus datenschutzrechtlicher Sicht, weil öffentliche Systeme eine grundsätzliche Sichtbarkeit von Daten auf der Blockchain erlauben. In die Gruppe der öffentlichen Blockchain-Systeme fallen all diejenigen Netzwerke, bei denen es keine Hürden für den Zugang zu den Daten auf der Blockchain und zur Nutzung des Netzwerks gibt. Es existieren keine Betreiber, die sich zur Bereitstellung zentraler Elemente der Infrastruktur verpflichten. Vielmehr sorgen ökonomische Anreizstrukturen für eine Ausdifferenzierung verschiedener Gruppen von Akteuren. Bekannte öffentliche Blockchain-Netzwerke wie Ethereum oder Bitcoin sorgen durch Ausgestaltung des zugrundeliegenden Protokolls dafür, dass ein solcher Anreiz als Folge des genutzten Konsensmechanismus existiert.

Mittlerweile erlaubt das Ökosystem rund um öffentliche Blockchains nicht nur den unmittelbaren Zugang, sondern auch die mittelbare Teilnahme an Blockchain-Systemen. Unmittelbarer Zugang soll bedeuten, dass der Teilnehmer einen eigenen Private-Key besitzt und mit den Public-Keys am Blockchain-Netzwerk teilnimmt. Das ist zum Beispiel

- im Fall von Bitcoin gegeben, wenn die Nutzung einer Wallet zum Senden und Empfangen von Bitcoin auch einen Private Key bereitstellt,
- im Fall von Ethereum gegeben bei Erstellung eines Accounts zum Einrichten von Smart Contracts oder dem Verwenden von dApps.

Ein mittelbarer Zugang ist dann gegeben, wenn der Nutzer keinen eigenen Private Key für ein Blockchain-Netzwerk besitzt und einen Zugang über einen Dienstleister erhält. Der überwiegende Teil der Plattformen zum Handel von Kryptowährungen fällt in diese Kategorie, ebenso einige Walletanbieter. Im Fall des mittelbaren Zugangs erheben Handelsplattformen gemäß bestehender Regulierungsvorschriften in Abhängigkeit des jeweiligen Angebots KYC-Daten ihrer Nutzer. Der Nutzer ist in diesen Fällen nicht Teilnehmer am Blockchain-Netzwerk. Miner ebenso wie Nodes haben stets unmittelbaren Zugang.

Im Sinne der DS-GVO entstehen sowohl bei un- als auch mittelbarem Zugang Daten, die auf Personen zurückgeführt werden können. Ein Merkmal von vielen öffentlichen Blockchain-Systemen ist die transparente Darstellung aller eingespeisten Datensätze. In Verbindung mit der eindeutigen digitalen Referenz (öffentlicher Schlüssel), die einen Teilnehmer kennzeichnet, sind viele der Systeme für Nutzer deshalb nicht anonym. Für die Darstellung der Historie der Datensätze und zum Datensammeln, -analysieren und -aufbereiteten existieren frei zugängliche Dienste (Block-Explorer, Transaktionsgraphenanalyse, etc.). Aus Datenaggregation lässt sich mit Hilfe dieser Werkzeuge auch von vielen öffentlichen Schlüsseln auf einen dahinterstehenden Akteur schließen.

Ein Fokus der Entwicklung für öffentliche Blockchain-Systeme liegt deshalb darauf, Lösungen zu entwickeln, die anonymes Agieren in Blockchain-Systemen zulassen. Blockchains auf Basis des CryptoNote-Protokolls versprechen Transaktionen, bei denen die Nutzer anonym agieren können und auch der Transkationsinhalt verborgen wird. Gleichzeitig sind Funktionalitäten, die ausgewählten Gruppen selektiven Zugang zu bestimmten Aktivitäten eines Nutzers erlauben denkbar. Monero, eine Kryptowährung auf Basis des CryptoNote-Protokolls, setzt diese Idee in Form eines »view keys« um. Diese Methode könnte etwa dem Regulierer erlauben, seiner Aufsichtsfunktion in Blockchain-Systemen nachzugehen – ohne dass es zentrale Punkte wie in heutigen Systemen gibt, die als Anlaufstelle dienen.

In privaten und konsortialen Blockchains ist die datenschutzrechtliche Perspektive eine andere, deshalb sind die verfolgten Ansätze andere. Wie zu Beginn vorgestellt, ist die Entwicklung von privaten und konsortialen Blockchain-Systemen Ausdruck der Anforderungen der Unternehmen gegenüber der Regulierung oder es liegt ein Anwendungsfall in einem geschlossen B2B-Prozess vor. Technologische Grundlage können hier Distributed Ledger oder Blockchain-Systeme sein. Die Verwendung von privaten Systemen stellt ein höheres Maß für den Schutz von Daten dar, wenn zentrale, identifizierte Punkte im System, die als Verantwortliche agieren, als Garant dafür verstanden werden bzw. der Zugang zum Netzwerk auf identifizierbare Teilnehmer beschränkt ist,

deren Zugang zu Transaktionen untereinander nochmals mit Rechtekonzepten beschränkt werden kann.

Gerade im Bereich von hochsensiblen Daten, etwa im Gesundheitsbereich, können Konzepte aus privaten Blockchains, die unter Sidechains, State Channels, Private Channels oder Off-chain Messaging firmieren, und sensible Daten aus der eigentlich Blockchain herausnehmen, in Kombination mit der anonymen Auditierbarkeit von Metadaten mit Vorbildern in öffentlichen Privacy-by-Design Blockchains, fortschrittliche Lösungen für den technisch gestützten Datenschutz bereitstellen.

Die Vereinbarkeit der Grundeigenschaft einer Blockchain, unveränderlich zu sein, mit Datenschutzaspekten wie z.B. dem Recht auf Löschung muss technisch im Design der Implementierung des Anwendungsfalles Rechnung getragen werden (Privacy by Design). Datenschutzrelevante Daten dürfen dann nicht in der eigentlichen Blockchain gespeichert werden, jedenfalls auf keinen Fall im Klartext.

Mögliche technische Optionen können sein:

- Diese Daten mit Encryption- und Decryption-Keys zu erstellen und im Falle der Löschung den Decryption-Key zu löschen.
- Dem Eigentümer der Daten einen Private-Key zur Verfügung zu stellen, der den Lesezugriff erst ermöglicht. Die Kontrolle liegt dann beim Eigentümer.
- Die Daten in einer referenzierten verschlüsselten Datenbank ablegen und den Pointer und Hash in der Blockchain ablegen. Der Hash dient dann als Nachweis, dass die Daten nicht verändert wurden. Bei Löschanforderung wird der Eintrag in der Datenbank gelöscht und der Pointer geht ins Leere.

3 Die Sicht des Datenschutzes auf Blockchain-Systeme

3 Die Sicht des Datenschutzes auf Blockchain-Systeme

3.1 Grundsätzliches

Die Offenheit der klassischen Blockchains, die sich aus dem Bedürfnis nach Nachvollziehbarkeit der einzelnen Transaktionen begründet, wurzelt in dem der Blockchain inhärenten Gedanken, dass nur durch diese Offenheit das Vertrauen in die Sicherheit und Nachvollziehbarkeit geschaffen werden kann, welches sonst durch den kontrollierenden Dritten, den Intermediär, geschaffen wird.

Die Architektur der Blockchain hat daher grundsätzliche Vorteile wie Transparenz und Sicherheit, die Transaktionen sind nicht nur kryptografisch gesichert sondern auch dauerhaft gespeichert und nicht manipulierbar. Die Sicherheit und Nicht-Manipulierbarkeit der Datensätze entsteht aus der dezentralen Speicherung der Daten, da jeder manipulierte Block bzw. jede manipulierte Blockchain sofort erkannt werden würde. Die dauerhafte Speicherung der Datensätze ist jedoch aus datenschutzrechtlichen Aspekten genauer zu untersuchen. Denn es ist offensichtlich, dass die dauerhafte Speicherung mit dem Recht auf Vergessen werden (Artikel 17 DS-GVO), Einschränkungs-(Artikel 18 DS-GVO) und Berichtigungspflichten (Artikel 16 DS-GVO) kollidieren kann.

3.1.1 Personenbezug als Bedingung für Anwendbarkeit des Datenschutzrechts

Ob und in welchen Fällen die Blockchain an datenschutzrechtlichen Anforderungen zu messen ist, richtet sich danach, ob die betroffenen Daten einen Personenbezug aufweisen. Die Personenbezogenheit der Daten ist notwendige Voraussetzung für die Anwendbarkeit des Datenschutzrechts. § 3 des Bundesdatenschutzgesetzes (BDSG) definiert personenbezogene Daten als

»Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)«.

Da das BDSG in weiten Teilen ab 25. Mai 2018 durch die dann europaweit geltende DS-GVO[11] abgelöst wird, wird dann die folgende, in der DS-GVO geregelte Definition gelten:

»›personenbezogene Daten‹ sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden ›betroffene Person‹) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.« (Artikel 4 Nr.1 DS-GVO)

Das für die Diskussion um die Anwendbarkeit der datenschutzrechtlichen Bestimmungen wesentliche Merkmal ist der relative Personenbezug, also die Identifizierbarkeit, die sich aus der

11 Da die bisherigen Datenschutzvorschriften durch die DS-GVO als vorrangige EU-Verordnung am 28. Mai 2018 abgelöst werden und dann auf nationaler Ebene nicht mehr das BDSG, sondern das BDSG-neu gelten wird, wird im Folgenden auch nur auf die neuen Rechtsgrundlagen Bezug genommen.

Zuordnung bestimmter Daten ergeben kann. Das heißt: nur weil die Blockchain keine Namen, sondern nur Konten und Transaktionsbewegungen kennt, heißt das nicht, dass keine personenbezogenen Daten verarbeitet werden.[12]

Die in der Blockchain gespeicherten Hashes, die mittels der zugeteilten Schlüssel als Nutzererkennung dienen, sind nach dem Begriff des relativen Personenbezugs für diejeinigen Personen als Informationen personenbezogen, wenn die Person über das notwendige Zusatzwissen verfügt oder dieses erlangen kann, um die entsprechende Information mit verhältnismäßigen Mitteln einer bestimmten Person zuzuordnen.[13] Das ist zum Beispiel dann nicht der Fall, wenn die Identifizierung der betreffenden Person gesetzlich verboten oder praktisch nicht durchführbar wäre, weil sie zum Beispiel mit einem unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskräften verbunden ist, sodass das Risiko einer Identifizierung de facto vernachlässigbar erschiene.[14]

Der EuGH hat zu der Identifizierbarkeit hinsichtlich dynamischer IP-Adressen ausgeführt, dass die IP Adresse für den Anbieter dann personenbezogen ist, wenn er über (rechtliche) Mittel verfügt, die es ihm erlauben, die betreffende Person anhand der Zusatzinformationen über die der Internetzugangsanbieter verfügt, bestimmen zu lassen (verschärfter relativer Personenbezug). Wenn also die verantwortliche Stelle mit den ihr zur Verfügung oder erreichbaren stehenden Mitteln dazu in der Lage ist, die betreffenden Angaben einer bestimmten Person zuzuordnen, ist die Information/das Datum personenbezogen. Die zur Identifizierung erforderlichen Informationen müssen dabei allerdings gerade nicht in den Händen einer einzigen Person liegen.

Bei der privaten bzw. der öffentlichen aber zulassungsbeschränkten Blockchain sind die Nutzer daher grundsätzlich identifizierbar: der Administrator kann durch die Vergabe der Nutzerkennung auch auf die Person hinter dem vergebenen öffentlichen Schlüssel rückschließen.[15] Der Administrator ist insofern vergleichbar mit Providern, die Nutzer ebenfalls über die erfasste (auch dynamische) IP-Adresse der Nutzer identifizieren können.[16] Aber auch bei der klassischen öffentlichen Blockchain kann eine Identifizierbarkeit der Nutzer in vielen Fällen angenommen werden.[17] Dies ist zum Beispiel dann der Fall, wenn die Nutzer Dienste Dritter nutzt, die eine Identifizierung erfordern, wie z.B. Bitcoin-Marktplätze, das Tätigen von Onlinekäufen mit Bitcoins.[18]

12 Martini/Weinzierl: Die Blockchain-Technologie und das Recht auf Vergessenwerden (NVwZ 2017, 1252).

13 Martini/Weinzierl: Die Blockchain-Technologie und das Recht auf Vergessenwerden (NVwZ 2017, 1252) mit Verweis auf EuGH, Urteil vom 19.10.2016 – C-582/14.

14 EuGH, Urteil vom 19.10.2016 – C-582/14, Para 46.

15 Martini/Weinzierl: Die Blockchain-Technologie und das Recht auf Vergessenwerden (NVwZ 2017, 1251, 1253).

16 Martini/Weinzierl: Die Blockchain-Technologie und das Recht auf Vergessenwerden (NVwZ 2017, 1253) mit Verweis auf BGH, Urteil vom 16.05.2017 – VI ZR 135/13.

17 Martini/Weinzierl: Die Blockchain-Technologie und das Recht auf Vergessenwerden (NVwZ 2017, 1253).

18 Martini/Weinzierl: Die Blockchain-Technologie und das Recht auf Vergessenwerden (NVwZ 2017, 1251, 1253); Schrey/Thalhofer: Rechtliche Aspekte der Blockchain (NJW 2017, 1431, 1433); Guggenberger: Datenschutz durch Blockchain – eine große Chance (ZD 2017, 49, 50); Bechtolf/Vogt: Blockchain und Datenschutz – Recht technologisch(DSRITB 2017, 873, 880); mit Verweis darauf, dass die Bitcoin-Marktplätze und Register die jeweiligen Adressen von Empfängern und Absendern beinhalten: Hofert: Blockchain - Profiling (ZD 2017, 161, 162).

Feststellen lässt sich also, dass die in der Blockchain abgelegten Informationen in zugangsbeschränkten Systemen häufig als personenbezogene Daten zu klassifizieren sein werden. Der Anwendungsbereich der datenschutzrechtlichen Vorschriften, insbesondere der DS-GVO, ist damit eröffnet.

3.1.2 Anonymisierung als Ausweg

Die Anwendung von Anonymisierungstechniken kann einen Ausweg darstellen. Blockchain Technologien werden häufig ganz automatisch mit Anonymisierung in Verbindung gebracht. Hier ist jedoch Vorsicht geboten:

Exkurs: Pseudonymisierung – Anonymisierung und Verschlüsselung: Ein Überblick

An dieser Stelle soll ein kurzer Überblick über die Begrifflichkeiten Pseudonymisierung, Anonymisierung und Verschlüsselung gegeben werden. Die Trennung der einzelnen Verfahren ist insbesondere im Hinblick auf die rechtliche Einordnung und die daraus resultierende Anwendbarkeit des Datenschutzrechts in Bezug auf die verschiedenen Verfahren von Bedeutung.

Pseudonymisierung

Die Datenschutzgrundverordnung definiert den Begriff Pseudonymisierung in Art. 4 Nr. 5. Darin heißt es: Pseudonymisierung (ist) die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden. In Blockchain-Systemen wird der Nutzer z.B. durch die Zuteilung eines Schlüssels (i.d.R. eine alphanumerische Zahlenfolge) pseudonymisiert.

Beispiel

Speichert ein Unternehmen Kundendaten in einer MySQL-Datenbank, verknüpft jeden Datensatz mit einem öffentlichen Schlüssel und nutzt diesen öffentlichen Schlüssel in einer von der MySQL-Datenbank getrennten Blockchain, so spricht man hier von Pseudonymisierung: Der öffentliche Schlüssel ist ein Pseudonym für den vollen Kundendatensatz.

Auch Erwägungsgrund 26 der DS-GVO äußert sich zur Pseudonymisierung und gibt Aufschluss darüber, ob und wann auch pseudonymisierte Daten noch den für die Anwendbarkeit des Datenschutzrechts wichtigen Personenbezug aufweisen. Dort heißt es: Die Grundsätze des Datenschutzes sollten für alle Informationen gelten, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Einer Pseudonymisierung unterzogene personenbezogene Daten, die durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten, sollten als Informationen über eine identifizierbare natürliche Person betrach-

tet werden. Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern. Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind.

Dass die Pseudonymisierung aber auch für die Erreichung von Datenschutz eingesetzt werden kann, stellt Art. 32 Abs.1lit.1 DS-GVO klar, der in Bezug auf die Sicherheit der Verarbeitung die Pseudonymisierung als eine der technischen und organisatorischen Maßnahmen nennt. Und auch Art. 20 DS-GVO erwähnt die Pseudonymisierung explizit bei Datenschutz durch Technikgestaltung und datenschutzfreundlichen Voreinstellungen.

Für die Frage, ob pseudonymisierte Daten personenbezogen sind gilt also im Ergebnis: Pseudonymisierte Daten sind noch immer personenbezogen (wenn sie es vor der Pseudonymisierung auch waren). Datenschutz muss daher beachtet werden.

Anonymisierung

Anonymisierte Daten sind solche Daten, die sich gerade nicht/nicht mehr auf eine identifizierte oder identifizierbare natürliche Person beziehen.

Das zeigt sich ebenfalls an Erwägungsgrund 26: Die Grundsätze des Datenschutzes sollten daher nicht für anonyme Informationen gelten, d. h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht mehr identifiziert werden kann.

Durch die Inbezugnahme des Satzes »Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind.« wird auch hier deutlich, dass die Anonymisierung das Verändern der Daten dergestalt ist, dass sie nicht mehr oder nur mit unverhältnismäßig großem Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können (derart auch der frühere § 3 Abs. 6 BDSG: Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können).

Liegt also ein anonymisiertes Datum vor, gelten die Datenschutzgrundsätze nicht.

Beispiel

Ein Reisebüro erstellt Auswertungen seiner Kunden, löscht dabei aber die Kundennummer,-den Namen und die Kontaktdaten der Kunden. Zurück bleiben Daten auf Grund derer kein Bezug zu einer individuellen Person möglich sind.

Verschlüsselung

Der Begriff Verschlüsselung wird in der DS-GVO nicht definiert, sondern lediglich an verschiedenen Stellen neben der Pseudonymisierung u.a. als eine technische und organisatorische Maßnahme genannt. Nach Simitis/Ernestus ist Verschlüsselung (Kryptographie) ein Querschnittsthema der Datensicherheit und dient dem Schutz der Informationen und der Organisation vor dem Zugriff unberechtigter Dritter. Kryptografie beschreibt die Technik, lesbare Informationen zu modifizieren, so dass diese nur mittels eines dazu geschaffenen Schlüssels wieder lesbar werden. Technisch beschreibt die Verschlüsselung/die Kryptografie die Umwandlung von Informationen mithilfe eines Verschlüsselungsverfahrens in eine nicht mehr zu interpretierende Zahlen- oder Zeichenfolge.[19] Dabei werden ein oder mehrere Schlüssel eingesetzt.

Wichtig: Entgegen verbreiteter Ansichten ändert die Verschlüsselung der Daten grds. nichts an deren Personenbezug. Solange derjenige, der die Daten verschlüsselt,über den entsprechenden Schlüssel und damit die Mittel zu Re-Identifizierung des Nutzers verfügt, sind die verschlüsselten Daten personenbeziehbar und fallen daher unter den Begriff der personenbezogenen Daten.

Pseudonymisierte und anonymisierte Daten in der Blockchain

In Blockchains werden sämtliche im System vorgenommenen Transaktionen erfasst. Sie sind dauerhaft in der Blockchain abgelegt. Die Nutzer der jeweiligen Transaktionen sind dabei nicht namentlich (Stand heute der Regelfall in öffentlichen Systemen) aufgeführt, sondern durch die öffentlichen Schlüssel pseudonymisiert. Diese Pseudonymisierung bedeutet jedoch lediglich, dass die Daten nicht mehr ohne Hinzuziehung weiterer Informationen einer Person zugeordnet werden können.

Um anonymisierte Daten handelt es sich bei den in der Blockchain abgelegten Daten nicht, wenn die Identität der hinter den pseudonymisierten Schlüsseln stehenden Personen durch Zusatzinformationen ermittelt werden kann. Diese Zusatzinformationen können sich zum Beispiel aus Rechnungsdaten ergeben. Auch Kundeninformationen aus Onlinekäufen können die Identifizierung ermöglichen, wenn der Nutzer die Transaktion z.B. mit Bitcoin oder einer anderen Kryptowährung bezahlt. Häufig wird es auch möglich sein, durch die Zusammenführung und Kombination der einzelnen Transaktionen zu einem (pseudonymisierten) Profil Rückschlüsse auf die Identität des Nutzers zu ziehen. Auch der Organisator in einer zulassungsbeschränkten Blockchain kann die Schlüssel bestimmten Personen zuordnen. Die fehlende tatsächliche Ano-

19 Vergleiche Walter Ernestus, in: Simitis, Bundesdatenschutzgesetz, BDSG § 9 Technische und organisatorische Maßnahmen, 8. Auflage 2014, Rn. 166.

nymisierug und die Möglichkeit der Identifizierung durch Zusammenführung von verfügbaren Daten ist durch einzelne Studien auch immer wieder bestätigt worden.[20]

Beispiel

Akzeptiert ein Online-Händler Bitcoin als Zahlungsmittel, so erhält er den öffentlichen Schlüssel des Bitcoin-Wallets des Kunden und kann diesen mit dem übrigen Kundendatensatz verknüpfen. Auf Grund der Transparenz der Bitcoin-Blockchain ermöglicht es dies dem Online-Händler, alle weiteren getätigten Transaktionen des Kunden einzusehen. Der öffentliche Schlüssel ist damit nicht mehr nur für den Kunden, sondern auch für den Online-Händler ein personenbezogenes Datum.

Hashwerte

Da in Blockchains häufig mit Hashwerten von Rohdaten gearbeitet wird (also ein meist 32 Byte großer und in hexadezimaler Notierung 64 Zeichen langer Fingerabdruck von Daten beliebiger Länge), stellt sich die Frage, ob auch solche Hashwerte personenbezogen sind. Hashwerte lassen grundsätzlich keinen Rückschluss auf Rohdaten zu, weswegen sie nicht mit verschlüsselten Daten verglichen werden können. Eine Ausnahme besteht nur dort, wo die möglichen Rohdaten abschließend und bekannt sind und damit auch die dazugehörigen Hashwerte erstellt und mit den Hashwerten in der Blockchain verglichen werden können. Ist der Kreis der möglichen Rohdaten indes nicht bekannt, so wird man mit dem EuGH unter Anwendung des verschärften relativen Personenbezugs danach fragen müssen, ob zusätzliche Mittel ersichtlich sind, um von den Hashwerten Rückschlüsse auf Personen ziehen zu können. Die Frage dürfte in der Regel zu verneinen sein. Vergleichbar zum Fall der IP-Adressen bestehen Ausnahmen nur dort, wo tatsächlich ein Rechtsanspruch auf Herausgabe der Rohdaten besteht, beispielsweise auf Grund von Rechtsverletzungen.

Eine gute Hashing-Funktion zeichnet sich dadurch aus, dass sie wie eine Einbahnstraße funktioniert. Es gibt eine Vielzahl an Hash-Funktionen, die als unterschiedlich sicher gelten.[21] Im Bitcoin-Blockchain-Protokoll wird an verschiedenen Stellen auf den SHA-256 (Secure Hash Algorithm-256) zurückgegriffen (unter anderem auch die Hashcash-Funktion zum »Verketten« der Blöcke, siehe ↗Abbildung 3). Dieser gehört zur SHA-2-Familie standardisierter kryptologischer Hashfunktionen, die als sicher gelten. Die Wahrscheinlichkeit, dass zwei verschiedene originäre Datensätze, den selben gehashten Ausgabewert ausweisen, liegt im Fall des SHA-256 bei 2^{128}.

20 Siehe zum Beispiel die Besprechung verschiedener Studien in: Fergal Reid and Martin Harrigan, An Analysis of Anonymity in the Bitcoin System, 202, ↗http://www.item.ntnu.no/_media/studies/courses/ttm4546/bitcoin_article.pdf.

21 Vergleiche. BSI – Technische Richtlinie – Kryptographische Verfahren: Empfehlungen und Schlüssellängen, 2017, S. 41 (↗https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile&v=4).

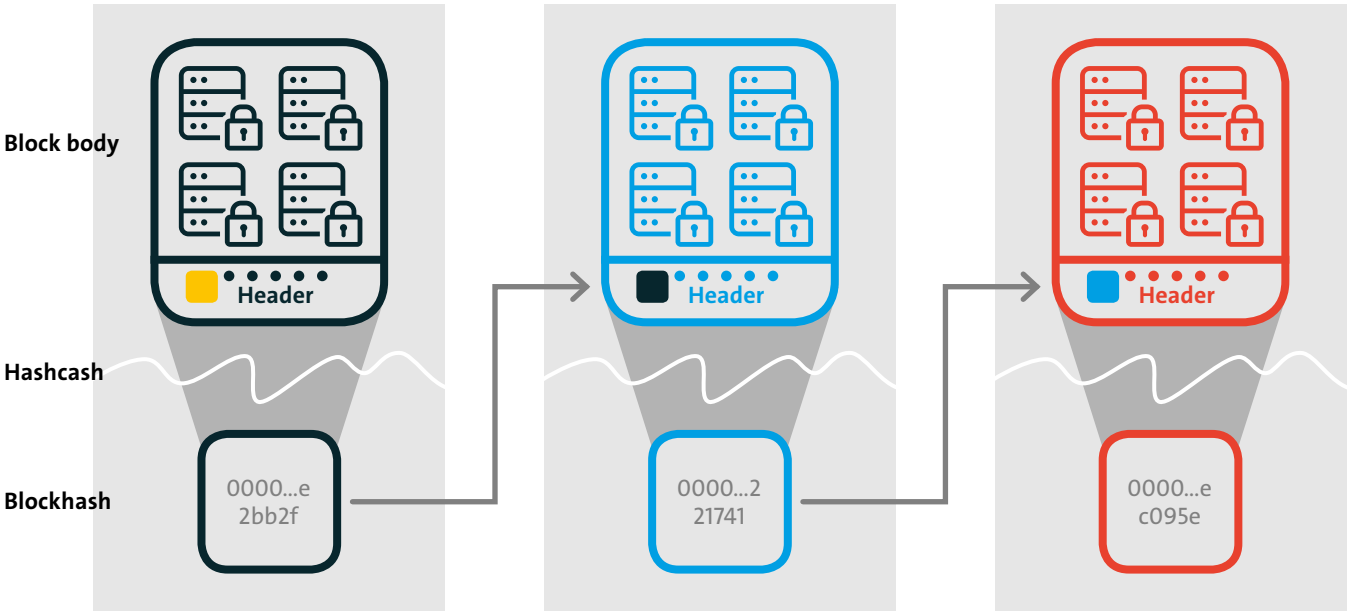

Abbildung 3: Schaubild zur »Hash-Verkettung« am Beispiel der Bitcoin-Blockchain. In der Bitcoin Blockchain enthält der Header 6 Elemente, unter anderem den Hash des vorhergehenden Blocks (in der Abbildung als ausgefüllte farbiges Quadrat dargestellt). In die Hashcash-Funktion gehen noch fünf weitere Datenfelder ein (in der Abbildung durch die farbigen Punkte dargestellt). Ein Datenfeld ist die sogenannte Nonce – eine Zählvariable, die nach jedem abgeschlossenen Hash-Vorgang um 1 erhöht wird. Ein weiteres Datenfeld ist die Wurzel-Hash des Merkel Trees.

Während sich aus originären Daten relativ einfach ein eindeutiger Hashwert ermitteln lässt, ist die Umkehrung der Funktion ausgeschlossen. Werden Daten nur noch durch ihren Hash-Wert repräsentiert, wie es z.B. in Merkle-Trees in der Blockchain umgesetzt werden kann, dann sind die originären Daten mit vertretbarem Aufwand nicht erratbar. Merkle-Trees haben den Nachteil, dass die ihnen zu Grunde liegenden Daten nicht mehr transparent nachvollziehbar sind, sondern dass ihre Korrektheit als gegeben vorausgesetzt wird.

In der Bitcoin-Blockchain werden Merkel-Trees als Datenstruktur verwendet, um die Hashes der einzelnen Transaktionen eines Blocks zusammenzuführen. Letztlich geht nur der Wurzel-Hash des Merkle-Trees in die Hash-Funktion zur Erzeugung eines neuen Block-Hashes[22] ein. Dieses Verfahren ist der Grund dafür, dass die Verkettung der Blöcke auch die Unveränderlichkeit jeder einzelnen Transaktion bedingt. Gleichzeitig bleibt die Eingabe in die Hashfunktion stets gleich und die Block-Hash-Erzeugung ist unabhängig von der Anzahl an Transaktionen in einem Block.

Allerdings ist die Blockchain nicht mehr nachvollziehbar, wenn keine Transaktionen mehr bekannt sind, über deren Herkunft sich Besitzrechte herleiten lassen. So kann das Hashen ohne offene Kenntnis der Transaktionen ein Design-Element einer sicheren Blockchain sein, welches jedoch nur in bestimmten Kontexten angewendet werden sollte. So finden z.B. die Repräsentation von vollen Blöcken nur durch Block-Hashes durch so genannte Bloom-Filter ihre Anwendung.

22 Die im Bitcoin-Protokoll genutzte Funktion zur Erzeugung des Block-Hashes heißt Hashcash. Darauf beruht der Proof-of-Work-Mechanismus (↗https://en.wikipedia.org/wiki/Hashcash).

Durch den Filter hat ein Client keinen Vollzugriff auf die gesamte Blockchain.

Beispiel

Wenn es neuere Transaktionen gibt, können ältere Transaktionen der Blockchain »gelöscht« werden, indem die Nutzungsdaten nur noch durch ihre Hashwerte dargestellt werden. Allerdings sind diese alten Transaktionen dann nicht mehr sichtbar, ein Vorteil der Blockchain wäre weg. Außerdem ist auch nicht ausschließbar, dass einzelne Nutzer des dezentralen Netzes sich einen alten Stand der Blockchain gesichert haben und somit noch immer über die personenrelevanten Daten verfügen.

3.1.3 Zusammenfassung

Entgegen der landläufigen Meinung, bei Blockchains würden anonymisierte Daten verwendet, wird man bei genauerer Betrachtung häufig davon ausgehen müssen, dass hier je nach Ausgestaltung der Technologie personenbezogene Daten vorliegen, wenn auch in pseudonymisierter Form. Da die in den »Profilen« und Transaktionen gespeicherten Informationen pseudonymisiert und nicht nur anonymisiert sind, kann auch hierüber der Anwendungsbereich der DS-GVO (und des BDSG-neu) nicht ausgeschlossen werden. Wird ein Datum gehasht verliert das Datum den ursprünglichen Informationsgehalt, denn der Rückschluss von Hash auf ursprünglichen Datensatz ist nicht möglich. Für diesen Fall kann eine Personenbeziehbarkeit ausgeschlossen werden. Gehashte Daten können jedoch in den Anwendungsbereich fallen, wenn die ursprünglichen Rohdaten bekannt sind und damit Hashes erzeugt werden, die zum Vergleich mit den in der Blockchain hinterlegten Hashes dienen können.

Es stellen sich daher nun weitere Fragen in Bezug auf die konkrete Anwendung der datenschutzrechtlichen Vorschriften. Hierzu gehört die im Datenschutzrecht als Anknüpfungspunkt wesentliche Komponente der »Verantwortlichkeit«, die Frage nach der Legitimationsgrundlage für die Verarbeitung und die Ausgestaltung der Betroffenenrechte.

3.2 Verantwortliche Stelle

Anknüpfungspunkt des Datenschutzes ist nicht nur der Betroffene der Datenverarbeitung, sondern stets auch der Verantwortliche. Er ist Hauptadressat der datenschutzrechtlichen Verpflichtungen, die sich aus der DS-GVO und dem BDSG-neu ergeben.

In der Standardsituation, dass zum Beispiel ein Diensteanbieter die Daten seines Kunden zur Rechnungstellung erhebt, speichert und verarbeitet, ist der Kunde der datenschutzrechtlich »Betroffene«, der Diensteanbieter der »Verantwortliche«.

Artikel 4 Nr. 7 DS-GVO definiert den Verantwortlichen daher wie folgt:

Verantwortlicher ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (...)

Im kollaborativen System der Blockchain stößt diese Definition naturgemäß an Grenzen, da der Blockchain eine Verteilung und Dezentralisierung der Speicherung und Verarbeitung von Daten zugrunde liegt.[23] Verschiedene Akteure kommen deshalb durch ihre Teilnahme an der Blockchain als Verantwortliche in Betracht:

- der Programmierer der Blockchain,
- der Initiator,
- der Teilnehmer, der eine Transaktion vornimmt,
- der Miner, der neue Blöcke vor Aufnahme prüft und an die Blockchain anhängt,
- der Teilnehmer, der als Node fungiert.[24]

Die tatsächliche Verantwortlichkeit hängt jedoch vom konkreten System ab.

3.2.1 Verantwortlicher in zulassungsfreier Blockchain

Der Initiator der Blockchain bzw. der Programmierer des zugrunde liegenden Codes »erdenkt« zwar die konkrete Art und Ausgestaltung der Blockchain, verliert aber mit dem Launch der Blockchain und der Veröffentlichung des von ihm erstellten Codes die Kontrolle über Zwecke und Mittel der Verarbeitungen.[25] Eben diese Kontrolle setzt aber Artikel 4 Nr. 7 DS-GVO als Merkmal der Verantwortlichkeit voraus. Eine Verantwortlichkeit lässt sich daher für den Programmierer und Initiator nicht feststellen.

Auch der einzelne Teilnehmer, der eine Transaktion vornimmt, hat keine Kontrolle über Zwecke und Mittel der Verarbeitung in der Blockchain.

Die Miner nehmen innerhalb des Blockchain Systems eine Schlüsselrolle ein. Durch die Proof-of-Work- oder Proof-of-Stake-Leistung der Miner (also das Verfahren, mit dem Einigkeit über den jeweils finalen Zustand der Datensätze erreicht wird) wird ein wichtiger Beitrag für die Blockchain und deren Absicherung geleistet. Die Miner haben durch die Vergütung, die sie für das Minen neuer Blöcke und aus Transaktionsgebühren erhalten, ein wirtschaftliches Interesse an der Fortentwicklung der Blockchain.[26] Auf die Transaktionen innerhalb der Blöcke, den Inhalt der Datensätze haben sie jedoch keinen Einfluss.[27] Ihnen fehlt daher ebenfalls die Kontrolle über Zweck und Mittel der Verarbeitung, sodass sie nicht als Verantwortliche anzusehen sind.[28]

Als Verantwortliche in der öffentlichen und zulassungsfreien Blockchain kommen daher nur die Betreiber der Nodes in Betracht, also diejenigen Teilnehmer, die selbst Transaktionen vornehmen können und damit die Informationen an die anderen Nodes und/oder die entsprechenden Informationen in ihre Kopie der Blockchain übertragen.[29] Durch die Be- und Verarbeitung der Transak-

23 Martini/Weinzierl: Die Blockchain-Technologie und das Recht auf Vergessenwerden (NVwZ 2017, 1251, 1253).

24 Ebenda.

25 Ebenda.

26 Ebenda.

27 Ebenda.

28 Ebenda.

29 Martini/Weinzierl: Die Blockchain-Technologie und das Recht auf Vergessenwerden (NVwZ 2017, 1251, 1253).

tionen erhebt, speichert und verarbeitet der Betreiber Node die Daten und ist damit, sofern die Daten personenbezogen sind, Verantwortlicher im Sinne der DS-GVO.[30]

Die Betreiber der Nodes kommen je nach Ausgestaltung und der Art ihrer Teilnahme als alleinige oder auch gemeinsam Verantwortliche in Betracht.[31]

Nach Artikel 26 Absatz 1 Satz 1 DS-GVO liegt gemeinsame Verantwortlichkeit vor, wenn zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung festlegen.[32]

Gemeinsam Verantwortliche müssen jedoch hinsichtlich der Ausgestaltung der Vereinbarung auch die weiteren besonderen Anforderungen beachten, die die DS-GVO ihnen auferlegt (Artikel 26 Absatz 1 Satz 2 und 3 DS-GVO):

Gemeinsam Verantwortliche legen in einer Vereinbarung in transparenter Form fest, wer von ihnen welche Verpflichtung gemäß dieser Verordnung erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht, und wer welchen Informationspflichten gemäß den Artikeln 13 und 14 nachkommt, sofern und soweit die jeweiligen Aufgaben der Verantwortlichen nicht durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen die Verantwortlichen unterliegen, festgelegt sind. In der Vereinbarung kann eine Anlaufstelle für die betroffenen Personen angegeben werden.

Mangels einer solchen Vereinbarung werden Betreiber von Nodes im Regelfall aber nicht als gemeinsam Verantwortliche angesehen werden können.[33] Als Verantwortliche gelten sie aber dennoch. Unabhängig von der Einordnung als gemeinsam oder alleinige Verantwortliche wären sie in jedem Fall Adressaten der DS-GVO, zum Beispiel der Betroffenenrechte, Artikel 26 Absatz 3 DS-GVO.

Insbesondere in der nicht zulassungsbeschränkten Blockchain entsteht durch die dezentrale Verantwortlichkeit und die Selbstständigkeit der agierenden Nodes die Problematik der Durchsetzbarkeit von Ansprüchen.[34] Das gilt einerseits für einen etwaig bestehenden Löschungsanspruch der Betroffenen und anderseits aber auch für die aufsichtsbehördliche Arbeit und deren Auskunftsersuchen.[35] Hier zeigt sich erneut, dass das System der DS-GVO für den Anwendungsbereich der Blockchain z.T. nur schwerlich kompatibel ist. Art. 56 Abs. 1 und 60 ff DS-GVO knüpfen an die Zusammenarbeit unter einer federführenden Aufsichtsbehörde an die Hauptniederlassung und ggf. weitere Niederlassungen eines Verantwortlichen an. Im System mehrerer, ggf. gemeinsamer Verantwortlicher, kommt diese Zuständigkeitsverteilung zu keinem schlüssigen Ergebnis.

30 Martini/Weinzierl: Die Blockchain-Technologie und das Recht auf Vergessenwerden (NVwZ 2017, 1251, 1253); anders: Schrey/Thalhofer: Rechtliche Aspekte der Blockchain (NJW 2017, 1431, 1433).

31 Martini/Weinzierl: Die Blockchain-Technologie und das Recht auf Vergessenwerden (NVwZ 2017, 1254).

32 Ebenda.

33 Ebenda.

34 Ausführlich zur Problematik der aufsichtsbehördlichen Zuständigkeit und Durchsetzbarkeit der Ansprüche: Martini/Weinzierl: Die Blockchain-Technologie und das Recht auf Vergessenwerden (NVwZ 2017, 1251, 1255 f.).

35 Martini/Weinzierl: Die Blockchain-Technologie und das Recht auf Vergessenwerden (NVwZ 2017, 1251, 1255).

Abgesehen vom Regelfall der allein verantwortlichen Nodebetreiber mag es auch Fälle geben, in denen die Nodebetreiber als Auftragsverarbeiter (Artikel 28 DS-GVO) auftreten.[36] Man denke nur an die Konstellation, dass ein Blockchain-Netzwerk eine Datenbank betreibt, in die ein Auftraggeber Daten speichert. Käme hier nicht die Blockchain-Technologie in Betracht, sondern würde die Datenbank von einem Dienstleister in der Cloud betrieben, so länge zweifelsohne ein Fall der Auftragsverarbeitung vor, wenn der Dienstleister im Auftrag des Auftraggebers Daten verarbeitet und bei dieser Datenverarbeitung keine eigenen Zwecke verfolgt.[37] Ersetzt man diesen einen Dienstleister nun durch eine Gruppe von Nodebetreibern, wird nichts anderes gelten. Es stellt sich hier nur die Frage der faktischen Ausgestaltung: Liegt ein weisungsgebundenes Auftragsverarbeitungsverhältnis vor, oder verarbeiten die Nodebetreiber die Daten für eigene Zwecke (wie etwa im Falle von Bitcoin)?

3.2.2 Verantwortlicher in zulassungsbeschränkter Blockchain

Bei den zulassungsbeschränkten Blockchains ist die Situation bezüglich der Verantwortlichkeit häufig einfacher zu beurteilen. Die zulassungsbeschränkte Blockchain zeichnet sich in der Regel dadurch aus, dass es eine organisierende Einheit gibt, die über Zugangsrechte zur Blockchain entscheidet. Diese Organisationseinheit übt daher die Kontrolle über Zwecke und Mittel der Verarbeitung aus, sodass sie als Verantwortlicher klassifiziert werden kann.[38] In diesen Fällen spricht viel dafür, von einer Auftragsverarbeitung auszugehen.[39] Allerdings entscheidet auch hier der Einzelfall und es ist danach zu fragen, wie das (vertragliche) Verhältnis aller Beteiligten ausgestaltet ist.

3.3 Erlaubnistatbestand für Datenverarbeitung

Aus Artikel 6 Absatz 1 DS-GVO ergibt sich, dass die Datenverarbeitung nur erlaubt ist, wenn für sie eine Legitimationsgrundlage vorliegt (Verbot mit Erlaubnisvorbehalt). Artikel 6 DS-GVO listet zugleich die Erlaubnistatbestände auf, die für Daten gelten, die nicht in die Gruppe der besonderen Kategorien (Artikel 9 DS-GVO) gehören. Die Verarbeitung ist daher dann rechtmäßig, wenn der Betroffene eingewilligt hat oder/und ein gesetzlicher Erlaubnistatbestand eingreift.

3.3.1 Einwilligung

Als Erlaubnis kann für die Verarbeitung der Daten in der Blockchain die Einwilligung dienen. Artikel 4 Nr. 11 DS-GVO definiert die Einwilligung mit:

»jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgege-

36 Martini/Weinzierl: Die Blockchain-Technologie und das Recht auf Vergessenwerden (NVwZ 2017, 1251, 1254).

37 Ebenda.

38 Martini/Weinzierl: Die Blockchain-Technologie und das Recht auf Vergessenwerden (NVwZ 2017, 1251, 1255).

39 Martini/Weinzierl: Die Blockchain-Technologie und das Recht auf Vergessenwerden (NVwZ 2017, 1251, 1255); zum Teil wird das System der Auftragsverarbeitung für nicht kompatibel mit der Blockchain-Technologie gehalten, so zum Beispiel: ↗https://bundesblock.de/wp-content/uploads/2017/10/bundesblock_positionspapier_v1.1.pdf, S. 26.

bene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.«

Erwägungsgrund 32 DS-GVO stellt zusätzlich klar, dass die Einwilligung sich auf alle zu demselben Zweck oder denselben Zwecken vorgenommenen Verarbeitungsvorgänge beziehen sollte. Wenn die Verarbeitung mehreren Zwecken dient, sollte für alle diese Verarbeitungszwecke eine Einwilligung gegeben werden.

Erwägungsgrund 42 DS-GVO verdeutlicht außerdem die Anforderungen, die an den Kenntnisstand des Einwilligenden gestellt werden. Denn der Erwägungsgrund verlangt, dass die betroffene Person, damit sie in Kenntnis der Sachlage ihre Einwilligung geben kann, mindestens wissen sollte, wer der Verantwortliche ist und für welche Zwecke ihre personenbezogenen Daten verarbeitet werden sollen.

Diese Voraussetzung stellt hohe Anforderungen an die Formulierung der Einwilligung. Zum Beispiel weiß der Betroffene bei öffentlichen Blockchains nicht, wer der Verantwortliche ist und in welche Länder die Daten übermittelt werden, da die Betreiber der Nodes nicht zwingend bekannt sind.

3.3.2 Gesetzlicher Erlaubnistatbestand

Wer eine Node einer öffentlichen Blockchain betreibt, mittels derer Betroffene etwa mit Bitcoins bezahlen, wird sich stets auf den Erlaubnistatbestand des überwiegenden Interesses (Artikel 6 Absatz 1 lit. f DS-GVO) stützen können. Denn ein schutzwürdiges Interesse des Betroffenen ist nicht ersichtlich, wenn dieser doch freiwillig Bitcoins versendet. Auf der anderen Seite muss auch berücksichtigt werden, dass der Betreiber der Node die Betroffenen nicht kennt und auch aus diesem Grund schützenswerter ist, was die durch ihn verarbeiteten und aus seiner Sicht anonymen Daten anbelangt.

Gerade im Bereich der zulassungsbeschränkten Blockchains wird überdies die Erforderlichkeit zur Vertragserfüllung (Artikel 6 Absatz 1 lit. b DS-GVO) eine Rolle spielen. Wenn Gegenstand der (im diesem Fall wohl in der Regel bestehenden) Vertragsverhältnisse die Nutzung der Blockchain ist, so ist die Nutzung der Blockchain und damit auch die Datenverarbeitung durch die Betreiber der Nodes Vertragsgegenstand.

3.4 Betroffenenrechte

Der Verantwortliche ist Adressat der in Artikel 17 bis 19DS-GVO genannten Betroffenenrechte.[40]

Artikel 17 DS-GVO, das Recht auf Löschung (»Recht auf Vergessenwerden«) erlegt dem Verant-

40 Zu Ausführungen zu den Betroffenenrechten siehe auch: Martini/Weinzierl: Die Blockchain-Technologie und das Recht auf Vergessenwerden (NVwZ 2017, 1251); Schrey/Thalhofer: Rechtliche Aspekte der Blockchain (NJW 2017, 1431); Bechtolf/Vogt: Blockchain und Datenschutz – Recht technologisch(DSRITB 2017, 873, 880).

wortlichen die Pflicht auf, personenbezogene Daten in bestimmten Fällen zu löschen (Art.17 Absatz 1 lit. a – f DS-GVO).

Artikel 17 der DS-GVO, das Recht auf Löschung (»Recht auf Vergessenwerden«) besagt:

(1) Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, und der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zulöschen, sofern einer der folgenden Gründe zutrifft:

a) Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.
b) Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung.
c) Die betroffene Person legt gemäß Artikel 21 Absatz 1 Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor, oder die betroffene Person legt gemäß Artikel 21 Absatz 2 Widerspruch gegen die Verarbeitung ein.
d) Die personenbezogenen Daten wurdenunrechtmäßig verarbeitet.
e) Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich, dem der Verantwortliche unterliegt.
f) Die personenbezogenen Daten wurden in Bezugauf angebotene Dienste der Informationsgesellschaft gemäß Artikel 8 Absatz 1erhoben.

(2) Hat der Verantwortliche die personenbezogenen Daten öffentlich gemacht und ist er gemäß Absatz 1 zu deren Löschung verpflichtet, so trifft er unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen, auch technischer Art, um für die Datenverarbeitung Verantwortliche, die die personenbezogenen Daten verarbeiten, darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser personenbezogenen Daten verlangt hat.

3.4.1 Recht auf Löschung (»Recht auf Vergessenwerden«) – Grundsätzliches

Artikel 17 DSGVO regelt also das Recht auf Löschung von personenbezogenen Daten und das sogenannte »Recht auf Vergessenwerden«, welches wohl insbesondere in Art. 17 Absatz 2 DSGVO zum Tragen kommt. Das lässt sich insbesondere aus dem Erwägungsgrund 66 ableiten: »Um dem ›Recht auf Vergessenwerden‹ im Netz mehr Geltung zu verschaffen, sollte das Recht auf Löschung ausgeweitet werden, indem ein Verantwortlicher, der die personenbezogenen Daten öffentlich gemacht hat, verpflichtet wird, den Verantwortlichen, die diese personenbezogenen Daten verarbeiten, mitzuteilen, alle Links zu diesen personenbezogenen Daten oder Kopien oder Replikationen der personenbezogenen Daten zu löschen. Dabei sollte der Verantwortliche, unter Berück-

sichtigung der verfügbaren Technologien und der ihm zur Verfügung stehenden Mittel, angemessene Maßnahmen — auch technischer Art — treffen, um die Verantwortlichen, die diese personenbezogenen Daten verarbeiten, über den Antrag der betroffenen Person zu informieren.«

Adressat der Vorschrift sind alle Verantwortlichen im Sinne der DS-GVO. Wie bereits dargestellt kommen als Verantwortliche in der zulassungsfreien Blockchain nur die Betreiber der Nodes in Betracht (diejenigen Teilnehmer, die selbst Transaktionen vornehmen können und damit die Informationen an die anderen Nodes weitergeben und/oder die entsprechenden Informationen in ihre jeweilige Kopie der Blockchain übertragen haben).

Bei zulassungsbeschränkten Blockchains ist der Verantwortliche wohl derjenige, der die Zugangsrechte vergibt und verwaltet. Diese Organisationseinheit übt die Kontrolle über Zwecke und Mittel der Verarbeitung aus, sodass sie als Verantwortlicher klassifiziert werden kann.

Der Löschungsanspruch, der die Kontrolle des Betroffenen über seine Daten sicherstellen will, gilt allerdings nicht absolut. Dies zeigt sich schon daran, dass Absatz 1 Voraussetzungen für die Löschung formuliert, z.B. »Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig«. Das Recht leitet sich maßgeblich aus den Artikel 7 und 8 der Charta der Grundrechte der Europäischen Union ab. Auch das führt aber nicht dazu, dass das Recht auf Löschung (»Recht auf Vergessenwerden«) unbeschränkt gelten soll, da die Grundrechte ihrerseits durch Rechte Dritter eingeschränkt werden können, wobei insbesondere an die Meinungs- und Informationsfreiheit nach Artikel 11 der Charta der Grundrechte der Europäischen Union und Artikel 16, die Unternehmerische Freiheit, zu denken ist.[41] Sollte durch das Löschverlangen die Existenz der gesamten Blockchain gefährdet werden, weil die Löschung den Weiterbetrieb der Nodes unmöglich machen würde, kann hier die Interessenabwägung zugunsten der verantwortlichen Node-Betreiber ausfallen. Bei der Ausführung der Löschung muss daher stets geprüft werden, wie und ob der Löschungsanspruch mit den eventuell entgegenstehenden Rechten in Einklang zubringen ist. Die Interessenabwägung sollte auch berücksichtigen, ob ein Betroffener sich der Unveränderbarkeit der Blockchain vor Nutzung derselben bewusst war.

Nicht zuletzt auch vor dem Hintergrund von Privacy by Design verdeutlicht Vorgenanntes aber, wie wichtig es ist, keine personenbezogene Daten in der Blockchain zu speichern. Alternative technische Lösungen – wie im Abschnitt »Datenschutz in Blockchain-Systemen« näher ausgeführt – sind allerdings denkbar: So könnten die in der Blockchain gespeicherten IDs nachträglich durch Entfernung des Links zu den personenbezogenen Daten des Betroffenen anonymisiert werden. Alternativ könnte die Blockchain änderbar ausgestaltet werden, was allerdings ihrem ursprünglichen Konzept im Einzelfall zuwiderlaufen mag.

3.4.2 Recht auf Löschung (»Recht auf Vergessenwerden«) – Pflicht zur Information Dritter

Die in Artikel 17 Absatz 1 DS-GVO niedergelegten Regeln zur Löschverpflichtung werden durch

41 Nolte/Werkmeister, in: Gola, DSGVO (2017), Artikel 17, Rn. 4.

Absatz 2 ergänzt für Situationen, wenn der Verantwortliche die personenbezogenen Daten öffentlich gemacht hat. Öffentlich gemacht sind die Informationen dann, wenn sie für die Öffentlichkeit, d.h. für die Allgemeinheit zugänglich gemacht wurden (z.B. Veröffentlichung von Daten auf einer Webseite) und eine nicht bestimmbare Anzahl von Personen ohne wesentliche Zulassungsschranken die Daten einsehen können.[42]

Bei einer nicht zulassungsbeschränkten Blockchain dürften die Daten somit als veröffentlicht gelten. Hat der Verantwortliche (Betreiber der Node) daher in der nicht zulassungsbeschränkten Blockchain die Daten öffentlich gemacht und ist er nach Art. 17 Absatz 1 DS-GVO zur Löschung verpflichtet, trifft ihn neben der eigenen Löschverpflichtung die Pflicht zur Information Dritter. Der Verantwortliche, den der Löschungsantrag des Betroffenen erreicht müsste in diesem Fall »unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen, auch technischer Art, (treffen) um für die Datenverarbeitung Verantwortliche, die die personenbezogenen Daten verarbeiten, darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser personenbezogenen Daten verlangt hat.« Diese Pflicht beschränkt sich also auf die Information Dritter – die Löschung selbst muss der Verantwortliche bei den Dritten nicht erwirken.

3.4.3 Recht auf Löschung (»Recht auf Vergessenwerden«) – Einschränkungen

Artikel 17 sieht auch weitere Einschränkungendes Löschungsrechts vor. So regelt Artikel 17 Absatz 3 DSGVO:

Die Absätze 1 und 2 gelten nicht, soweit die Verarbeitung erforderlich ist

a) zur Ausübung des Rechts auf freie Meinungsäußerung und Information;

b) zur Erfüllung einer rechtlichen Verpflichtung, die die Verarbeitung nach dem Recht der Union oder der Mitgliedstaaten, dem derVerantwortliche unterliegt, erfordert, oder zur Wahrnehmung einer Aufgabe, dieim öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;

c) aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit gemäß Artikel 9 Absatz 2 Buchstaben h und i sowie Artikel 9 Absatz 3;

d) für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1, soweit das in Absatz 1 genannte Recht voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt, oder

e) zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

42 BeckOK DatenschutzR/Wolff, 21. Ed. (2015) BDSG § 28 Rn. 253.

3.5 Datenschutz-Folgenabschätzung für die Blockchain

Für alle Blockchain-Node-Betreiber ist zusätzlich noch ein weiterer wesentlicher Punkt zu beachten: möglicherweise müssen sie eine Datenschutz-Folgenabschätzung (DSFA, oder engl. PIA) durchführen. Die DSFA, geregelt in Artikel 35 DS-GVO und ein Mittel der Umsetzung des bereits erwähnten Grundsatzes Privacy by Design, sieht vor, dass der Verantwortliche eine Folgenabschätzung durchführen muss, wenn die Form der Datenverarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Die DSFA dient daher dem Schutz der personenbezogenen Daten. Wie immer im Rahmen der DS-GVO gilt daher auch hier: wenn in der Blockchain keine personenbezogenen oder personenbeziehbaren Daten gespeichert sind, ist die DS-GVO nicht anwendbar und auch keine DSFA durchzuführen.

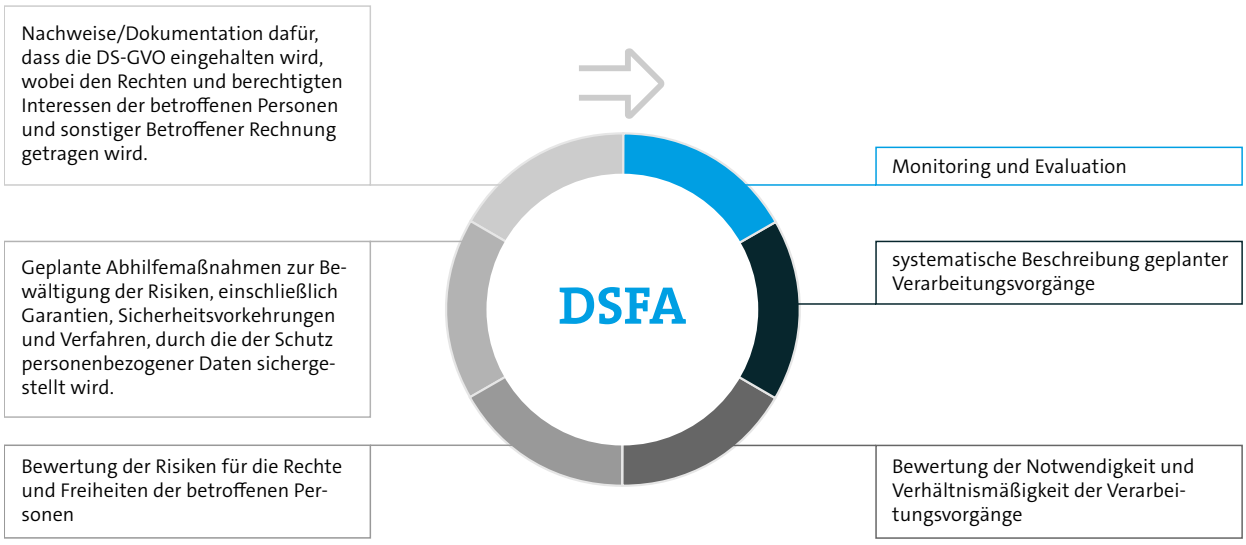

Abbildung 4: Darstellung eines sinnvollen Vorgehens zur Datenschutzfolgenabschätzung.

Gemäß Artikel 35 Absatz 3 DS-GVO ist eine DSFA insbesondere in folgenden Fällen erforderlich:

a) systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;

b) umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 oder

c) systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.

Diese Anwendungsbereiche werden auf die meisten Blockchains nicht zutreffen. Daraus sollte aber nicht abgeleitet werden, dass für Blockchains keine DSFA durchgeführt werden muss.

Aufschluss darüber, wann eine solche DSFA notwendig ist, ergibt sich auch aus einem aktuellen Leitfaden der Artikel-29-Datenschutzgruppe. Diese ist der Zusammenschluss der nationalen Datenschutzbehörden in Europa (durch die DS-GVO wird der neue EU Datenschutzausschuss dann die Nachfolge der Art-29-Datenschutzgruppe antreten, Art. 68 DS-GVO).

Die Art-29-Gruppe hat bereits im April 2017 eine neue Leitlinie herausgegeben, die sich mit der Auslegung der DSFA beschäftigt. Sie macht darin vor allem Ausführungen dazu, wann das »hohe Risiko« vorliegt, welches Artikel 35 DS-GVO zugrunde legt.

Die Art-29-Gruppe geht im Working Paper 248 unter anderem davon aus, dass der Einsatz neuer Technologien ein »hohes Risiko« darstellen kann (Punkt b(a)(8) des Working Papers). Außerdem soll wohl auch dann eine DSFA notwendig sein, wenn die Art der Datenverarbeitung den Betroffenen daran hindert, seine Rechte geltend zu machen (Punkt b(a)10 des Working Papers). Beide Fälle dürften in vielen Blockchain Systemen der Fall sein. Die Blockchain ist zum einen eine neue Technologie und zum anderen ist wie bereits beschrieben die Löschung einzelner Datensätze aus einer Blockchain bisher häufig nicht vorgesehen, was den Betroffenen an der Durchsetzung seines Löschungsanspruchs hindert.

Auch hier zeigt sich, dass die Verantwortlichen die Blockchain so konzipieren sollten, dass Löschungsmechanismen ermöglicht werden (s.o.). Die Grundeigenschaft der Blockchain unveränderlich zu sein, muss deshalb mit den erforderlichen Datenschutzanforderungen in Einklang gebracht werden. Personenbezogene Daten sollten grds. nicht in der Blockchain gespeichert werden, insbesondere nicht im Klartext. Außerdem können technische Optionen genutzt werden (Einsatz von Encryption und Decryption Keys; Lesezugriff nur über private Keys, Ablage in referenzierter verschlüsselter Datenbank und den Pointer und Hash in der Blockchain ablegen).

Versionshistorie

Versionshistorie

Dokumentversion 1.1 – Aktualisiert am 05.04.2018

Kapitel	Art	Seite	Änderung
2	sprachlich	10, 11, 12, 13	
2	inhaltlich	12	[…] oder Anteil an einem Unternehmen, […] *für* […] oder eines Unternehmens, […]
		12	[…] Web 3 […] *für* […] dezentralen Web […]
		12	[…] verringern […] *für* […] schwächen […] jedoch ab […]
		12	[…] in Form von Initial Coin Offerings (ICOs) […] *für* […] , auch als Initial Coin Offerings (ICOs) bezeichnet, […]
3	inhaltlich	34	[…] in Artikel 35 […] *für* […] in Artikel 25 […]
	inhaltlich	21, 28, 29, 30, 31	Verweise ergänzt

Bitkom vertritt mehr als 2.500 Unternehmen der digitalen Wirtschaft, davon gut 1.700 Direktmitglieder. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen 1.000 Mittelständler, mehr als 400 Start-ups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10
10117 Berlin
T 030 27576-0
F 030 27576-400
bitkom@bitkom.org
www.bitkom.org