Paulina Pesch, Rainer Böhme

Datenschutz trotz öffentlicher Blockchain?

Chancen und Risiken bei der Verfolgung und Prävention Bitcoin-bezogener Straftaten

In ihrem im Juli 2016 vorgestellten Vorschlag[1] zur Anpassung der Geldwäsche-Richtlinie[2] sieht die Europäische Kommission die Einbeziehung virtueller Währungen und damit von Bitcoins vor. Dies gibt Anlass, die Verfolgung und Prävention Bitcoin-bezogener Straftaten – mit besonderem Blick auf den Schutz personenbezogener Daten – näher zu beleuchten.

1 Problemaufriss

Das Bitcoin-System[3] ermöglicht Online-Transaktionen unter seinen Nutzern. Eine Besonderheit dieses Zahlungssystems liegt in seiner dezentralen Organisation. Dementsprechend ist es zur Nutzung des Systems nicht erforderlich, sich gegenüber einem zentralen Anbieter zu identifizieren. Dies macht das Bitcoin-System – und andere virtuelle Währungen[4] – auch für kriminelle Akteure attraktiv. Strafverfolger und Regulierer stellt die Neu- und Eigenartigkeit virtueller Währungen vor praktische und rechtliche Herausforderungen. Das Forschungsprojekt BITCRIME[5] hat sich deshalb die Entwicklung praktikabler Ansätze für die Verfolgung und Prävention von Kriminalität mit virtuellen Währungen zum Ziel gesetzt. Besonderes Augenmerk wird dabei auf die Interessen und den Schutz legitimer Nutzer gelegt. Dieser Beitrag stellt ausgewählte Ergebnisse des Projekts vor, wobei die in diesem Zusammenhang bislang kaum thematisierte[6] Datenschutz-Perspektive von Verfolgung und Regulierung Bitcoin-bezogener Straftaten besondere Berücksichtigung findet.

2 Funktionsweise des Bitcoin-Systems[7]

Das Verständnis der Datenschutzproblematik setzt ein Grundverständnis der Funktionsweise von Bitcoin voraus. Im Bitcoin-System haben Nutzer Adressen, denen Bitcoin-Guthaben zugeordnet sind. Die den eigenen Adressen zugeordneten Bitcoins lassen sich direkt an andere Nutzer transferieren. Die Nutzung des Bitcoin-Systems erfolgt im einfachsten Fall mit einem Bitcoin-Client. Das ist eine Software, in der Nutzer Bitcoin-Adressen selbst erzeugen sowie verwalten können und aus der heraus Bitcoin-Transaktionen angestoßen werden können. Eine Bitcoin-Transaktion besteht in der Regel aus der Nachricht, einen bestimmten Betrag an eine bestimmte Adresse zu übertragen. Bitcoin-Transaktionen strukturieren sich dabei in zwei Listen aus Referenzen, je eine für so genannte Eingänge und Ausgänge. Eingän-

1 Abrufbar unter http://ec.europa.eu/justice/criminal/document/files/aml-directive_en.pdf (letzter Abruf: 15.12.16). Im Folgenden ist vom Kommissionsvorschlag die Rede.

2 Richtlinie (EU) 2015/849 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung.

3 Dazu schon *Sorge/Krohn-Grimberghe*, DuD 2012, 479 ff.

4 Der Begriff der virtuellen Währung erfasst an sich auch zentrale virtuelle Währungen wie Linden Dollar oder WoW-Gold, meint aber hier nur dezentrale kryptographische Währungen. Der Währungsbegriff ist dabei pragmatisch, d.h. unabhängig von staatlichen Währungen zu verstehen. Die Definition gem. Art. 3 Nr. 18 des Kommissionsvorschlags (Fn. 1) reicht weiter.

5 Das Projekt wird vom BMBF im Zuge der Bekanntmachung „Zivile Sicherheit – Schutz vor organisierter Kriminalität" im Rahmen des Programms „Forschung für die zivile Sicherheit" der Bundesregierung gefördert. Homepage abrufbar unter https://www.bitcrime.de/deutschland/ (letzter Abruf: 15.12.16).

6 *Kaulartz*, CR 2016, 474, 479 f.

7 Erstmalig beschrieben in *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, abrufbar unter https://bitcoin.org/bitcoin.pdf (letzter Abruf: 15.12.16). Näher etwa *Tschorsch/Scheuermann*, IEEE (COMST) 2016, 2084 ff.; *Zohar*, CACM 09/2015, 104 ff.

Dr. Paulina Pesch

ist wissenschaftliche Mitarbeiterin am Institut für Wirtschaftsinformatik der Westfälischen Wilhelms-Universität Münster in der Forschungsgruppe IT-Sicherheit. Foschungsschwerpunkte: Dezentrale virtuelle Währungen, Internet- und IT-Recht.
E-Mail: paulina.pesch@uni-muenster.de

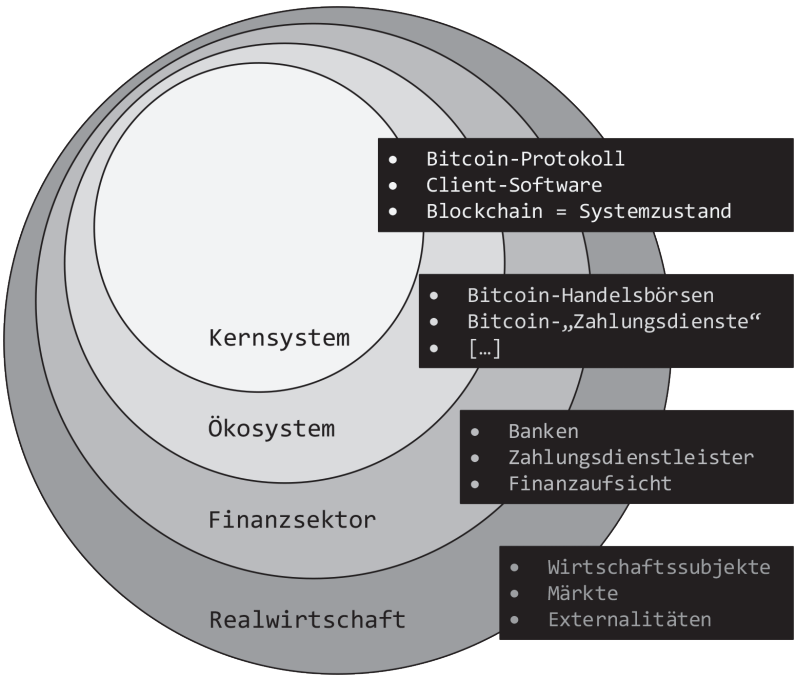
Prof. Dr. Rainer Böhme

ist Inhaber des Lehrstuhls für Security and Privacy am Institut für Informatik der Universität Innsbruck. Forschungsschwerpunkte: Digitale Forensik, virtuelle Währungen, Privacyenhancing technologies (PET), ökonomische Aspekte von Informationssicherheit und Privatheit, Cybercrime.
E-Mail: rainer.boehme@uibk.ac.at

ge verweisen auf die in Ausgängen vorhergehender Transaktionen enthaltenen Bitcoins des Senders. Ausgänge weisen Beträge der in eine Transaktion eingegangenen Bitcoins Zieladressen zu. Die Summe der Ausgangsbeträge darf die Summe der Eingangsbeträge nicht überschreiten.[8]

In Ermangelung einer zentralen Instanz, die Transaktionsaufträge entgegennimmt und die Guthaben der Nutzer anpasst, werden Bitcoin-Transaktionen an die anderen Nutzer des Systems verschickt und auch von diesen verarbeitet. Den Nachweis, dass er über die in den Eingängen referenzierten Bitcoins verfügt, erbringt der sendende Nutzer durch eine digitale Signatur, welche auf asymmetrischer Kryptographie beruht:[9] Jede Bitcoin-Adresse entspricht einem öffentlichen Schlüssel. Mit dem passenden (geheim zu haltenden) privaten Schlüssel werden Transaktionen signiert. Die Signatur lässt sich daraufhin mit dem öffentlichen Schlüssel überprüfen. Möchte ein Nutzer Bitcoins übertragen, die einer bestimmten Adresse zugeordnet sind, ist dies nur möglich, wenn er die Transaktion mit dem zur Adresse gehörenden privaten Schlüssel signiert.

Abb. 1 | Das Verhältnis von Bitcoin zur Realwirtschaft.[10]



Durch Signaturen allein lässt sich allerdings nicht ausschließen, dass der Nutzer dieselben Bitcoins mehrfach ausgibt. Diese Aufgabe, das Verhindern des so genannten *Double-Spending*, kommt im dezentralen Bitcoin-System der Gemeinschaft der Nutzer selbst zu. Sämtliche Nutzer müssen aller Transaktionen im System gewahr sein, um verhindern zu können, dass Transaktionen über bereits übertragene Bitcoins verarbeitet werden. Dafür werden alle Bitcoin Transaktionen in einer öffentlichen Datenstruktur gespeichert, der so genannten Blockchain. Die Blockchain ist auf den Rechnern aller Nutzer gespeichert und enthält die gesamte – unverschlüsselte – Transaktionshistorie seit Initialisierung des Bitcoin-Systems. Erst wenn eine Transaktion in die Blockchain aufgenommen worden ist, ist sie erfolgt. Aus der Blockchain ergibt sich, von welcher Bitcoin-Adresse wann welcher Bitcoin-Betrag an welche Zieladresse übertragen wurde. So lässt sich für jedermann jeder Bitcoin-Betrag beliebig weit zurückverfolgen.[10]

Die Blockchain wird von den Nutzern des Systems selbst fortgeschrieben, wobei zur Absicherung dieses Prozesses gegen Manipulationen ein Arbeitsnachweis („Proof of Work“) zu erbringen, also Rechenleistung aufzuwenden ist. Als Anreiz, die damit verbundenen Kosten aufzubringen, werden Nutzern, die die Blockchain fortschreiben, im Gegenzug Bitcoins gutgeschrieben. Die Gutschriften speisen sich aus neu geschöpften Geldeinheiten und gehen nach einem festgelegten Schema im Zeitverlauf auf Gebührenfinanzierung über. Nutzer, die sich an diesem Prozess beteiligen, bezeichnet man als Miner.

Erworben werden können Bitcoins aber insbesondere auch an speziellen Online-Handelsbörsen. Diese sind in der Regel zentral organisiert. Dasselbe ist der Fall bei allen Angeboten im um das Kernsystem entstandenen Bitcoin-Ökosystem (Abb. 1), zum Beispiel Bitcoin-Zahlungsdiensten, die für Händler „Zahlungen“ in Bitcoin entgegennehmen.[12]

3 Verfolgung und Prävention Bitcoin-bezogener Kriminalität

Die öffentliche Blockchain macht das Bitcoin-System in besonderem Maße transparent. Bei dieser Transparenz lässt sich sowohl bei der Verfolgung Bitcoin-bezogener Straftaten, als auch bei der Entwicklung präventiver Regulierungskonzepte ansetzen. Gleichzeitig gebietet die Transparenz des Systems die besondere Berücksichtigung des Schutzes personenbezogener Daten der Nutzer.

3.1 Personenbeziehbare Daten in der Blockchain

Die Relevanz des Datenschutzgrundrechts[13] für die staatliche Verfolgung und Prävention Bitcoin-bezogener Kriminalität ergibt sich aus der Blockchain, die mit der Transaktionshistorie des Bitcoin-Systems personenbezogene Daten enthält. Dabei handelt es sich nach der einfachgesetzlichen Definition aus § 3 Abs. 1 BDSG um *Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person*.[14] Mit den Trans-

8 Eine eventuelle Differenz wird als Transaktionsgebühr abgeführt.

9 Asymmetrische Kryptographie lässt sich einerseits zur Verschlüsselung von Nachrichten verwenden, andererseits zur Signierung von Nachrichten. U. a. weil Bitcoin und andere virtuelle Währungen digitale Signaturen nutzen, ist auch von kryptographischen Währungen die Rede. Bitcoin und die meisten anderen kryptographischen Währungen setzen aber keinerlei Verschlüsselung ein.

10 *Möser/Böhme/Breuker*, in: Proceedings of the APWG eCrime Researchers Summit, San Francisco, IEEE 2013, S. 2 ff., 12.

11 *Möser/Böhme/Breuker*, in: Böhme/Brenner/Moore/Smith, Financial Cryptography and Data Security, 1st Workshop on Bitcoin Research (FC 2014), Barbados, 1. Aufl. 2014, S. 18.

12 Etwa Bitpay, Homepage abrufbar unter https://bitpay.com/ (letzter Abruf: 15.12.16).

13 Das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG. Auf europäischer Ebene Art. 8 EMRK, Art. (7,) 8 GRCh, dazu Kommissionsvorschlag (Fn. 1), S. 11; näher *Rückert*, Virtual Currencies and Fundamental Rights, Working Paper, S. 17 ff., abrufbar unter http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2820634 (letzter Abruf: 15.12.16).

14 *Di Fabio*, in Maunz/Dürig, GG-Kommentar, 76. EL, Art. 2, Rn. 177; *Starck*, in: v. Mangoldt/Klein/Starck, GG Kommentar, Band 1, 6. Aufl. 2010, Art. 2, Rn. 114. Zu

aktionsdaten enthält die Blockchain zumindest Angaben über wirtschaftliche beziehungsweise geschäftliche und damit persönlich-sachliche[15] Verhältnisse der Nutzer, insbesondere die den einzelnen Bitcoin-Adressen zugeordneten Guthaben sowie Transaktionen, denen reale Verträge, z. B. Schenkungsverträge bei Spenden, zugrunde liegen. Allerdings erscheint die Beziehung zu bestimmten oder bestimmbaren Personen insofern zweifelhaft, als die Nutzer des Systems sich hinter Bitcoin-Adressen als Pseudonymen verbergen. Die Daten in der Blockchain beziehen sich deshalb zwar nicht unmittelbar auf bestimmte Personen, allerdings genügt es für den Personenbezug von Daten, dass diese sich auf nur bestimmbare Personen beziehen, also auf bestimmte Personen beziehbar sind.[16]

Die Identität von sich hinter Bitcoin-Adressen verbergenden Nutzern kann sich mit Zusatzinformationen ermitteln lassen, z. B. durch Informationen über Online-Geschäfte, bei denen durch eine bestimmte Person ein bestimmter Betrag an eine bestimmte Bitcoin-Adresse zu entrichten ist. Ein anderes Beispiel bildet ein Nutzerkonto bei einer Bitcoin-Handelsbörse, das mit einer bestimmten Bitcoin-Adresse und daneben mit dem Klarnamen oder einem anderen Identifikator des Nutzers verknüpft ist. Zudem existieren Heuristiken, mit denen sich mit gewisser Wahrscheinlichkeit mehrere Bitcoin-Adressen als derselben Person zugehörig zuordnen lassen, sodass sich ein umfassenderes Bild der Bitcoin-Aktivitäten eines Nutzers ergeben kann.[17] Diese Möglichkeit erklärt die Entwicklung von Anonymisierungsdiensten für Bitcoin-Transaktionen, welche durch Vermischung der Ein- und Ausgänge mehrerer Transaktionen eine Anonymitätsmenge herstellen und die Anwendung der genannten Heuristiken erschweren.[18] Auch Regulierungskonzepte könnten eine Personenbeziehbarkeit von Blockchain-Daten zur Folge haben. Das wäre insbesondere die Konsequenz des Vorschlags der Kommission, virtuelle Währungen in den Anwendungsbereich der Geldwäscherichtlinie aufzunehmen, weil dadurch Bitcoin-Dienste dem *Know-Your-Customer*(KYC)-Prinzip unterstellt würden.[19]

3.2 Verfolgung Bitcoin-bezogener Straftaten

Ermittlungen in Fällen mit Bezug zu Bitcoin stellen Strafverfolgungsbehörden in zweierlei Hinsicht vor Herausforderungen. Einerseits ist nicht abschließend geklärt, welche Handlungen mit Bezug zu Bitcoin existierenden Strafvorschriften im Einzelnen unterfallen. Andererseits stoßen herkömmliche Ermittlungsmethoden an ihre Grenzen und unterliegen neue Ermittlungsmethoden rechtlichen Unsicherheiten.

(Potentiell) Kriminelle Handlungen mit Bitcoin

Im Rahmen des Forschungsprojekts BITCRIME gewonnene Ergebnisse lassen Rückschlüsse auf die Bedeutung von Bitcoin und anderen virtuellen Währungen für kriminelle Akteure zu. Bei einer von den Wissenschaftlern durchgeführten Nutzerstudie hat fast jeder fünfte der Befragten eingeräumt, Bitcoin (auch) für illegale Zwecke zu verwenden.[20] Eine anschließende Auswertung von dem Bundeskriminalamt (BKA) vorliegenden Daten aus dem Jahr 2015 führt zu der Einschätzung, dass im Zusammenhang mit Bitcoins primär Cybercrime-Delikte i.e.S. (z. B. bei der Nutzung fremder Rechner zum Mining[21]), Vermögensdelikte, Betäubungsmitteldelikte und Erpressungen auftreten.

Strafbarkeit Bitcoin-bezogener Handlungen

Weist ein Sachverhalt Bezug zu Bitcoin auf, stellt sich angesichts der Rechtsnatur von Bitcoins nicht selten die Frage, ob Strafvorschriften überhaupt einschlägig sind. Dies ist auch dann der Fall, wenn die Anwendbarkeit deutschen Rechts im Grunde gegeben ist, weil der Täter im Inland gehandelt hat oder der tatbestandliche Erfolg im Inland eingetreten ist (§§ 3, 9 Abs. 1 StGB). Weil Bitcoins weder als Sache noch als Geld eingeordnet werden können,[22] können sie wegen des Verbots täterbelastender Analogien im Strafrecht[23] nicht das Objekt von Straftaten sein, deren Tatbestände sich nur auf Sachen oder Geld beziehen. Angesichts dessen, dass der Gegenstandsbegriff des § 261 Abs. 1 StGB traditionell auf diese klassischen Rechtsgegenstände bezogen wird,[24] ist insbesondere die Anwendbarkeit des Geldwäschetatbestands diskutabel. Sinn und Zweck der Vorschrift sprechen aber für ein weiteres Begriffsverständnis, dem auch Bitcoins unterfallen.[25] Bei anderen Straftaten, die typischer-, aber nicht notwendigerweise mit dem Einsatz von Geld verbunden sind, können Bitcoins dieses substituieren.[26] Die besonders relevanten Konstellationen der Erpressung von Bitcoins sowie ihres Einsatzes als Gegenleistung beim Erwerb illegaler Güter sind daher strafbar.[27]

Ermittlungen in der Blockchain

Selbst wenn eine Bitcoin-bezogene Straftat vorliegt, stellt die Neuartigkeit virtueller Währungen Ermittlungsbehörden vor besondere Herausforderungen. Klassische Ermittlungsinstrumente wie Auskunftsbegehren bei Banken und anderen Anbietern mit Kenntnis von Kundeninformationen laufen beim dezentralen Bitcoin-System per se ins Leere. Gleichzeitig bietet die Block-

Art. 8 GRCh *Jarass*, Charta der Grundrechte der Europäischen Union, Kommenar, 3. Aufl. 2016, Art. 8, Rn. 5. Zu Art. 8 EMRK *ECHR*, Internet: case-law of the European Court of Human Rights, Std. Juni 2015, S. 7, abrufbar unter http://www.echr.coe.int/Documents/Research_report_internet_ENG.pdf (letzter Abruf: 15.12.16).

15 Plath/*Schreiber*, in: Plath, BDSG, 2. Aufl. 2016, § 3 BDSG, Rn. 8; *Weichert*, in: Däubler/Klebe/Wedde/Weichert, BDSG, 5. Aufl.2016, § 3, Rn. 2.

16 *Plath/Schreiber* (Fn. 14), Rn. 12; *Weichert* (Fn. 14), Rn. 13. Vgl. auch Art. 3 Nr. 1 der RL (EU) 2016/680 und Art. 4 Nr. 1 EU-DSGVO.

17 *Meiklejohn/Pomarole/Jordan/Levchenko/McCoy/Voelker/Savage*, in: Proceedings of the 2013 Internet Measurement Conference, S: 127 ff.; *Reid/Harrigan*, in: Altshuler/Elovici/Cremers/Aharony/Pentland, Security and Privacy in Social Networks (2013), S. 197 ff.; *Ron/Shamir*, in Sadeghi, Financial Cryptography and Data Security (2013), S. 6 ff.

18 Dazu *Möser/Böhme*, in: 15th Annual Workshop on the Economics of Information Security, Berkeley, 2016, abrufbar unter http://weis2016.econinfosec.org/wp-content/uploads/sites/2/2016/05/WEIS_2016_paper_58.pdf (letzter Abruf: 15.12.16).

19 Kommissionsvorschlag (Fn. 1), S. 11.

20 *Abramova/Böhme*, in: Proceedings of the 37th International Conference on Information Systems (ICIS), Dublin, Irland 2016, S. 15, abrufbar unter http://aisel.aisnet.org/icis2016/Crowdsourcing/Presentations/19/ (letzter Abruf: 15.12.2016).

21 *BGH*, Beschl. v. 21.7.2015 – 1 StR 16/15, NJW 2015, 3463 f.; *LG Kempten*, Urt. v. 29.10.2014 – 6 KLs 223 Js 7897/13 jug; *Heine*, NStZ 2016, 441 ff.

22 Siehe nur im strafrechtlichen Kontext *Grzywotz/Köhler/Rückert*, Strafverteidiger 11/2016 (in Erscheinung) sowie zu § 242 StGB *Boehm/Pesch*, in: FC 2014 (Fn. 10), S. 48 f.; *Kütük-Markendorf*, Rechtliche Einordnung von Internetwährungen im deutschen Rechtssystem am Beispiel von Bitcoin, 1. Aufl. 2016, S. 203; *v. Unruh*, in: Hoegner, The Law of Bitcoin, 1. Aufl. 2015, S. 112.

23 Dazu *Eser/Ecker*, in: Schönke/Schröder, StGB, 29. Aufl. 2014, § 1, Rn. 25.

24 BT-Drs. 12/989, S. 27; *Altenhain*, in Kindhäuser/Neumann/Paeffgen, StGB, 4. Aufl. 2013, § 261, Rn. 26.

25 *Boehm/Pesch*, in: FC 2014 (Fn. 10), S. 47 f.

26 *Boehm/Pesch*, in: FC 2014 (Fn. 10), S. 47.

27 *Grzywotz/Köhler/Rückert* (Fn. 21).

chain als öffentliche, globale Transaktionshistorie einen Ansatzpunkt für die Entwicklung neuartiger Ermittlungsinstrumente.

Eine wichtige Frage ist, ob sich typische Merkmale bestimmter krimineller Transaktionen in der Blockchain – automatisiert – ermitteln lassen. Ein einfaches Beispiel mit zugegeben begrenzter Aussagekraft wäre das Aufspüren von Transaktionen, deren Betrag der geforderten Summe in massenhaften Erpressungsfällen, wie etwa denen mithilfe des Erpressungstrojaners „Locky",[28] entspricht. Technisch bietet die Blockchain die Möglichkeit, die Herkunft bestimmter Bitcoin-Beträge entlang ihrer individuellen Transaktionshistorie zurückzuverfolgen. Tatsächlich hat sich bereits ein Markt für Werkzeuge zur forensischen Blockchain-Analyse entwickelt. Die meisten der Lösungen sind Cloud-basiert, sodass bei der Nutzung durch Ermittler sensible Ermittlungsdaten an den Anbieter übertragen würden. Deshalb wird im Rahmen des Projekts BITCRIME ein Blockchain-Explorationswerkzeug entwickelt, bei dem keine Ermittlungsdaten an Dritte übermittelt werden. Die mit der Auswertung von Blockchain-Daten verbundene Verarbeitung personenbezogener Daten setzt Ermittlungen durch Strafverfolgungsbehörden jedoch weitere Grenzen.[29] Zwar handelt es sich um öffentliche Daten, allerdings ist auch die Verwertung öffentlicher Daten im Ermittlungsverfahren nicht schrankenlos zulässig. Die Anwendung der Ermittlungsgeneralklauseln der §§ 161, 163 StPO ist zwar nicht durch die spezielle Regelung des § 100a StPO gesperrt, weil die Transaktionshistorie in der Blockchain nicht als nicht-öffentliche Kommunikation begriffen werden kann, die der Vorschrift aber nur unterfällt.[30] Die Ermittlungsgeneralklauseln vermögen indes nur solche Maßnahmen zu rechtfertigen, die bloß mit Grundrechtseingriffen geringer Intensität verbunden sind.[31]

Weiterhin stellt sich die Frage, ob Bitcoins im Strafverfahren sichergestellt werden können. Während eine Sicherstellung bestimmter Bitcoins zu Beweiszwecken nach § 94 Abs. 1 StPO nie erforderlich ist, weil sich alle ermittlungsrelevanten Daten schon aus der öffentlichen Blockchain ergeben, besteht an einer die Vermögensabschöpfung vorbereitenden Sicherstellung nach §§ 111b, 111c StPO ein praktisches Bedürfnis. Denn streitbefangene Bitcoins könnten während des Verfahrens von jedem, der über den zugehörigen privaten Schlüssel verfügt, auf eine andere Adresse übertragen werden und in der Folge dem Zugriff der Strafverfolgungsbehörden dauerhaft entzogen werden. § 111b Abs. 1 Satz 1 StPO setzt allerdings voraus, dass die Voraussetzungen für Einziehung (§ 74 StGB) oder Verfall (§ 73 StGB) vorliegen. Dies kommt für Bitcoins aber nur eingeschränkt in Betracht, weil die Vorschriften auf Sachen und Rechte zugeschnitten sind.[32]

In der Praxis scheitert die Verfolgung Bitcoin-bezogener Straftaten häufig daran, dass die Aufklärung der Identität der beteiligten Akteure nicht gelingt. Denn den Ermittlern fehlt es regelmäßig an verwertbaren Zusatzinformationen zur Identifikation der sich hinter Bitcoin-Adressen verbergenden Nutzer. Dies gilt insbesondere in den praktisch relevanten Erpressungsfällen. Klug agierende Täter können hier das Risiko ihrer Entdeckung gegen Null treiben, indem sie verschiedene Bitcoin-Adressen verwenden und deren Zugehörigkeit zu einem Nutzer verschleiern.[33] Entsprechende Anleitungen kursieren in Täterkreisen, aber auch unter legalen Nutzern seit Jahren.[34]

3.3 Prävention Bitcoin-bezogener Straftaten

Die praktischen Grenzen der Verfolgung bereits begangener Bitcoin-bezogener Straftaten schaffen ein Bedürfnis nach einem Regulierungskonzept zur Prävention ihrer Begehung.[35] Die zur Regulierung von Bitcoin oder vergleichbaren virtuellen Währungen vorgeschlagenen Ansätze sind vielfältig. Daher folgt zunächst eine systematische Darstellung, bevor eine Bewertung der Vorschläge vorgenommen wird.

Regulierungsansätze

BITCRIME hat die Erforschung von Regulierungsansätzen zum Ziel, die abseits pauschaler Verbote – wie sie vereinzelt in nationalen Gesetzgebungen anzutreffen sind[36] – Kriminalität vorbeugen und legitime Nutzer schützen. Auf den Kommissionsvorschlag wird im Kontext spezifischer Vorschläge Bezug genommen.

a) Verpflichtung oder freiwillige Kontrolle

Die verschiedenen Konzepte lassen sich zunächst danach unterscheiden, ob sie verpflichtend sind. Eine Regulierung ohne Verpflichtung könnte etwa in einer gesetzlichen Regelung von Zertifizierungsstellen liegen, die Bitcoin-Adressen identifizierter, vertrauenswürdiger Nutzer zertifizieren,[37] ähnlich wie die eIDAS-Verordnung[38] Vertrauensdienste für die Erstellung, Überprüfung und Validierung von elektronischen Signaturen regelt, ohne damit die eigenverantwortliche Erstellung von Signaturschlüsseln auszuschließen.

b) Adressierung von einfachen Nutzern oder Intermediären des Bitcoin-Ökosystems

Verpflichtende Regulierungsansätze lassen sich wiederum danach differenzieren, welche Adressaten verpflichtet werden. In Ermangelung einer zentralen Instanz ließen sich im Bitcoin-Kernsystem nur Nutzer verpflichten. Konkret könnten Miner dazu verpflichtet werden, Transaktionen, die mit kriminellen Vorgängen zusammenhängen, zum Beispiel die Transaktion eines Erpressungsopfers, nicht in der Blockchain zu verarbeiten.[39] Eine Bitcoin-Regulierung könnte aber auch ganz außerhalb des Kernsystems ansetzen. Insbesondere kommt die Verpflichtung von Anbietern zentraler Dienste im Bitcoin-Ökosystem in Betracht.

28 *Eikenberg*, Krypto-Trojaner Locky wütet in Deutschland: Über 5000 Infektionen pro Stunde, abrufbar unter http://www.heise.de/security/meldung/Krypto-Trojaner-Locky-wuetet-in-Deutschland-Ueber-5000-Infektionen-pro-Stunde-3111774.html (letzter Abruf: 15.12.16).

29 Die Vorgaben auf EU-Ebene konkretisiert RL (EU) 2016/680.

30 *Safferling/Rückert*, MMR 2015, 788, 792 f.

31 *BGH*, Beschl. v. 31.1.2007 – StB 18/06, NJW 2007, 930, 932; *Hilger*, NStZ 2000, 561, 564; *Safferling/Rückert*, MMR 2015, 788, 794.

32 Eingehend *Rückert*, MMR 2016, 295 ff. A.A. *Goger*, MMR 2016, 431, 433; *Heine*, NStZ 2016, 441, 444; *Greier*, wistra 2016, 249, 251 ff.

33 *Möser/Böhme/Breuker* (Fn. 9), S. 3 ff.

34 Bsp. unter https://www.cryptocompare.com/coins/guides/how-to-use-a-bitcoin-mixer/ (letzter Abruf: 15.12.16).

35 Einschränkend *Lerch*, ZBB 2015, 190, 202.

36 Z.B. die Finanzinstitute betreffende Regulierung in China, vgl. European Parliamentary Research Service, Briefing (11/04/2014), Bitcoin – Market, economics and regulation, Annex B, abrufbar unter http://www.europarl.europa.eu/RegData/bibliotheque/briefing/2014/140793/LDM_BRI(2014)140793_REV1_EN.pdf (letzter Abruf: 15.12.16).

37 Vgl. Kommissionsvorschlag (Fn. 1), S. 9: „a system of voluntary self-identification of virtual currency users".

38 Verordnung (EU) Nr. 910/2014.

39 Vgl. *Dinesh/Erlich/Gilfoyle/Jared/Richard/Pouwelse*, Operational Distributed Regulation for Bitcoin, 2014, S. 4, abrufbar unter https://arxiv.org/pdf/1406.5440.pdf (letzter Abruf: 15.12.16).

Dies sieht auch der Kommissionsvorschlag vor, nach dem Bitcoin-Handelsplattformen und Anbieter von Wallets in den Verpflichtetenkreis der Geldwäscheregulierung integriert werden sollen.[40]

Denkbar ist auch der Versuch einer indirekten Regulierung des Kernsystems durch die Adressierung äußerer Akteure. So ließe sich das Miner-Verhalten durch eine Regulierung von Herstellern spezifischer Mining-Hardware oder durch eine Regulierung am Mining beteiligter Intermediäre und von Betreibern so genannter *Mining-Pools*, in denen Miner ihre Rechenleistung zusammenschließen, beeinflussen. Vorstellbar wäre auch, die verwendeten kryptografischen Algorithmen über eine Regulierung der Entwickler einzuschränken, was extremen Forderungen nach einem Verbot oder einer Regulierung von Kryptographie nahesteht.[41] Abwegig ist dagegen die Vorstellung, dass staatliche Stellen dauerhaft in der Lage sein könnten, kryptographische Verfahren zu brechen und somit die Strafverfolgung zu ermöglichen.

c) Whitelisting oder Blacklisting

Eine Regulierung, die bei Intermediären im Bitcoin-Ökosystem ansetzt, ließe sich auf verschiedene Weisen ausgestalten. Ausgangspunkt der Regulierung kann zunächst die Identifizierung legaler Nutzer sein. Dem steht der Kommissionsvorschlag der Geldwäsche-Richtlinie nahe, weil mit einer Inanspruchnahme zur Kundenidentifizierung verpflichteter Intermediäre im Wesentlichen durch legale Nutzer zu rechnen ist. Spezifische Regulierungsansätze, die legale Nutzer erfassen wie etwa die unter a) genannte freiwillige Zertifizierung von Adressen können als Whitelisting-Ansätze bezeichnet werden. Konsequenz einer solchen Regulierung wäre es, dass jeder nicht registrierte Bitcoin-Nutzer unabhängig von einer tatsächlichen kriminellen Nutzung als zweifelhaft einzuordnen wäre. Demgegenüber setzen sogenannte Blacklisting-Ansätze bei der Erfassung krimineller Nutzung (in „Sperrlisten") an.

d) Adress- oder Transaktions-Blacklisting

Blacklisting-Ansätze lassen sich wiederum nach ihrem Bezugspunkt unterscheiden. Erfasst werden könnten zunächst Adressen, die mit kriminellen Vorgängen assoziiert sind.[42] Beispielhaft genannt werden kann eine Adresse, an die ein Erpressungsopfer eine Transaktion zu veranlassen aufgefordert worden ist. So könnten Intermediäre dazu verpflichtet werden, keine Verträge mit den Inhabern der gelisteten Adressen zu schließen. Einen alternativen Bezugspunkt zu Adressen bieten Transaktionen.[43] So könnte z. B. bei einer erfolgreichen Erpressung statt der Adresse des Erpressers die Transaktion, die das Opfer einer erfolgreichen Erpressung veranlasst hat, erfasst werden. Verbunden wäre die Listung krimineller Transaktionen mit dem Gebot Bitcoins, die aus dieser Transaktion stammen, als wertlos oder teilentwertet zu betrachten. Ein solches Gebot wäre nicht auf unmittelbar auf die gelistete Transaktion folgende Transaktionen beschränkt, sondern könnte sämtliche Folgetransaktionen betreffen. Denn in der Blockchain lassen sich Bitcoin-Beträge über beliebig viele Transaktionen verfolgen.

e) Blacklisting-Grundsätze und Vermischungsproblematik

Bei der Erfassung von Folgetransaktionen stellt sich die Frage, wie mit Transaktionen mit zwei oder mehr Eingängen umzugehen ist, in denen sich „saubere" und inkriminierte Bitcoin-Beträge vermischen. Das Blacklisting kann hier verschiedenen Grundsätzen folgen:[44] Möglich wäre hier einerseits ein Totalvergiftungsmodell, bei dem der Eingang gelisteter Bitcoins in eine Transaktion stets die Entwertung des gesamten transferierten Betrags zur Folge hat. Andererseits denkbar wäre in solchen Fällen eine nur teilweise Entwertung der transferierten Bitcoins (Teilvergiftungsmodell). Eine solche könnte wiederum verschiedenen Ausprägungen folgen, insbesondere kommt eine dem Anteil der in die Transaktion eingehenden inkriminierten Bitcoins entsprechende Entwertung (*Haircut*-Modell) in Betracht. Darüber hinaus sind Mischformen denkbar, die auch die Anordnung der Ein- und Ausgänge in der Transaktion berücksichtigen. Diese könnte man als Senioritätsmodell bezeichnen, angelehnt an die Sprachregelung bei der Rangfolge von Verbindlichkeiten im Finanzwesen.

Bewertung der Regulierungsansätze

Weil die Regulierungsansätze jeweils mit Eingriffen in die Grundrechte betroffener Akteure verbunden sind, hängt ihre Bewertung zunächst von ihrer Eignung zur Erreichung des prinzipiell legitimen Ziels der Prävention Bitcoin-bezogener Straftaten ab; darüber hinaus ist erforderlich, dass es keine milderen ebenso effektiven Regulierungsmöglichkeiten gibt, und der Grundrechtseingriff auch verhältnismäßig im engeren Sinne ist.[45] Besonderes Augenmerk liegt bei der Beurteilung auf dem Datenschutzgrundrecht, also dem Grundrecht auf informationelle Selbstbestimmung als Komponente des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG.[46]

a) Vorzugswürdigkeit einer zwingenden Intermediärsregulierung

Gegen eine Regelung ohne zwingende Wirkung spricht die fehlende Eignung zur Prävention krimineller Transaktionen. Gerade kriminelle Akteure und auch von ihnen unter Druck gesetzte Opfer – z. B. in Erpressungsfällen – werden eine freiwillige Regulierung im Zweifel nicht beachten.[47] Zwingende Maßnahmen sind eher, aber nicht in jedem Falle als geeignet einzustufen.

Eine Verpflichtung von einfachen Nutzern des Bitcoin-Kernsystems wäre schwerlich durchsetzbar, während die Adressierung von Intermediären erfolgversprechender ist. Die Durchsetzung von Mining-bezogenen Ansätzen wäre zwar denkbar, denn bei vielen Minern handelt es sich um für eine Regulierung greifbare Intermediäre. Die Schwäche liegt aber – abseits der da-

40 Kommissionsvorschlag (Fn. 1), S. 7. Auf Grundlage der Einordnung von Bitcoin als Finanzinstrument entspricht die erklärte Praxis der BaFin dem Vorschlag bereits bei einigen Anbietern, vgl. *Münzer*, Bitcoins: Aufsichtsrechtliche Bewertung und Risiken für Nutzer, abrufbar unter https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2014/fa_bj_1401_bitcoins.html (letzter Abruf: 11.10.16).

41 Einen Überblick über die „Krypto-Debatte" in Deutschland bietet *Koops*, Cryptolaw Survey, Germany, abrufbar unter http://www.cryptolaw.org/cls2.htm#ge (letzter Abruf: 15.12.16).

42 Vgl. *Dinesh/Erlich/Gilfoyle/Jared/Richard/Pouwelse* (Fn. 38), S. 4.

43 *Möser/Böhme/Breuker*, in: FC 2014 (Fn. 10), S. 16 ff.

44 Alle genannten sind beschrieben in *Möser/Böhme/Breuker*, in: FC 2014 (Fn. 10), S. 21 f.

45 *Grzeszick*, in Maunz/Dürig, GG-Kommentar, 77. EL, Art. 20, Rn. 107, 110 ff.; *Jarass*, Charta der Grundrechte der EU, 2. Aufl. 2013, Art. 52, Rn. 35 ff.; *Harris/O'Boyle/Warbrick*, Law of the European Convention on Human Rights, 3. Aufl. 2014, S. 519 f.

46 Daneben sind die Schutzbereiche zahlreicher weiterer Grundrechte betroffen. Siehe zur europäischen Ebene *Rückert* (Fn. 12), S. 16 ff.

47 Zur zweifelhaften Strafbarkeit der Opfer von Erpressungen mit Ransomware Salomon, MMR 2016, 575 ff.

mit verbundenen Eingriffe in Informations-[48] und ggfs. Berufsfreiheit[49] – schon praktisch darin begründet, dass sich unschwer zu Bitcoin alternative virtuelle Währungen konstruieren lassen, bei denen Mining-Regulierung nicht greift.[50] Ein Ansetzen bei den Entwicklern des Systems oder gar Entwicklern der verwendeten kryptographischen Algorithmen wäre mit einem intensiven Eingriff in die Freiheiten der Entwickler verbunden und liefe der Pflicht des Staates zur Förderung des Datenselbstschutzes[51] zuwider. Der Nutzen einer Änderung des Bitcoin-Protokolls ist angesichts eines möglichen Ausweichens auf alternative virtuelle Währungen[52] ohnehin als gering einzustufen. Da allen Nutzern des Systems frei steht, welche von Entwicklern vorgeschlagenen Modifikationen des Protokolls sie adaptieren, hätte eine Regulierung der Entwickler aber voraussichtlich keine Änderung des von der maßgeblichen Mehrheit genutzten Protokolls zur Folge.

b) Vorzugswürdigkeit des Blacklistings

Für die Frage, ob für eine Intermediäre adressierende Regulierung Whitelisting- oder Blacklisting-Ansätze als vorzugswürdig anzusehen sind, spielt ebenfalls die jeweilige Eignung eine Rolle: Ansätze, die auf der Erfassung legaler, identifizierter Nutzer beziehungsweise deren Adressen beruhen, sind zur Prävention illegaler Nutzung kaum geeignet. Ein Erpressungsopfer wird eine Transaktion an die vom Erpresser genannte Bitcoin-Adresse ohne Rücksicht darauf veranlassen, dass diese keiner identifizierten natürlichen Person zugeordnet ist.

Gegen Whitelisting-Ansätze – und ebenso den Kommissionsvorschlag – spricht jedoch insbesondere die Intensität des mit ihnen verbundenen Eingriffs in das Recht auf informationelle Selbstbestimmung von Nutzern. Denn die Erfassung von Identitäten hinter Bitcoin-Adressen macht Transaktionen von oder auf diese Adressen personenbeziehbar.

Umso problematischer wird es, wenn die Regulierung dazu führt, dass Nutzer nur noch eine oder wenige mit ihrer Person verknüpfte Bitcoin-Adresse(n) verwenden, weil dann nicht bloß einzelne Transaktionsvorgänge, sondern die gesamten Bitcoin-Aktivitäten der jeweiligen Nutzer für jedermann personenbeziehbar werden. Während im konventionellen Finanzsystem der Verlust von Kundeninformationen lediglich dazu führt, dass die jeweiligen Informationen bekannt werden, führt der Verlust der Identifikationsdaten von Bitcoin-Nutzern zugleich dazu, dass alle vom Nutzer jemals getätigten Transaktionen diesem zuordenbar werden. Die Transaktionsflüsse können aber ein detailliertes Bild der privaten Lebensführung zeichnen. Auf die Identifikation von Nutzern gerichtete Ansätze gefährden damit die Rechte legaler Nutzer, ohne diese zugleich effektiver vor Angriffen durch Kriminelle zu schützen. Dem lässt sich auch nicht entgegenhalten, dass es den Nutzern überlassen bleibe, ob sie Adressen mit ihrer Identität verknüpfen beziehungsweise zur Identifikation verpflichtete Dienste überhaupt nutzen. Denn eine auf Identifikation zielende Regulierung würde zugleich bewirken, dass Nutzer nicht identifizierter Adressen den Ermittlungsbehörden – und beim Whitelisting auch potenziellen Geschäftspartnern – zweifelhaft erscheinen. Zudem werden selbst Nutzer nicht identifizierter Adressen mittelbar in ihrem Recht auf informationelle Selbstbestimmung betroffen, weil die Identifikation ihrer eigenen Geschäftspartner oder deren Geschäftspartner auch ihre eigene Identifikation ermöglichen kann.

c) Vorzugswürdigkeit der Anknüpfung an Transaktionen

Betrachtet man – die in Bezug auf den Nutzerdatenschutz milderen – Blacklisting-Ansätze, so spricht gegen die Geeignetheit des Adress-Blacklistings, dass Bitcoin-Adressen durch jedermann in beliebiger Zahl erzeugt werden können. Folglich wäre es ein Leichtes für Kriminelle, die Listung ihrer Adresse durch Erzeugung einer neuen zu umgehen und ihre Bitcoins auf die nicht gelistete, frische Adresse zu übertragen. Dagegen ermöglicht die Anknüpfung an Transaktionen die Erfassung von Folgetransaktionen, sodass solche nicht zu einer Umgehung der Regulierung führen können.

d) Ausblick: Grundrechtliche Implikationen für Sperrlistengrundsätze

Bei der Wahl eines dem Transaktions-Blacklisting zugrunde gelegten Sperrlistengrundsatzes für den Umgang mit Transaktionen, in die legale und inkriminierte Bitcoin-Beträge eingehen, spielen ebenfalls grundrechtsbezogene Erwägungen eine Rolle. In einer totalen Entwertung aller Bitcoins aus Transaktionen, in die saubere wie inkriminierte Bitcoins eingehen, läge ein intensiverer Eingriff in das Eigentumsgrundrecht[53] vor als in anteiligen Entwertungen. Diesen und zahlreichen weiteren praktischen und rechtlichen Fragen, etwa nach den technischen und rechtlichen Rahmenbedingungen der Führung und Abfrage von Sperrlisten – auch mit Blick auf die personenbezogenen Daten in der Sperrliste –, wird im Projekt BITCRIME nähere Aufmerksamkeit gewidmet. Laufende Forschungsarbeiten nähern sich diesen Fragen aus technischer, ökonomisch-spieltheoretischer und rechtlicher Perspektive.

4 Fazit

Große Bedeutung für die Strafverfolgung und Prävention Bitcoin-bezogener Straftaten hat die Transparenz des Bitcoin-Systems, dessen Transaktionsflüsse in der öffentlichen Blockchain lückenlos nachvollziehbar sind. Die Identifikation von Nutzern bestimmter Adressen birgt die Gefahr, dass Bitcoin-Aktivitäten identifizierter und auch weiterer Nutzer umfassend nachvollziehbar werden. Ansätze zur Verfolgung und Prävention Bitcoin-bezogener Straftaten sollten legalen Nutzern deshalb nicht die Möglichkeit entziehen, Bitcoin unter größtmöglicher Wahrung ihrer Pseudonymität zu nutzen. Dieser Anforderung wird der Vorschlag der Kommission nicht gerecht. Die Alternative des Transaktions-Blacklistings, welche freilich noch zahlreiche zu klärende Fragen aufwirft, macht sich die Transparenz der Blockchain zunutze, ohne in seiner Funktionalität auf die Identifikation der Nutzer von Adressen mit zweifelhaften Transaktionsvorgängen angewiesen zu sein.

48 Zur europäischen Ebene *Rückert* (Fn. 12), S. 26 ff.

49 Viele gewerbliche Intermediäre beteiligen sich am Mining. Zur Berufsfreiheit von Intermediären auf europäischer Ebene *Rückert* (Fn. 12), S. 23 f.

50 Das Fortschreiben von authentisierten Datenstrukturen wie der Blockchain lässt sich auch anders als durch Erbringung eines Arbeitsnachweises absichern, siehe etwa https://en.bitcoin.it/wiki/Proof_of_Stake (letzter Abruf: 15.12.16). Ohne das Erfordernis des für Bitcoin charakteristischen Arbeitsnachweises bedarf rentables Mining weder besonderer Hardware noch der Bündelung von Rechenkapazitäten, sodass es an greifbaren Regulierungsadressaten weitgehend fehlt.

51 *Weichert*, DuD 2009, 7, 10.

52 Z.B. das anonyme ZCash-System, https://z.cash/ (letzter Abruf: 15.12.16).

53 Zur europäischen Ebene *Rückert* (Fn. 12), S. 20 ff.