CHRISTOPH SAFFERLING / CHRISTIAN RÜCKERT

Telekommunikationsüberwachung bei Bitcoins

Heimliche Datenauswertung bei virtuellen Währungen gem. § 100a StPO?

Telekommunikations- und Medienrecht

Die neue Technologie der virtuellen Krypto-Währungen eröffnet ein neues Feld für Kriminalität und eine neue Herausforderung für Staatsanwaltschaften und Polizeibehörden. Die technischen Gegebenheiten – insbesondere die Pseudonymität der Bitcoin-Nutzer – verhindert die Anwendung „klassischer" Ermittlungsansätze, ermöglicht aber, nicht zuletzt wegen der öffentlichen Einsehbarkeit der Blockchain (also der Liste aller vorgenommenen Transaktionen), die Entwicklung neuer Fahndungsmethoden. Bei diesen stellt sich, da es sich bei einer Bitcoin-Transaktion um eine Form der Online-Kommunikation handelt, die Frage, ob in Art. 10 Abs. 1 GG eingegriffen wird und ob es sich um eine Form der Telekommunikationsüberwachung i.S.v. § 100a StPO handelt. Beide Fragen sind – trotz einer nicht zu leugnenden Nähe zur Telekommunikationsüberwachung – letztlich, wegen der öffentlichen Zugänglichkeit der ausgewerteten Informationen aus der Blockchain, zu verneinen. Offen bleibt, ob die neuen Fahndungsmaßnahmen auf die §§ 161, 163 StPO gestützt werden können oder ob eine neue Rechtsgrundlage geschaffen werden muss.

I. Virtuelle Währungen als neue strafprozessuale Herausforderung

Trotz zahlreicher Änderungen der StPO zur Erfassung neuer technischer Fahndungsinstrumente in den letzten Jahrzehnten[1], wird bei dem Versuch der Anwendung der strafprozessrechtlichen Eingriffsbefugnisse bei Ermittlungsverfahren im Bereich virtueller Krypto-Währungen wie den Bitcoins, schnell klar, dass die rechtliche Entwicklung schon lange nicht mehr mit der technischen Entwicklung Schritt halten kann. Nicht zuletzt wegen der Pseudonymisierung durch Verwendung öffentlicher Schlüssel und des Fehlens von zentralen, verwaltenden Stellen im Peer-to-Peer (P2P) Bitcoin-Netzwerk, stoßen die Ermittlungsbehörden bei der Nutzung „klassischer" Ermittlungsmethoden im Bereich von virtuellen Krypto-Währungen schnell an die Grenzen der geregelten Ermittlungsbefugnisse. Besondere Bedeutung kommt hierbei der Frage zu, ob die heimliche Überwachung und Auswertung einer bzw. mehrerer Bitcoin-Transaktionen (also eine Überweisung von Bitcoins von einem „Bitcoin-Konto" auf ein anderes) unter den Begriff der Telekommunikationsüberwachung (TKÜ) des § 100a StPO fällt. Dieser Frage kommt insbesondere deswegen immense Bedeutung zu, weil ihre Bejahung gleichzeitig eine Heranziehung der Ermittlungsgeneralklauseln der §§ 161, 163 StPO wegen der abschließenden Wirkung des § 100a StPO für heimliche Ermittlungsmaßnahmen im TK-Bereich verhindert.[2] Der Gesetzgeber wollte die heimliche Überwachung von „Telekommunikation" abschließend und umfassend in §§ 100a, 100b StPO regeln.[3] Nach neuerer Rechtsprechung des *BVerfG* ist zwar nicht automatisch jeder Eingriff in die TK-Freiheit nach Art. 10 Abs. 1 GG an § 100a StPO zu messen.[4] Insbesondere kann die offene Beschlagnahme von E-Mails beim E-Mail-Provider auf die §§ 94 ff. StPO gestützt werden.[5] Dagegen verbleibt es für heimlich vorgenommene Eingriffe in Art. 10 Abs. 1 GG bei der abschließenden Regelung des § 100a StPO.[6] Gleiches gilt wegen der großen Eingriffsintensität auch für eine laufende Überwachung der Telekommunikation[7] in Abgrenzung zu einem einzelnen Zugriff auf gespeicherte Daten (wie zu einem bestimmten Zeitpunkt beim Provider gespeicherte E-Mails). Jedes neue Fahndungsinstrument, das auf die heimliche und/oder dauerhafte Überwachung und Auswertung der Blockchain abzielt[8] – sei es in Form einer Analyse oder Überwachung der Transaktionen in der Blockchain, automatisierte Merkmalerkennungen oder die Anlage von Datenbanken, in welchen Transaktionen miteinander und mit weiteren, außerhalb der Blockchain liegenden Informationen verknüpft werden – müsste sich an § 100a StPO messen lassen. Falls die Befugnisse, welche § 100a StPO den Ermittlungsbehörden verleiht, nicht ausreichen, um ein neu entwickeltes Fahndungsinstrument anwenden zu können, so müsste der Gesetzgeber eine neue Regelung schaffen. Dass hierfür ein Bedürfnis besteht, lässt sich angesichts der steigenden Anzahl von Delikten, welche im Zusammenhang oder unter Zuhilfenahme virtueller Währungssysteme begangen werden, kaum von der Hand weisen. Neben „klassischen" Delikten wie Erpressung (häufig mit sog. „ransom ware"), Betrug und anderen Vermögensdelikten, bei denen Bitcoins erpresst bzw. durch Täuschung erlangt werden[9], bieten sich die virtuellen Währungssysteme aus krimineller Sicht vor allem für den Handel mit illegalen Gütern[10] und Geldwäschedelikte[11] an.

II. „Vorteile" des Bitcoin-Netzwerks für kriminelle Aktivitäten

Für Kriminelle bietet sich der Rückgriff auf virtuelle Währungen vor allem wegen deren technischen Funktionsweise[12] an. Anders als der Begriff „Bitcoin" suggeriert, existieren im Bitcoin-Netzwerk keine „digitalen Münzen".[13]

1. Bitcoins als Kette digitaler Signaturen

Bitcoins sind vielmehr eine Kette digitaler Signaturen im Bitcoin-Netzwerk.[14] Die Zuweisung von Wert erfolgt im Netzwerk nicht über „digitale Münzen", die als Datenpaket gespeichert und übertragen werden[15], sondern durch die Zuweisung eines Werts mit einem System, welches dem der digitalen Rechteverwaltung (DRM) ähnelt.[16] Im Bitcoin-Netzwerk gibt es dafür aber keine zentrale Ausgabe- oder Verwaltungsstelle wie z.B. eine Bank, es handelt sich beim Bitcoin-Netzwerk vielmehr um ein sog. P2P-Netzwerk.[17] Jedes teilnehmende Gerät (sei es PC, Laptop oder

---

1 Vgl. z.B. Begleitgesetz zum Telekommunikationsgesetz v. 17.12.1997; Gesetz zur Neuregelung der Telekommunikationsüberwachung v. 21.12.2007; Gesetz zur Änderung des Telekommunikationsgesetzes und zur Neuregelung der Bestandsdatenauskunft v. 20.6.2013.

2 Zum abschließenden Charakter der Regelung: BGHSt 31, 304, 306 für die Aufzeichnung und Überwachung von Telefongesprächen; BGHSt 34, 39, 50; *Schmitt,* in: Meyer-Goßner, StPO, 58. Aufl. 2015, § 100a Rdnr. 2; a.A.: *Brodowski,* JR 2009, 402, 407.

3 BGHSt 31, 304, 306: „eindeutige Gesetzeslage"; s.a. BGHSt 34, 39, 50.

4 BVerfGE 124, 43, 58 f. = MMR 2009, 673, 675 f.; erst recht darf nicht von der Eröffnung des Schutzbereichs des Art. 10 Abs. 1 GG automatisch auf die Deckung eines Eingriffs durch § 100a StPO geschlossen werden: *Kudlich,* JuS 1998, 209, 213 f.; *ders.,* JA 2000, 227, 232 f.

5 BVerfGE 124, 43, 58, 62 f., 65 = MMR 2009, 673, 676 f.; a.A. mit beachtlichen Argumenten *Jahn,* JuS 2009, 1048; *LG Hamburg* MMR 2008, 186 f. m. Anm. *Störing.*

6 Vgl. BVerfGE 124, 43, 62 f., 65 = MMR 2009, 673, 677; *BGH* MMR 2010, 444; so auch *Schmitt* (o. Fußn. 2), § 100a Rdnr. 6c; *Sieber,* Gutachten, 69. DJT, I C 112; *Zimmermann,* JA 2014, 321, 325; *Brunst,* CR 2009, 591, 592; *Singelnstein,* NStZ 2012, 593, 597; *Park,* Durchsuchung und Beschlagnahme, 3. Aufl. 2015, Rdnr. 805 ff., 810; *Bruns,* in: KK-StPO, 7. Aufl. 2013, § 100a Rdnr. 18; *Gaede,* StV 2009, 97, 99 f.; *Kasiske,* StraFo 2010, 228, 234; *Klein,* NJW 2009, 2996, 2998; *Neuhöfer,* ZD 2012, 178, 179; abweichend, aber durch die Entscheidung des *BVerfG* überholt: *BGH* MMR 2009, 391; *Bär,* TK-Überwachung, 2010, § 100a Rdnr. 30; *Graf,* in: BeckOK StPO, Ed. 21 2015, § 100a Rdnr. 30 ff., wobei deren Ansicht, nach der § 99 StPO anzuwenden ist, für die hiesige Fallkonstellation schon deswegen nicht relevant wird, weil die Daten in der Blockchain keinesfalls als „Postsendungen" oder „Telegramme" i.S.v. § 99 StPO angesehen werden können; für Facebook-Nachrichten: *AG Reutlingen* CR 2012, 93.

7 *Brunst,* CR 2009, 591, 592.

8 Offene Ermittlungsmaßnahmen nach §§ 94 ff. StPO scheiden wegen der technischen Struktur des Bitcoin-Netzwerks aus, vgl. hierzu unten.

9 Vgl. http://www.spiegel.de/netzwelt/web/erpressung-mit-bitcoin-pizza-lieferanten-sollen-schutzgeld-zahlen-a-977840.html; zur sog. „ransom-ware": http://www.spiegel.de/netzwelt/web/loesegeld-trojaner-us-polizisten-gehen-auf-erpressung-ein-a-1019970.html; s.a. *Boehm/Pesch,* MMR 2014, 75.

10 Vgl. z.B. zur sog. „silk road": Die Zeit, Ausgabe 12/2014, Silkroad: Kokain vom „Pfandleiher" aus Bayern, abrufbar unter: http://www.zeit.de/2014/12/drogenhandel-silk-road-pfandleiher; http://www.spiegel.de/netzwelt/netzpolitik/silk-road-betreiber-von-online-drogenboerse-schuldig-gesprochen-a-1016783.html; http://www.spiegel.de/netzwelt/netzpolitik/silk-road-vier-jahre-gefaengnis-fuer-bitcoin-haendler-a-1014228.html; s.a. *Boehm/Pesch,* MMR 2014, 75.

11 http://www.spiegel.de/netzwelt/web/zwei-jahre-haft-bitcoin-aktivist-shrem-verurteilt-a-1009926.html; http://www.sueddeutsche.de/digital/virtuelle-waehrung-us-regierung-friert-bitcoin-konten-ein-1.1674306.

12 Die Verfasser danken Herrn *Malte Möser, BSc* von der Westfälischen Wilhelms-Universität Münster für die technische Beratung.

13 *Sorge/Krohn-Grimberghe,* DuD 2012, 479, 480; *Kütük/Sorge,* MMR 2014, 643; *Spindler/Bille,* WM 2014, 1357, 1358; *Bollen,* JBFLP – Journal of Banking and Finance Law and Practice 2013 (v. 1.5.2013), 1, 7; missverständlich dagegen *Engelhardt/Klein,* MMR 2014, 355 sowie *Kaplanov,* TLR – Temple Law Review 2012 (v. 31.3.2012), 1, 4.

14 *Nakamoto,* Bitcoin: A Peer-to-Peer Electronic Cash System, S. 2, abrufbar unter: https://bitcoin.org/bitcoin.pdf.

15 Natürlich besteht eine Überweisung im Bitcoin-Netzwerk aus einer bestimmten Datenmenge, die sich (im Wesentlichen) aus den öffentlichen Schlüsseln („Kontonummern") der an der Transaktion beteiligten Nutzer, einem Verweis auf vorherige Transaktionen, die dem öffentlichen Schlüssel des Überweisenden Bitcoins übertragen haben, und einer Signatur des Überweisenden zusammensetzt, vgl. *Schroeder,* JurPC Web-Dok. 104/2014, Abs. 10. Diese Datenmenge repräsentiert jedoch nicht für sich genommen einen bestimmten Wert, der der Datenmenge innewohnt, vgl. *Sorge/Krohn-Grimberghe,* DuD 2012, 479, 480; *Bollen,* JBFLP 2013 (v. 1.5.2013), 1, 7, dies wird vor allem auch daran deutlich, dass in der Blockchain auch beliebige andere Daten per „Transaktion" versendet und gespeichert werden können.

16 *Engelhardt/Klein,* MMR 2014, 355.

17 *Kütük/Sorge,* MMR 2014, 643; *Engelhardt/Klein,* MMR 2014, 355; *Boehm/Pesch,* MMR 2014, 75; *Kuhlmann,* CR 2014, 691, 692; *Bollen,* JBFLP 2013 (1.5.2013), 1, 9; *Djazayeri*, jurisPR-BKR 6/2014 Anm. 1, S. 1; *Kaplanov,* TLR 2012 (31.3.2012), 1, 4.

Smartphone), das einen sog. Full-Client (also das umfassendste Endnutzer-Programm zum Zugriff auf das Bitcoin-Netzwerk) installiert hat, speichert fortlaufend die gesamte Transaktionslegende, die sog. Blockchain.[18] Damit fungiert jeder Full-Client-Teilnehmer prinzipiell gleichzeitig als Server für das Bitcoin-Netzwerk.

2. Öffentliche und private Schlüssel

Innerhalb dieses Netzwerks kreiert jeder Client eines oder mehrere (beliebig viele[19]) Schlüsselpaare.[20] Die Schlüssel eines Paares stehen zueinander in einem speziellen Verhältnis und dienen zur Verwaltung der Bitcoins.[21] Der öffentliche Schlüssel jedes Schlüsselpaares dient dabei als eine Art Kontonummer.[22] Dieser Kontonummer kann im Netzwerk ein bestimmter Wert in Bitcoins zugewiesen werden. Der private Schlüssel eines jeden Schlüsselpaares dient zur Autorisierung einer Transaktion (= Überweisung) von dem dazugehörigen öffentlichen Schlüssel.[23] Man könnte die mit dem privaten Schlüssel erzeugte digitale Signatur somit in etwa mit der Unterschrift auf einem Überweisungsträger bzw. mit dem TAN-Verfahren des Online-Bankings vergleichen.[24] Die Nutzer können nun im Netzwerk von ihrem öffentlichen Schlüssel eine Transaktion der ihrem öffentlichen Schlüssel zugewiesenen Bitcoins an einen oder mehrere andere öffentliche Schlüssel vornehmen.

3. Die Blockchain

Dabei könnte jedoch durch mehrfache Autorisierung mit einem privaten Schlüssel und mangels Überprüfung durch eine zentrale Stelle der Inhaber eines Bitcoins den „selben" Bitcoin mehrfach an verschiedene Empfänger-Adressen (öffentliche Schlüssel) überweisen (sog. „double spending"-Problem).[25] Dieses Problem löst das Bitcoin-Konzept, indem der Überweisende seine Transaktionsdaten an alle Teilnehmer des Netzwerks sendet, welche alle erhaltenen Transaktionsdaten in Datenblöcken sammeln und dann (freiwillig) versuchen können, mit ihrem Rechner ein kompliziertes mathematisches Problem zur Bestätigung der Datenblöcke und damit der in ihnen enthaltenen Transaktionen (proof-of-work) zu errechnen.[26] Derjenige Teilnehmer, der als erstes das Problem gelöst hat, schickt den so bestätigten Datenblock wieder an alle anderen Teilnehmer, die dann ihrerseits den errechneten Block bestätigen müssen[27] und wieder versuchen können, weitere Blöcke mit neuen Transaktionen zu errechnen.[28] Da jeder Datenblock mathematisch mit dem vorherigen Datenblock verknüpft ist, entstehen so Ketten von Datenblöcken (sog. Blockchain).[29] Nur die längste dieser Ketten wird vom Netzwerk als die korrekte Transaktionskette akzeptiert.[30] Der längsten Kette widersprechende Transaktionen, die in anderen, kürzeren Ketten enthalten sind, sind somit im Netzwerk ungültig und werden so behandelt, als hätten sie nie stattgefunden. Da es mit fortschreitender Länge der Blockchain somit exponentiell unwahrscheinlicher wird, dass eine in ihr enthaltene Transaktion nachträglich als ungültig angesehen wird und es auch für Hacker exponentiell schwieriger wird, die Berechnungen anzustellen, die nötig wären, um eine in der Blockchain enthaltene Transaktion nachträglich zu verändern, sieht das Bitcoin-Netzwerk im Allgemeinen eine Transaktion erst als vollständig abgeschlossen an, wenn auf dem Block, in dem sie enthalten ist, noch mindestens sechs weitere Blöcke aufbauen.[31] Zusammenfassend lässt sich sagen, dass das gesamte P2P-Netzwerk somit fortlaufend anhand der Blockchain nachprüft, ob die nun überwiesenen Bitcoins vom Inhaber des öffentlichen Schlüssels schon einmal überwiesen wurden.[32]

4. Öffentlichkeit der Blockchain – Pseudonymität der Nutzer

Die Blockchain ist also letztlich eine vollständige Auflistung sämtlicher jemals getätigter, verifizierter Bitcoin-Transaktionen.[33] Diese Liste wird nicht nur auf sämtlichen Full-Clients des Bitcoin-Netzwerks fortlaufend gespeichert[34], sondern kann auch öffentlich im Internet – z.B. auf www.blockchain.info – eingesehen werden.[35] Da jedoch nur der Inhaber eines öffentlichen Schlüssels weiß, welche Person hinter diesem Schlüssel steckt, kann kein Rückschluss auf die beteiligten Personen gezogen werden.[36] Denn jeder Client kann beliebig viele öffentliche Schlüssel erzeugen[37] und es ist keine Identifizierung in der Realwelt[38] (wie z.B. bei der Eröffnung eines Kontos bei einer Bank) erforderlich (kein sog. „know your customer" – KYC). Die erzeugten privaten Schlüssel werden digital in sog. „wallets" verwahrt und dienen damit als „Geldbörse" im Bitcoin-Netzwerk. Man kann sich die „wallet" als Sammlung von Schlüsseln zu Schließfächern (die öffentlichen Schlüssel) vorstellen, welche somit den gesamten Betrag der Bitcoins „enthalten", den öffentlichen Schlüsseln des jeweiligen Nutzers zugewiesen sind.[39]

5. Erwerb von Bitcoins durch Kauf oder Mining

Bitcoins können von den Nutzern auf verschiedene Arten erworben werden. Zum einen existieren Tauschbörsen, bei welchen „echtes" Geld in Bitcoins gewechselt werden kann. Zum anderen erhalten Netzwerkteilnehmer, welche die Rechenkapazität ihres Endnutzergeräts zur Verfügung stellen, um den „proof-of-work" für neue Transaktionsblöcke zu berechnen und diese an die Blockchain anzuhängen (sog. „mining"[40] (= schürfen))[41], zur Belohnung eine bestimmte Menge neu entstehender Bitcoins (und evtl. Transaktionsgebühren von den anderen Bitcoin-Nutzern) gutgeschrieben.[42] Die Errechnung des „proof-of-work" ist so konzipiert, dass in regelmäßigen Zeitabschnitten ein Block errechnet wird. Da sich die verfügbare Rechenleistung ständig ändern kann, wird durch einen Regelkreis die Schwierig-

18 *Bollen,* JBFLP 2013 (v. 1.5.2013), 1, 9 f.
19 *Spindler/Bille,* WM 2014, 1357, 1358.
20 *Kaplanov,* TLR 2012 (v. 31.3.2012), 1, 5; *Sorge/Krohn-Grimberghe,* DuD 2012, 479, 480; *Kütük/Sorge,* MMR 2014, 643.
21 *Kaplanov,* TLR 2012 (v. 31.3.2012), 1, 5; *Sorge/Krohn-Grimberghe,* DuD 2012, 479, 480; *Kütük/Sorge,* MMR 2014, 643.
22 *Djazayeri*, jurisPR-BKR 6/2014 Anm. 1, S. 2; *Sorge/Krohn-Grimberghe,* DuD 2012, 479, 480; *Boehm/Pesch,* MMR 2014, 75, 76.
23 *Sorge/Krohn-Grimberghe,* DuD 2012, 479, 480; *Kütük/Sorge,* MMR 2014, 643.
24 Vgl. *Boehm/Pesch,* MMR 2014, 75, 76.
25 Vgl. *Sorge/Krohn-Grimberghe,* DuD 2012, 479, 480; *Spindler/Bille,* WM 2014, 1357, 1358; *Kütük/Sorge,* MMR 2014, 643.
26 *Sorge/Krohn-Grimberghe,* DuD 2012, 479, 480; *Nakamoto* (o. Fußn. 14), S. 3; *Spindler/Bille,* WM 2014, 1357, 1358; *Boehm/Pesch,* MMR 2014, 75, 76.
27 *Antonopoulos,* Mastering Bitcoin, Chap. 8, abrufbar unter: http://chimera.labs.oreilly.com/books/1234000001802/index.html.
28 *Sorge/Krohn-Grimberghe,* DuD 2012, 479, 480; *Spindler/Bille,* WM 2014, 1357, 1358.
29 *Sorge/Krohn-Grimberghe,* DuD 2012, 479, 480.
30 *Sorge/Krohn-Grimberghe,* DuD 2012, 479, 480; *Antonopoulos* (o. Fußn. 27).
31 *Antonopoulos* (o. Fußn. 27), Chap. 2 (Überblick), Chap. 8 (technische Details).
32 *Boehm/Pesch,* MMR 2014, 75, 76; *Kütük/Sorge,* MMR 2014, 643, 644.
33 *Spindler/Bille,* WM 2014, 1357, 1358: „Kassenbuch"; *Boehm/Pesch,* MMR 2014, 75, 76: „Kontobuch".
34 *Kaplanov,* TLR 2012 (31.3.2012), 1, 6; *Sorge/Krohn-Grimberghe,* DuD 2012, 479, 480.
35 *Djazayeri*, jurisPR-BKR 6/2014 Anm. 1, S. 2; *Grinberg,* HSTLJ – Hastings Science & Technology Law Journal 2011 (9.12.2011), 159, 164 f.; *Boehm/Pesch,* MMR 2014, 75, 76.
36 *Nakamoto* (o. Fußn. 14), S. 6; *Grinberg,* HSTLJ 2011 (v. 9.12.2011), 159, 164 f.
37 *Boehm/Pesch,* MMR 2014, 75, 76.
38 *Bollen,* JBFLP 2013 (v. 1.5.2013), 1, 7; *Boehm/Pesch,* MMR 2014, 75, 76.
39 Es sei noch einmal daran erinnert, dass in den „wallets" nicht die Bitcoins als Datenmenge gespeichert sind, sondern nur die Schlüssel, um über die zugewiesenen Bitcoins verfügen zu können; vgl. auch *Spindler/Bille,* WM 2014, 1357, 1358.
40 Der Begriff ist an die Goldschürfer angelehnt, die durch ihre Tätigkeit neues Gold in den Wirtschaftskreislauf speisen, vgl. *Nakamoto* (o. Fußn. 14), S. 4.
41 *Spindler/Bille,* WM 2014, 1357, 1358.
42 *Spindler/Bille,* WM 2014, 1357, 1358; *Kaplanov,* TLR 2012 (v. 31.3.2012), 1, 8; *Sorge/Krohn-Grimberghe,* DuD 2012, 479, 480; *Boehm/Pesch,* MMR 2014, 75, 76; *Kütük/Sorge,* MMR 2014, 643.

keit regelmäßig angepasst, sodass ungefähr alle 10 Minuten ein Block gefunden werden kann.[43] Die Gesamtmenge der zu „minenden" Bitcoins ist zur Vermeidung von Inflation auf 21 Mio. Bitcoins begrenzt.[44]

6. Attraktivität des Bitcoin-Systems für kriminelle Nutzer

Für Nutzer mit kriminellen Absichten sind das Fehlen eines KYC-Systems und die Pseudonymität (§ 3 Abs. 6a BDSG)[45], ermöglicht durch die Verwendung der öffentlichen Schlüssel als „Kontonummer", besonders attraktiv. Die Verwendung des Tor-Netzwerks[46] sowie von Bitcoin-Mixern[47] (Programme, welche die Zuordnung von Bitcoins verschleiern, indem mehrere Bitcoins von verschiedenen Nutzern gesammelt werden und nach dem Zufallsprinzip wieder auf die Empfänger verteilt werden[48]) und das ständige Wechseln der verwendeten Bitcoin-Adressen[49] (öffentliche Schlüssel) erschweren zusätzlich die Nachverfolgbarkeit. Selbst der Eintausch von Bitcoins in „echtes" Geld ist weltweit – und damit fernab nationaler Strafverfolgungsbefugnisse – und dank Netzwerken wie „local bitcoins"[50] auch unproblematisch zwischen Privatleuten gegen Bargeld möglich.[51]

III. Auswirkungen der technischen Funktionsweise auf „klassische" Fahndungsmethoden

Für Strafverfolger stellt – neben der Pseudonymisierung – vor allem die Dezentralisierung und das damit einhergehende Fehlen eines KYC-Systems eine neue Herausforderung dar. Bei Ermittlungen im Bereich des „normalen" Bankings können die Ermittler die nach § 24c KWG pflichtmäßig zu speichernden Bestandsdaten der Kontoinhaber bei den Banken durch Herausgabeverlangen nach §§ 161, 95 StPO[52] oder durch eine Auskunft nach § 24c Abs. 3 Nr. 2 Alt. 2 KWG erlangen. Als schwerwiegendere Maßnahmen stehen daneben noch die Durchsuchung in den Geschäftsräumen der Bank mit anschließender Beschlagnahme der Bestandsdaten nach den §§ 103, 105, 94 StPO sowie die Befragung von Bankmitarbeitern als Zeugen zur Verfügung. All diese Fahndungsinstrumente stehen den Ermittlern mangels zentraler, verwaltender Stelle bei Ermittlungen im Bitcoin-Bereich im Regelfall[53] nicht zur Verfügung. Insbesondere kommt auch eine „Beschlagnahme" von Daten aus der Blockchain nach den §§ 94 ff. StPO mangels verwaltender Stelle als Adressat einer solchen offenen Maßnahme nicht in Betracht.

IV. Überwachung und Auswertung der Transaktionen in der Blockchain

Einen möglichen Ausweg bietet die öffentliche Zugänglichkeit der gesamten Blockchain. Da diese offen im Internet einsehbar ist[54], können alle Transaktionen zurückverfolgt werden. Auf diese kann entweder über die Internetseite www.blockchain.info zugegriffen werden oder der Ermittler lädt sich einen sog. Full-Client der Bitcoin-Software herunter, da dieser die Blockchain fortlaufend vollständig herunterlädt und als Teil des P2P-Netzwerks speichert.[55] Wegen der Pseudonymisierung können die Ermittler zwar zunächst nur die öffentlichen Bitcoin-Adressen der beteiligten Personen und den Betrag der überwiesenen Bitcoins auslesen.[56] Es ist jedoch denkbar, Methoden zu entwickeln, die eine Verknüpfung dieser Informationen aus der Blockchain mit weiteren, außerhalb der Blockchain liegenden Informationen ermöglichen und so Rückschlüsse auf die beteiligten realen Personen, deren Identitäten und möglicherweise strafrechtlich relevante Sachverhalte zulassen.[57] Auch sind manuelle oder automatisierte Merkmalerkennungsmethoden denkbar, die einen Anfangsverdacht oder zusätzliche Informationen zu laufenden Ermittlungsverfahren aus der Blockchain gewinnen können.[58] Neben den zu überwindenden technischen Schwierigkeiten stellt sich in diesem Zusammenhang – unabhängig von der konkreten Ausgestaltung möglicher Fahndungsinstrumente – die Frage, ob die fortlaufend im P2P-Netzwerk weiterberechnete und gespeicherte Blockchain unter die TK-Begriffe der Art. 10 Abs. 1 GG, § 100a StPO, § 3 Nr. 22 TKG zu subsumieren ist.

V. Folgerungen aus einer Anwendbarkeit des § 100a StPO

Würde nämlich die heimliche Überwachung und Auswertung der Blockchain dem Anwendungsbereich des § 100a StPO unterfallen, so ergäben sich erhebliche Schwierigkeiten für die Fahndung. Wegen des abschließenden Charakters der Regelung des § 100a StPO für heimliche Eingriffe in die TK-Freiheit[59] müsste sich jede neue Fahndungsmethode an dieser Vorschrift messen lassen. Ein Rückgriff auf andere Normen oder die Generalklauseln der §§ 161, 163 StPO wäre nicht möglich. Da § 100a StPO an enge Anwendungsvoraussetzungen gebunden ist[60], wären neuen Ermittlungsmethoden (zu) enge Grenzen gesetzt. Ihre Effektivität wäre in Frage gestellt. Insbesondere können Ermittlungsmaßnahmen nach § 100a StPO nur gegen bestimmte Einzelpersonen gerichtet werden.[61] Zwar kommen neben dem Beschuldigten auch nicht verdächtige Personen als Betroffene einer solchen Anordnung in Betracht, allerdings nur, wenn auf Grund bestimmter Tatsachen anzunehmen ist, dass die nicht verdächtigen Betroffenen für den Beschuldigten bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder dass der Beschuldigte ihren Anschluss benutzt (§ 100a Abs. 3 StPO).[62] Damit wären sämtliche neuen

43 Vgl. auch *Kütük/Sorge,* MMR 2014, 643.
44 *Spindler/Bille,* WM 2014, 1357, 1358; *Kaplanov,* TLR 2012 (v. 31.3.2012), 1, 8.
45 Vgl. zur Terminologie *Härting,* NJW 2013, 2065, 2066.
46 Überblick zum Tor-Netzwerk bei *Thiesen,* MMR 2014, 803.
47 Z.B.: Bitcoin Fog, BitLaundry oder die „Send Shared"-Funktion von Blockchain.info, vgl. *Möser/Böhme/Breuker,* An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem, abrufbar unter: https://maltemoeser.de/paper/money-laundering.pdf; *Boehm/Pesch,* MMR 2014, 75, 76 Fußn. 12.
48 Vgl. *Spindler/Bille,* WM 2014, 1357, 1359.
49 *Spindler/Bille,* WM 2014, 1357, 1359; *Sorge/Krohn-Grimberghe,* DuD 2012, 479, 480.
50 https://localbitcoins.com/. Die Seite ist jedoch nicht mehr von Deutschland aus abrufbar, vgl. hierzu: http://bitcoinblog.de/2014/12/08/localbitcoins-aus-grunden-der-regulierung-nicht-mehr-in-deutschland-verfugbar/ .
51 Vgl. *Boehm/Pesch,* MMR 2014, 75, 76.
52 Zu diesem – nicht explizit geregelten – Herausgabeverlangen, das – anders als die Beschlagnahme nach § 98 StPO – nach strittiger Ansicht einiger Instanzgerichte auch StA und Polizei auch ohne Gefahr im Verzug stellen können, vgl. *Schmitt* (o. Fußn. 2), § 95 Rdnr. 1 f.; sowie restriktiv: *Singelnstein*, NStZ 2012, 593, 603.
53 Vereinzelte kommerzielle Dienstleistungsanbieter wie z.B. bitcoin.de haben ein eigenes KYC-System eingeführt und kooperieren auch mit den Ermittlungsbehörden, vgl. § 10 der AGB von bitcoin.de, abrufbar unter: https://www.bitcoin.de/de/agb. Dies betrifft aber nur einen kleinen Teil der Nutzer und vor allem wohl eher die „legalen" Nutzer; vgl. zur Anwendbarkeit des GwG auf kommerzielle Anbieter im Bitcoin-Bereich *Spindler/Bille,* WM 2014, 1357, 1366 f.
54 www.blockchain.info
55 Idealerweise noch kombiniert mit einem lokalen Blockchain-Explorer zur grafischen Aufbereitung der Blockchain-Daten, wie z.B. *Abe* (abrufbar unter: https://github.com/bitcoin-abe/bitcoin-abe) oder *insight* (abrufbar unter: https://github.com/bitpay/insight).
56 Zur Analyse des Transaktionsgrafen der Blockchain: *Ober/Katzenbeisser/Hamacher,* Structure and Anonymity of the Bitcoin Transaction Graph, abrufbar unter: http://www.mdpi.com/1999-5903/5/2/237.
57 Vgl. zu einer solchen Idee: *Reid/Harrigan*, An Analysis of Anonymity in the Bitcoin System, in: Altshuler/Elovici/Cremers/Aharony/Pentland (Hrsg.), Security and Privacy in Social Networks, S. 197, 210 ff.
58 S. als Beispiel für eine solche Idee: *Fleder/Kester/Pillai*, Bitcoin Transaction Graph Analysis, abrufbar unter: http://people.csail.mit.edu/spillai/data/papers/bitcoin-project-paper.pdf.
59 BGHSt 31, 304, 306; BGHSt 34, 39, 50; *Schmitt* (o. Fußn. 2), § 100a Rdnr. 2.
60 *Schmitt* (o. Fußn. 2), § 100a Rdnr. 9 ff.
61 *Schmitt* (o. Fußn. 2), § 100a Rdnr. 16.
62 Vgl. auch *BVerfG* MMR 2007, 500; *LG Hamburg* StV 2009, 236.

Fahndungsinstrumente darauf beschränkt, die Transaktionen von Tatverdächtigen oder den oben beschriebenen nicht Tatverdächtigen im Einzelfall auf Grund besonderer, gerichtlicher (§ 100b Abs. 1 StPO) Anordnung zu überwachen und auszuwerten, und dies auch nur, wenn die übrigen Voraussetzungen des § 100a StPO wie z.B. das Vorliegen einer Katalogtat nach Absatz 2 bejaht werden können.

VI. Der Schutzbereich des Art. 10 Abs. 1 GG und die Reichweite von § 100a StPO

Um entscheiden zu können, ob § 100a StPO die einschlägige Ermächtigungsnorm ist, ist zu klären, was § 100a StPO überhaupt mit „Telekommunikation" meint.

1. Technischer und normativer TK-Begriff

Der Begriff taucht außer in § 100a StPO noch in § 1 des G10 auf und wird in § 3 Nr. 22 TKG definiert. Danach ist Telekommunikation der technische Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels TK-Anlagen. Dieser rein technische TK-Begriff hilft indes für die Definition des Schutzbereichs einer Ermächtigungsgrundlage nicht weiter. Es geht bei § 100a StPO demnach (wie in § 1 des G10)[63] vielmehr um Grundrechtsträger und deren Schutzbedürftigkeit auf Grund der Einschaltung Dritter in einen vertraulichen Kommunikationsvorgang.[64] Namentlich steht der Schutz des Fernmeldegeheimnisses, das in Art. 10 GG verfassungsrechtlich gesondert geschützt ist, bei der Eingriffsbefugnis im Vordergrund. Auch wenn nach der neueren Rechtsprechung des *BVerfG* eine gewisse „Aufweichung" der Verbindung zwischen Art. 10 Abs. 1 GG und § 100a StPO in der Art zu beobachten ist, dass strafprozessuale Eingriffe, wenn sie offen und punktuell erfolgen, auch an §§ 94 ff. StPO gemessen werden können[65], hat die Schutzbereichsbestimmung des Art. 10 Abs. 1 GG doch immer noch große Bedeutung für die Auslegung des § 100a StPO. Denn die strengen Voraussetzungen des § 100a StPO sollen gerade der großen Intensität heimlicher Eingriffe in das TK-Geheimnis Rechnung tragen.[66] Danach soll gewährleistet sein, dass der Rechtsunterworfene frei kommunizieren kann, und zwar auch dann, wenn er technische Hilfsmittel zur Kommunikation verwendet, die er nicht selbst kontrollieren kann, deren Abläufe er im Einzelnen auch gar nicht nachvollziehen kann.[67] Das Fernmeldegeheimnis schützt demnach die unkörperliche Übermittlung von Informationen an individuelle Empfänger mit Hilfe des TK-Verkehrs, also auch mittels Kommunikationsdiensten des Internets.[68]

2. Nur laufende Kommunikation geschützt

Art. 10 Abs. 1 GG ist aber nur eröffnet, solange auch der Kommunikationsvorgang läuft. Ist dieser Übertragungsvorgang abgeschlossen und sind die Inhalte im Herrschaftsbereich eines Kommunikationsteilnehmers[69] gespeichert, liegt der Grundrechtsschutz von Art. 10 Abs. 1 GG nicht mehr vor.[70] Werden demnach Speichermedien im Herrschaftsbereich des Kommunikationsteilnehmers überwacht oder durchsucht, bedarf es keiner Ermächtigung nach § 100a StPO. Diese lebt auch dann nicht wieder auf, wenn die Überwachung oder Durchsuchung über eine TK-Verbindung etwa in der Form eines Online-Zugriffs durchgeführt wird.[71] In einem solchen Fall ist das Vertrauen des Rechtsunterworfenen in die unbeschwerte Kommunikation mit technischen Mitteln nicht gestört.

3. Kein Schutz öffentlich geführter Kommunikation

Kein Fall des § 100a StPO liegt ferner vor, wenn die Kommunikation für jedermann zugänglich, öffentlich geführt wird, unabhängig davon, ob sie mit TK-Mitteln durchgeführt wird. Der Meinungsaustausch z.B. in einem öffentlichen Chatroom basiert deshalb nicht auf wechselseitiger Vertraulichkeit der Kommunikationsteilnehmer und kann von Strafverfolgern entsprechend ohne Ermächtigung nach § 100a StPO gelesen und verwertet werden. Gleiches gilt für den Abruf sonstiger öffentlich zugänglicher Informationen auf Internetseiten.[72] Hier gibt es keinen Unterschied etwa zu einem in Printmedien veröffentlichten Artikel oder Leserbrief. Der Begriff der Telekommunikation ist deshalb nicht rein technisch zu verstehen, sondern ist insoweit normativ überlagert, als es maßgeblich auf die erwartete Vertraulichkeit des Kommunikationsmediums ankommt.[73]

4. Recht auf informationelle Selbstbestimmung

Ist aber der Schutzbereich von Art. 10 Abs. 1 GG nicht eröffnet, ist die Kommunikation damit grundrechtlich nicht vollkommen schutzlos. Vielmehr treten nun das Recht auf freie Entfaltung der Persönlichkeit und das Recht auf informationelle Selbstbestimmung auf den Plan. Auch hier gilt, dass die reine Wahrnehmung und Erhebung von frei verfügbarer Information im Internet durch staatliche Behörden grundsätzlich keinen Grundrechtseingriff darstellen.[74] Eine besondere Gefahrenlage für die Persönlichkeit des Betroffenen ergibt sich erst dann, wenn Inhalte, seien sie auch allgemein zugänglich, gezielt zusammengetragen, gespeichert und durch Abgleich mit anderen Daten ausgewertet werden.[75] So lassen sich Rückschlüsse auf das Kommunikationsverhalten, auf die sozialen Kontakte, das Kaufverhalten und die Vermögensverhältnisse des Betroffenen insgesamt generieren.[76] So wird zwar nicht durch die einzelne Information, aber durch das gezielte Verknüpfen der verfügbaren Informationen der Mensch für den Staat – zumindest partiell – transparent. Dies bedeutet einen Eingriff in die informationelle Selbstbestimmung des Betroffenen und bedarf einer Ermächtigungsgrundlage.[77]

VII. Überwachung und Auswertung der Blockchain als TKÜ i.S.v. § 100a StPO?

Fraglich ist nach alledem, ob eine Überwachung und/oder Auswertung der Daten aus der Blockchain ein Eingriff ist, der sich an § 100a StPO messen lassen muss. Auf den ersten Blick scheint einiges für eine Einordnung einer Transaktion in der Blockchain

63 § 1 des G10-Gesetzes (G10) bringt den Begriff der „Telekommunikation", in die durch Nachrichtendienste auf der Grundlage dieses Gesetzes eingegriffen werden kann. Der Unterschied zu § 100a StPO besteht nur im Anlass. Während das G10 auf nachrichtendienstliche Informationsbeschaffung bezogen ist, dient § 100a StPO der Beweisgewinnung zur Strafverfolgung.

64 BVerfGE 124, 43, 55 f. = MMR 2009, 673, 675; vgl. auch BVerfGK 9, 62, 75 = MMR 2006, 805, 806.

65 BVerfGE 124, 43, 58, 62 f., 65 = MMR 2009, 673, 676 f.

66 So auch *Schmitt* (o. Fußn. 2), § 100a Rdnr. 1 ff.; *Graf* (o. Fußn. 6), § 100a Rdnr. 6 ff.; *Bruns* (o. Fußn. 6), § 100a Rdnr. 1 f.

67 Vgl. *Schmitt* (o. Fußn. 2), § 100a Rdnr. 1.

68 Vgl. BVerfGE 115, 166, 182 = MMR 2006, 217, 219; BVerfGE 124, 43, 54 = MMR 2009, 673, 674.

69 Anders ist dies, wenn die Daten außerhalb des Herrschaftsbereichs eines Kommunikationsteilnehmers gespeichert sind, vgl. BVerfGE 124, 43, 54 = MMR 2009, 673, 674.

70 BVerfGE 120, 274, 307 f. = MMR 2008, 315, 316; BVerfGE 115, 166, 183 f. = MMR 2006, 217, 219 f.

71 Klarstellend: BVerfGE 120, 274, 308 = MMR 2008, 315, 316 f.

72 Zum Ganzen: BVerfGE 120, 274, 341 = MMR 2008, 315, 324; BT-Drs. 16/5846, S. 64; *Kudlich,* StV 2012, 560, 566; *Schmitt* (o. Fußn. 2), § 100a Rdnr. 7 m.w.Nw.

73 Nur zur Klarstellung sei erwähnt, dass es hier nicht um das Vertrauen in den jeweiligen Kommunikationspartner geht, sondern um das Vertrauen in den Übertragungsvorgang selbst. Das Vertrauen in den Gesprächspartner ist nach BGHSt 42, 139, 154 gerade nicht geschützt.

74 Vgl. BVerfGE 120, 274, 344 f. = MMR 2008, 315, 325; *Singelnstein*, NStZ 2012, 593, 599 f.

75 Vgl. BVerfGE 120, 274, 345 = MMR 2008, 315, 325.

76 Vgl. BVerfGE 118, 168, 185 f.

77 BVerfGE 120, 274, 345 = MMR 2008, 315, 325; *Singelnstein*, NStZ 2012, 593, 600.

unter den TK-Begriff zu sprechen, handelt es sich doch um eine Übertragung von Daten über das TK-Medium Internet.

1. Heimlicher Zugriff auf laufende Kommunikation

Dabei kommt es zunächst auch nicht auf den Zeitpunkt an, in dem der Ermittler von der Transaktion Kenntnis nimmt. Eine Bitcoin-Transaktion wird über Internetseiten wie www.blockchain.de in dem Moment öffentlich sichtbar, in dem sie ins Bitcoin-Netzwerk geschickt wird. Wegen des „double spending"-Problems und möglicher Hackerangriffe wird eine Transaktion jedoch im Regelfall erst nach dem Anhängen von mindestens sechs weiteren Datenblöcken als Erfüllung akzeptiert.[78] Die fortlaufende Erweiterung der Blockchain kann somit wegen der damit einhergehenden, fortlaufend größer werdenden Vertrauenswürdigkeit der in ihr enthaltenen Transaktionen als laufende Internetkommunikation auch bzgl. der Transaktionen betrachtet werden, die bereits in der Blockchain eingebettet sind. Selbst wenn man dies anders sehen würde, ist es nach dem modernen, normativ geprägten TK-Begriff nicht mehr entscheidend, dass auf Daten während eines laufenden Übertragungsvorgangs zugegriffen wird, sondern vielmehr, ob sich die Daten bereits im Herrschaftsbereich eines TK-Teilnehmers befinden. Damit sind auch außerhalb eines solchen Herrschaftsbereichs gespeicherte Daten – wie die Daten in der Blockchain – vom modernen TK-Begriff des Art. 10 Abs. 1 GG und des § 100a StPO erfasst.[79] Dass das *BVerfG* §§ 94 ff. StPO als taugliche Eingriffsnormen für die Beschlagnahme von beim Service-Provider (und damit außerhalb des Herrschaftsbereichs eines Teilnehmers) gespeicherten E-Mails ansieht[80], ändert nichts daran, dass die E-Mails grundsätzlich auch den TK-Begriff von Art. 10 Abs. 1 GG und § 100a StPO erfüllen.[81] Die §§ 94 ff. StPO kamen in der o.g. Entscheidung nur deswegen in Betracht, weil die Beschlagnahme offen erfolgte. Für einen heimlichen Zugriff auf Daten außerhalb des Herrschaftsbereichs eines Kommunikationsteilnehmers verbleibt es bei den hohen Anforderungen des § 100a StPO.[82] Eine offene Beschlagnahme der Daten aus der Blockchain kommt mangels zentraler, verwaltender Stelle jedoch nicht in Betracht. Anzumerken ist an dieser Stelle noch, dass es sich bei dem Zugriff auf die in der Blockchain „gespeicherten" Daten auch nicht um eine unzulässige, verdeckte „Online-Durchsuchung" handelt.[83] Denn anders als bei der Online-Durchsuchung, bei der mittels einer Schadsoftware auf den PC und damit in den Herrschaftsbereich des Betroffenen und nicht in einen TK-Vorgang eingegriffen wird[84], wird beim Zugriff auf die Daten in der Blockchain auf einen außerhalb des Herrschaftsbereichs eines Kommunikationsbeteiligten liegenden Datenbestand zugegriffen.

2. Vermögensübertragung als Kommunikation

Weiterhin schadet es im Hinblick auf den TK-Begriff auch nicht, dass es sich bei den übertragenen Daten überwiegend um Vermögensübertragung und nicht um die Übermittlung „klassischer" Nachrichten handelt. Dies ergibt sich zum einen daraus, dass es auf Grund der vorhandenen technischen Möglichkeiten zur Datenverknüpfung kaum noch nicht personenbezogene Daten gibt.[85] Insbesondere lassen sich aus dem Empfänger der Transaktion (sofern dieser de-pseudonymisiert werden kann) Rückschlüsse auf das Privatleben des Überweisenden ziehen.[86] Folgerichtig muss also auch der TK-Begriff dahingehend ausgelegt werden, dass es nicht mehr primär auf die Übermittlung von klassischen Nachrichten ankommt, sondern jegliche Übermittlung von Daten ausreicht.[87] Zum anderen ist es technisch möglich, neben den typischen Transaktionsdaten auch noch weitere Daten beliebigen Inhalts an einer Transaktion anzuhängen und somit in die Blockchain einzubetten, sodass in der Blockchain auch „klassische" Nachrichteninhalte zu finden sind.[88]

3. Transaktionsempfänger als Kommunikationsempfänger

Obwohl in Art. 10 Abs. 1 GG und § 100a StPO mit Telekommunikation die Datenübermittlung an einen oder mehrere individuelle Empfänger gemeint ist[89], schadet es an dieser Stelle noch nicht, dass die Blockchain-Daten insgesamt öffentlich eingesehen werden können. Denn trotz der Möglichkeit anderer Internetnutzer (inklusive der Ermittlungsbehörden), jede beliebige Transaktion der Blockchain einzusehen, lässt sich doch der Empfänger der Transaktion klar als der individuelle Empfänger der Daten ansehen. Denn zum einen ist er es, der den konkreten Nutzen aus der Datensendung, nämlich die Verfügung über die transferierte Menge Bitcoins, ziehen soll. Zum anderen ist er es, der im Regelfall als einziger, abgesehen vom Überweisenden, Kenntnis davon hat, wer das Geld überweist und warum es überwiesen wird.[90]

4. Die Öffentlichkeit der Blockchain als entscheidendes Gegenargument

Das entscheidende Argument gegen eine Subsumtion von Überwachung und Auswertung der Blockchain durch Ermittlungsbehörden unter § 100a StPO ist die Öffentlichkeit der Blockchain. Wie oben bereits dargestellt, schützt Art. 10 Abs. 1 GG die erwartete Vertraulichkeit eines Kommunikationsvorgangs außerhalb der beherrschbaren Sphäre eines Kommunikationsteilnehmers. Auch die hohen Hürden des § 100a StPO finden ihre Begründung im heimlichen Zugriff auf Informationen, die von den Kommunikationsbeteiligten in der Erwartung der Vertraulichkeit der Übermittlung ausgetauscht wurden. Da jedoch ein Wesensmerkmal des Bitcoin-Systems die öffentliche Zurverfügungstellung der Transaktionslegende (Blockchain) als Ersatz für eine zentrale ausgebende und verwaltende Stelle ist, kann sich kein Teilnehmer darauf berufen, er sei von der Vertraulichkeit des Datenübertragungsvorgangs in der Blockchain ausgegangen. Die Wahrnehmung der Transaktionen durch die Teilnehmer des Bitcoin-Netzwerks ist gewollt, die Wahrnehmung durch die restliche Öffentlichkeit (über www.blockchain.info) ist zumindest allgemein bekannt. Insoweit besteht kein Unterschied zu sonstigen, in öffentlich zugänglichen Kommunikationsmedien veröffentlichten Nachrichten, mögen diese auch für individuelle Empfänger bestimmt sein (z.B. Posts in öffentlich zugänglichen Foren oder auf den (teil-)öffentlich einsehbaren Seiten sozialer Netzwerke).

5. Kein Eingriff in Art. 10 Abs. 1 GG und keine Anwendbarkeit des § 100a StPO

I.E. handelt es sich bei der Überwachung und Auswertung von Daten aus der Blockchain also weder um einen Eingriff in Art. 10

78 S. bereits oben detailliert unter II.; vgl. auch *Antonopoulos* (o. Fußn. 27), Chap. 2.

79 Vgl. hierzu die E-Mail-Entscheidung des *BVerfG* BVerfGE 124, 43, 55 f. = MMR 2009, 673, 675.

80 BVerfGE 124, 43, 58 ff. = MMR 2009, 673, 675 ff.

81 Für den TK-Begriff des Art. 10 Abs. 1 GG ausdrücklich: BVerfGE 124, 43, 55 f. = MMR 2009, 673, 675.

82 Vgl. BVerfGE 124, 43, 62 ff. = MMR 2009, 673, 677.

83 Hierzu BGHSt 51, 211 = MMR 2007, 237.

84 BGHSt 51, 211, Rdnr. 18 = MMR 2007, 237.

85 Vgl. BVerfGE 120, 274, 311 = MMR 2008, 315, 318; vgl. auch BVerfGE 65, 1, 45; BVerfGE 118, 168, 185 (für Kontodaten); BVerfGE 120, 378, 398 f. = MMR 2008, 308 f.

86 Dies kann sogar erheblich in die Privatsphäre eingreifen, man denke nur an eine Überweisung an einen Arzt oder Anwalt.

87 In diese Richtung: BVerfGE 124, 43, 54 = MMR 2009, 673, 674: „sämtliche Übermittlung von Informationen" und „privater, geschäftlicher, politischer oder sonstiger Natur" m.w.Nw. aus der Rspr.

88 Allerdings wird davon bislang nur wenig Gebrauch gemacht.

89 Vgl. BVerfGE 67, 157, 172; BVerfGE 106, 28, 35 f. = MMR 2003, 35, 36; BVerfGE 124, 43, 54 = MMR 2009, 673, 674 .

90 Dies ist jedoch keinesfalls zwingend, weil eine Transaktion auf Grund der Pseudonymität des öffentlichen Schlüssels auch möglich ist, ohne dass der Empfänger weiß, von wem oder warum das Geld überwiesen wurde.

Abs. 1 GG noch um einen solchen, der an § 100a StPO zu messen ist.

VIII. Ausblick: Eingriff in das Recht auf informationelle Selbstbestimmung und Heranziehung der §§ 161, 163 StPO

Die Verneinung eines Eingriffs in Art. 10 Abs. 1 GG hat, wie oben bereits gezeigt, noch nicht zur Folge, dass gar kein Grundrechtsschutz besteht. Im Falle eines gezielten Zusammentragens, Speicherns und der Auswertung durch einen Abgleich mit anderen personenbezogenen Daten liegt ein Eingriff in das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG vor. Ob ein solcher Eingriff konkret auf die Ermittlungsgeneralklauseln der §§ 161, 163 StPO gestützt werden kann, hängt vor allem von der jeweiligen Eingriffsintensität ab, da die §§ 161, 163 StPO nur geringfügige Grundrechtseingriffe erlauben[91]. Intensitätsbestimmende Faktoren können hierbei insbesondere die Heimlichkeit der Maßnahme[92], ihre Streubreite (also Erfassung auch nicht-tatverdächtiger Personen und Transaktionen)[93] und die Datenspeicherung „auf Vorrat"[94] sein. Eine detaillierte Darstellung weiterer möglicher Grundrechtseingriffe und die Anforderungen an eine zu schaffende Rechtsgrundlage müssen einem eigenen Beitrag vorbehalten bleiben.

Professor Dr. Christoph Safferling, LL.M. (LSE)
ist Inhaber des Lehrstuhls für Strafrecht, Strafprozessrecht, Internationales Strafrecht und Völkerrecht an der Friedrich-Alexander-Universität Erlangen-Nürnberg.

Ass. iur. Christian Rückert
ist wissenschaftlicher Mitarbeiter am Lehrstuhl für Strafrecht, Strafprozessrecht, Internationales Strafrecht und Völkerrecht an der Friedrich-Alexander-Universität Erlangen-Nürnberg.

Die Verfasser sind an dem vom Bundesministerium für Bildung und Forschung finanzierten Forschungsprojekt „Bitcrime" (www.bitcrime.de) beteiligt, das sich mit der Prävention und Strafverfolgung von Straftaten im Zusammenhang mit virtuellen Währungen beschäftigt.

91 BGHSt 51, 211, 218 = MMR 2007, 237, 239; *Hilger,* NStZ 2000, 563, 564; *Schmitt* (o. Fußn. 2), § 161 Rdnr. 1.
92 BVerfGE 118, 168, 197 f.; BVerfGE 120, 274, 325, 342, 348 = MMR 2008, 315, 320, 324; BGHSt 51, 211, Rdnr. 12 = MMR 2007, 237, 238.
93 BVerfGE 120, 274, 323; BVerfGE 125, 260, 318 = MMR 2010, 356, 360.
94 BVerfGE 125, 260, 316 f. (zwingende Erforderlichkeit vorher bestimmter Zwecke), 319 f. (Missbrauchspotenzial), 323 f. (Berücksichtigung bereits vorhandener Datensammlungen), 325 ff. (erforderliche Sicherheitsstandards) = MMR 2010, 356, 359 f.; BVerfGE 130, 151, 187 = MMR 2012, 410, 412.