BLOCKCHAIN UND DSGVO

Jörn Erbguth

Diplom-Informatiker, Diplom-Jurist, Berater zu Blockchain, Smart Contracts und Datenschutz, Promovend Uni Genf
Chemin du Champ d'Annier 15, 1209 Genf, CH
joern@erbguth.net; https://erbguth.ch sowie https://erbguth.ch/QuickCheck

Schlagworte: ***Blockchain, Peer-to-Peer, DSGVO, Smart Contracts, Verantwortlicher, Auftragsverarbeiter, Betroffener, Hash-Funktion, Hash-Wert, personenbezogene Daten***

Abstract: *Die französische CNIL hat eine Stellungnahme zur datenschutzrechtlichen Bewertung der Blockchain-Technologie abgegeben. Der Autor stellt zwei Konfliktfelder öffentlicher Blockchains mit der DSGVO dar:*
a) Wann haben Hash-Werte von personenbezogenen Daten noch einen Personenbezug?
b) Wie verteilen sich die Rollen der DSGVO, also Verantwortliche, Auftragsverarbeiter und Betroffene, bei Peer-to-Peer-Technologien wie öffentlichen Blockchains?
Schließlich präsentiert der Autor einen Legal-Tech-Prototypen, der in einem interaktiven Dialog Datenschutzprobleme bei Blockchain-Anwendungen identifiziert.

1. Einleitung

Ein Ziel der Nutzung von Blockchains ist die Disintermediation. Bei dezentralen Systemen werden Daten technisch gesichert. Man muss daher nicht zentralen Akteuren wie Facebook oder Google vertrauen. Damit sollten öffentliche Blockchains eigentlich natürliche Verbündete des Datenschutzes sein. Trotzdem sind Blockchain und DSGVO kein Traumpaar. Das liegt vor allem daran, dass Blockchain Privacy by Design dadurch schafft, in dem die Verarbeitung von Daten technisch jeder fremden Kontrolle entzogen werden. Die DSGVO stellt dagegen Datenschutz überwiegend dadurch sicher, dass die Verarbeiter und Verantwortlichen die Datenverarbeitung kontrollieren und dann ihrerseits kontrolliert werden.

Aus diesem Spannungsverhältnis ergeben sich grundsätzliche Konflikte, die noch nicht ausreichend geklärt sind. Die DSGVO ist nicht technikneutral, sondern setzt bestimmte hierarchische Organisationsformen voraus. Daher muss geklärt werden: Kann die DSGVO so interpretiert werden, dass dieser technische Datenschutzansatz möglich bleibt? Schutzzweck der DSGVO ist der Datenschutz. Er selbst ist Grundrecht (Art. 8 GRCh). Mit Blick auf den Normzweck lässt sich argumentieren, dass die DSGVO besseren Datenschutz nicht verhindern darf. Die Stellungnahme der französischen Aufsichtsbehörde CNIL[1] kann als Versuch der positiven Einordnung der atypischen Blockchain-Technologie in das etwas zu starre Gerüst der DSGVO gewertet werden.

Die aktuelle Rechtsunsicherheit lähmt, allerdings lassen sich klar bestimmte Konstellationen als eher nicht datenschutzkonform und andere als datenschutzoptimiert klassifizieren. Dies soll im Folgenden versucht werden. Die Publikation der französischen Aufsichtsbehörde CNIL bietet hierbei einen ersten Orientierungspunkt.

[1] Die CNIL hat 2018 hierzu zunächst zwei französische Dokumente und anschließen die englischen Übersetzungen veröffentlicht:CNIL, Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data, Dokument 1: https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data (alle Links aufgerufen am 14. Januar 2019), Dokument 2: https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf CNIL, Blockchain et RGPD: quelles solutions pour un usage responsable en présence de données personnelles ? Dokument 1: https://www.cnil.fr/en/node/24807, Dokument 2: https://www.cnil.fr/sites/default/files/atoms/files/la_blockchain.pdf

Auf eine grundlegende Erläuterung des Konzeptes von Blockchains oder der Kernbestandteile des Datenschutzes verzichte ich hier aus Platzgründen.[2] Im Folgenden möchte ich stattdessen zwei Konfliktpunkte herausgreifen. Der eine betrifft die Frage, in welchen Fällen Hashwerte von personenbezogenen Daten noch als personenbezogene Daten anzusehen sind. Der zweite Punkt bezieht sich darauf, wer welche Rolle bei einer öffentlichen Blockchain hat und wie mit den sich daraus ergebenden Pflichten umgegangen werden kann.

2. Verwendung von Hashwerten

Speicherplatz auf einer öffentlichen Blockchain ist teuer. Schon aus diesem Grund speichern die meisten Blockchain-Applikationen die eigentlichen Daten extern. Das hat den Nebeneffekt, dass sie dort einem Zugriffsschutz unterliegen, korrigiert und auch gelöscht werden können. Zum Nachweis, dass die Daten nicht nachträglich manipuliert wurden, werden Hashwerte – also eine Art digitaler Fingerabdruck – auf der Blockchain abgelegt. Da die Blockchain gegen Veränderung gesichert ist, kann der dort abgelegte Hashwert nicht verändert werden. Dieser passt jedoch nur dann zum eigentlichen Datenobjekt, wenn das Datenobjekt unverändert ist. Sollte das eigentliche Datenobjekt gelöscht worden sein, ist eine Rekonstruktion meistens ausgeschlossen. Sind die auf einer Blockchain abgelegten kryptographischen Hashwerte personenbezogener Daten ihrerseits immer noch als personenbezogene Daten anzusehen?

2.1. Hashfunktionen

Die Hashwerte werden mit Hilfe von kryptographischen Hashfunktionen berechnet. Die Hashwerte sind in der Regel recht kurz – typischerweise z.B. 256 Bit, also etwa 43 Zeichen in Base64-Schreibweise. Da lassen sich keine umfangreichen Daten speichern. Ein Hashwert ist daher eher vergleichbar mit einem klassischen Fingerabdruck und nicht mit einem genetischen Fingerabdruck. Der klassische Fingerabdruck gibt direkt auch keine Informationen über den Menschen preis, während der genetische Fingerabdruck die Information über Geschlecht, Haarfarbe etc. beinhaltet.

Hat man eine Datenbank mit den Fingerabdrücken des Betroffenen, so kann man mit einem klassischen Fingerabdruck jedoch auch die Betroffenen identifizieren. Im Gegensatz zum klassischen Fingerabdruck besteht darüber hinaus die Gefahr das digitale Objekt zu erraten. Das Erraten wird dadurch erleichtert, dass das Bitcoin-Mining dazu geführt hat, dass extrem schnelle Hardware für diesen Zweck entwickelt wurde. Dies beeinträchtigt nun die Sicherheit der Verwendung von Hashwerten. Ein Bitcoin-Miner, der in der Größenordnung von 1500 Franken kostet, kann 37 Billiarden Hashwerte pro Sekunde berechnen.[3] Eine dreizehnstellige Zahlenkombination kann damit in Sekundenbruchteilen erraten werden. Die gehashten Daten müssen daher deutlich komplexer sein. Falls die Daten nicht genügend Komplexität (Entropie) aufweisen, müssen sie ggf. vor dem Berechnen des Hashwertes um zufällige Zusatzwerte[4] ergänzt werden.

Kryptographische Hashfunktionen zeichnen sich dadurch aus, dass sie praktisch nicht umgekehrt werden können. Aus einem Hashwert lässt sich nie weder das Ursprungsobjekt noch ein passendes anderes Objekt errechnen. Viele kryptographische Hashfunktionen sind jedoch inzwischen als unsicher eingestuft.[5] Es gibt auch keinen mathematischen Beweis, dass eine der aktuell verwendeten kryptographischen Hashfunktionen auf Dauer sicher sein wird. Allerdings trifft diese Aussage auf praktisch jede andere Software auch zu, die Sicherheitslücken haben kann. Die dauerhafte Speicherung auf einer Blockchain verschärft zwar die Problematik von unsicher werdenden Hashverfahren. Doch auch bei Blockchains ist eine Migration auf sichere Verfahren möglich. Ein Konsens der Teilnehmenden für diese Migration wäre zudem wahrscheinlich.

---

2 Einführend etwa Laschewski, Der Blockchain-Algorithmus, WPg 2017, 359; Erbguth/Fasching, Wer ist Verantwortlicher einer Bitcoin-Transaktion? ZD 2017, 560; weitergehend Lauerence/Muhr, Blockchain für Dummies, Wiley – VCH, Weinheim 2018.

3 Z.B. EBANG EBIT E11+ mit 37 Terra Hashes pro Sekunde für 1500 US-Dollar, http://miner.ebang.com.cn/goods-13.html.

4 Diese Zufallswerte werden je nach Art der Verwendung *Pfeffer* bzw. *Salz* genannt.

5 So etwa MD4, MD5, SHA vgl. Wikipedia, Kryptographische Hashfunktion, https://de.wikipedia.org/wiki/Kryptographische_Hashfunktion.

2.2. Personenbezogene Daten

Die DSGVO findet auf eine Blockchain Anwendung, wenn diese Hashwerte personenbezogener Daten auch selbst noch als personenbezogene Daten zu betrachten sind. Was dabei personenbezogene Daten sind, wird in Art. 4 Nr. 1 definiert. Es sind Daten, die sich auf eine *identifizierbare Person* beziehen. Welcher Maßstab bei der Identifizierbarkeit anzulegen ist, erläutert der Erwägungsgrund 26: Es sollen dabei *alle Mittel berücksichtigt werden, die ... nach allgemeinem Ermessen wahrscheinlich genutzt werden*.[6]

2014 hat die WP29 eine Stellungnahme zu Anonymisierungstechniken verfasst.[7] Ähnlich einer Anonymisierung geht es bei der Blockchain um die Frage, ob mit den Daten auf der Blockchain Personen identifiziert werden können. Bei einer Anonymisierung sollen z.B. medizinische Daten so aufbereitet werden, dass eine wissenschaftliche Auswertung noch möglich, eine Identifizierung der Betroffenen aber unmöglich ist. Das ist häufig auf Blockchains anders. Hier sollen die Daten auf der Blockchain oft nur im Zusammenspiel mit externen Daten sinnvoll einsetzbar sein. Werden die externen Daten gelöscht, sollen auch die auf der Blockchain abgespeicherten digitalen Fingerabdrücke unbrauchbar werden.

Die WP29 kommt in ihrer Stellungnahme zu einem negativen Ergebnis: Die Techniken würden die Kriterien einer wirksamen Anonymisierung nicht zuverlässig erfüllen. Dies wird ergänzt um den Zusatz, *dass einige ... Risiken mit einer bestimmten Technik vollständig oder teilweise ausgeschlossen* werden können.[8] Es könnte also – muss aber nicht – die Gefahr der Identifizierbarkeit von Personen verbleiben.

Da die Ablage von Daten auf einer Blockchain jedoch nicht identisch mit dem Vorgang einer Pseudonymisierung/Anonymisierung ist, lohnt es sich, das von der WP29 konkret untersuchte Szenario zu betrachten. In einer personenbezogenen Tabelle wurden die Identifikatoren durch Hashwerte ersetzt. Dies bedeutet, dass die eigentlichen personenbezogenen Informationen bestehen bleiben, aber der Personenbezug durch Ersatz des Identifikators durch den Hashwert entfernt werden soll.

2.3. Pseudonymisierungsbeispiel

Das folgende Beispiel (Tabelle 1) zeigt etwa eine Liste von Buchbestellungen. Vorname und Nachname werden dann durch deren Hashwerte ersetzt (Tabelle 2, Tabelle 3). Da es nur etwa 8 Milliarden Menschen gibt, könnten Bitcoin-Miner eine Liste aller Namen innerhalb von Sekundenbruchteilen durchgehen. Um das zu erschweren, wird eine Zufallszahl (*Salz*) vor dem Berechnen des Hashwertes hinzugefügt (vgl. 2.1.) Dies erhöht die kombinatorischen Möglichkeiten (Entropie) so sehr, dass ein Rückschluss auf die Ausgangswerte durch Ausprobieren nicht mehr möglich ist.

Vorname	Name	Artikel	Menge	Preis	Datum
John	Smith	1984 by George Orwell	1	10	3.1.2019
Lisa	Doe	Ulysses by James Joyce	1	20	7.1.2019
John	Smith	Inside Wikileaks by Domscheit-Berg	1	15	9.1.2019

Tabelle 1: Ursprüngliche Daten

Trotz Hinzufügen von *Salz* ist diese Vorgehensweise für eine Anonymisierung jedoch ungeeignet. Die WP29 listet drei Probleme auf:

---

6 Der angelegte Maßstab wird dabei als überzogen kritisiert: Jaccard/Tharin, GDPR & Blockchain: the Swiss take, in: Jusletter IT 4. Dezember 2018, Rz 30.

7 WP29, Stellungnahme 5/2014 zu Anonymisierungstechniken, 10. April 2014, WP216, 0829/14/DE.

8 WP29, Stellungnahme 5/2014 zu Anonymisierungstechniken, 10. April 2014, WP216, 0829/14/DE, S. 28.

2.3.1. Herausgreifen

Würden wir kein Salz verwenden, könnten wir direkt mit Vornamen und Nachnamen den Hashwert berechnen. Durch das Hinzufügen muss für die Berechnung zusätzlich das Salz verwendet und auch zusammen mit den Daten abgelegt werden. Ist das Salz jedoch bekannt, ist ein Herausgreifen möglich.

2.3.2. Verknüpfbarkeit

In unseren Daten finden sich zwei Bestellungen durch *John Smith*. Wenn wir wissen, dass John Smith das erste Buch bestellt hat und niemand anderes in der Zeit ebenfalls dieses Buch bestellt hat, können wir direkt die zweite Bestellung von John Smith identifizieren. Selbst wenn wir pro Originalzeile unterschiedliche Werte für das Salz nehmen, könnte eine Identifizierung z.B. auf Grund eines wiederkehrenden Merkmales wie eines bestimmten Rabatts, eines Lieferorts oder einer Verpackungsmethode erfolgen.

Vorname	Nachname	Salz	Hashwerte
John	Smith	87683746776923452362	→ 87627648267459265308697
Lisa	Doe	98793603485743636365	→ 98796983579348569273643

Tabelle 2: Für die Identifikatoren *Vorname* und *Nachname* werden Hashwerte berechnet

2.3.3. Inferenz

Durch externe Daten könnte ein Personenbezug hergestellt werden. Liegen z.B. Abbuchungsdaten der Bank oder Lieferdaten der Post mit genauer Gewichtsangabe vor, so könnte damit identifiziert werden, welche Bücher an wen geliefert worden sind. Das wäre selbst dann möglich, wenn der Hashwert komplett entfernt worden wäre. Sofern diese externen Daten verfügbar sind oder z.B. im Rahmen eines Gerichtsbeschlusses herausgegeben werden müssen, sind diese Daten zu berücksichtigen. Aus dem gleichen Grunde sind auch die an sich nichtssagenden IP-Adressen vom EuGH als personenbezogene Daten angesehen worden.[9]

Hashwerte	Arikel	Menge	Preis	Datum
87627648267459265308697	1984 by George Orwell	1	10	3.1.2019
98796983579348569273643	Ulysses by James Joyce	1	20	7.1.2019
87627648267459265308697	Inside Wikileaks by Domscheit-Berg	1	15	9.1.2019

Tabelle 3: In der eigentlichen Tabelle werden Vorname und Nachname durch Hashwerte ersetzt

Im Ergebnis liegt das Problem der mangelnden Anonymisierung daher häufig nicht an den Hashfunktionen selbst, sondern bei den zusammen mit den Hashwerten gespeicherten Daten.

2.4. Blockchain-Beispiel

Auf Blockchains sieht das typische Szenario anders aus. Als Beispiel möchte ich die von mir realisierte Zertifizierung von Universitäts-Diplomen auf einer Blockchain betrachten: Ein Diplom wird dadurch vor Manipulation geschützt, dass ein Hashwert auf einer Blockchain abgelegt wird. Dazu wird für ein eingescanntes Dokument ein Hashwert berechnet. Auf der Blockchain wird nur dieser Hashwert abgelegt. Damit lässt sich lediglich die ungefähre Zeit der Ablage sowie die Institution, welche das Diplom abgelegt hat – also die Universität – ableiten. Wie sieht es nun mit den Kriterien aus, die die WP29 als Problemfälle aufgeführt hat:[10]

2.4.1. Herausgreifen

Ein Hashwert lässt sich darüber mit einer Person identifizieren, dass aus dem PDF des Diploms der entsprechende Hashwert berechnet wird. Dieser Hashwert findet sich dann auf der Blockchain wieder. Zu dem Hashwert findet sich jedoch dort keine direkte weitere Information. Indirekt bekommt man die Information,

[9] EuGH, Urteil vom 19. Oktober 2016, C-582/14, ECLI:EU:C:2016:779.

[10] WP29, Stellungnahme 5/2014 zu Anonymisierungstechniken, 10. April 2014, WP216, 0829/14/DE, S. 13.

wann der Hashwert dort abgelegt wurde, wie alt das Diplom mindestens ist und welche Universität es dort abgelegt hat. Das sind alles Informationen, die bereits im Diplom selbst stehen.

Ist etwas ein personenbezogenes Datum, wenn genau die Information mitgebracht werden muss, die danach aus dem Blockchain-Eintrag abgeleitet werden kann? Machen wir ein kleines Gedankenexperiment: Sie kennen Ihr Geburtsdatum. Nun schlagen Sie eine Zeitung auf und suchen die einzelnen Ziffern Ihres Geburtsdatums, aber markieren diese nicht. Stehen nun in der Zeitung Ihre personenbezogenen Daten? Erst einmal sieht es ganz danach aus. Die Ziffern sind in der Zeitung gedruckt. Genauso wie beim Hashing müssen Sie allerdings die Information erst einmal mitbringen um sie dann in der Zeitung wiederzufinden. Die Ziffern haben Ihnen daher keine zusätzliche Information übermittelt. Das Datum des Diploms kann über den Hashwert zugeordnet werden. Das Datum befindet sich jedoch bereits auf dem Diplom selbst. Dadurch erhält man also keine zusätzliche Information.

Allerdings erhält man Gewissheit, dass die Daten im Dokument nicht nachträglich manipuliert wurden. Ich würde die Gewissheit selbst nicht als eigenes personenbezogenes Datum sehen. Selbst wenn man die Gewissheit jedoch als solches ansehen würde, dürfte nach Art. 6 Abs. 1 S. 1 lit. f (DSGVO) ein berechtigtes Interesse vorliegen, dass derjenige, der eine Urkunde vorgelegt bekommt, diese auch auf ihre Echtheit überprüfen kann.

2.4.2. Verknüpfbarkeit

Eine Verknüpfbarkeit ist im Fall der Diplom-Zertifizierung zunächst nicht gegeben.

Allerdings können Diplome aberkannt werden. Dies ist etwa der Fall, wenn ein Plagiat festgestellt wurde. Dann erfolgt ein zweiter Eintrag auf der Blockchain, der mit dem ersten Eintrag verknüpft wird. Hier ist die Verknüpfungsmöglichkeit gewünscht: Alle, die das ursprüngliche Diplom präsentiert bekommen, sollen den Widerruf sehen können. Das ist natürlich eine Information, die im ursprünglichen PDF nicht erhalten war.

Im Ergebnis ist der Widerrufeintrag auf der Blockchain ein personenbezogenes Datum, dessen Verarbeitung nach Art. 6 Abs. 1 S. 1 lit. f (DSGVO) gerechtfertigt sein dürfte.

2.4.3. Inferenz

Hatten die Daten genügend Entropie, so kann aus dem Hashwert alleine nichts geschlossen werden. Selbst sein Kontext gibt keine weiteren Daten frei. Allerdings muss beachtet werden, dass nicht implizit weitere Informationen auf die Blockchain geschrieben würden. Dies wäre etwa der Fall, wenn die Hashwerte nach Noten sortiert auf die Blockchain geschrieben würden, dann würde man – mit dieser Zusatzinformation – das Ranking sehen. Zwar ist die Note in den Diplomen bereits vorhanden. Das Ranking wäre jedoch eine weitere personenbezogene Information, die ggf. über den Hashwert des Diploms auch dem Absolventen zugeordnet werden könnte. Bei sorgfältiger Handhabung können solche Inferenzen jedoch vermieden werden.

2.5. Der Ansatz der CNIL

Die CNIL unterscheidet nicht danach, welche Daten wie zugreifbar wären, sondern nur nach der verwendeten Technik.[11] Damit kommt sie zu einer Prioritätenreihenfolge der Techniken, die in der dargestellten Allgemeinheit wenig nachvollziehbar ist. So präferiert sie generell eine Verschlüsselung gegenüber der Verwendung von kryptographischen Hashwerten.[12] Auch das EU Blockchain Observatory hat festgestellt, dass eine Einzelbetrachtung der jeweiligen Anwendung erforderlich ist.[13]

---

[11] CNIL, Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data, https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf, S. 7.

[12] So hätte z.B. bei Diplomen eine verschlüsselte Ablage der Information auf der Blockchain ein höheres Risiko als die Ablage von Hashwerten.

[13] The EU Blockchain Observatory and Forum, Blockchain and the GDPR, 16. Oktober 2018, https://www.eublockchainforum.eu/reports, S. 23.

2.6. Ergebnis

Richtig eingesetzte Hashfunktionen können die vermittelte Information massiv reduzieren. Wenn es nur um einen Dokument-Zeitstempel geht, sind damit keine zusätzlichen personenbezogenen Daten verbunden. Schließt man sich dieser Argumentation nicht an oder legt gezielt weitere Informationen ab, so lässt sich damit zumindest eine zielgenaue Datenminimierung auf diejenigen Daten erreichen, für die ggf. dauerhaft Rechtfertigungsgründe vorliegen. Damit sind Hashfunktionen ein ideales Werkzeug für die Realisierung von *privacy by design*. Im Ergebnis scheint eine pauschale Annahme des Personenbezugs von gehashten personenbezogenen Daten überzogen.[14] Vielmehr muss im Einzelfall geprüft werden, ob sich jemand über den Zugriff auf die Hashwerte und ihrem Kontext personenbezogene Daten erschließen kann, und ob hierfür eine Rechtfertigung vorliegt. Besonders an dem Hashing ist dabei eine gewisse *Echofunktion*: Bestimmte Daten kann man sich nur erschließen, wenn man sie bereits hat. Solche Daten sollten wir bei der Betrachtung ausklammern.

3. Rollenverteilung

Die DSGVO teilt die Datenverarbeitung in Verantwortliche und Auftragsverarbeiter auf der einen Seite und Betroffene auf der anderen Seite auf. Während die Betroffenen geschützt werden sollen, werden die beiden ersten Gruppen mit vielerlei Pflichten wie z.B. Informations-, Lösch- und Berichtigungspflichten belastet. Dieses Modell entspricht der Datenverarbeitung in den 70er Jahren, als unvorstellbar war, dass Betroffene selbst auch Datenverarbeitungen kontrollieren könnten. Inzwischen hat sich das gewandelt und es gibt viele Situationen, in denen Betroffene selbst zu Verantwortlichen werden. Gerade bei Peer-to-Peer-Netzwerken stehen sich alle Teilnehmenden auf gleicher Ebene gegenüber und eine Aufteilung in die verschiedenen Rollen scheint problematisch. So schützt die DSGVO die Identität der Betroffenen, verpflichtet aber Verantwortliche, ihre Identität offen zu legen.

3.1. Wer ist Verantwortlicher für Transaktionen auf öffentlichen Blockchains?

Öffentliche Blockchains sind so gebaut, dass dort nur die Anwender mit ihren privaten Schlüsseln darüber entscheiden können, welche Information hinzugefügt wird. Knotenbetreiber und Miner haben – sofern sie sich nicht insgesamt absprechen – keinerlei Entscheidungsfreiheit. Daher sieht auch die französische Aufsichtsbehörde CNIL die Anwender und nicht die Miner oder Knotenbetreiber als Verantwortliche an.[15]

3.2. Was gilt für Smart Contracts?

Smart Contracts auf einer Blockchain fallen ggf. auch unter Artikel 22 DSGVO – als automatisierte Entscheidung.[16] Bei genauerer Betrachtung sind aber auch die fest in einer Blockchain programmierten Regeln der gleichen Natur. Das würde dafürsprechen, auch bei Smart Contracts die Anwender, die Transaktionen signieren und an den Smart Contract senden, als Verantwortliche einzustufen. Die CNIL irritierte hier mit der Bemerkung, dass Smart Contract Entwickler als Auftragsverarbeiter eingestuft werden könnten. Allerdings beschränkt sie dies auf den Fall, dass die Entwickler in die Verarbeitung eingreifen.[17] Smart Contracts, die dies möglich machen, bieten jedoch nicht die Garantien einer unbeeinflussbaren Verarbeitung und sind daher nicht mit den fest kodierten Regeln öffentlicher Blockchains vergleichbar. Wurde ein Smart Contract ohne Update-Möglichkeit und ohne Master-Key programmiert, so haben die Entwickler keinen Einfluss mehr auf die Verarbeitung. Damit gibt es aber außer den direkt über den Smart Contract agierenden Parteien nieman-

[14] Auch die deutsche Bundesregierung sieht Klärungsbedarf in ihrer Antwort vom 20. November 2018 auf eine kleine Anfrage der Fraktion Bündnis 90/Die Grünen, Bundestags Drucksache 19/5868, S.8.

[15] CNIL, Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data, https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf, S. 3; davor Erbguth/Fasching, ZD 2017, S. 565.

[16] Finck, Smart Contracts as a Form of Solely Automated Processing Under the GDPR, Max Planck Institute for Innovation and Competition Research Paper No. 19-01, 8. Januar 2019.

[17] CNIL, Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data, https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf, S. 3.

den mehr, der Kontrolle ausübt. Daher spricht auch hier vieles dafür, dass die Partei, die eine Transaktionen an einen Smart Contract sendet, als Verantwortliche anzusehen ist. Bei mehreren, über einen Smart Contract agierenden (Vertrags-)Parteien muss analysiert werden, ob die Parteien jeweils nur isoliert für ihre Transaktionen verantwortlich sind, ob gemeinsame Verantwortliche vorliegen oder eine Partei die alleinige Verantwortliche ist.

3.3. Welche Rolle haben Knotenbetreiber und Miner?

Knotenbetreiber und Miner erhalten Transaktionen und Blöcke und verarbeiten und verbreiten diese dann weiter. Sie haben dabei kaum Entscheidungsspielraum, insbesondere können sie keine Transaktionen fälschen. Einzelne Knotenbetreiber und Miner können auch keine Transaktionen zurückweisen. Die CNIL sieht sie daher potentiell als Auftragsverarbeiter an, zögert aber auf Grund der sich daraus ergebenden Konsequenzen.[18] Verantwortliche müssten Auftragsverarbeiter kontrollieren. Dazu müssen diese Verträge abschließen. Fraglich ist, wie das bei einer öffentlichen Blockchain realisiert werden kann. Wäre es denkbar, den Code der Blockchain als Smart Contract anzusehen, der die Auftragsverarbeiter kontrolliert und sie bei Regelverletzung automatisch von der weiteren Verarbeitung ausschließt? Da die Daten sowieso öffentlich sind, ist die einzige Sanktion, die ein Verantwortlicher gegen einen sich falsch verhaltenden Auftragsverarbeiter durchsetzen muss, sowieso nur der Ausschluss von der weiteren aktiven Teilnahme an einer Blockchain. Neuere Blockchains wie z.B. EOS gehen da noch einen Schritt weiter und verpflichten jeden Teilnehmenden mit dem Start der Software eine «Verfassung» zu akzeptieren.[19] Andere, wie z.B. Worbli, verpflichten alle Teilnehmer dazu, sich bei einem KYC-Check zu identifizieren. Allerdings sind weder EOS noch Worbli komplett öffentliche Blockchains, sondern statten Blockproducer sowie eine Foundation mit speziellen Befugnissen aus.

3.4. Pflicht der Verantwortlichen sich zu identifizieren

Die DSGVO erlegt den Verantwortlichen umfangreiche Informations-, Berichtigungs- und Löschpflichten auf (Art. 12-22). So müssen sich Verantwortliche identifizieren und Kontaktdaten nennen (Art. 13 Abs. 1 lit. a DSGVO).[20] Dies erscheint bei privaten Anwendern einer öffentlichen Blockchain nicht nur wenig praktikabel, sondern steht auch in einem gewissen Widerspruch zu ihrem Recht als Betroffene auf Privatsphäre.

3.5. Haushaltsausnahme

Art. 2 Abs. 2 lit. c schließt die Anwendung der DSGVO auf Verarbeitung durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten aus. Eine fast wortgleiche Formulierung war bereits in der Art. 3 Abs. 2 der alten EU-Datenschutzrichtlinie enthalten. Dazu urteilte der EuGH etwas weltfremd in der Lindqvist-Entscheidung, dass Veröffentlichungen im Internet, die einer unbegrenzten Zahl von Personen zugänglich sind, nicht zum Privat- und Familienleben von Einzelpersonen gehörten.[21] Erwägungsgrund 18 der DSGVO stellt aber klar, dass auch die Verwendung von sozialen Netzen sowie private Online-Aktivitäten unter diese Ausnahme fallen. Die CNIL sieht wohl daher die Öffentlichkeit der Transaktionen auf öffentlichen Blockchains nicht als Hinderungsgrund für das Vorliegen der Haushaltsausnahme an.[22]

---

18 CNIL, Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data, https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf, S. 3f.

19 Phoenix, Review # 5 (for beginners) EOS constitution 2.0 (Block.one proposal), 8. Oktober 2018, Medium, https://medium.com/trybe-network/review-5-for-beginners-eos-constitution-2-0-block-one-proposal-8d11cce7c97b.

20 Jaccard/Tharin, GDPR & Blockchain: the Swiss take, in: Jusletter IT 4. Dezember 2018, Rz 24.

21 EuGH, Urteil vom 6. November 2003, C-101/01, ECLI:EU:C:2003:596.

22 CNIL, Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data, https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf, S. 2.

3.6. Ergebnis

Das gleichberechtigte Rollenmodell öffentlicher Blockchains stellt eine Herausforderung für die DSGVO dar. Die Anwender selbst als Verantwortliche zu bezeichnen, ist ungewohnt. Doch es ist konsequent, nur die Personen als Verantwortliche (engl. Controller) zu sehen, die tatsächlich Kontrolle haben. Damit werden echte öffentliche Blockchains privilegiert. Wer bei Blockchains dagegen Kontrolle über die Teilnehmer hat (Permissioned Blockchains), wird auch mit den vollen Pflichten der DSGVO konfrontiert.

Schließlich interpretiert die CNIL die Haushaltsausnahme relativ weit. Damit können eine Reihe von Wertungswidersprüchen vermieden werden, bei denen Privatpersonen zu Verantwortlichen würden und dadurch durch die DSGVO in ihrer Privatsphäre tangiert wären.

4. Legal Tech Prototyp

Unter dem Motto *Quick Check*[23] wird ein Online-Dialog zur DSGVO-Konformität von Blockchain-Anwendungen angeboten. Da auf Grund fehlender Rechtssicherheit aktuell niemand (erst recht kein automatisiertes System) seriös eine Konformität von Blockchain-Applikationen mit der DSGVO garantieren kann, dient der Quick Check vor allem dazu, kritische Punkte zu identifizieren und technische Verbesserungsmöglichkeiten aufzuzeigen.

5. Resumé und Ausblick

Viele Rechtfertigungen zur Verarbeitung personenbezogener Daten unterliegen einer zeitlichen Begrenzung oder können widerrufen werden. Da Daten auf Blockchains nicht gelöscht werden können, wird versucht, dort keine personenbezogenen Daten abzulegen. Hashing personenbezogener Daten kann bei geeigneter Vorgehensweise den Personenbezug aufheben. Risiken liegen dabei in der Technologie selbst und in der Art ihrer Anwendung. Einen absoluten Schutz verlangt die DSGVO (Erwägungsgrund 26) nicht. An die Beurteilung des verbleibenden Risikos beim Datenschutz durch Technik im Kontext von Blockchains sollten daher keine höheren Anforderungen als an den Schutz durch organisatorische Maßnahmen gestellt werden.

Die DSGVO ist nicht technikneutral, sondern setzt das hierarchische Rollenmodell der konventionellen Datenverarbeitung voraus. Damit ergeben sich Wertungsprobleme bei öffentlichen Blockchains. Die CNIL findet dabei eine Rollenzuordnung, die dem Prinzip gerecht wird, diejenigen verantwortlich zu machen, die tatsächlich Kontrolle haben. Eine breite Interpretation der Haushaltsausnahme vermeidet zudem Wertungswidersprüche, wenn Betroffene im privaten Kontext personenbezogene Daten Dritter öffentlich verarbeiten.

Die CNIL war die erste Aufsichtsbehörde, die substantiell zu Blockchains Stellung genommen hat. Sie hat dabei vieles geklärt, aber auch noch viele Fragen offengelassen.

6. Literatur

Erbguth, Jörn/Fasching, Joachim Galileo, Wer ist Verantwortlicher einer Bitcoin-Transaktion? ZD 2017, S. 560.

Jaccard, Gabriel/Tharin, Adrien, GDPR & Blockchain: the Swiss take, in: Jusletter IT 4. Dezember 2018.

Laurence, Tiana/Muhr, Judith (Übs.), Blockchain für Dummies, WILEY – VCH Verlag GmbH & Co. KGaA, Weinheim 2018.

Laschewski, Christian, Der Blockchain-Algorithmus, WPg 2017, 359.

Phoenix, Luke, Review # 5 (for beginners) EOS constitution 2.0 (Block.one proposal), 8. Oktober 2018, Medium, https://medium.com/trybe-network/review-5-for-beginners-eos-constitution-2-0-block-one-proposal-8d11cce7c97b.

[23] Erbguth, Quick Check, https://erbguth.ch/QuickCheck.