Maximilian Eibl, Martin Gaedke. (Hrsg.): INFORMATIK 2017,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2017 1025

Die Blockchain im Spannungsfeld der Grundsätze der Datenschutzgrundverordnung

Ninja Marnau[1]

Abstract: Blockchain-Technologie und auf ihr basierende Smart Contracts erfahren aktuell große Aufmerksamkeit. Egal ob Finanztransaktionen, eHealth oder eGovernment, für zahlreiche Anwendungsfelder wird der Einsatz von Blockchain-Technologie in Betracht gezogen. In jüngster Zeit mehren sich jedoch auch kritische Stimmen, die die kryptographischen und Konsens-Prinzipien dieser Technologie für unvereinbar mit der Verarbeitung personenbezogener Daten und somit den Grundsätzen des Datenschutzrechts halten. Ziel dieses Beitrags ist es, die Eignung verschiedener Blockchain-Technologien für die Erfüllung der Grundsätze für die Verarbeitung personenbezogener Daten gemäß Artikel 5 der EU Datenschutzgrundverordnung wie u.a. Rechenschaftspflicht, Speicherbegrenzung und Betroffenenrechten zu analysieren.

Keywords: Blockchain, Redactable Blockchain, Privacy, Datenschutz, DSGVO, Transparenz, Rechenschaftspflicht, Speicherbegrenzung, immutability, right to be forgotten, distributed ledger, distributed consensus

1 Einleitung

Die Blockchain-Technologie erlebt aktuell einen Hype, ähnlich wie vor einigen Jahren das Cloud-Computing. Blockchain-Technologie soll Datenspeicherung und Transaktionswesen revolutionieren und wird nicht nur für eine Vielzahl von Anwendungsfeldern der Datenverarbeitung vorgeschlagen, sondern durch Unternehmen und staatliche Stellen bereits in ersten Testfeldern eingesetzt. Start-Ups, die Blockchain-Lösungen anbieten, haben bereits mehr als 1,5 Billionen US Dollar an Venture Capital erhalten [Cd17]. Die Diskussion darüber, ob und unter welchen Voraussetzungen die Blockchain und ihre Charakteristika mit den Anforderungen des europäischen Datenschutzrechts vereinbar ist, hat jedoch gerade erst begonnen.[2]

Blockchain-Technologie und insbesondere die darauf beruhende Währung Bitcoin ermöglichen es, dass sich gegenseitig nicht vertrauende Parteien (Finanz-)Transaktionen durchführen und diese transparent und integer speichern, ohne einen zentralen, vertrauenswürden Treuhänder oder Vermittler einzubinden. Die von Nakamoto [Na09] vorgestellte Technologie gab dabei erstmals kryptographische Garantien, die die doppelte

[1] Center for IT-Security, Privacy and Accountability (CISPA), Saarland Informatics Campus, Universität des Saarlandes, Campus E 9.1, 66123 Saarbrücken, marnau@cispa.saarland

[2] So forderte der EDPS in seinem Newsletter von Oktober 2016: „It is essential that data protection experts begin to examine the concepts behind blockchain technology and how it is implemented in order to better understand how data protection principles can be applied to it" [ED16].

doi:10.18420/in2017_105

Ausgabe von Währungseinheiten wirksam verhinderte und somit die tatsächliche Nutzung der Währung Bitcoin als Zahlungsmittel ermöglichte.

Der wirtschaftliche Erfolg der „Krypto-Währung“ Bitcoin brachte der Blockchain-Technologie globale Aufmerksamkeit. Die rechtswissenschaftliche Diskussion um die zivil- und finanzaufsichtsrechtliche Bewertung von Bitcoin und Bitcoin-Transaktionen[3] ist daher bereits weiter fortgeschritten als die datenschutzrechtliche.

Die oben genannten Eigenschaften machen die Technologie neben Finanztransaktionen jedoch für eine Vielzahl von weiteren Anwendungsfeldern attraktiv: z.B. verteilte Datenspeicherung in der Cloud, verteilte Datenverarbeitung im Internet der Dinge, Speicherung und Weitergabe von Gesundheitsdaten, Datenverarbeitung innerhalb einer Lieferkette.[4] Durch den Einsatz von Blockchain-Technologie für Smart Contracts ließen sich prinzipiell beliebige Vertragsbeziehungen in der Blockchain darstellen und beim Eintreten von Vertragsbedingungen automatisch ausführen.[5]

Dieser Beitrag konzentriert sich darauf, die der Blockchain-Technologie immanenten Charakteristika dahingehend zu analysieren, ob sie gegebenenfalls mit Prinzipien und Anforderungen des Datenschutzrechts im Konflikt stehen und ob der Einsatz verschiedener Arten der Blockchain zur Verarbeitung personenbezogener Daten ratsam im Hinblick auf datenschutzrechtliche Compliance und dementsprechenden Rechenschaftspflichten ist.

2 Charakteristika der Blockchain-Technologie und ihr Verhältnis zu den Datenschutzgrundsätzen der DSGVO

Die wesentlichen Innovationen der Blockchain sind die unveränderbare Speicherung von Daten (immutability), die dezentrale, verteilte Registerführung (distributed ledger) und die Entscheidungsfindung per Mehrparteienkonsens (peer-to-peer consensus protocol). Diese Charakteristika werden im Folgenden detailliert dargestellt und mit den relevanten Grundsätzen für die Verarbeitung personenbezogener Daten gemäß Art. 5 DSGVO abgeglichen.

Blockchains werden durch ein peer-to-peer Netzwerk von Teilnehmern (Nodes) geführt. In der offenen und dezentralen Grundform der Blockchain („Permissionless Blockchain“) speichert und verarbeitet jeder Teilnehmer in diesem Netzwerk eine eigene Kopie der Blockchain. Da alle Teilnehmer gleiche Befugnisse im Hinblick auf die Blockchain haben, spricht man von dezentraler, verteilter Registerführung.

Sobald das Netzwerk eine Mehrheitsentscheidung über das Hinzufügen eines neuen

[3] Mit weiteren Nachweisen [EK14] zur zivilrechtlichen Einordnung; [Le15] zur finanzaufsichtsrechtlichen Einordnung.
[4] Zur technischen Eignung von Blockchain-Technologie für die diskutierten Anwendungsfelder siehe [WG17].
[5] Zur rechtlichen Analyse von Smart Contracts und dem Einsatz von Blockchain-Technologie siehe [KH16].

Blocks trifft, werden alle Kopien um diesen Block ergänzt. Konflikte durch nicht aktualisierte Kopien im Netzwerk werden dadurch gelöst, dass immer die längste valide Blockchain die gültige ist.

In Abgrenzung zu dieser offenen, dezentralen Grundform der Blockchain wurden sog. „Permissioned Blockchains" eingeführt[6], die ihr Netzwerk von Teilnehmern nur auf einen bestimmten Kreis von Berechtigten beschränken. Bei dieser Art der Blockchain-Nutzung gibt es eine zentrale Stelle, die die Teilnehmer des Netzwerks festlegt und ihnen Lese- und gegebenenfalls Schreibrechte einräumt. Dies erlaubt den Einsatz von Blockchain-Technologie z.B. innerhalb einer Unternehmensgruppe, um dort Transaktionen zwischen Tochterfirmen nachvollziehen zu können. Die zentrale Stelle kann hierbei einer Untergruppe auch lediglich Lese- aber keine Schreibrechte geben.

Grundsätzlich ist im Hinblick auf eine Bewertung der Blockchain-Technologie und ihrer Eignung zur Erfüllung der Datenschutzgrundsätze aus Art. 5 DSGVO zu beachten, dass diese den Charakter von strukturellen Prinzipien[7] haben und untereinander durchaus in einem Zielkonflikt stehen können[8]. Verschiedene Kriterien, die sich eher auf rechtlichen Erlaubnistatbestand für den Verantwortlichen und die vertragliche Ausgestaltung des Verhältnisses zum Betroffenen beziehen, können nur anhand des konkreten Einzelfalls aber nicht für die Technologie generell geprüft werden und müssen daher außer Acht bleiben: Rechtmäßigkeit sowie Verarbeitung nach Treu und Glauben (in der Tabelle 1 n/a markiert).

2.1 Transparenz (Art. 5 Abs. 1 lit. a Var. 3 DSGVO)

Die dezentrale und verteilte Registerführung führt zu maximaler technischer Transparenz des Systems. Jeder Teilnehmer besitzt eine gleichberechtigte Kopie und kann anhand von dieser jede vergangene Transaktion oder jeden Datenverarbeitungsschritt nachvollziehen und überprüfen. Durch die dezentrale Speicherung und Änderung nur mit dem Mehrheitskonsens ist eine manipulierte Datenverarbeitung einzelner böswilliger Teilnehmer kaum möglich. Je mehr Teilnehmer das Netzwerk hat, desto unwahrscheinlicher ist das Zusammenwirken einer Mehrheit der Teilnehmer.

Sofern die Teilnehmer selbst eine Transaktion beauftragen oder empfangen, z.B. im Rahmen einer Bitcoin-Transaktion, sind sie selbst Betroffene einer Datenverarbeitung. Sobald die Transaktion mit dem Pseudonym (Bitcoin Wallet) von Sender und Empfänger durch einen Teilnehmer des Netzwerks einem validen Block hinzugefügt wurde und dieser

[6] Die am Weitesten verbreiteten Permissioned Blockchains sind laut [WG17] Hyperledger Fabric (https://hyperledger-fabric.readthedocs.io/en/latest/ abgerufen am 23. Mai 2017) und R3 Corda [He16].

[7] Die Grundsätze werden jeweils durch Einzelnormen der DSGVO konkretisiert, verlangen aber als Prinzipien durch den Verantwortlichen und dessen Datenverarbeitung größtmögliche, kumulative Entsprechung aller Grundsätze, siehe auch Kommentierung Heberlein, Art. 5, Rn. 5 in [ES17].

[8] So stehen z.B. traditionell die Grundsätze Transparenz und Vertraulichkeit oder Speicherbegrenzung und Integrität in einem Zielkonflikt, der für jede einzelne Datenverarbeitung abgewogen werden muss, siehe dazu schon im Vorwege der DSGVO [RB11].

durch Mehrheitskonsens an die Blockchain angefügt wird, ist die Transaktion für die Betroffenen und jeden anderen Teilnehmer ersichtlich und damit vollständig transparent.[9] Die Adresse des Bitcoin-Wallets ist aufgrund ihrer Verknüpfung mit einer IP-Adresse regelmäßig nicht anonym, sondern stellt ein Pseudonym dar[10], falls nicht zusätzlich noch Coin-Mixing Werkzeuge verwendet werden, die die Identität und Historie einzelner Teilnehmer verschleiern.

Sofern mit Blockchain-Technologie personenbezogene Daten verarbeitet werden von Betroffenen, die nicht Endpunkt der Transaktion oder Teilnehmer des Netzwerks sind, muss Transparenz auf andere Weise garantiert werden: z.B. im Rahmen von Einwilligungs- oder Datenschutzerklärung, Informationspflichten und Auskunftgabe durch den Verantwortlichen.[11]

2.2 Zweckbindung (Art. 5 Abs. 1 lit. b DSGVO)

Personenbezogene Daten dürfen nach dem Grundsatz der Zweckbindung nur für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und in einer mit dem ursprünglichen Zweck zu vereinbarenden Weise weiterverarbeitet werden. Die Blockchain ist dabei weitgehend davon abhängig, dass die durch den Verantwortlichen zur Verarbeitung und Speicherung eingegebenen Daten bereits dem Grundsatz der Zweckbindung entsprechen. Bei der Berechnung der Blöcke und Speicherung in der Blockchain handelt es sich nicht um eine Zweckänderung, da der Verantwortliche bei der Erhebung und der Bekanntgabe der Transaktion gegenüber dem Netzwerk gerade diese Art der Verarbeitung und Speicherung beabsichtigte. Aufgrund der öffentlichen Verfügbarkeit der Daten sind sie jedoch im besonderen Maße dem Risiko einer zweckändernden Weiterverarbeitung durch Dritte ausgesetzt. [12]

2.3 Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO)

Die DSGVO gibt vor, dass die Menge der Daten für den jeweiligen Zweck angemessen, erheblich und auf das notwendige Maß beschränkt sein muss. Insbesondere ist durch den Verantwortlichen jeweils zu prüfen, ob auch eine Verarbeitung von anonymen Daten oder jedenfalls pseudonymisierten Daten ausreichend ist. Im Falle von Bitcoin agieren die Teilnehmer des Netzwerks jeweils unter einem Pseudonym. Die gespeicherte Transaktion selbst ist auf das notwendige Maß zur Durchführung und des Nachweises der Transaktion beschränkt. Problematisch ist, dass theoretisch beliebiger (auch personenbezogener) weiterer Inhalt Teil eines Blocks werden kann. Hier ist jeweils der Auftraggeber der

[9] [Ho17] begründet für das Beispiel von Bitcoin-Transaktionen warum diese als Verarbeitung zur Erfüllung eigener Geschäftszwecke sowohl für Sender und Empfänger als auch für den Plattformanbieter nach § 28 Abs. 1 Satz 1 Nr. BDSG erlaubt seien.

[10] So auch [SK13] und [Ho17].

[11] Die Transparenzanforderungen werden in Art. 12 bis Art. 15 DSGVO weiter konkretisiert.

[12] Im Hinblick auf die Zulässigkeit einer zweckändernden Weiterverarbeitung der öffentlich verfügbaren Bitcoin-Daten nach BDSG und die Gefahr von Profiling der Teilnehmer siehe [Ho17] S. 165 f.

Transaktion oder Datenspeicherung als Verantwortlicher für die Rechtmäßigkeit verantwortlich.[13]

Fraglich ist, ob die redundante Speicherung von einer Vielzahl von Kopien dem Prinzip der Datenminimierung zuwiderläuft. Dies ist jedoch abzulehnen, da sich das Gebot der Datenminimierung auf den Informationswert der Daten und die Menge unterschiedlicher Datenpunkte bezieht, insbesondere im Hinblick auf die Gefahr von Profilbildung. Redundante Kopien zur Wahrung von Integrität oder Ausfallsicherheit sind daher als bloße Kopien derselben Datenmenge keine Verletzung des Grundsatzes.

2.4 Richtigkeit (Art. 5 Abs. 1 lit. d DSGVO)

Die Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. Für diesen Grundsatz ist das verteilte peer-to-peer Prinzip des Blockchain-Netzwerks durchaus förderlich. Sobald die Teilnehmer eine Mehrheitsentscheidung über das Hinzufügen eines neuen validen Blocks treffen, werden alle Kopien im Netzwerk um diesen Block ergänzt. Da jeder neue Block mit dem vorangehenden durch eine kryptographische Hash-Funktion verknüpft ist, können nur vollständige Kopien den nächsten weiteren Block anfügen. Konflikte durch nicht aktualisierte Kopien im Netzwerk werden dadurch gelöst, dass die längste valide Blockchain Gültigkeit hat. Das Netzwerk stellt so durch sein Protokoll sicher, dass alle Teilnehmer am Netzwerk eine aktuelle und insofern formal richtige Kopie der Blockchain besitzen. Teilnehmer mit einer veralteten Kopie bemerken dies dadurch, dass sie nicht mehr erfolgreich an der Berechnung neuer Blöcke teilnehmen können.

Die Aktualität der Blockchain-Daten und ihre formale Richtigkeit sagt jedoch nichts über ihre Richtigkeit im Hinblick der Betroffenenrechte auf Berichtigung oder ihre sachliche Richtigkeit aus. Hierfür ist grundsätzlich der Verantwortliche der Verarbeitung zuständig.

Eine Kerneigenschaft der Blockchain ist ihre Unveränderbarkeit (immutability). Die Blockchain speichert eine Abfolge von Transaktionen oder Datenverarbeitungsschritten in Blöcken, die je nach Vorgabe des Protokolls eine unterschiedliche Anzahl dieser Transaktionen umfassen. Diese Blöcke werden nun nach der Mehrheitsentscheidung über die Validität des Blocks der Blockchain hinzugefügt. Grundsätzlich kann ein einmal hinzugefügter Block nicht mehr entfernt oder verändert werden, da jeder neue Block mit dem vorangehenden durch eine kryptographische Hash-Funktion dauerhaft verknüpft ist. Wird ein Block verändert, müssten alle nachfolgenden Blöcke ebenfalls neu berechnet werden. Da die Erstellung eines neuen validen Blocks eine rechenintensive Operation ist, wird ein Block umso sicherer im Hinblick auf seinen dauerhaften Verbleib in der Blockchain, je mehr Folgeblöcke nach ihm kommen.

Diese beabsichtigte „Ewigkeit“ der Blöcke garantiert ein integres Archiv von

[13] Zum rechtlichen Verhältnis von Auftraggeber einer Transaktion und anderen verarbeitenden Teilnehmern des Netzwerks siehe unter 2.8.

Transaktionen oder Datenverarbeitungsschritten. Dieses Archiv steht jedem Teilnehmer der dezentralen Registerführung zur Verfügung. Ein einzelner Teilnehmer kann keine dauerhafte Änderung eines Blocks bewirken, ohne dass die anderen Teilnehmer die Veränderung bemerken und per Mehrheitsprinzip die Änderung zurückweisen können.

Diese Unveränderlichkeit steht im direkten Konflikt zu Betroffenenrechten auf Berichtigung, Löschung und dem Recht auf Vergessenwerden. Zwar besteht die Möglichkeit, in einem neuen Block Informationen oder Transaktionen in älteren Blöcken für ungültig zu erklären. Die alten unrichtigen oder zu löschenden Informationen bleiben aber vorhanden und für alle Teilnehmer lesbar. Daher entspricht diese Lösung nicht den datenschutzrechtlichen Anforderungen an die Umsetzung von Betroffenenrechten.

Um diesen Konflikt aufzulösen, wurde 2016/17 das Konzept der „redactable blockchain" vorgestellt, die eine nachträgliche Änderung alter Blöcke erlaubt, ohne dass alle nachfolgenden Blöcke ungültig werden.[14]

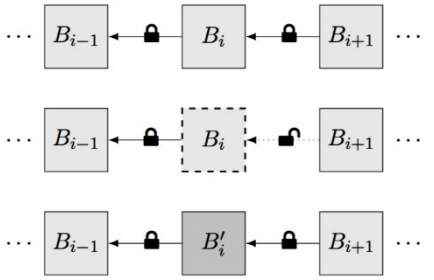

Abb. 1: Funktionsweise der Redactable Blockchain nach [At17]

Die Autoren nutzen für ihr Konzept eine Weiterentwicklung der „chameleon hash function". Die einzelnen Blöcke werden wie in Abb. 1 gezeigt mit dieser Hash-Funktion verbunden. Diese Hash-Verbindung der Blöcke lässt sich mit einem geheimen Schlüssel auftrennen, so dass der zu ändernde Block durch einen neuen ersetzt werden kann, ohne dass alle nachfolgenden Blöcke ihre Gültigkeit verlieren und neu berechnet werden müssten.

Dieser geheime Schlüssel könnte im Fall der Permissionless Blockchain so unter den Teilnehmern verteilt sein, dass nur eine Mehrheit ihn gemeinsam einsetzen könnte.[15] Im Fall der Permissioned Blockchain könnte die zentrale Stelle oder ggf. mehrere vertrauenswürdige Instanzen Inhaber des Schlüssels sein.

Die nachträgliche Veränderung eines Blocks in der Kette geschieht dabei nicht unsichtbar.

[14] [At17] haben ihr Konzept einer Redactable Blockchain zunächst 2016 online veröffentlicht und nach einer weiteren Ausarbeitung auf der Peer Review Konferenz EuroS&P2017.

[15] Bei einer Verteilung auf mehrere oder eine Vielzahl von Teilnehmern soll Secure Multiparty Computation genutzt werden.

Vielmehr hinterlässt die Bearbeitung eine „Narbe“, die für alle Teilnehmer des Netzwerks sichtbar ist. Teilnehmer, die während der Veränderung aktiv sind, könnten auch die alte Kopie gegenüber der veränderten vergleichen und die Änderung dadurch prüfen.

Dieses neue Konzept der Redactable Blockchain löst allerdings den Konflikt zwischen Blockchain-Technologie und Betroffenenrechten nur bedingt auf. Die Autoren selbst gehen davon aus, dass solche Korrektureingriffe nur selten vorgenommen werden.[16] Dies entspricht jedoch nicht der Realität der Verarbeitung personenbezogener Daten. Löschpflichten z.B. würden regelmäßig greifen. Im Hinblick auf das Recht auf Vergessenwerden erhielt Google innerhalb der ersten 12 Monate über 200.000 Anfragen, von denen 48% zu einer Löschung in der Liste der Suchergebnisse führten [Gu15]. In den Szenarien, in denen der geheime Schlüssel auf mehrere oder eine Vielzahl von Teilnehmern verteilt ist, würde das eingesetzte Secure Multiparty Computation Protokoll signifikanten Overhead von Zeit- und Rechenaufwand bedeuten. Im zentral verwalteten Szenario der Permissioned Blockchain errechneten die Autoren hingegen nur geringen Overhead bei der Erstellung der Blockchain und dem Austausch von Blöcken. Das vorgeschlagene Konzept scheint daher für den Einsatz im Rahmen einer internen Permissioned Blockchain deutlich besser geeignet, um Betroffenenrechte effektiv umzusetzen.

2.5 Speicherbegrenzung (Art. 5 Abs. 1 lit. f Var. 1)

Der Grundsatz der Speicherbegrenzung bezieht sich nur auf die zeitliche Länge der Speicherung nicht auf die Anzahl der Kopien. Daher sind das peer-to-peer Prinzip und die dezentrale Speicherung selbst zunächst kein Widerspruch zu diesem Grundsatz. Allerdings ist aus Transparenzgründen keine Löschung alter Blöcke nach Erfüllung des Verarbeitungszwecks vorgesehen. Die Währung Bitcoin bezieht ihre Vertrauenswürdigkeit unter anderem aus diesem ewigen Archiv aller Transaktionen.

Das Konzept der Redactable Blockchain erlaubt auch das Löschen oder Komprimieren mehrerer Blöcke in einer Operation. Allerdings stellt dies ebenfalls nur im Rahmen einer Permissioned Blockchain eine gangbare Lösung zur Erfüllung der Speicherbegrenzung dar, da es in einem dezentralen, verteilten Netzwerk keine Möglichkeit gäbe, alle im Umlauf befindlichen Kopien zur Löschung zu verpflichten.[17]

[16] Die Autoren selbst rechnen mit einer ähnlichen Häufigkeit wie von hard forks der Blockchain: „As for hard forks, we expect redactions to occur in rare and exceptional circumstances“ [At17].

[17] Dies erkennen die Autoren der redactable blockchain selbst als Nachteil. Zwar führen sie zutreffend aus, dass eine redactable blockchain nicht aufgrund ihrer Unveränderlichkeit auf Beschluss eines Gerichts komplett von einer Plattform entfernt werden könnte (z.B. kann ein Block mit kriminellem Inhalt wie Kinderpornographie auch Jahre später in einer Redactable Blockchain gelöscht werden) [At17]. Die Autoren berücksichtigen aus datenschutzrechtlicher Perspektive jedoch nicht, dass der datenschutzrechtlich Verantwortliche auch für die Löschung aller von ihm in Umlauf gebrachten Kopien haftbar sein kann.

2.6 Vertraulichkeit (Art. 5 Abs. 1 lit. f Var. 2)

In der Form der Permissionless Blockchain kann prinzipiell jeder (auch mehrfach mit verschiedenen Pseudonymen) ein Teilnehmer des Netzwerks werden. Da alle Blöcke zu Beweiszwecken allen Teilnehmern zugänglich gemacht werden, bietet diese Form der Blockchain für die Inhalte der Blöcke keine Vertraulichkeit.

Bei der Permissioned Blockchain ist die Vertraulichkeit der Informationen dadurch umrissen, dass die zentrale Stelle nur selektiv Lese-Zugriff zum Netzwerk gibt. Da der Kreis der Teilnehmer am Netzwerk bei einer Permissioned Blockchain wesentlich kleiner ist, ist die Möglichkeit zur Manipulation durch Absprachen der Teilnehmer mit Schreibrechten allerdings dementsprechend größer. Die Vertraulichkeit des Netzwerkes geht damit zu Lasten der Vertrauenswürdigkeit des peer-to-peer Prinzips beim Berechnen und Hinzufügen neuer Blöcke.[18]

2.7 Integrität (Art. 5 Abs. 1 lit. f Var. 1)

Durch das transparente Archiv und die kryptographische Verknüpfung der fortlaufenden Blöcke liefert die Blockchain-Technologie starke Integritätsgarantien. Die Integritätsgarantien beruhen dabei auf der notwendigen Rechenleistung, die ein böswilliger Akteur erbringen müsste, um die Blöcke zu manipulieren.

Jeder einzelne Teilnehmer versucht aus den im Netzwerk neu bekanntgegebenen Transaktionen valide neue Blöcke zu errechnen. Ein valider Block wird dann nach dem Konsensprinzip an die Blockchain angehängt. Da die Errechnung eines Blocks rechenintensiv ist, ist eine Manipulation eines Blocks durch einen böswilliger Akteur umso unwahrscheinlicher, je mehr Blöcke bereits an diesen angehängt worden sind. Denn der Akteur müsste auch alle folgenden Blöcke neu berechnen, da jeweils nur die längste Kette Gültigkeit hat. Je älter ein Block also ist (<5 Folgeblöcke), desto größer ist die mathematische Integritätsgarantie.

Im Hinblick auf die Redactable Blockchain gilt diese Integritätsgarantie nur für die Blöcke die erkennbar unverändert sind. Aufgrund der bleibenden Narbe in der Blockchain bei Eingriffen, ist dies jedoch im Rahmen z.B. eines Audits zu erkennen.

2.8 Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO)

Die Rechenschaftspflicht umfasst, dass der für die Verarbeitung Verantwortliche für die Einhaltung der genannten Grundsätze verantwortlich ist und diese Einhaltung auch nachweisen kann.

[18] Denkbar wäre eventuell ein Szenario mit einer Vielzahl von schreibenden Teilnehmern (z.B. Sensoren von smarten Geräten) und einem nur sehr kleinen Kreis von Teilnehmern mit Leserechten, die diese Daten dann auswerten dürfen.

Im Rahmen der dezentralen, verteilten Registerführung ist es jedoch bereits schwierig festzustellen, wer der Verantwortliche ist. Grundsätzlich ist davon auszugehen, dass derjenige, der die Finanztransaktion oder einen anderen Datenverarbeitungsvorgang initiiert, der Verantwortliche der Datenverarbeitung nach Art. 4 Nr. 7 DSGVO ist. Allerdings verliert dieser Verantwortliche die Kontrolle über die weitere Verarbeitung zu dem Zeitpunkt, an dem er die Transaktion dem Netzwerk mitteilt, damit sie durch Berechnung anderer Teilnehmer einem Block und dann der Blockchain hinzugefügt wird. Zunächst könnte man intuitiv annehmen, dass alle anderen Teilnehmer des Netzwerks für diese Transaktion Auftragsdatenverarbeiter nach Art. 4 Nr. 8 DSGVO seien. Allerdings unterliegen die anderen Teilnehmer keinerlei Weisung des Verantwortlichen; ebensowenig gibt es im Regelfall schriftliche oder mündliche Vereinbarungen über die Art und Weise der Verarbeitung, die über das Blockchain-Protokoll hinausgehen, was jedoch keinesfalls die umfangreichen Pflichten nach Art. 28 DSGVO zum Verhältnis zwischen Verantwortlichem und Auftragsdatenverarbeiter erfüllt. Am ehesten entspricht die Handlung des Verantwortlichen, die Bekanntgabe der Transaktion, einer Übermittlung an einen unbestimmten Personenkreis (Veröffentlichung). Formal würde dies im Fall von Bitcoin-Transaktionen erfordern, dass der Verantwortliche gemäß Art. 6 Abs. 1 DSGVO entweder vorab die Einwilligung des Empfängers der Transaktion (lit. a) einholt oder im Rahmen einer Abwägung feststellt, dass sein eigenes berechtigtes Interesse an der Transaktion eventuelle Interessen des Empfängers überwiegt (lit. f).

Während man im Falle von Bitcoin und anderen Finanztransaktionen diese Berechtigung zur Übermittlung nach Art. 6 Abs. 1 DSGVO annehmen kann, da der Empfänger selbst Teilnehmer des Netzwerks ist und darüber hinaus einen finanziellen Vorteil von der Transaktion hat[19], lässt sich diese Einschätzung nicht verallgemeinern für die Fälle, in denen weitere personenbezogene Daten oder Daten von Nicht-Teilnehmern des Netzwerks übermittelt werden.

Möglich wäre, dass alle Teilnehmer des Netzwerks als gemeinsam für die Verarbeitung Verantwortliche („joint controller“) gemäß Art. 26 DSGVO agieren. Dies hätte zur Folge, dass es erstens eine Vereinbarung zur Wahrung der Betroffenenrechte zwischen den Teilnehmer gäbe und zweitens jeder Teilnehmer vollumfänglich gegenüber dem Betroffenen für die Umsetzung von dessen Rechten in die Verantwortung genommen werden kann. Ob diese gemeinsame Verantwortung in bestimmten Szenarien sinnvoll und für die Umsetzung der Betroffenenrechte zielführend ist, muss anhand des Einzelfalls entschieden werden.

Grundsätzlich lässt sich festhalten, dass das europäische Datenschutzrecht auch in seiner neuen Fassung dezentralisierte Datenverarbeitung von personenbezogenen Daten weder fördert noch überhaupt vorsieht.

Auch im Hinblick auf die Rechenschaftspflicht erscheint lediglich die Permissioned Redactable Blockchain geeignet, um die Umsetzung der Grundsätze zu fördern und durch ihren kryptographisch gesicherten Datenspeicher gegebenenfalls auch gegenüber einer

[19] Mit ähnlicher Argumentation schon [Ho17] zur Berechtigung nach § 28 Abs. 1 Satz 1 Nr. BDSG.

Aufsichtsbehörde nachzuweisen. In diesem Szenario ist es auch realistisch, zwischen der zentralen Stelle als Verantwortlichem und allen Teilnehmern Auftragsdatenverarbeitungsvereinbarungen abzuschließen.

2.9 Übersicht

	Permissionless Blockchain	Permissioned Blockchain	Permissioned Redactable Blockchain
Rechtmäßigkeit	n/a	n/a	n/a
Treu und Glauben	n/a	n/a	n/a
Transparenz	+	+	+
Zweckbindung	-	+	+
Datenminimierung	n/a	n/a	n/a
Richtigkeit	-	-	+
Speicherbegrenzung	-	-	+
Vertraulichkeit	-	+	+
Integrität	+	+	+
Rechenschaftspflicht	-	-	+

Tab. 1: Verhältnis von Blockchain-Typen zu Datenschutzgrundsätzen (Bewertung: + (förderlich), - (abträglich), n/a (nicht beantwortbar))

3 Fazit

Die Analyse legt nahe, dass sich Blockchain-Technologie nur sehr bedingt für den Einsatz zur Verarbeitung und Speicherung personenbezogener Daten in der Blockchain anbietet. Zwar bietet die Technologie kryptographische Garantien im Hinblick auf Integrität und Aktualität sowie durch die verteilte Registerführung ein großes Maß an Transparenz für die Beteiligten. Um aber die Grundsätze von Vertraulichkeit, Rechenschaftspflicht und Betroffenenrechte z.B. auf Berichtigung umsetzen zu können, muss die Technologie so weit verändert werden, dass von den ursprünglichen Vorteilen und Garantien der dezentralen Verarbeitung zwischen sich nicht vertrauenden Parteien wenig bleibt. Eine zentral verwaltete, korrigierbare Blockchain (Permissioned Redactable Blockchain) kann zwar zu Verarbeitung personenbezogener Daten eingesetzt werden, unterscheidet sich

jedoch kaum von herkömmlichen Lösungen zur redundanten und kryptographisch abgesicherten Datenspeicherung [WG17].

Auch wenn dezentrale Datenverarbeitung in vielen Anwendungsfällen wünschenswert ist, geht das europäische Datenschutzrecht nach wie vor von einer zentralen Stelle aus, die die gesamte Verarbeitung unter ihrer Kontrolle hat. Dies garantiert zwar, einen Verantwortlichen für die Wahrung der Betroffenenrechte zu haben, forciert aber auch zentralisierte, geschlossene Systeme.

Dies spiegelt sich ebenfalls wider im prominentesten Anwendungsbeispiel von Blockchain-Technologie in den EU Mitgliedsstaaten:

So arbeitet die estnische eHealth Foundation gemeinsam mit dem Blockchain Start Up Guardtime an einem Blockchain-basierten System, um die Integrität der Patientendaten von über einer Million Esten zu schützen [IBT16]. Die Teilnehmer des Blochchain-Systems sind Institute im Gesundheitswesen wie Hausärzte, Fachärzte und Krankenhäuser. Diese speichern Hashes der Patientendaten in der Blockchain, wann immer diese Patientendaten geändert werden. So können andere Teilnehmer erkennen, ob die Patientendaten, die sie verwenden, aktuell sind und falls nicht, wer die Daten seitdem verändert hat.

Das System speichert somit nicht die Patientendaten selbst, sondern lediglich Metadaten, die eine Veränderung der Daten für alle Teilnehmer erkennen und rückverfolgen lassen.

Doch selbst in einem derart geschlossenen System, das die Blockchain nur als Proof of Existence bzw. Proof of Freshness nutzt für sensible Daten, die an anderer Stelle gespeichert sind, bleiben Datenschutzbedenken. So ließen sich beispielsweise allein anhand der Frequenz der Aktualisierung der Hashwerte Rückschlüsse über die Häufigkeit von Arztbesuchen und somit auf den Gesundheitszustand einzelner Betroffener ziehen.

Die Europäische Kommission, die sich bisher explizit bei der Regulierung von Blockchain zurückgehalten hat, um die Innovation nicht zu bremsen, investiert daher in Entwicklung, die versucht, die verteilte Registerführung mit zusätzlichen Kontrollinstrumenten und Anonymisierungsmethoden zu kombinieren.[20] Die geförderten Projekte streben dabei bewusst an, gegebenenfalls auch Vorschläge zu Änderungen des Rechtsrahmens für dezentrale Datenverarbeitung vorzulegen.[21] An dieser Diskussion sollten sich insbesondere Datenschützer und Rechtswissenschaftler beteiligen, um sinnvolle regulatorische Lösungen für das skizzierte Spannungsfeld zu erarbeiten.

[20] Kommissar Ansip verwies im Februar 2017 auf Anfrage des Parlaments auf die Forschungsprojekte DECODE, D-Cent und My Health My Data und kündigte an, die Förderungsbemühungen der Kommission in den nächsten Monaten noch auszuweiten [An17].

[21] Das erst vor wenigen Monaten gestartete H2020 Projekt My Health My Data listet als Objective: „definition of a proper legal and regulatory framework and creation of new rules and best practices for uncovered processes, solutions and methodologies" [My17].

Literaturverzeichnis

[An17] Ansip, A.: Answer given by Vice-President Ansip on behalf of the Commission, 17.02.2017. http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2016-009012&language=EN, Stand: 29.05.2017.

[At17] Ateniese, G.; Magri, B.; Venturi, D.; Andrade, E.: Redactable Blockchain – or – Rewriting History in Bitcoin and Friends. Proceedings of the 2nd IEEE European Symposium on Security and Privacy (EuroS&P), 2017.

[Cd17] Coindesk. Bitcoin Venture Capital. http://www.coindesk.com/bitcoin-venture-capital/ , Stand: 29.05.2017.

[ED16] European Data Protection Supervisor: Newsletter No. 49/Oct. 2016. https://edps.europa.eu/sites/edp/files/publication/newsletter_49_en.pdf, Stand: 29.05.2017.

[EK14] Engelhardt, C.; Klein, S.: Bitcoins – Geschäfte mit Geld, das keines ist - Technische Grundlagen und zivilrechtliche Betrachtung. Multimedia & Recht (MMR) 2014, S. 355-360, 2014.

[ES17] Ehmann, E.; Selmayr, M. (Hrsg): DSGVO. Kommentar. Beck-Verlag, München, 2017.

[Cd17] The Guardian. Tippman/Powles: Google accidentally reveals data on 'right to be forgotten' requests v. 14.07.2015. https://www.theguardian.com/technology/2015/jul/14/google-accidentally-reveals-right-to-be-forgotten-requests, Stand: 29.05.2017.

[He16] Hearn, M.: Bitcoin: Corda: A distributed Ledger. https://docs.corda.net/_static/corda-technical-whitepaper.pdf, 2016, Stand: 29.05.2017.

[Ho17] Hofert, E.: Blockchain-Profiling – Verarbeitung von Blockchaindaten innerhalb und außerhalb der Netzwerke. Zeitschrift für Datenschutz (ZD) 2017, S. 161-166, 2017.

[IBT16] International Business Times. Allison, I.: Guardtime secures over a million Estonian healthcare records on the blockchain, vom 04.03.2016. http://www.ibtimes.co.uk/guardtime-secures-over-million-estonian-healthcare-records-blockchain-1547367, Stand: 29.05.2017.

[Le15] Lerch, M.: Bitcoin als Evolution des Geldes. Zeitschrift für Bankrecht und Bankwirtschaft (ZBB) 2015, S. 190-204, 2015.

[KH16] Kaulartz, M.; Heckmann, J.: Smart Contracts – Anwendungen der Blockchain-Technologie. Computer & Recht (CR) 2016, S. 618-624, 2016.

[RB11] Rost, M.; Bock, K.: Privacy By Design & die Neuen Schutzziele. DuD, S. 30-35,2011.

[SK13] Sorge, C.; Krohn-Grimberghe, A.: Bitcoin – das Zahlungsmittel der Zukunft? Wirtschaftsdienst 10/2013, S. 720-722, 2013.

[My17] My health My data, http://www.myhealthmydata.eu/objectives/, Stand: 29.05.2017.

[Na09] Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system. 2009.

[WG17] Wüst, K.; Gervais, A.: Bitcoin: Do you need a Blockchain? Cryptology ePrint Archive: Report 2017/375, 2017.