JÖRN ERBGUTH / JOACHIM GALILEO FASCHING

Wer ist Verantwortlicher einer Bitcoin-Transaktion?

Anwendbarkeit der DS-GVO auf die Bitcoin-Blockchain

Personenbezug
Geldwäsche
Handelsplattformen
Kontrollmöglichkeit

■ Eine Betrachtung der Abläufe und Analysemöglichkeiten der Bitcoin-Blockchain ergibt eine Personenbeziehbarkeit vieler dort abgelegter Transaktionen. Bei der Bestimmung des datenschutzrechtlich Verantwortlichen wird zwischen den über einen Bitcoin-Handelsplatz oder einen Bitcoin-Geldbörsen-Dienst vorgenommenen Transaktionen auf der einen Seite und den direkt durch den Nutzer durchgeführten Transaktionen auf der anderen Seite unterschieden. Im ersten Fall haben die beauftragten Dienstleister die Kontrolle und sind daher als Verantwortliche zu betrachten. Im zweiten Fall dagegen sorgt das technische Konstrukt der Blockchain dafür, dass nur der die Transaktion vornehmende Nutzer Zweck und Mittel der Datenverarbeitung bestimmen kann und als Verantwortlicher angesehen wird. In der Konsequenz wird damit eine Regulierungslücke in Kauf genommen, um Systeme nicht zu verbieten, die direkte, Peer-to-Peer vorgenommene Transaktionen ermöglichen. Das Ergebnis harmoniert mit dem Vorschlag zur 5. Geldwäsche-RL der EU, welche ebenfalls nur die Bitcoin-Handelsplätze und Bitcoin-Geldbörsen-Dienstleister als Gatekeeper reguliert.

■ An observation of the processes and possibilities for analysis of the Bitcoin blockchain provides a possibility for personal reference of many concluded transactions. In determining the data protection law person responsible, a differentiation is made between transactions that occurred on the Bitcoin trading venue or a Bitcoin wallet service on the one hand and the transactions undertaken directly by the user on the other hand. In the first case, the instructed service providers have control and thus are to be seen as being responsible. In the second case, in turn, the technical construct of the blockchain leads to the fact that only the user undertaking the transaction can determine the purpose and means of data processing and is considered to be responsible. As a consequence, a regulatory gap is accepted in order to not prohibit systems which enable direct transactions undertaken on a peer-to-peer level. The result is in harmony with the proposal regarding the 5th Money Laundering Directive of the EU, which also merely regulates the Bitcoin trading venues and the Bitcoin wallet service providers as gate keepers.
Lesedauer: 24 Minuten

I. Einleitung

Bitcoin bietet eine Menge interessanter juristischer und insbesondere datenschutzrechtlicher Fragestellungen. Häufig stand etwa die Frage der Rechtsnatur von Bitcoins oder der Frage des Vertragstyps beim Eintauschen von oder „Bezahlen" mit Bitcoins im Fokus.[1] In diesem Aufsatz gehen wir auf zwei zentrale datenschutzrechtliche Fragen zu Bitcoin ein: Liegen auf der Bitcoin-Blockchain personenbezogene Daten i.S.v. Art. 4 Nr. 1 DS-GVO und wer ist Verantwortlicher i.S.v. Art. 4 Nr. 7 DS-GVO? Für die Beantwortung dieser beiden Fragen sind technische Grundlagen – wie etwa bei *Böhme/Pesch*[2] diskutiert – unabdingbar. Daher wird im Beitrag gelegentlich auch auf technische Details und die Funktionsweise des Bitcoin-Netzwerks eingegangen.

II. Bitcoin – eine dezentrale virtuelle Währung

Bitcoin basiert auf der Blockchain-Technologie – oder auch Distributed Ledger-Technologie genannt. Bitcoin kennt keine Zentralbank, keinen Herausgeber oder Kontrolleur. Das Vertrauen basiert auf den offen gelegten Algorithmen[3] und nicht auf Vertrauen in die Personen, die die Blockchain betreiben.

1. Die Bitcoin-Mineure

Jeder Bitcoin-Knoten kontrolliert alle Transaktionen. Damit ist sichergestellt, dass ungültige Transaktionen nicht aufgenommen werden. Allerdings ist bei einer digitalen Währung genauso wichtig, dass ein Betrag nicht zweimal ausgegeben werden kann. Würden einige Knoten einige Transaktionen weglassen oder auch nur die Reihenfolge ändern, so hätte das dramatische Konsequenzen. Ein Betrag könnte in einem Teil des Netzes an A und im anderen Teil an B transferiert werden. Mit der Blockchain-Technologie wird jedoch garantiert, dass eine Transaktion – einmal aufgenommen – nach relativ kurzer Zeit sicher auf allen Knoten der Blockchain enthalten ist und nicht wieder entfernt werden kann. Dies wird bei Bitcoin dadurch erreicht, dass zum korrekten Fortschreiben der Blockchain eine hohe Rechenleistung erforderlich ist und die Regel eingeführt wurde, dass stets die längere Kette bevorzugt wird. Wer daher auf der Bitcoin-Blockchain eine Transaktion entfernen und diese so modifizierte Blockchain dann im Netzwerk durchsetzen wollte, müsste die echte Blockchain „überholen" und bräuchte dazu mehr Rechnerleistung als alle anderen Blockchain-Mineure zusammen.

Ein Bitcoin-Mineur kann zwar auswählen, welche Transaktionen er in einen neuen Block aufnimmt. Will er aber bestimmte Transaktionen boykottieren, so können sie von anderen Mineuren in darauffolgenden Blöcken dennoch aufgenommen werden. Selbst wenn viele Mineure bestimmte Transaktionen boykottieren würden, würde daher eine kleine Anzahl an Boykottbrechern ausreichen, um diese Transaktionen dennoch aufzunehmen. Selbst wenn zusätzlich noch die Blöcke der Boykottbrecher boykottiert würden, so müssten die Boykotteure doch mindestens die halbe Rechenleistung aller Mineure auf sich vereinen, um erfolgreich zu sein. Wenn Gruppen von Mineuren ihre Blöcke gegenseitig nicht mehr anerkennen, so kommt es zu einem sog. „Hard Fork". Dabei spaltet sich eine Blockchain und wird unabhängig in zwei Versionen weitergeführt.[4]

2. Wie erhält man Bitcoins?

Einen Bitcoin-Account erstellt man sich durch die Generierung eines Schlüsselpaars aus einem privatem und einem öffentlichen Schlüssel. Um auf diesem Account Bitcoins zu bekommen, gibt es vier Möglichkeiten:

- Es gibt Tauschbörsen[5], bei denen Bitcoins z.B. mit Realwährungen oder anderen Kryptowährungen gekauft werden können. Häufig ordnet die Tauschbörse einem zunächst ein Bitcoin-Konto zu, zu dem die Tauschbörse den privaten Schlüssel hat. Sobald man auf einem Gegenkonto z.B. einen ausreichend hohen Euro-Betrag eingezahlt hat, kann man über die Tauschbörse Bitcoins kaufen. Diese Tauschbörsen bieten häufig auch an, die privaten Schlüssel der Nutzer zu verwahren. Sie stellen den Nutzern damit eine sog. Wallet oder Geldbörsenfunktionalität zur Verfügung. Dies ist ein Dienst, der an das klassische e-Banking angelegt ist und eine eigene Authentifizierungsschicht hat. Diese Tauschbörsen und Anbieter von Geldbörsenfunktionalitäten sind nun Adressat der EU-Regulierung zur Geldwäsche geworden und haben voraussichtlich künftig die Pflicht, ihre Nutzer zu identifizieren.[6] Bitcoin-Geldbörsen gibt es aber auch als Open Source Software ohne zentrale Server-Komponente. In diesem Fall behält der Anwender die volle Kontrolle über seine Transaktionen und vermeidet zudem das Risiko, dass seine Bitcoins bei einem Hackerangriff auf den Dienstleister gestohlen werden.
- Es gibt Verkaufsstellen, die Bitcoins verkaufen. Das können Automaten sein, die gegen Geldeinwurf oder Geldabbuchung Bitcoins transferieren. Dies bieten in der Schweiz z.B. alle Fahrkartenautomaten der SBB an. In Österreich werden Bitcoins in allen Postfilialen verkauft.

Zwei weitere Optionen haben in der Praxis inzwischen eine geringere Bedeutung.

- Zum einen besteht die Möglichkeit, sich von anderen Personen ohne Mitwirkung Dritter Bitcoins übertragen zu lassen. Dies kann z.B. beim Verkauf von Waren oder Dienstleistungen gegen Bitcoins erfolgen.
- Zum anderen ist das Mining zu nennen, welches allerdings auf Grund der dafür nötigen Hardware hohe Einstiegshürden aufweist.

III. Personenbezogene Daten i.S.v. Art. 4 Nr. 1 DS-GVO

Bei der datenschutzrechtlichen Betrachtung beschränkt sich der Beitrag auf die Fragen des Personenbezugs und der Person des Verantwortlichen.

1. Kriterien zur Beurteilung des Personenbezugs

Nach Art. 2 Abs. 1 DS-GVO findet die DS-GVO Anwendung, wenn es sich bei den auf die Bitcoin-Blockchain geschriebenen Daten um personenbezogene Daten handelt. Art. 4 Nr. 1 DS-GVO definiert „personenbezogene Daten" als Daten, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Viel diskutiert wird dabei die Frage, auf wen abzustellen ist, wenn die Personenbeziehbarkeit beurteilt wird. Während es nach der absoluten Theorie reicht, dass irgendjemand den Per-

1 Um nur einige zu nennen: *Boehm/Pesch*, MMR 2014, 75; *Sorge/Krohn-Grumberghe*, DuD 2012, 479; *Engelhardt/Klein*, MMR 2014, 355; *Auffenberg*, NVwZ 2015, 1184, *Rückert*, MMR 2016, 295; *Piska*, ecolex 2017, 632, *Ehrke-Rabel/Eisenberger/Hödl/Pachinger/Schneider*, jusIT 2017, 87.

2 *Böhme/Pesch*, DuD 2017, 473.

3 *Satoshi Nakamoto* (Pseudonym), „A Peer-to-Peer Electronic Cash System", z.B. abrufbar unter: https://bitcoin.org/bitcoin.pdf.

4 Ethereum hatte ein Hard Fork, da keine Einigkeit bestand, ob die Folgen des DAO-Bugs revidiert werden sollten; CryptoCompare, 5.7.2017, abrufbar unter: https://www.cryptocompare.com/coins/guides/the-dao-the-hack-the-soft-fork-and-the-hard-fork/). Bei Bitcoin droht zum 1.8.2017 ein Hardfork; *Bovaird*, Cryptocurrency Market Resilient As Bitcoin Approaches Potential Hard Fork, Forbes, 26.7.2017, abrufbar unter: https://www.forbes.com/sites/cbovaird/2017/07/26/cryptocurrency-market-resilient-amid-bitcoins-possible-hard-fork/#2b0023a75497).

5 So z.B. Bity in der Schweiz, Bitpanda in Österreich oder coinbase in den USA.

6 COM/2016/0450 final – 2016/0208 (COD).

sonenbezug herstellen kann, wird nach der relativen Theorie auf die verarbeitende Stelle abgestellt.[7] Der *EuGH* ist bei der Beurteilung des Personenbezugs von IP-Adressen in der Rs. Breyer der relativen Theorie gefolgt.[8] Allerdings hat er sie darum erweitert, dass Informationen Dritter einzubeziehen sind, falls der Verarbeiter einen Rechtsanspruch hat, auf diese Informationen zuzugreifen. Die Frage, nach welchem Maßstab die Identifizierbarkeit zu beurteilen ist, adressiert Erwägungsgrund 26 der DS-GVO. Dieser stellt darauf ab, „ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind". Hier wird von „objektiven Faktoren" gesprochen. Dies bedeutet nicht, dass die DS-GVO damit der absoluten Theorie folgt, die teilweise auch objektive Theorie genannt wird. Vielmehr bedeutet dies, dass bei der Beurteilung der Identifizierungsmöglichkeiten der Verarbeiter nicht deren subjektive Fähigkeiten, sondern objektivierte Maßstäbe anzulegen sind. Bei der objektivierten Betrachtung der Verarbeiter wird dann die theoretische Identifizierbarkeit durch die Begriffe „allgemeines Ermessen", „wahrscheinlich" und „erforderlicher Zeitaufwand" eingeschränkt. Damit reicht entgegen *Heidrich/Hansen-Oest*[9] eben nicht die „abstrakte Identifizierbarkeit" oder gar die reine „Ansprechbarkeit"[10] einer Person, sondern es muss einen praktisch gangbaren Weg geben, die Personen hinter den Adressen zu identifizieren.

Nach der relativen Theorie ist für die Beurteilung des Personenbezugs auf die Verarbeiter abzustellen. Im Fall der Bitcoin-Blockchain sind die Daten öffentlich zugreifbar und unverschlüsselt.[11] Damit ist nicht nur jeder Knotenbetreiber, sondern potenziell jede Person Verarbeiter. Fraglich ist dabei, ob bei der Beurteilung auch auf den Betroffenen abzustellen ist. Zweck des Datenschutzes ist jedoch nicht, die Daten vor dem Betroffenen zu schützen. Daher kann eine Identifizierbarkeit durch den Betroffenen nicht zur Annahme des Personenbezugs führen.[12] Betreiber von Bitcoin-Handelsplätzen und Bitcoin-Dienstleister verarbeiten die Daten der Blockchain zusammen mit der Identifikation der Konten ihrer Kunden auf Grund eines Auftragsverhältnisses, expliziter Einwilligung oder/und gesetzlicher Erlaubnistatbestände. Die öffentliche Zugreifbarkeit auf die Daten der Blockchain führt dabei nicht dazu, dass sie darüber hinaus Daten über ihre Kunden erlangen würden. Daher ist bei der allgemeinen Beurteilung des Personenbezugs auch nicht auf diese abzustellen. Allerdings ist relevant, inwieweit Dritte diese Daten von ihnen z.B. auf Grund rechtlicher Auskunftsansprüche erlangen können.

Abhängig davon, wie die Bitcoins erworben und verwendet werden, gibt es verschiedene Möglichkeiten, die hinter einer Bitcoin-Adresse stehende Person zu identifizieren.

2. Bitcoin-Tauschbörsen und Bitcoin-Geldbörsen-Dienstleister

Für Bitcoin-Tauschbörsen und Bitcoin-Geldbörsen-Dienstleister möchte die EU eine Pflicht zur Erfassung und Speicherung der Identitäten der Nutzer vorsehen. Bereits heute verlangen praktisch alle uns bekannten Tauschbörsen eine Identifizierung der Nutzer. Damit sind für die Bitcoin-Tauschbörsen die Daten ihrer Kunden auf der Bitcoin-Blockchain personenbeziehbar. Wie oben erörtert, ist für die allgemeine Personenbeziehbarkeit der Daten auf der Bitcoin-Blockchain entscheidend, ob diese Daten an Dritte herausgegeben werden. Die Börsen geben diese Daten zumindest im Rahmen der Strafverfolgung oder auf Grund sonstiger gerichtlicher Anordnung weiter. Von daher ist eine Identifizierung durch Dritte prinzipiell möglich.

3. Weitergabe im Zahlungsverkehr

Wenn ein Nutzer Bitcoins erhalten möchte, muss er dazu notwendigerweise seine Bitcoin-Adresse weitergeben. Umgekehrt wird die Bitcoin-Adresse auch offenbart, wenn eine Zahlung vorgenommen wird und der Verkäufer z.B. für den Versand der Ware die Identität des Käufers kennen muss. Damit sind auch Transaktionen mit Dritten einsehbar.

4. Kombination von Beträgen verschiedener Konten

Um die Identifikation der Nutzer zu erschweren, wird empfohlen, für jede empfangene Zahlung ein eigenes Konto zu verwenden.[13] Es gibt auf der Bitcoin-Blockchain keine Begrenzung der Anzahl der Konten, die eine Person haben kann. Wird mit Bitcoins bezahlt, so wird aber notwendigerweise ein Zusammenhang zwischen der aktuellen Transaktion und der Transaktion zum Empfang dieser Bitcoins hergestellt. Sind darüber hinaus auf einem einzelnen Konto nicht genügend Bitcoins verfügbar, so können für eine Zahlung auch verschiedene Konten kombiniert werden. Durch diese Kombination wird offenbart, dass hinter den Konten die gleiche Person steht. Solche Analysen sind ohne technische Vorbedingungen oder Beihilfe Dritter möglich[14] und als Cloud-Dienstleistungen[15] verfügbar. Anlasslos sind sie möglicherweise datenschutzrechtlich unzulässig.[16] Es wäre jedoch ein Zirkelschluss, wegen einer datenschutzrechtlichen Unzulässigkeit den Personenbezug der Daten auf der Bitcoin-Blockchain zu verneinen.

5. Lokalisierung der Identifizierungsdaten zu einer Bitcoin-Adresse

Auch wenn es in vielen Fällen Stellen gibt, die bestimmte Bitcoin-Kontonummern Personen zuordnen können, reicht dies für die Identifizierbarkeit nicht unbedingt aus. Vielmehr müsste es für Dritte einen Weg geben, diese Stellen zu ermitteln. Bei IP-Adressen gibt es Verzeichnisse, die den verantwortlichen Provider nennen. Für Bitcoin-Adressen gibt es diese bislang nicht. Der Entwurf der 5. Geldwäsche-RL sieht allerdings die Einrichtung vieler vernetzter nationaler Register im neuen Art. 32a Nr. 1 vor. Doch auch ohne solche Verzeichnisse ist eine Ermittlung der IP-Adresse in den meisten Fällen möglich.[17] Über die IP-Adresse kann dann der Inhaber der Bitcoin-Adresse oder zumindest die Bitcoin-Tauschbörse ermittelt werden.

In einigen Fällen verwenden Kontoinhaber Mixer-Services, die

---

7 Eine ausf. und überzeugende Abhandlung findet sich dazu bei *Hoffmann/Johannes*, ZD 2017, 221; a.A. etwa *Breyer*, ZD 2014, 400.

8 *EuGH* ZD 2017, 24 m. Anm. *Kühling/Klar* – Breyer.

9 *Heidrich/Hansen-Oest*, c't 2016, 166.

10 *Moos/Rothkegel*, MMR 2016, 842, 847.

11 Andere Kryptowährungen wie z.B. z-cash verschlüsseln die Transaktionen, abrufbar unter: https://z.cash/technology/zksnarks.html. Bei Bitcoin werden die Transaktionen zwar auch künftig nicht verschlüsselt, jedoch ist es ab Anfang August 2017 mit dem Segwit-Patch möglich, viele Transaktionen außerhalb der Bitcoin-Blockchain zu sammeln und diese dann saldiert auf die Bitcoin-Blockchain zu schreiben, abrufbar unter: http://www.investopedia.com/-/bitcoin-after-segwit-software-upgrade/.

12 So auch *Schrey/Thalhofer*, NJW 2017, 1431, 1433, die jedoch nicht nachvollziehbar bei selbstgewählten Pseudonymen den Personenbezug generell ausschließen.

13 So z.B. das Bitcoin-Wiki, welches sich gegen die „Wiederverwendung von Bitcoin-Adressen" ausspricht, abrufbar unter: https://en.bitcoin.it/wiki/Address_reuse

14 *Leonhardt*, Sicherheit und Datenschutz bei Bitcoin. Technical Report, Technische Universität Dresden, 2012; *Androulaki et al.*, Evaluating User Privacy in Bitcoin, International Conference on Financial Cryptography and Data Security, 2013, S. 34-51.

15 *Pesch/Böhme*, DuD 2017, 93; s.a. das deutsch-österreichische Forschungsprojekt Bitcrime, abrufbar unter: http://bitcrime.de.

16 *Hofert*, Blockchain-Profiling, ZD 2017, 161.

17 *Koshy/Koshy/McDaniel*, An Analysis of Anonymity in Bitcoin Using P2P Network Traffic, International Conference on Financial Cryptography and Data Security FC 2014, S. 469-485.

viele Bitcoin-Konten miteinander vertauschen, um das Tracking zu erschweren. Auch werden zur Unkenntlichmachung der IP-Adresse VPN-Services oder TOR eingesetzt. Die IP-Adressen hinter den Bitcoin-Adressen lassen sich jedoch in den meisten Fällen trotzdem rückverfolgen.[18] Doch selbst wenn es Mixer-Services gibt, die sich nicht zurückverfolgen lassen, hat dies datenschutzrechtlich wenig Relevanz, da auf den gewöhnlichen Nutzer und nicht denjenigen Nutzer abgestellt werden muss, der einen maximalen Aufwand zur Verschleierung seiner Identität betreibt.

6. Ergebnis

Die Identifizierung der Kontoinhaber von Bitcoin-Konten ist in vielen Fällen möglich. Damit liegt eine Personenbeziehbarkeit der Daten i.S.v. Art. 4 Abs. 1 DS-GVO vor. Dies gilt erst recht mit dem Vorschlag zur 5. Geldwäsche-RL der EU, wonach diese Daten zudem zentral zugreifbar zum Zwecke der Strafverfolgung vorgehalten werden.[19]

IV. Verantwortlicher gem. Art. 4 Abs. 7 DS-GVO

Der „Verantwortliche" i.S.d. Art. 4 Nr. 7 DS-GVO ist jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Beim dezentralen Bitcoin-Netzwerk gibt es keinen zentralen Verantwortlichen. Vielmehr gibt es viele Teilnehmer am Bitcoin-Netzwerk, die zusammenwirken, ohne sich jedoch dabei abzusprechen. Dabei sind zwei Fallkonstellationen zu unterscheiden:

- Im ersten Fall agiert ein Nutzer direkt mit der Blockchain. Dafür installiert er in seinem Verantwortungsbereich eine Client-Software[20], die sich mit dem Bitcoin-Netzwerk verbindet und Transaktionen an andere Knoten in der Bitcoin-Blockchain sendet. Diese Client-Software dient auch zur Aufbewahrung seiner privaten Schlüssel. Alternativ können die Schlüssel auch auf spezieller Hardware[21] oder offline auf Papier gespeichert werden.
- Im zweiten Fall bedient sich der Nutzer einer der bereits oben erwähnten Plattformen, die Tausch- und Geldbörsen-Dienste anbieten. Im Gegensatz zur direkten Interaktion über das Bitcoin-Protokoll wird bei Interaktionen mit einem Dienstleister der Account-Schlüssel von eben diesem generiert, verwahrt, zur Signierung der Transaktionen verwendet und die signierten Transaktionen an die Bitcoin-Blockchain übermittelt.

1. Verantwortlicher im Fall der direkten Vornahme von Bitcoin-Transaktionen

In der ersten Fallkonstellation der direkten Interaktion mit anderen Bitcoin-Knoten gibt es keinen direkten Ansprechpartner, der Verantwortlicher i.S.v. Art. 4 Nr. 7 DS-GVO sein könnte. Bitcoin ist ein Peer-to-Peer-Netzwerk, bei dem sich generell die Frage stellt, wer Adressat einer Regulierung sein kann.

a) Betreiber von Bitcoin-Knoten als gemeinsam Verantwortliche?

Verantwortliche könnten alle Betreiber eines Bitcoin-Knoten sein. Art. 4 Nr. 7 DS-GVO sieht ausdrücklich auch eine Mehrheit von Verantwortlichen vor.[22] Fraglich ist jedoch, ob die Knotenbetreiber über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheiden.

Die Knotenbetreiber haben sich entschieden, dass sie einen Bitcoin-Knoten auf ihren Computersystemen betreiben. Um über Zwecke und Mittel der Verarbeitung von personenbezogenen Daten zu entscheiden, reicht das bloße Betreiben eines Servers nicht.[23] Bitcoin-Knotenbetreiber betreiben nicht nur einen Server, sondern darauf auch die Bitcoin-Applikation. Sie haben aber ähnlich dem bloßen Server-Betreiber inhaltlich keinen Einfluss. Sie können lediglich ihre Knoten an- oder abschalten. Das liegt nicht in erster Linie daran, dass sie auf Grund fehlenden Wissens die Bitcoin-Software nicht beeinflussen könnten. Der Code ist quelloffen und jeder kann ihn nach eigenen Vorstellungen verändern. Vielmehr ist der Code so geschrieben, dass ein abweichender Knoten im Netzwerk ignoriert wird. Wenn sich also ein Knotenbetreiber entscheiden würde, vom Protokoll abzuweichen, käme dies einem Abschalten des eigenen Knotens gleich. Auch das Abschalten eines Knotens hat keinen Einfluss auf die Bitcoin-Blockchain. Wenn aber ein Knotenbetreiber praktisch keinen Einfluss auf die Verarbeitung hat, ist zweifelhaft, ob er über die Zwecke der Verarbeitung bestimmt.

Möglicherweise könnten allerdings die Knotenbetreiber in ihrer Gesamtheit gemeinsam Verantwortliche sein. Gemeinsam hätten sie die Möglichkeit, die Blockchain inhaltlich zu beeinflussen. Art. 26 DS-GVO beschreibt die Pflichten gemeinsam Verantwortlicher. Dabei wird in Art. 26 Abs. 1 Satz 1 DS-GVO auch nochmal die gemeinsame Verantwortlichkeit beschrieben: „Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche." Es reicht also nicht, dass mehrere Parteien agieren, sondern sie müssen gemeinsam die Zwecke festlegen. Zwischen den Knotenbetreibern gibt es jedoch in der Regel gar keine Absprache über die Zwecke.

Erwägungsgrund 79 DS-GVO nennt zudem als Ziel, dass es zum Schutz der Betroffenen klare Verantwortlichkeiten geben müsse. Es ist zweifelhaft, ob dies dadurch erreicht wird, dass eine sehr große Anzahl von wechselnden Knotenbetreibern ohne effektiven Einfluss auf die Zwecke der Verarbeitung als Verantwortliche angenommen wird.

b) Mineur eines konkreten Blocks als Verantwortlicher der darin enthaltenen Transaktionen?

Der Mineur, der die Lösung des mathematischen Rätsels für einen Block als Erstes findet und damit diesen an alle anderen Knoten verteilen kann, könnte Verantwortlicher i.S.v. Art. 4 Nr. 7 DS-GVO für die darin enthaltenen Transaktionen sein. Alle Mineure versuchen für den nächsten Block ein mathematisches Rätsel zu lösen. Nur wer dieses Rätsel als Erstes löst, kann damit den nächsten Block definieren und erhält die festgelegte Vergütung. Daher soll hier zunächst betrachtet werden, ob der Mineur eines konkreten Blocks als Verantwortlicher für diesen konkreten Block in Frage kommt. Mineure können jedoch keine Transaktionen verändern oder Transaktionen für fremde Konten erstellen. Doch haben Mineure die Möglichkeit, einzelne Transaktionen zu selektieren oder auszuschließen. So werden z.B. Transaktionen, die nur geringe Transaktionsgebühren zahlen, zu Gunsten von Transaktionen mit höheren Transaktionsgebühren zurückgestellt. Von einem Mineur nicht aufgenommene Transaktionen werden jedoch nicht dauerhaft abgelehnt, sondern können mit dem nächsten Block aufgenommen werden, zu

---

18 *ShenTu, QingChun/JianPing Yu*. Research on Anonymization and De-anonymization in the Bitcoin System. arXiv preprint arXiv:1510.07782 (2015); vgl. auch *Guggenberger*, ZD 2017, 49.

19 So auch *Pesch/Böhme*, DuD 2017, 93, 95; ebenso *Santiago*, Technology and Security Officer at the European Data Protection Supervisor in einer Präsentation am 17.6.2016: Data protection and blockchain technologies, abrufbar unter: https://trustindigitallife.eu/wp-content/uploads/2016/07/fidel_santiago.pdf.

20 Er kann dabei zwischen einem Lightweight-Client oder einem Full-node wählen. Eine Liste verfügbarer Clients findet sich z.B. im Bitcoin-Wiki, abrufbar unter: https://en.bitcoin.it/wiki/Clients.

21 Eine Liste von Hardware Wallets findet sich z.B. im Bitcoin Wiki, abrufbar unter: https://en.bitcoin.it/wiki/Hardware_wallet.

22 So etwa *Schrey/Thalhofer*, NJW 2017, 1431, 1433 f.

23 *Jotzo*, MMR 2009, 232, 233.

dem ein anderer Mineur die Lösung als Erster findet. Nimmt umgekehrt ein einzelner Mineur eine ungültige Transaktion in seinen Block auf, so wird sein Block von den übrigen Mineuren verworfen werden. Er verliert damit die Belohnung dafür, dass er als Erster die Lösung für den vom ihm generierten Block gefunden hat. Es ist gerade das Sicherheitskonzept der Blockchain, dass eine Minderheit von Mineuren nicht darüber entscheiden kann, welche Transaktionen in die Blockchain aufgenommen werden. Damit scheidet der einzelne Mineur, der einen Block erstellt, als Verantwortlicher für die darin enthaltenen Transaktionen aus.

c) Gesamtheit der Mineure der Bitcoin-Blockchain als gemeinsam Verantwortliche?

Die Gesamtheit der Mineure der Bitcoin-Blockchain könnten gemeinsam Verantwortliche i.S.v. Art. 4 Nr. 7 DS-GVO sein. Gemeinsam haben die Mineure die Möglichkeit, bestimmte Transaktionen auszuschließen. Allerdings legen sie ihre Ziele nicht gemeinsam fest (Art. 26 Abs. 1 Satz 1 DS-GVO). Die Gruppe der Mineure kann auch nicht klar bestimmt werden. Jeder, der auf der Suche nach einem passenden Nounce-Wert (der Wert, der zur Validierung eines Blocks notwendig ist) ist, ist ein Mineur. Im Nachhinein könnte man allenfalls die Gruppe der erfolgreichen Mineure bestimmen.

Etwas anderes gilt, wenn sich eine Gruppe von Mineuren zusammenschließt, die mehr als 50% der Rechenleistung der Bitcoin-Blockchain vereinen. Bitcoin-Mineure haben sich zu einem großen Teil in Miningpools[24] zusammengeschlossen. Da ein Miningpool mit mehr als 50% der Bitcoin-Gesamtrechenleistung auch die Sicherheit und das Vertrauen in Bitcoin in Frage stellt, achten die Miningpools aber selbst darauf, dass sie unterhalb der 50%-Grenze bleiben.[25] Poolübergreifende Absprachen gibt es nur bei grundsätzlichen Entscheidungen z.B. über das Einspielen bestimmter Software-Updates – sog. Hard- oder Soft Forks.[26] Damit haben die Mineure keinen Einfluss auf die Aufnahme der Transaktionen in die Blockchain. Sie entscheiden damit nicht über den Zweck und die Mittel der Datenverarbeitung und scheiden als Verantwortliche aus.

d) Softwareentwickler als Verantwortliche?

Erwogen werden könnte auch, dass die Entwickler der Bitcoin-Software Verantwortliche i.S.v. Art. 4 Nr. 7 DS-GVO sind. Dafür spricht, dass sie tatsächlich die technischen Abläufe auf der Blockchain beeinflussen können. Allerdings haben sie weder eine Kontrolle über den Einsatz der Software noch darauf, welche Inhalte konkret darauf gespeichert werden. Sie bestimmen damit weder die konkreten Zwecke noch die Mittel der Datenverarbeitung.

e) Nutzer als Verantwortlicher?

Wer direkt eine Bitcoin-Transaktion vornimmt, entscheidet alleine, wieviel Bitcoins von welcher Adresse auf welche andere Adresse übertragen werden sollen. Eine Clearingstelle, die diese Transaktion inhaltlich z.B. auf Berechtigung oder unerlaubte Geldwäsche überprüft, gibt es nicht. Es gibt lediglich eine technische Überprüfung auf die Gültigkeit der Signatur mit den privaten Schlüsseln der Bitcoin-Adressen, von denen die Bitcoins transferiert werden sollen. Bitcoin-Transaktionen zeichnen sich gerade dadurch aus, dass alleine der Besitzer des privaten Schlüssels einer Bitcoin-Adresse über die Transaktion autonom bestimmen kann und Einflüsse von Dritten bestmöglich ausgeschlossen sind. Der Nutzer kann daher sehr konkret die Zwecke der Datenverarbeitung beeinflussen. Gegen die Annahme des Nutzers als Verantwortlicher der Bitcoin-Transaktion könnte sprechen, dass er nur eine signierte Nachricht an das Netzwerk sendet. Allerdings ist die Bitcoin-Blockchain nichts anderes als die Gesamtheit der formal validierten und in Blöcke zusammengefassten Nachrichten. Ausschließlich der einzelne Nutzer hat die Kontrolle darüber, dass die Transaktion auf der Blockchain aufgenommen wird, und niemand kann die Transaktion von der Blockchain entfernen. Mit der Übermittlung an die Blockchain entscheidet der Nutzer über die Mittel der Datenverarbeitung. Zwar entscheidet er nicht über die Mittel, mit denen die konkreten Knoten betrieben werden. Dies hat jedoch keinen Einfluss auf das Ergebnis, die Sicherheit oder die öffentliche Verfügbarkeit der Datenverarbeitung. Im Vergleich zu anderen Szenarien der Datenverarbeitung wie etwa Portale oder klassische Banken haben die Betreiber der Bitcoin-Knoten praktisch keine Möglichkeit, die Nachrichten zu verändern oder zu löschen. Daher tritt unserer Auffassung nach die theoretisch mögliche und mit hohen Hürden und Risiken verbundene Beeinflussung der Inhalte der Bitcoin-Blockchain durch die Mineure gegenüber der ganz konkreten Beeinflussung durch den Nutzer zurück.

Im Ergebnis ist daher derjenige, der eine Transaktion erstellt, signiert und in das Bitcoin-Netzwerk gibt, der Verantwortliche i.S.v. Art. 4 Nr. 7 DS-GVO.

2. Nutzung von Bitcoin-Handelsplätzen oder Geldbörsen-Diensten

Wird für die Bitcoin-Transaktion ein Bitcoin-Handelsplatz verwendet, so ändert sich die Rolle der Bitcoin-Knotenbetreiber und Mineure nicht. Der Nutzer gibt jedoch die Kontrolle über seine Bitcoins aus der Hand. Gleiches gilt für Bitcoin-Geldbörsen-Dienste. Der Nutzer generiert sein Bitcoin-Konto nicht selbst und verfügt dann auch nicht über seinen privaten Schlüssel. Transaktionen werden vielmehr erst einmal zwischen Nutzer und Handelsplatz authentifiziert. Der Handelsplatz kontrolliert die Transaktion und legt Begrenzungen fest[27]. Bei Handelsplätzen und Geldbörsen initiiert der Nutzer zwar auch die Transaktionen, die Handelsplätze und zentral betriebene Geldbörsen übernehmen jedoch die finale Prüfung. Sie können Transaktionen effektiv blockieren und wären technisch auch in der Lage, die ihnen anvertrauten Bitcoins zu veruntreuen. Der Nutzer gibt dem Intermediär nur den Auftrag, bestimmte Transaktionen durchzuführen. Dabei muss der Nutzer darauf vertrauen, dass der Dienstleister den Auftrag wie gewünscht in eine signierte Nachricht an die Bitcoin-Blockchain vereinbarungsgemäß umsetzt. Einen direkten Einfluss auf die Datenverarbeitung hat der Nutzer in dieser Fallkonstellation nicht. Auch im Vergleich mit Knotenbetreibern, Mineuren oder Softwareentwicklern haben Handelsplätze und zentral betriebene Geldbörsen den entscheidenden Einfluss auf die Datenverarbeitung. Handelsplätze und Geldbörsendienstleister sind zudem als Vertragspartner der Nutzer klar identifizierbar.

Der Vorschlag zur 5. Geldwäsche-RL geht in die gleiche Richtung. Er sieht die Handelsplätze und Geldbörsen als „Gatekeeper" und bewertet sie als geeignete Adressaten einer Regulie-

24 Eine aktuelle Darstellung der Anteile der verschiedenen Miningpools findet sich bei *Tuwiner*, abrufbar unter: https://www.buybitcoinworldwide.com/mining/pools/.

25 *Hajdarbegovic*, Bitcoin Miners Ditch Ghash.io Pool Over Fears of 51% Attack, coindesk 9.1.2014, abrufbar unter: https://www.coindesk.com/bitcoin-miners-ditch-ghash-io-pool-51-attack/.

26 Eine Liste der Updates findet sich z.B. unter: https://bitcoin.org/en/version-history. Dabei bleiben die meisten Updates kompatibel, sodass kein Risiko eines Aufsplittens („Fork") der Bitcoin-Blockchain bestand. Aktuell wird jedoch ein inkompatibles Update kontrovers diskutiert. Dabei geht es um verschiedene Verfahren, um das Transaktionslimit anzuheben: *Jim Urquhart/Relief Rally*, Bitcoin is booming because a split in the cryptocurrency has been narrowly averted, abrufbar unter: https://qz.com/1035565/bitcoin-price-and-segwit-the-cryptocurrency-is-surging-because-a-hard-fork-has-been-averted/ sowie Bitcoin Miners Hold "Emergency Meeting", trustnodes 25.7.2017, abrufbar unter: http://www.trustnodes.com/2017/07/25/bitcoin-miners-hold-emergency-meeting.

27 Z.B. coinbase, abrufbar unter: https://support.coinbase.com/customer/en/portal/articles/1767231-payment-methods-for-european-customers oder Bity https://bity.com/faq.

rung.[28] Sie werden durch die Richtlinie zur Datenerfassung und Verarbeitung verpflichtet.

Der Vorschlag zur 5. RL verwendet den Begriff „Geldbörsen". Er definiert ihn im künftigen Art. 2 Abs. 1 lit. H als „Anbieter von elektronischen Geldbörsen, die Verwahrungsdienstleistungen für Referenzen anbieten", die für den Zugang zu virtuellen Währungen benötigt werden. Solche Börsen – meist englisch „wallet" genannt – gibt es als Software, Hardware oder als Dienstleistung. Fraglich ist hier, ob dieser Richtlinienvorschlag auch die Software- und Hardwarevarianten mit umfasst. Dagegen spricht zum einen der Wortlaut, der von Dienstleistung spricht. Zudem würden massive Bedenken dagegensprechen, reine Softwareentwickler als Verpflichtete zu definieren, die entsprechende Datenabflüsse in ihre Software einbauen müssten und dann auch noch dafür geradestehen müssten, dass diese Datenabflüsse vom Nutzer nicht deaktiviert werden. Dadurch besteht zwar eine Regulierungslücke. Dies wird auch von der Richtlinie gesehen, aber in Erwägungspunkt 7 ausdrücklich in Kauf genommen.

3. Ergebnis

Werden Transaktionen über Bitcoin-Handelsplattformen oder zentralisierte Bitcoin-Geldbörsen-Dienste durchgeführt, so sind diese Verantwortliche i.S.d. Art. 4 Nr. 7 DS-GVO. Übernimmt der Nutzer jedoch selbst die direkte Interaktion mit der Blockchain, so ist er selbst Verantwortlicher für seine Transaktionen – das gilt insbesondere auch für die Bitcoin-Adressen der Empfänger.

Welche datenschutzrechtlichen Einwilligungen der einzelne Nutzer als Verantwortlicher dazu einholen muss und welche Informationspflichten dieser hat, hängt vom Kontext der Transaktion ab. Wird mit der Transaktion eine vertragliche Pflicht gegenüber dem Nutzer erfüllt, so ist die Erfüllung bereits über Art 6 Abs. 1 lit. b DS-GVO gerechtfertigt. Eine weitere Information des betroffenen Zahlungsempfängers kann hierbei ebenfalls entfallen, da die Datenablage auf der Bitcoin-Blockchain eine im Vertrag beschriebene Hauptpflicht des Zahlungsauslösers ist.

Welche Pflichten Bitcoin-Handelsbörsen und Bitcoin-Geldbörsen-Dienstleister haben, hängt ebenso von der konkreten Vertragskonstellation ab. Zudem wird sich dies wohl künftig an den Regelungen der 5. Geldwäsche-RL der EU ausrichten.

28 Begründung Nummer 2 Unterpunkt „Verhältnismäßigkeit" sowie Nummer 5 lit. A.

V. Bewertung

Es mag unbefriedigend erscheinen, im Falle des autonom agierenden Nutzers keine anderweitigen datenschutzrechtlich Verantwortlichen auszumachen. Deshalb Knotenbetreiber, Mineure oder gar Softwareentwickler für konkrete Transaktionen verantwortlich zu halten, die sie selbst gar nicht beeinflussen können, würde jedoch über das Ziel hinausschießen. Sie wären technisch gar nicht in der Lage, die Verpflichtungen als datenschutzrechtlich Verantwortliche zu erfüllen. Die prinzipielle Frage, ob bei Peer-to-Peer-Diensten lieber eine Regulierungslücke oder eine den Dienst effektiv verbietende Überregulierung in Kauf genommen werden sollte, adressiert die DS-GVO nicht direkt. In einer offenen Gesellschaft sollte Raum für Peer-to-Peer-Systeme ohne zentrale Kontrollstellen bleiben. Die Regelungslücke ist hinzunehmen und kann bei Bitcoin durch die von der EU vorgeschlagene Regulierung zentraler Intermediäre in der Peripherie des Systems ausreichend ausgeglichen werden.

VI. Fazit

Auf der Bitcoin-Blockchain sind in der Kombination von Bitcoin-Adressen und Bitcoin-Transaktionen personenbeziehbare Daten abgelegt, sodass die DS-GVO Anwendung findet. Bedient sich der Nutzer Dienstleister wie Bitcoin-Handelsplattformen oder Bitcoin-Geldbörsen, so sind diese Verantwortliche i.S.d. Art. 4 Nr. 7 DS-GVO. Führt er die Transaktionen selbst durch, so ist der Nutzer selbst Verantwortlicher. Die dadurch theoretisch entstehende Regulierungslücke ist zum einen in einer offenen Gesellschaft hinzunehmen und zum anderen in ihren Auswirkungen durch entsprechende Regulierung der Dienstleister von geringer praktischer Relevanz.

Dipl.-Inform. Jörn Erbguth
ist Jurist, externer Datenschutzbauftragter, Lehrbeauftragter an der Geneva School of Diplomacy und promoviert an der Universität Genf zum Thema Blockchain und Governance.

Mag. Joachim Galileo Fasching, LL.M.,
ist Geschäftsführer einer Unternehmensberatung in Wien.