Das Blockchain-System und die Gesetzgebung zu personenbezogenen Daten

Grigol Abashidze

I . Einführung

Blockchain ist eine der aktuellen Technologien des 21. Jahrhunderts, deren Entwicklung auf verschiedenen Ebenen lebhaft diskutiert wird. Tatsächlich gibt es kein einzelnes spezifisches Blockchain-Systemmodell. In der Praxis ist es möglich, Blockchain-Technologie mit einer nahezu unendlichen Vielfalt von Konfigurationen zu verwenden.[1]

Die Blockchain-Technologie wird bereits in verschiedenen Bereichen aktiv eingesetzt. Zum Beispiel, um medizinische Unterlagen im Gesundheitssektor zu speichern. Das deutlichste Beispiel für den Einsatz von Technologie im öffentlichen Sektor ist die Speicherung von Grundbuchdaten durch das Justizministerium von Georgien im Blockchain-System, bei Fintech-Unternehmen sind Kryptowährungen hervorzuheben.

Die aktive Nutzung der Blockchain-Technologie im Netzwerk generiert eine große Menge Informationen, was zwangsläufig Fragen zur Einhaltung des Gesetzes zum Schutz personenbezogener Daten aufwirft.

Am 25. Mai 2018 trat Die EU-Datenschutz-Grundverordnung in Kraft (im Folgenden DSGVO). Die Verordnung ersetzte gemäß ihres § 94 Abs.1 die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr und ist für alle EU-Mitgliedstaaten verbindlich.

Daher ist es interessant, die Kompatibilität der Blockchain-Technologie mit personenbezogenen Daten im Rahmen der DSGVO zu untersuchen[2].

II. Allgemeine technologische Beschreibung der Blockchain

Eine detaillierte Beschreibung der Blockchain-Technologie und ihrer vollständigen technischen Spezifikationen geht über den Rahmen dieses Aufsatzes hinaus. Da das Thema des Schutzes personenbezogener Daten eng mit dem Betrieb der Blockchain-Technologie verbunden ist, kann man aber einzelne technische Aspekte der Technologie, die eng mit personenbezogenen Daten zusammenhängen, nicht außer Acht lassen.

1. Interaktion zwischen Blockchain und Nutzer

Wenn eine Person einen Computer dazu verwendet, eine Verbindung zum Internet herzustellen, wird die Verbindung nicht mit ihrem richtigen Vor- und Nachnamen hergestellt, sondern der Benutzer tritt nur in Form seiner eigenen IP-Adresse in Erscheinung, die durch das Netzwerk identifiziert wird.

Ein ähnliches Prinzip wird für die Interaktion mit dem Benutzer und dem Blockchain-System verwendet, diesmal wird jedoch zusätzlich der „öffentliche Schlüssel“ (lange, zufällig ausgewählte Zahlen und eine Anzahl lateinischer Buchstaben) verwendet, der als Adresse des Benutzers in der Blockchain fungiert. Der öffentliche Schlüssel kann nur durch einen priva-

[1] *W. Maxwell/J. Salmon*, Ein Leitfaden zu Blockchain und Datenschutz, 16, https://www.hlengage.com/_uploads/downloads/5425GuidetoblockchainV9FORWEB.pdf (Datum der letzten Verwendung aller in diesem Artikel angegebenen Links ist der 16.1.2020).

[2] Zur Beziehung zwischen Blockchain-Technologie und GDPR siehe Forschung – EPRS, Europäischer Parlamentarischer Forschungsdienst , Blockchain und die Allgemeine Datenschutzverordnung, Juli 2019, https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_DE.pdf.

ten Schlüssel verwendet werden, der nur dem Benutzer bekannt ist und auf die gleiche Weise wie eine elektronische Signatur eingesetzt wird, d.h. sein Zweck ist die Validierung bzw. Bestätigung von Online-Transaktionen im Blockchain-System.[3]

Der persönliche Schlüssel wird durch geschützte, zufällige mathematische Funktionen generiert, was eine Rekonstruktion oder Wiederherstellung nahezu unmöglich macht. Wenn ein Benutzer seinen persönlichen Schlüssel verliert oder er ihm gestohlen wird, gelten seine Daten als verloren und er kann nicht auf die Daten zugreifen.[4]

2. Knoten

Jeder mit dem Blockchain-Netzwerk verbundene Computer erhält eine Kopie der Blockchain, die Informationen zu verschiedenen Handelsvorgängen beinhaltet.

Der mit dem Blockchain-Netzwerk verbundene Computer, der den mathematischen Algorithmus öffnet und somit den Betrieb des Netzwerks sicherstellt, ist ein Node[5].

Ein Node tritt aus freien Stücken dem Netzwerk bei, wodurch letztendlich ein dezentrales Netzwerk entsteht.

Die Anzahl der mit einer geschlossenen Blockchain verbundenen Noden ist begrenzt und jeder Node ist eindeutig identifiziert. Die Anzahl der an einer öffentlichen Blockchain beteiligten Noden dagegen ist unbegrenzt, und jede Entität kann dem öffentlichen Blockchain-Netzwerk beitreten.

3. Dezentralisierung

Entsprechend der Struktur ist das Hauptmerkmal der Blockchain-Technologie die dezentrale Struktur.

Jede Aktion (Transaktion), die in der Blockchain stattfindet, wirkt sich auf das gesamte Netzwerk aus. Daher ist ein Konsens der Netzwerkteilnehmer, der Nodes, erforderlich, um eine Entscheidung zu treffen. Je mehr Nodes am Netzwerk beteiligt sind, desto sicherer ist die jeweilige Blockchain, da es technisch schwieriger wird, eine falsche Entscheidung zu treffen oder einen Hackerangriff auf ein Netzwerk durchzuführen.

III. Blockchain-Technologie und persönliche Daten

Die Verwendung einer öffentlichen Blockchain wie der Bitcoin-Blockchain verstößt gegen das Gesetz zum Schutz personenbezogener Daten: Alle Transaktionen - auch wenn sie verschlüsselt sind - sind immer sichtbar.[6] Blockchain basiert auf einer verteilten webbasierten Datenbank-Technologie (Distributed-Ledger-Technologie), die in erster Linie dadurch gekennzeichnet ist, dass eingegebene Informationen nicht abgerufen werden können. Schließlich validiert ein Konsensmechanismus die neuen Einträge unwiderruflich.

Vor diesem Hintergrund müssen wir uns angesichts der Blockchain-Technologie auf zwei wichtige Funktionen konzentrieren[7]:

Nachträgliche Unveränderlichkeit der Daten (immutability) und die unwiderlegbare Vermutung der Richtigkeit der Daten (irrefutability).

Beide oben genannten Blockchain-Funktionen, die separat betrachtet werden, sind äußerst problematisch, da sie in direktem Konflikt mit der DSGVO stehen, wie beispielsweise dem Recht zum Bearbeiten (Löschen).

Die betroffene Person hat nach der DSGVO das Recht, über ihre eigenen personenbezogenen Daten nach eigenem Willen zu verfügen. Unweigerlich muss man auch an das durch den Europäischen Gerichtshof (EuGH) statuierte Recht auf „Vergessenwerden“ den-

[3] *B. Maurenbrecher/U. Meier* , Insolvenzrechtlicher Schutz der nützlichen Virtuellen Währungen, Jusletter, 4.12.2017, 3.

[4] Siehe öffentliche und private Schlüssel. Details *Dylan Yaga, Peter Mell, Nik Roby, Karen Scarfone,* Überblick über die Blockchain-Technologie, NISTIR 8202, Oktober 2018, US-Handelsministerium, Nationales Institut für Standards und Technologie; https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf.

[5] Ausführliche Informationen zu Nodes unter https://medium.com/coinmonks/blockchain-what-is-a-node-or-masternode-and-what-does-it-do-4d9a4200938f.

[6] *Fasching*, Anwendungsbereiche und Rechtsfragen der Blockchain-Technologie, Wien 2017, 9, http://www.it-law.at/publikation/anwendungsbereiche-und-ausgewaehlte-rechtsfralogen-der-blockin; *Nakamoto*, Bitcoin: Ein elektronisches Peer-to-Peer-Geldsystem, 6, https://bitcoin.org/bitcoin.pdf.

[7] *Rainer Böhme/Paulina Pesch*, Technische Grundlagen und datenschutzrechtliche Fragen der Blockchain-Technologie, in: Datenschutz und Datensicherheit 2017, 473.

ken, das in Art. 17 DSGVO[8] als weitreichendes Löschungsrecht kodifiziert wurde. Die datenschutzrechtlichen Betroffenenrechte sind ebenso unverjährbar und unverzichtbar.

Angesichts der Tatsache, dass die in die Blockchain geladenen Informationen unbegrenzt gespeichert sind und nicht geändert werden können, ist auf den ersten Blick klar, dass diese Merkmale die Blockchain-Technologie mit der Gesetzgebung zu personenbezogenen Daten unvereinbar machen.

IV. Gesetzliche Regelung des Schutzes der personenbezogenen Daten im Blockchain-System

Nach einer ziemlich verbreiteten Meinung[9] ist die Unvereinbarkeit des Blockchain-Systems mit der Gesetzgebung zu personenbezogenen Daten kein problematisches Thema.

Obwohl die in der Blockchain enthaltenen Informationen öffentlich verfügbar sind, ist es nicht möglich, vorhandene Informationen mit einer bestimmten Person zu verknüpfen, was deren Identifizierung sofort ausschließt.

Ein Zweck der Bitcoin-Blockchain besteht beispielsweise darin, Zahlungsvorgänge zu anonymisieren[10]. Die Anonymität der an der Transaktion beteiligten Partei wird von dieser Partei und dem dezentralen Netzwerk garantiert[11]. Aufgrund der Anonymität ist es unmöglich, Informationen mit einer identifizierten oder identifizierbaren Person zu verknüpfen, was an sich die Qualifizierung der oben genannten Daten als personenbezogene Daten ausschließt. Nach dieser Auffassung kann davon ausgegangen werden, dass die Blockchain-Technologie trotz ihrer uneingeschränkten Publizität nicht gegen die gesetzlichen Normen für personenbezogene Daten verstößt.

1. Personenbezug

Gemäß Art. 4 DSGVO sind personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Jede Information enthält eine Reihe von Informationen, die auf irgendeine Weise auf eine bestimmte Person hinweisen. In der juristischen Literatur gibt es zwei Theorien zur Bestimmung des Zusammenhangs zwischen Informationen und der Identifizierung einer natürlichen Person:

Nach der absoluten/objektiven Theorie genügte die hypothetische Möglichkeit, dass eine beliebige Stelle die hinter einer einzelnen Angabe stehende Person mit verhältnismäßigen Mitteln identifizieren könnte.[12] Demnach wären alle Absender- und Empfängeradressen personenbezogen, denn zumindest der Inhaber kennt seine Identität.

Diese Theorie berücksichtigt nicht, ob es einem Dritten technisch möglich ist, die Person zu identifizieren. Angesichts der Tatsache, dass beispielsweise Kryptowährungsanbieter-Unternehmen oder Krypto-Börsen zusätzliche Informationen über die an der Blockchain beteiligten Entitäten haben, können wir zu dem Schluss kommen, dass die Adresse jedes Absenders und Empfängers einer in der Blockchain angegebenen Transaktion personenbezogene Daten sind.

Nach der relativen/subjektiven Theorie ist danach zu fragen, ob es der konkreten speichernden Stelle ohne weiteres möglich ist, Daten einer Person zuzuordnen.[13]

---

[8] EuGH, Urt. v. 13.5.2014, C 131/12; http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=de&mode=lst&mir=&occ=first&part=1&cid=475998.

[9] *Francesco Rampone*, Ciberspazio e diritto, vol. 19, n. 61 (3 - 2018), pp. 457-20; https://poseidon01.ssrn.com/delivery.php?ID=310013021027066030080095031005119123059041038044021064118028087030123015002096030104053039042027114097000125127070086097101074019061023049001005067105092118013097104038043001072125029108091003116022006124001115085086007123101012111030110117086115074115&EXT=pdf .

[10] *Alexander Schmid*, Bitcoin – eine Einführung in die Funktionsweise sowie eine Auslegeordnung und erste Analyse möglicher rechtlicher Fragestellungen, in: Jusletter 4.6.2012, Rz 9.

[11] Satoshi Nakamoto: "Privacy can still be maintained by breaking the flow of information in another place:
by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone." Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 6; https://bitcoin.org/bitcoin.pdf

[12] *Pahlen-Brandt, I. Datenschutz braucht scharfe Instrumente Beitrag zur Diskussion um „personenbezogene Daten". Datenschutz und Datensicherheit (DuD) 2008, 34; https://doi.org/10.1007/s11623-008-0009-8*.

[13] *Gola/Schomerus*, BDSG, 12. Aufl. 2015, § 3 Rn.10.

Der EuGH[14] hat diese Frage in Bezug auf die Verarbeitung von dynamischen IP-Adressen als personenbezogene Daten entschieden, wonach IP-Adressen jedenfalls dann personenbezogene Daten seien, wenn die verantwortliche Stelle über rechtliche Mittel verfügt, mit denen die betreffende Person anhand von Zusatzinformationen bestimmt werden kann. Mit diesen Ausführungen schloss sich der EuGH im Ergebnis der Theorie vom relativen Personenbezug an.

Auf den ersten Blick werden personenbezogene Daten wie Vor- und Nachname oder Wohnadresse in öffentlichen Blockchain-Transaktionen nicht gefunden.

Versender und Empfänger in einem dezentralen Netzwerk müssen ihre Identität nicht offenlegen. Vor diesem Hintergrund gibt uns die öffentliche Adresse der Blockchain auf den ersten Blick keinen direkten Aufschluss über die Person, die dahintersteht.

Die Anonymität von Transaktionen in einer Blockchain ist in der Tat nur eine Meinung, die auf Annahmen basiert. Der an der Transaktion teilnehmende Benutzer verwendet einen kryptografischen öffentlichen Schlüssel, der ein Pseudonym ist.[15]

Von der Cornell University Research[16] wurde es nachgewiesen, dass es möglich ist, Bitcoin-Adressen von Zahlungsauslösern und Zahlungsempfängern mit der IP Adresse zu verknüpfen, von welcher die Transaktion ausgelöst wurde. Soweit der öffentliche Schlüssel nicht laufend geändert wird, lassen sich auch Transaktionshistorien zurückverfolgen und auf diese Weise Profile erstellen und die IP-Adressen der Transaktionsentitäten bestimmen.

Folgt man der Rechtsprechung des Bundesgerichthofs und des EuGH zum Personenbezug von IP-Adressen[17], können wir, wenn das Subjekt die IP-Adresse des Transaktionsausführers kennt und zusätzliche Informationen von der Person hinter der IP-Adresse erhalten hat, die zur Identifikation ausreichend sind, sicher schließen, dass es sich bei den Transaktionen in der Blockchain um personenbezogene Daten handelt.

In der Praxis ist zu beachten, dass das Blockchain-System eine große Anzahl von Drittenanbietern enthält, z. B. Krypto-Börsen und Kryptowährungsanbieter, die rechtmäßig über persönliche Informationen zu ihren Begünstigten verfügen.

Daher ist die Folgerung ratsam, dass das Blockchain-System in den Geltungsbereich der DSGVO fällt, da es sich um Informationen handelt, die sich auf eine identifizierte oder identifizierbare Person beziehen. Es wäre daher verfehlt, im Blockchain-Kontext pauschal von Anonymität zu sprechen.

2. Verantwortliche Person

a) Verarbeitungsstelle füt personenbezogene Daten

aa) Schweiz

Da das schweizerische Gesetz zum Schutz personenbezogener Daten (im Folgenden als DSG bezeichnet) die Frage der Datenverarbeitung anders regelt als die DSGVO, ist es interessant, den Schwerpunkt auf die schweizerische Gesetzgebung zu legen. Nach den Vorschriften des DSG muss jeder Bearbeiter sich an die Bearbeitungsgrundsätze gemäß Art. 4 DSG halten, sich über die Richtigkeit der Personendaten vergewissern (Art. 5 DSG) und für eine ausreichende Datensicherheit sorgen (Art. 7 DSG). Eine Bündelung dieser Pflichten bei einer einzigen oder mehreren verantwortlichen Stellen sah der schweizerische Gesetzgeber nicht vor[18]. Auf dieser Grundlage können wir den Schluss ziehen, dass nach schweizerischem Recht alle am Blockchain-System beteiligten Unternehmen als Informationsverarbeiter betrachtet werden können und die im DSG festgelegten Verantwortlichkeiten und Pflichten auf diese ausgedehnt werden können.

Diese Bestimmung beschreibt einen relativ großen Kreis von Personen, die zur Erfüllung solche Garantien verpflichtet sind und für die Nichterfüllung dieser

[14] EuGH, Urt. v. 19.10.2016, C 2016/779

[15] *Rainer Böhme/Paulina Pesch,* Technische Grundlagen und datenschutzrechtliche Fragen der Blockchain-Technologie, in: Datenschutz und Datensicherheit 2017, 478.

[16] *Alex Biryukov/Dmitry Khovratovich/Ivan Pustogarov*, Deanonymisation of Clients in Bitcoin P2P Network, 5.7.2014, https://arxiv.org/abs/1405.7418.

[17] EuGH, Urt. v. 19.10.2016, C 2016/779

[18] *David Rosenthal/Yvonne Jöhri* (Hrsg.), Handkommentar zum Datenschutzgesetz, 2008, Art. 3 Bst. j DSG, N 116.

Verpflichtungen verantwortlich sind, deren Umsetzung im Blockchain-System praktisch unmöglich ist.

bb) DSGVO

Im Gegensatz zum schweizerischen Recht berücksichtigt die DSGVO nicht alle Subjekte bei der Verarbeitung von Daten und legt nicht allen die gleichen Verpflichtungen auf. Vielmehr kann man 4 wichtige Subjekte unterscheiden:

- betroffene Person - identifizierte oder identifizierbare natürliche Person;
- Verantwortlicher - 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; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann das Unionsrecht oder das Recht der Mitgliedstaaten regeln, wer der Verantwortliche ist oder wie er bestimmt wird;
- Auftragsverarbeiter - eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;
- Dritte - eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten.

Diese Liste basiert auf der Idee, dass Datenverarbeitung immer in einer hierarchischen Reihenfolge erfolgt. Der Verantwortliche bestimmt selbst den Zweck und die Mittel der Datenverarbeitung. Er führt sie dann entweder selbst durch oder delegiert sie an einen Auftragsverarbeiter. Deswegen liegt die Haftung für die Verarbeitung entweder allein beim Verantwortlichen (wenn er selbst die Verarbeitung durchführt) oder beim Auftragsverarbeiter[19]. Anders als beim schweizerischen Gesetz gibt es eine Differenzierung der Verantwortlichkeiten, so dass die befugte Person und den Verantwortlichen nicht die gleichen Pflichten und Zuständigkeiten treffen.

Artikel 26 der DSGVO sieht eine kollektive Verantwortung vor, d.h. mehrere Unternehmen können gemeinsam die Verpflichtung und Verantwortung zur Datenverarbeitung übernehmen. Dieser Artikel zielt darauf ab, die tatsächlichen Umstände zu regeln, unter denen die Verarbeiter verschiedener Informationen eine organisierte Entscheidung treffen, Informationen gemeinsam zu verarbeiten, um ein gemeinsames Ziel zu erreichen. Die Regelung will die Akteure komplexer Interaktionssysteme, in denen mehrere Personen in intransparenter Weise zusammenwirken, in das System der organisierten und kontrollierten Verantwortung mit klar definierten Kompetenzen einordnen[20].

Dieser Regulierungsansatz versagt bei der öffentlichen Blockchain von Vornherein[21]. Personen, die an der öffentlichen Blockchain teilnehmen, verarbeiten Daten nicht gemeinsam, um illegale Ergebnisse zu erzielen. Ihr Ziel ist es, die Transaktionen zu bestätigen und das ordnungsgemäße Funktionieren des Blockchain-Systems sicherzustellen, was den Zielen von Art. 6 der DSGVO nicht widerspricht.

b) Bestimmung der Verantwortlichen Stelle in der Blockchain

In einem Blockchain-System, bei dem es sich um eine Art kollaboratives System handelt, ist es sehr schwierig, den Auftragsverarbeiter oder die verantwortliche Person zu identifizieren.

Der Grund dafür ist, dass die Technologie, insbesondere die Aufzeichnung und Verarbeitung der in der Blockchain enthaltenen Daten, auf dem Prinzip der Dezentralisierung basiert.

Unter potentiell verantwortlichen Personen kann man die Person verstehen, die die Blockchain programmiert hat, aber ebenso auch die Person, die die Blockchain zum ersten Mal im Netzwerk implemen-

[19] Zur Definition siehe https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf.

[20] *Jürgen Kühling/Benedikt Buchner* (Hrsg.), DS-GVO Kommentar, 2017, Art. 26, N 10.

[21] *Rainer Böhme/Paulina Pesch*, Technische Grundlagen und datenschutzrechtliche Fragen der Blockchain-Technologie, in: Datenschutz und Datensicherheit 2017, 479.

tiert hat oder jede Person, die an einem Blockchain-System teilnimmt und Transaktionen ausführt und/oder bestätigt.

In der Literatur werden verschiedene Möglichkeiten diskutiert, dieses Problem zu lösen. *Fasching*[22] ordnet die Rolle der Verantwortlichen bei der Blockchain der Gruppe von Entwicklern zu, die laufend Änderungen testen und implementieren. Leider lässt dieser Ansatz sich allerdings nicht mit dem Regelungskonzept der DSGVO vereinbaren. Der sachliche Anwendungsbereich der DSGVO ist auf Datenverarbeitungen beschränkt. Dementsprechend können Personen, die die Daten nicht verarbeiten, nach der DSGVO nicht für die Datenverarbeitung verantwortlich sein.

System- und Programmentwickler, in diesem Fall die Entwickler des Blockchain-Systems, sind keine Datenverarbeiter[23]. Der Entwickler des Blockchain-Systems ist selbst kein Benutzer dieses Systems. Er beteiligt sich auch nicht mit einem Zustimmungsvorbehalt am Konsensmechanismus und hat daher keine Möglichkeit, Zwecke und Mittel der Datenverarbeitungen auf einer öffentlichen Blockchain festzulegen.

Nach einer weit verbreiteten Meinung[24] sind die Entscheidungsträger (Miners, Nodes) die Personen, die für die Verarbeitung personenbezogener Daten verantwortlich sind. Wenn wir dieser Ansicht folgen, sind die Nodes verpflichtet, die Erfüllung aller Verpflichtungen sicherzustellen, die die Gesetzgebung dem Datenverarbeiter auferlegt. In diesem Fall wäre es angebracht, öffentliche und private Blockchains getrennt zu betrachten. Wenn der Miner (Node) in einer geschlossenen Blockchain angewiesen wird, um bestimmte Informationen zu ändern, ist es ihm theoretisch und technisch möglich, diese Informationen zu ändern. Im Gegensatz zu einer öffentlichen Blockchain besteht eine private Blockchain nur aus identifizierten Personen mit einer begrenzten Anzahl von Teilnehmern und es besteht die Möglichkeit, dass sie einer Änderung der Informationen zugestimmt haben. In Bezug auf die öffentliche Blockchain steht man zusätzlich zu den tatsächlichen Schwierigkeiten, wie der Identifizierung jedes Miners (Knotens), vor einem weiteren bedeutenden Problem: Wenn der Gesetzgeber die in seiner Zuständigkeit befindlichen Miners verpflichtet, eine Änderung der spezifischen personenbezogenen Daten sicherzustellen, wird es diesen Minern technisch unmöglich sein, diese spezifische Verpflichtung allein zu erfüllen[25].

Die ungarische Datenschutzaufsichtsbehörde zur Anwendbarkeit der DSGVO auf die Blockchain hat sich dazu bekannt, jeden teilnehmenden Datenempfänger als Verantwortlichen zu qualifizieren.[26] Diese Ansicht zieht den Kreis der Verantwortlichen noch weiter als die vorangehende Theorie und ist daher mit gleicher Begründung abzulehnen.

Die öffentliche Blockchain basiert, wie bereits erwähnt, vollständig auf der Idee der Dezentralisierung. Folglich handelt es sich um ein verteiltes System, das keine einzige zentrale Steuerungseinheit hat. Daher ist es nach der derzeitigen DSGVO technisch unmöglich, Datenverarbeiter zu identifizieren und ihnen bestimmte Verpflichtungen oder Verantwortlichkeiten aufzuerlegen.

3. Rechte der betroffenen Person

Das oben erwähnte Merkmal des Blockchain-Systems, das die Unveränderlichkeit der darin enthaltenen Daten sicherstellt, steht in direktem Widerspruch zu den Bestimmungen der DSGVO, insbesondere den Rechten der betroffenen Person auf Auskunft (15. GDPR), Widerspruch (21 DSGVO), Löschung (17 I DSGVO), das Recht auf Vergessenwerden[27] (17 II DSGVO), das Recht auf Korrektur (16 DSGVO) und auf

[22] *Joachim Galileo Fasching*, Anwendungsbereiche und ausgewählte Rechtsfragen der Blockchain-Technologie, 2017, 9, abrufbar unter http://www.it-law.at/publikation/anwendungsbereiche-und-ausgewaehlterechtsfragen-der-blockchain-technologie.

[23] *Jürgen Hartung, in: Jürgen Kühling/Benedikt Buchner* (Hrsg.), DS-GVO Kommentar, 2017, Art. 24 Rn.12.

[24] *Jacek Czarnecki*, Blockchains and Personal Data Protection Regulations Explained, in: Coindesk, 26.4.2017, https://www.coindesk.com/blockchains-personal-data-protection-regulations-explained/.

[25] *Rainer Böhme/Paulina Pesch*, Technische Grundlagen und datenschutzrechtliche Fragen der Blockchain-Technologie, in: Datenschutz und Datensicherheit 2017, 478.

[26] *Dóra Petrányi/Marton Domokos*, Hungary: Data Protection Aspects of Blockchain, 17.8.2017, http://www.cms-lawnow.com/ealerts/2017/08/hungary-data-protection-aspects-of-blockchain.

[27] Weitere Informationen unter *Kubis,* Das „Recht auf Vergessenwerden", DuD 9/2017, 583.

Einschränkung der Verarbeitung/Sperrung (18 DSGVO).

Es ist daher notwendig, zu klären, ob einer Person, die am Blockchain-System teilnimmt, die ihr von der DSGVO gewährten Rechte gewährt werden, ob diese Rechte in einem System ausgeübt werden können, das Änderungen der darin enthaltenen Daten ausschließt und diese Daten auf unbestimmte Zeit öffentlich gespeichert werden.

a) Anspruch auf Berichtigung oder Korrektur personenbezogener Daten

Ein Anspruch auf Berichtigung oder Korrektur der erhobenen Daten ist im Hinblick auf die Unveränderbarkeit mit einer Blockchain nicht vereinbar.

Aus praktischer Sicht ist eine Änderung des Blockchain-Systems nur durch die Implementierung des sogenannten 51%-Angriffs (51% Attack) möglich[28]. Das Blockchain-System soll demnach tatsächliche Transaktionen initiieren, die von 51 Prozent der Teilnehmer am System vereinbart werden, und dann werden die Informationen im Block generiert.

In der Praxis ist es theoretisch möglich, dies in einer privaten Blockchain umzusetzen, da die daran beteiligten Personen identifiziert werden und es ihnen theoretisch möglich ist, die entsprechende Änderung durchzuführen.

Was die öffentliche Blockchain betrifft, so sind in verschiedenen Gerichtsbarkeiten eine ziemlich große Anzahl von Nodes vorhanden, weswegen es unmöglich wird, eine solche fiktive Transaktion durchzuführen. Dementsprechend hat die betroffene Person keine Möglichkeit, nach Art. 21 DSGVO eine Änderung der personenbezogenen Daten zu beantragen.

b) Recht auf Löschung

Ebenso, wie das Recht auf Korrektur, hat die betroffene Person keine Möglichkeit das Recht zum Löschen von Daten im Blockchain-System zu nutzen. In Übereinstimmung mit den Anforderungen der DSGVO müssen personenbezogene Daten so lange gespeichert werden, wie es erforderlich ist, um den Zweck der Datenverarbeitung zu erreichen[29]. Sobald der Informationsprozessor das Ziel erreicht hat, für das die Daten verarbeitet werden, müssen sie gelöscht werden[30].

Das Blockieren oder Ändern von Daten kann als eine Möglichkeit zur Lösung dieses Problems angesehen werden, die es unmöglich macht, Informationen ohne unverhältnismäßig großen Aufwand und Kosten zu erhalten.

Wenn wir einen der Hauptvorteile der Blockchain betrachten, der in ihrer Publizität und der Zuverlässigkeit des Systems liegt, ist es leicht zu erkennen, dass das Blockieren der darin enthaltenen Informationen in direktem Konflikt mit der Funktionalität der Blockchain steht. Darüber hinaus verursacht das Blockieren von Daten in der Blockchain viele technische Probleme, weshalb der Schluss gezogen werden kann, dass das Blockieren personenbezogener Daten nicht als ein Weg zur Lösung dieses Problems angesehen werden kann.

c) Recht auf Vergessenwerden

Gemäß Art. 17 II DSGVO hat derjenige, der zur Löschung der Daten verpflichtet ist, unter Berücksichtigung der verfügbaren Technologie und Implementierungskosten angemessene Maßnahmen zu ergreifen, um die datenverarbeitenden Stellen darüber zu informieren, dass eine betroffene Person die Löschung personenbezogener Daten verlangt hat, wenn er zuvor die zu löschenden Daten öffentlich gemacht hatte. Öffentlichmachen ist die Ermöglichung des Zugriffs durch einen unbestimmten Personenkreis, das heißt es müssten personenbezogene Daten aktiv für die Allgemeinheit zugänglich gemacht worden sein[31].

Da wir in einer öffentlichen Blockchain einem unbestimmten Kreis von Personen gegenüberstehen, die Zugang zu personenbezogenen Daten haben, kann eine betroffene Person einen Antrag auf der Grundlage von Artikel 17 II der DSGVO stellen. Leider kann eine solche Anforderung der betroffenen Person aus den oben genannten technischen Gründen

[28] Weitere Informationen über 51% der Angriffe unter https://blog.goodaudience.com/what-is-a-51-attack-or-double-spend-attack-aa108db63474.

[29] Artikel 5 der DSGVO "Grundsätze der Datenverarbeitung".

[30] Weiter *Hofert,* Zeitschrift für Datenschutz (ZD) 2017, 61.

[31] Gola DS-GVO/*Nolte/Werkmeister*, 2. Aufl. 2018, DS-GVO Art. 17 Rn. 34.

und der Besonderheiten der Blockchain-Technologie nicht in die Praxis umgesetzt werden.

V. Fazit

Die Blockchain-Technologie steht in vielerlei Hinsicht im Widerspruch zur Datenschutzgesetzgebung. Obwohl die Daten in der öffentlichen Blockchain auf den ersten Blick verschlüsselt sind, können diese Informationen dennoch mit einer identifizierten oder identifizierbaren Person verknüpft werden. Folglich können solche Daten als personenbezogene Daten qualifiziert werden.

Gleichzeitig stellt die dezentrale Architektur der öffentlichen Blockchain ein recht großes Problem für den Schutz personenbezogener Daten dar. Die wichtigste Erkenntnis aus der vorstehenden Analyse ist, dass sich bei einer auf unzählige Nodes verteilten Datenbank keine für die Datenbearbeitung verantwortliche Person finden lässt.

Trotz aller Kritik oder aller Vermutungen sollten wir nicht vergessen, dass die Blockchain-Technologie viele positive Eigenschaften aufweist, einschließlich des Schutzes personenbezogener Daten. Mit der Einführung der erforderlichen Vorschriften durch den Gesetzgeber kann die Blockchain-Technologie möglicherweise den Datenschutz verbessern.