ren, dann jedenfalls aus kompensatorischen Gründen – Kinder- und Jugendpsychiater und/oder -psychologen herangezogen werden, die sich mit den zu beleuchtenden Fragestellungen auskennen und notfalls die fehlende Sachkunde der Richter »aufzufangen« vermögen. Insofern kann man sogar in Ansatz bringen, was als Argument für die Vorrangzuständigkeit von Erwachsenengerichten angeführt wurde: gerade weil »der Idealismus Jugendlicher häufig von Erwachsenen zu politischen Zwecken *missbraucht* wird und dass Jugendliche in staatsrechtlichen Dingen und von den politischen Verhältnissen im allgemeinen *noch keine genauen Vorstellungen* haben«,[91] sind die Gründe, Auswirkungen, Entwicklungen sachkundig zu beleuchten und in Zusammenhang zu bringen mit dem in Rede stehenden Tatvorwurf: wie konnte es hierzu kommen? Wie können wir darauf reagieren? Anlehnend an die eingangs zitierten Worte *Hassemers* sollte die mit dem Jugendschutz einhergehende Hoffnung auf eine bessere Zukunft nicht von vornherein ausgeblendet und preisgegeben werden.

C. Staatsschutz versus Jugendschutz?

Die Gründe für die Vorrangzuständigkeit der Erwachsenengerichte bei erstinstanzlichen OLG-Verfahren überzeugen nicht, zumindest nicht so, dass gerechtfertigt wäre, ihnen den Vorzug gegenüber dem Jugendschutz zu geben. Verfahren gegen Jugendliche, aber auch gegen Heranwachsende vor Erwachsenengerichten sind dem Grundgedanken des JGG abträglich. Insofern ist § 102 JGG ein Fremdkörper im JGG und sollte einer Reform zugeführt werden. Der bereits in den 1990ern von *Schoreit* geäußerte Vorschlag, innerhalb der erstinstanzlichen OLG-Senate besondere Jugendsenate einzurichten, deren Aufgabe dann darin bestünde, Staatsschutzverfahren zu verhandeln, bei denen Jugendliche und Heranwachsende (mit-)angeklagt sind,[92] sollte aufgegriffen und umgesetzt werden. Diese Senate müssten in ihrer Besetzung den Anforderungen des § 37 JGG genügen. Damit könnte man den ohnehin problematischen Sachkunde-Widerstreit – Sachkunde im Bereich des Staatsschutzes versus Sachkunde im Bereich des Jugendrechts mit all' seinen Facetten – lösen und damit die Hoffnung verbinden, dass der Staatsschutz nicht zulasten des Erziehungsgedankens überbewertet wird.[93]

§ 37 JGG sollte ebenso in eine Muss-Vorschrift umgewandelt werden[94] wie § 43 Abs. 2 S. 2 JGG. Daneben sollten die Qualifikationsanforderungen i.R.d. § 37 JGG näher konkretisiert werden. Dies könnte, anlehnend an den nicht umgesetzten Entwurf, allerdings mit dem Zusatz der verpflichtenden Qualifikation, dahingehend geschehen, dass die Richter und Staatsanwälte »über Kenntnisse auf den Gebieten der Kriminologie, Pädagogik und Sozialpädagogik sowie der Jugendpsychologie verfügen müssen. Einem Richter oder Staatsanwalt, dessen Kenntnisse auf diesen Gebieten nicht belegt sind, dürfen die Aufgaben eines Jugendrichters oder Jugendstaatsanwalts erstmals nur zugewiesen werden, wenn der Erwerb der Kenntnisse durch die Wahrnehmung von einschlägigen Fortbildungsangeboten oder eine anderweitige einschlägige Weiterqualifizierung alsbald zu erwarten ist«.[95] Anlehnend an das, was *Mohr* in Zusammenhang mit »gemischten Verfahren« i.S.d. § 103 Abs. 1 JGG konstatiert hat, gilt auch hier: nur ein reines Jugendstrafverfahren kann dem jugendlichen (und auch dem heranwachsenden) Angeklagten am ehesten gerecht werden.[96] Ein im wahrsten Sinne des Wortes Staats-Schutz müsste dem Jugendschutz allein schon perspektivisch besondere Bedeutung beimessen. Nur dann würden beide Aufgaben ernst genommen und dem Jugendschutz (und damit auch dem Staatsschutz) gerecht werden.

91 S. bereits oben *Potrykus* (Fn. 31); Hervorh. nicht i. Orig.
92 *Schoreit* NStZ 1997, 69 (71).
93 Alternativ müsste § 102 JGG gestrichen werden mit der Konsequenz, dass auch die gegen Jugendliche und Heranwachsende geführten Staatsschutzverfahren vor Jugendkammern stattfinden würden; *Eisenberg* NStZ 1996, 263 (267) hält jedenfalls eine pauschale *Tat*orientierung für unzulässig und fordert wenigstens eine Differenzierung, in welchem Grad der Schutz des Staates bedroht sein soll.
94 So auch *Schoreit* NStZ 1997, 69 (71).
95 Vgl. hierzu – mit der Einschränkung, dass es dort »soll« und »sollen« statt »muss« und »dürfen« heißt – BT-Drs. 17/6261, S. 6.
96 Vgl. *Mohr* JR 2006, 499 (504).

Cybercrime mit Bitcoins – Straftaten mit virtuellen Währungen, deren Verfolgung und Prävention

Wiss. Mit. Johanna Grzywotz, Olaf Markus Köhler und Christian Rückert, Erlangen-Nürnberg und Münster*

Bitcoin als Tatmittel: Virtuelle Währungen wie Bitcoin sind ein modernes und legales Konzept, bieten sich aber auch bei klassischen Straftaten als Werkzeug an. Des Weiteren werfen sie gerade unter strafverfolgungsrechtlichen Aspekten zahlreiche rechtliche Fragen auf. Der Beitrag möchte einen Überblick über forschungs- und praxisrelevante Fragestellungen geben.

A. Neue strafrechtliche Herausforderungen durch virtuelle Währungen

Virtuelle Währungen[1] wie Bitcoin sind ein Phänomen, das immer mehr an Bedeutung gewinnt. Unabhängig von Notenbanken, Staaten und Kreditinstituten werden sie direkt zwischen den Nutzern gehandelt und eröffnen Kriminellen so insbesondere aufgrund ihrer Dezentralität vermeintliche

* Die Autoren *Grzywotz* und *Rückert* sind wiss. Mit. am Lehrstuhl für Strafrecht, Strafprozessrecht, Internationales Strafrecht und Völkerrecht der FAU Erlangen-Nürnberg, *Köhler* ist wiss. Mit. in der Forschungsgruppe für IT-Sicherheit an der WWU Münster. Alle *Verf.* 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.

1 Virtuelle Währungen in diesem Aufsatz meinen dezentrale, kryptographische Währungen. Der Begriff der Währung wird an dieser Stelle verwendet, auch wenn der juristische Währungsbegriff nur staatliche Währungen erfasst, vgl. dazu auch: EBA Opinion on ›virtual currencies‹, EBA/Op/2014/08, S. 11, https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf (zuletzt abgerufen, wie alle nachfolgenden URLs ohne gesonderte Kennzeichnung, am 23.03.2016).

Anonymität. Dabei stellt sich zunächst die Frage, welche Straftatbestände auf das Phänomen der virtuellen Währungen überhaupt anwendbar sind. Trotz der in der Praxis oftmals zu beobachtenden »klassischen« Begehungsweise (z.B. Phishing oder Erpressung mittels Cryptolockern[2]) ergeben sich aufgrund der Funktionsweise des Bitcoin-Netzwerks dabei oftmals Besonderheiten in der rechtlichen Bewertung. Schließlich ermöglicht die Bitcoin-Technologie völlig neuartige sozialschädliche Handlungsweisen, die auf ihren Unrechtsgehalt und ihre Strafwürdigkeit zu untersuchen sind. Für Strafverfolgung und Prävention stellen Dezentralität und Pseudonymität besondere Herausforderungen dar, gleichzeitig bietet die öffentliche Einsehbarkeit der Transaktionsliste, die sog. Blockchain, neue Chancen in beiden Bereichen. Dieser Beitrag versucht über die verschiedenen neuen Herausforderungen einen einführenden Überblick zu geben, ohne dabei jedoch die einzelnen Konstellationen abschließend oder vollständig behandeln zu können.

B. Technische Hintergründe

Virtuelle Währungssysteme – wie Bitcoin – unterscheiden sich in ihrer technischen Funktionsweise erheblich von den bisher bekannten elektronischen Bezahlsystemen. Die Besonderheiten des Bitcoin-Systems bestimmen dabei maßgeblich die (straf-)rechtliche Einordnung, weswegen zunächst eine kurze technische Einführung erforderlich ist.

Bitcoin bezeichnet ein währungsähnliches System, das Nutzern die dezentrale Übertragung von Werteinheiten (Bitcoins) ermöglicht.[3] Dabei werden, wie auch bei modernen elektronischen Bezahlsystemen, keine digitalen Münzen gespeichert und übertragen, sondern wertzuweisende Informationen geändert.[4] Den Anknüpfungspunkt für Wertzuweisungen im Bitcoin-System stellen dabei die Bitcoin-Adressen dar.

I. Adressen

Um Werte nachprüfbar zuzuweisen, ohne dabei eine zentrale Autorität zu benötigen, werden digitale Signaturen verwendet. Dieses kryptographische Verfahren basiert auf sogenannten Schlüsselpaaren, die jeweils aus einem öffentlichen und einem privaten Schlüssel bestehen.[5] Der private Schlüssel, mit dem Transaktionen signiert werden, wird von dem Nutzer geheim gehalten, während der öffentliche Schlüssel weitergegeben wird, um Zahlungen zu empfangen.[6] Entsprechend wird der öffentliche Schlüssel auch als Bitcoin-Adresse[7] bezeichnet und ist vergleichbar mit einer Kontonummer bei Geld-Transaktionen. Im Gegensatz zu Kontonummern, lassen sich Schlüsselpaare und damit auch Bitcoin-Adressen in beliebiger Anzahl von jedem Nutzer selbst generieren. Typischerweise werden bei Transaktionen Bitcoins einem öffentlichen Schlüssel zugeordnet. Die Verwendung der Bitcoins in einer erneuten Transaktion erfordert die digitale Signatur mit dem zugehörigen privaten Schlüssel. Ohne diesen lässt sich keine gültige Transaktion erstellen. Die tatsächliche Verfügungsgewalt über die Bitcoins liegt also grundsätzlich bei dem Nutzer, der das Schlüsselpaar generiert hat, aber auch bei jedem anderen, der von dem privaten Schlüssel Kenntnis erlangt hat.[8] Üblicherweise werden mehrere Schlüsselpaare eines Nutzers gemeinsam verwaltet. Diese Zusammenfassung wird als Wallet bezeichnet, ermöglicht die Verfügung über bestimmte Bitcoins und wird häufig als Wallet-Datei auf dem Computer oder auch Mobilgerät des Nutzers gespeichert. Eine Verschlüsselung der Wallet-Datei kann dabei den Zugriff von Schadsoftware auf die enthaltenen privaten Schlüssel, mit denen die Bitcoins transferiert werden können, erschweren.

II. Ökosystem

Die technische Umsetzung bzw. Funktionsweise des Bitcoin-Systems wird auch als Bitcoin-Protokoll[9] bezeichnet. Entsprechend des Grundgedankens der Dezentralität ist auch das Bitcoin-Protokoll von keiner zentralen Stelle definiert. Es befindet sich in stetiger Entwicklung, durch eine lose Gemeinschaft von Entwicklern, welche die Programme schreiben und modifizieren, die das Protokoll definieren.[10] Bei der Evaluierung von Regulierungskonzepten ist deshalb zu beachten, dass Änderungen am Bitcoin-Protokoll nur mit der mehrheitlichen Akzeptanz der Gemeinschaft umgesetzt werden können.

Um Bitcoin herum, aber außerhalb des Systems selbst, hat sich ein Ökosystem verschiedener Akteure herausgebildet.[11] Darunter befinden sich insbesondere Anbieter Bitcoin-bezogener Dienste, wie beispielsweise Handelsplattformen, an denen Bitcoins gegen andere virtuelle oder staatliche Währungen eingetauscht werden, Zahlungsdienstleister, die für Händler »Zahlungen« in Bitcoin abwickeln, Anonymisierungsdienste und Online-Wallet-Dienstleister.[12]

III. Bitcoin-Transaktionen

Als Zusammenfassung von Schlüsselpaaren enthält eine Bitcoin-Wallet keinen expliziten Kontostand. Vergleichbar mit einem Portemonnaie, welches von außen keinen sichtbaren Geldstand angibt, sondern dieser sich durch das Zählen der darin befindlichen Geldscheine/Münzen ergibt, geht der Bitcoin-Kontostand implizit aus den an die öffentlichen Schlüssel gerichteten Transaktionen, die nicht bereits eingelöst wurden, hervor.

---

2 Schadsoftware, deren Vorgehen auf der Verschlüsselung von lokalen Dateien basiert. Diese Dateien werden damit vorerst für den Nutzer unzugänglich. Gegen eine Zahlung wird die Entschlüsselung/Herausgabe des Schlüssels versprochen.

3 Siehe für eine umfassende Einführung *Aviv Zohar*, Bitcoin: Under the Hood. Communications of the ACM Sept. 2015, 104 (113), http://cacm.acm.org/magazines/2015/9/191170-bitcoin/fulltext; *Böhme/Christin/Edelman/Moore*, Bitcoin: Economics, Technology, and Governance. Journal of Economic Perspectives, 2015, 29(2): 213-38.

4 So auch *Safferling/Rückert* MMR 2015, 788 (789).

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

6 *Sorge/Krohn-Grimberghe* DuD 2012, 479 (480); *Kütük/Sorge* MMR 2014, 643; *Safferling/Rückert* MMR 2015, 788 (790).

7 Die Bitcoin-Adresse wird aus dem öffentlichen Schlüssel abgeleitet und wird typischerweise als Transaktionsempfänger angegeben, vgl. https://en.bitcoin.it/wiki/Technical_background_of_version_1_Bitcoin_addresses.

8 Siehe auch *Safferling/Rückert* MMR 2015, 788 (790) m.w.N.

9 Siehe https://en.bitcoin.it/wiki/Protocol_documentation.

10 Siehe https://bitcoin.org/en/development.

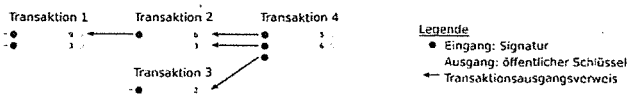
11 Siehe *Möser/Böhme/Breuker*, in: Böhme/Brenner/Moore/Smith (Hrsg.), Financial Cryptography and Data Security, 2014, S. 16 (17 f.).

12 Online-Wallet-Dienstleister bieten Kunden einen Zugang, ähnlich wie normales Online-Banking, und können genutzt werden, um mit Bitcoins zu handeln. Dabei bieten sie häufig einen vereinfachten Einstieg im Vergleich zur Nutzung anderer Bitcoin-Software. Es ist ein entsprechendes Vertrauen in den Dienstleister notwendig, da sich ein Nutzer technisch betrachtet die Verfügungsmacht über seine Bitcoins mit dem Dienstleister teilt.

Alle Transaktionen sind dauerhaft für alle Nutzer des Systems öffentlich einsehbar.[13] Die Blockchain bildet als Historie aller Transaktionen ein gemeinsames Hauptbuch, das zwischen den Nutzern ständig ausgetauscht und fortgeschrieben wird. Aufgrund des technischen Ablaufs von Bitcoin-Transaktionen, können sich neue Fragestellungen im Hinblick auf eine Geldwäschestrafbarkeit ergeben. Ebenso schließen sie die Anwendbarkeit der meisten »Standardermittlungsmaßnahmen« im Bereich der Finanzkriminalität weitgehend aus. Gleichzeitig bietet die öffentliche Einsehbarkeit der Blockchain und die vollständige Rückverfolgbarkeit der Transaktionskette einen Ansatzpunkt für die Entwicklung neuer Fahndungsinstrumente.

1. Transaktionen als elementare Information

Wie bei Geld-Transaktionen beschreibt auch eine Bitcoin-Transaktion die Weiterleitung der Zugriffsmöglichkeit. Im Gegensatz zu Geld-Transaktionen, bei denen diese Zugriffsmöglichkeit durch eine Bank zentral geregelt wird, ist der Zugriff auf Bitcoins durch digitale Signaturen geschützt. Dementsprechend wird bei einer Bitcoin-Transaktion die Zugriffsmöglichkeit auf bestimmte Bitcoins auf ein anderes bestimmtes Schlüsselpaar übertragen. Eine Transaktion besteht aus je einem oder mehreren Ein- und Ausgängen. Letztere beschreiben dabei im Regelfall eine Zieladresse und den Betrag, der an den entsprechenden Adressaten gehen soll. Eingänge beschreiben grundsätzlich die Referenz auf den einzulösenden Ausgang einer vergangenen Transaktion und eine digitale Signatur, die bestätigt, dass ein Inhaber des (zu dem Ausgang der vergangenen Transaktion) passenden privaten Schlüssels die Transaktion veranlasst.



2. Nachvollziehbarkeit des Geldweges

Betrachtet sei folgender Fall, der darin besteht, dass ein bestimmter Geldbetrag, welcher aus einer kriminellen Handlung herrührt, im Rahmen einer Geldwäscheuntersuchung nachverfolgt werden soll. Bei Banküberweisungen lässt sich Geld nur aufgrund von Indizien, wie zeitlichem Zusammenhang oder Betragsgröße, über mehrere Konten hinweg verfolgen. Im Gegensatz dazu ergibt sich im Fall Bitcoin nicht nur durch die Öffentlichkeit der Blockchain eine besondere Nachverfolgbarkeit des Geldweges:[14] Da Transaktionen nicht nur die Adresse spezifizieren, von der ein Transaktionseingang kommt, sondern zugleich auf konkrete frühere Transaktionsausgänge verweisen, aus denen das Geld verwendet wird, bekommen Bitcoins durch ihren lückenlos nachvollziehbaren Weg eine Identität.[15] Aus dieser Nachverfolgbarkeit ergibt sich aber eine nur unvollständige Information über den Handel zwischen Personen: Da jede Person beliebig viele Adressen erstellen und nutzen kann,[16] und aufgrund der Existenz verschiedener Dienstleistungen im Bitcoin-Ökosystem[17] auch die Bitcoins mehrerer Personen bei einer gemeinsamen Bitcoin-Adresse hinterlegt sein können, deuten Transaktionen im Bitcoin-System nicht zwingend auf den Wechsel der Inhaberschaft beziehungsweise dahinter stehende Geschäfte hin.

3. Anonymisierungsdienste

Um die Schlussfolgerung von Bitcoin-Transaktionen auf den tatsächlichen Handel zwischen Personen zu erschweren, haben sich Anonymisierungsdienste etabliert, die zur Verschleierung genutzt werden können. Es gibt Dienstleister (sog. Mixer), welche die Bitcoins verschiedener Nutzer automatisiert vermischen, tauschen und an zuvor definierte neue Adressen auszahlen.[18] Dabei können Bitcoins gegen die Bitcoins anderer Nutzer getauscht werden, auf mehrere Zieladressen aufgeteilt und mit zufälligen zeitlichen Abständen überwiesen werden, um die Herstellung von Verbindungen aufgrund von zeitlichen Zusammenhängen oder deckungsgleichen Beträgen zu erschweren.

4. Bedeutung der Blockchain im Rahmen des Strafrechts

Die weitgehende öffentliche Nachvollziehbarkeit der konkreten Geldwege unterscheidet Bitcoin deutlich von klassischen elektronischen Zahlungsmitteln. Trotz der nur losen Verknüpfung zwischen den Transaktionen – die in der Blockchain sichtbar sind und dem direkten Handel zwischen einzelnen Nutzern – ist die Blockchain als Informationsquelle dennoch sowohl im Rahmen der Betrachtung von Geldwäsche als auch als Ermittlungsansatz in der Strafverfolgung von besonderer Relevanz.

IV. Bitcoin-Mining

In einem dezentralen System, in dem jeder Teilnehmer die gleiche Rolle einnehmen kann, müssen die verwaltenden Aufgaben (welche sonst von einer zentralen Stelle übernommen werden) verteilt werden.[19] Hierbei ist besonders die Einigung auf das gemeinsame Hauptbuch eine technisch herausfordernde Notwendigkeit: Es soll technisch unmöglich sein, dass eine Minderheit den Zustand des Systems dauerhaft manipulieren kann. Die Zuordnung von Handlungen im Internet zu juristischen oder natürlichen Personen ist ohne den Einbezug zusätzlicher zentraler Stellen nicht ohne weiteres möglich, weshalb eine gleichmäßige Machtverteilung auf alle Teilnehmer nicht allgemein möglich ist. Stattdessen wird das Stimmgewicht im Bitcoin-System nach investierter Rechenkapazität verteilt. Dazu wird das kryptographische Konzept Proof-of-Work[20] eingesetzt. Um die Beteiligung am System durch mehr als die Erhaltung eines Machtgleichgewichts zu motivieren, wird diese durch die Ausschüttung neuer Bitcoins belohnt.[21] Dieser Prozess wird

13 *Boehm/Pesch* MMR 2014, 75 (76); *Safferling/Rückert* MMR 2015, 788 (790); *Spindler/Bille* WM 2014, 1357 (1358).

14 Geld ist hier nicht im rechtlichen Sinne gemeint, vgl. dazu schon **B.III.1.**

15 Diese Eigenschaft bemerken *Möser/Böhme/Breuker* (Fn. 11), S. 16 ff. erstmals in der wissenschaftlichen Literatur.

16 Mit dem Ziel der Stärkung der Privatsphäre sind Nutzer sogar dazu angehalten, für neue Transaktionen stets auch neue Adressen zu generieren. Dieser Konvention folgt aber nur ein Teil der Bitcoin-Software, vgl. https://en.bitcoin.it/wiki/Address_reuse.

17 Spezielle Dienstleister, die Bitcoins verschiedener Personen (ggf. temporär) auf gemeinsamen Bitcoin-Konten vereinen, z.B. Zahlungsdienstleister, Online-Wallets, Anonymisierungsdienste.

18 Bspw. bitmixer.io. Eine Untersuchung der Funktionsweise verschiedener solcher Dienste findet sich bei *Möser/Böhme/Breuker*, An Inquiry Into Money Laundering Tools in the Bitcoin Ecosystem, in: eCrime Researchers Summit (eCRS), 2013.

19 Teilnehmer können sich an den verwaltenden Aufgaben beteiligen, müssen dies aber nicht. Transaktionen können auch von Teilnehmern durchgeführt werden, die sich nicht an der Verwaltung beteiligen.

20 Vgl. https://en.bitcoin.it/wiki/Proof_of_work.

21 Ein zusätzlicher Anreiz sind die (auf freiwilliger Basis) gezahlten Transaktionsgebühren. Da Bitcoins eine begrenzte Ressource sind, werden Transaktionsge-

daher auch als Bitcoin-Mining bezeichnet.[22] Diese Mining-Belohnung wird alle 210.000 Mining-Vorgänge halbiert. Somit sind Bitcoins eine begrenzte Ressource.[23]

C. Probleme und Herausforderungen im materiellen Strafrecht

Virtuelle Währungen werden von Kriminellen oftmals bei klassischen Straftaten als Geldersatz eingesetzt. Neben einzelnen Tatbestandsmerkmalen der einzelnen Normen spielt dabei insbesondere die Frage nach der Anwendbarkeit des deutschen Strafrechts eine Rolle, da es sich beim Bitcoin-System um ein grenzüberschreitendes Netzwerk handelt.

I. Anwendbarkeit des deutschen Strafrechts

Hierfür maßgeblich sind § 3 und § 9 Abs. 1 StGB. Deutsches Strafrecht ist danach anwendbar, sobald der Handlungs- oder der Erfolgsort im Inland liegt.[24] Da der Handlungsort immer dort gelegen ist, wo der Täter die tatbestandsmäßige Ausführungshandlung vornimmt[25] und Internetkriminalität oftmals über das Internet im Ausland ausgeführt wird, befindet sich der Handlungsort in solchen Fällen nicht im Inland.[26] Folglich führt der Handlungsort dann nicht zu einer Anwendbarkeit des deutschen Strafrechts. Daneben besteht die Möglichkeit, diese mit Hilfe des Erfolgsortes nach § 9 Abs. 1 Var. 3 StGB zu begründen. Erfolgsort ist der Ort, an dem der zum Tatbestand gehörende Erfolg eintritt.[27] Erfolg ist dabei jede Veränderung der Außenwelt als Folge der Tathandlung,[28] was für jeden in Betracht kommenden Straftatbestand separat zu ermitteln ist,[29] wobei dabei für die einzelnen Deliktsarten Grundregeln festgelegt werden können.[30] Im Bitcoin-System stellt sich ergänzend zu der gängigen Problematik der Bestimmung des Handlungs- und Erfolgsorts die Schwierigkeit, dass die Blockchain bei jedem Nutzer, der einen Full-Client[31] verwendet, gespeichert ist und somit nicht zentral an einem bestimmten Ort vorliegt. Wie im Rahmen des Strafanwendungsrechts mit solch einer dezentralen Speicherung umzugehen ist, ist eine bisher noch kaum thematisierte Fragestellung, die an dieser Stelle jedoch nicht weiter abgehandelt werden soll.

II. Herkömmliche Fallkonstellationen im Zusammenhang mit Bitcoins

Aufgrund der Tatsache, dass virtuelle Währungen rechtlich weder Geld[32] noch – mangels Körperlichkeit – eine Sache darstellen,[33] kommen Geldfälschungsdelikte sowie solche Delikte, die eine Sache erfordern, von vornherein nicht als Straftatbestand in Betracht.

Es ist jedoch festzustellen, dass Bitcoins bei der Ausführung von Straftaten eine Geldersatzfunktion einnehmen. So spielen sie z.B. bei Phishing-Konstellationen,[34] Handel mit illegalen Gütern und Dienstleistungen über »virtuelle Schwarzmärkte«[35] oder auch der Unterstützung des sog. Islamischen Staates (IS) eine Rolle.[36] Wobei bislang mangels offizieller Bestätigung ungeklärt ist, ob und in welchem Umfang die Terrorismusfinanzierung mit Bitcoins tatsächlich existiert. Darüber hinaus konnten für das Bitcrime-Projekt Auswertungsergebnisse des Bundeskriminalamtes zu virtuellen Währungen genutzt werden,[37] im Rahmen derer festgestellt wurde, dass virtuelle Währungen in Deutschland besonders häufig bei Cybercrime-Delikten im engeren Sinne, Erpressungen[38] und betrügerischen Handlungen eingesetzt werden. Erpressungshandlungen erfolgten insbesondere im Zusammenhang mit Ransomware[39] und Cryptolockern[40] sowie der Kontamination von Waren und der Drohung mit DDoS-Attacken[41]. Neben den klassischen Straftatbeständen des Betrugs oder der Erpressung (§ 263 und § 253 StGB) kommt in diesen Fällen den §§ 202a ff., 303a ff. StGB eine bedeutende Funktion zu. Dies gilt insbesondere auch für die Konstellation des sog. »Bitcoin-Diebstahls«, bei dem die Täter oftmals im Sinne des »klassischen« Hackings in fremde Computersysteme eindringen, um Wallet-Zugangsdaten abzufangen und so an die privaten Schlüssel zu gelangen,[42] die zum Tätigen von Transaktionen benötigt werden. Werden die erlangten Schlüsselpaare zum Ausführen einer Transaktion verwendet, ist zu untersuchen, ob dies eine Täuschung im Rechtsverkehr bei der Datenverarbeitung

---

bühren der zentrale Anreiz zur Beteiligung am System sein; hierzu https://en.bitcoin.it/wiki/Transaction_fees.

22 Auf eine detaillierte Beschreibung des Mining Prozesses wird hier verzichtet, da sie für die weiteren Betrachtungen nicht benötigt wird. Weitere Details finden sich unter https://en.bitcoin.it/wiki/Mining und den verlinkten Seiten in der Dokumentation der Bitcoin-Community.

23 Die Begrenztheit folgt aus der Konvergenz der geometrischen Reihe, vgl. hierzu https://en.bitcoin.it/wiki/Controlled_supply.

24 *Werkmeister/Steinbeck* wistra 2015, 209 (211).

25 Matt/Renzikowski-StGB/*Basak*, 2013, § 9 Rn. 3; NK-StGB/*Böse*, 4. Aufl. 2013, § 9 Rn. 3.

26 So auch *Werkmeister/Steinbeck* wistra 2015, 209 (211).

27 BGHSt 20, 45; 44, 52; Matt/Renzikowski/*Basak* (Fn. 25), § 9 Rn. 7; *Fischer*, StGB, 62. Aufl. 2015, § 9 Rn. 4; *Safferling*, Internationales Strafrecht, 2011, § 3 Rn. 15 ff.

28 MüKo-StGB/*Ambos*, 2. Aufl. 2011, § 9 Rn 16; *Werkmeister/Steinbeck* wistra 2015, 209 (211).

29 *Jenssen*, Der Erfolg und seine Bedeutung für das Strafrecht, 1915, S. 44.

30 Beispielsweise liegt der Erfolgsort bei den Verletzungsdelikten dort, wo der Verletzungserfolg eingetreten ist, dazu: MüKo-StGB/*Ambos* (Fn. 28), § 9 Rn. 19; *Breuer* MMR 1998, 141 (142). Wohingegen bei den Tätigkeitsdelikten schlichtweg kein Erfolgsort existiert und nur auf die Handlung des Täters abgestellt werden kann, RGSt 1, 279 (281); OLG Stuttgart NStZ 2004, 402 (403); Sch/Sch-StGB/*Eser*, 29. Aufl. 2014, § 9 Rn. 6b.

31 Bei einem Full-Client lädt sich der Nutzer die gesamte Blockchain herunter und speichert diese. Momentan besitzt die Blockchain eine Größe von ca. 61 Gigabyte.

32 Vgl. *Kütük/Sorge* MMR 2014, 643 (644).

33 Bei Bitcoins handelt es sich nämlich nicht um greifbare Münzen, sondern im Prinzip nur um reine digitale Informationen, vgl. *Kütük/Sorge* MMR 2014, 643 (644).

34 Vgl. http://www.coindesk.com/bitcoins-popularity-boosts-phishing-scam-success/.

35 Zu erwähnen ist hier insbesondere der Fall Silk Road, vgl. dazu http://www.theguardian.com/technology/2013/nov/10/silk-road-internet-market-illegal-drugs-ross-ulbricht; http://nation.time.com/2013/10/04/a-simple-guide-to-silk-road-the-online-black-market-raided-by-the-fbi/.

36 Siehe http://www.spiegel.de/netzwelt/netzpolitik/anonymous-wie-hacker-die-is-propaganda-ausschalten-wollen-a-1063067.html; http://www.dw.com/en/bitcoin-islamic-states-online-currency-venture/a-18724856; http://www.dw.com/en/us-teenager-sentenced-to-prison-for-supporting-islamic-state-online/a-18680144.

37 *Verf.* danken dem BKA für die Überlassung der Auswertungsergebnisse.

38 Vgl. die Fallbeispiele unter http://www.heise.de/security/meldung/Erste-Erpressungen-nach-Patreon-Hack-3014624.html?wt_mc=nl.heisec-summary.2015-11-26 und http://www.spiegel.de/netzwelt/web/erpressung-mit-bitcoin-pizza-lieferanten-sollen-schutzgeld-zahlen-a-977840.html.

39 Erpresserische Schadsoftware, welche den Zugriff auf das befallene Gerät erschwert oder gänzlich verhindert. Die erneute Freigabe wird in Gegenleistung einer Zahlung versprochen.

40 Fallbeispiel zu einer Erpressung mittels Cryptolocker siehe unter http://thehackernews.com/2013/10/cryptolocker-ransomware-demands-300-to.html.

41 Berichte von Drohung mit DDos-Attacken sind z.B. unter https://blogs.akamai.com/2014/12/dd4bc-anatomy-of-a-bitcoin-extortion-campaign.html zu finden.

42 http://www.heise.de/newsticker/meldung/Bitcoin-Boerse-Bitstamp-19-000-Bitcoins-gestohlen-2511223.html, auch bei der ehemals größten Bitcoin Börse Mt. Gox wurde zunächst ein Angriff durch Hacker vermutet: http://www.spiegel.de/netzwelt/web/bitcoin-hacker-beschuldigen-mt-gox-geschaeftsfuehrer-a-957803.html.

nach § 270 StGB darstellt. Maßgebliche Frage in diesem Zusammenhang ist, ob bei einer erfolgten Transaktion eine unechte Urkunde vorliegen würde. Insbesondere die Ausstellererkennbarkeit ist, aufgrund der Pseudonymität des Bitcoin-Systems und der daraus folgenden schwierigen bzw. sogar in vielen Fällen (noch) unmöglichen Zuordnung eines öffentlichen Schlüssels zu einer bestimmten Person,[43] zu bezweifeln.

III. Neue Fallkonstellationen im Zusammenhang mit Bitcoins

Im Rahmen des Bitcoin-Minings entstehen neue Konstellationen, die auf eine Strafbarkeit hin zu untersuchen sind. Der Prozess des Minings rentiert sich, sofern es zu der Gutschrift von Bitcoins kommt, welche den durch die investierte Rechenleistung verursachten Ressourcenverbrauch (Strom und Abschreibung der Hardware) kompensiert. Einen größeren Gewinn erzielt man folglich, wenn das Mining auf fremde Rechnung stattfindet. Hierbei gibt es zahlreiche Vorgehensweisen. Als Beispiel soll ein Fall, den der *BGH* zur erneuten Verhandlung an das *LG Kempten* zurückverwiesen hat, dienen.[44] Hier entwickelten die Täter eine Schadsoftware, die u.a. ab einer Inaktivität des Nutzers von 120 Sekunden den infizierten Rechner zum Mining nutzte.[45] Da es sich bei derartigem Bitcoin-Mining laienhaft ausgedrückt um »Diebstahl von Rechenleistung« handelt, mag man zunächst an die Norm des § 248c StGB denken – die Entziehung elektrischer Energie. Die im Jahre 1900 eingeführte Norm[46] ist jedoch vom Wortlaut her auf solch technische Konstellationen nicht anwendbar, sodass eine Strafbarkeit hiernach auszuschließen ist. Für den soeben geschilderten Fall kann jedoch über die §§ 202a, 303a StGB Abhilfe geschaffen werden, auch ein Computerbetrug könnte in Betracht kommen. Insbesondere im Rahmen des § 202a StGB ist jedoch eine genaue technische Bestimmung der Funktionsweise der Schadsoftware – speziell eine detaillierte Ermittlung, welche Zugangssicherung bestand und wie diese umgangen wurde – erforderlich.[47]

IV. Insbesondere: Geldwäsche nach § 261 StGB

Neben den bisher erläuterten Straftatbeständen, kommt der Geldwäsche nach § 261 StGB bei Sachverhalten unter Einbezug von Bitcoins eine bedeutende Rolle zu.

1. Eignung von Bitcoins zur Geldwäsche

Verschiedene Institutionen, wie z.B. die für internationale Geldwäscheprävention zuständige Financial Action Task Force (on Money Laundering) (FATF) oder auch die Europäische Bankenaufsichtsbehörde (EBA) haben das neuartige Phänomen Bitcoin zum Anlass genommen, Stellungnahmen abzugeben.[48] Als eines der großen Risiken sämtlicher virtueller Währungen, und im Besonderen von Bitcoin, wird sehr häufig die Geldwäschegefahr hervorgehoben.[49] Zurückgeführt wird dies auf zwei wesentliche Eigenschaften des Bitcoin-Systems: die Pseudonymität und die Dezentralität. Zwar handelt es sich nicht um ein anonymes Zahlungssystem. Durch das ständige Wechseln der Bitcoin-Adressen,[50] was zu Anonymisierungszwecken sogar ausdrücklich empfohlen wird, ist die Verwendung von Bitcoins jedoch deutlich anonymer als bei gesetzlichen Zahlungsmitteln. Das gilt insbesondere dann, wenn Anonymisierungsdienste zur weiteren Verschleierung des »Geldflusses« eingesetzt werden.[51]

Die Eignung zur Geldwäsche ergibt sich zudem auch aus der zweiten wesentlichen Eigenschaft von Bitcoin – der Dezentralität. Dem System fehlt es an einer zentral verwaltenden Stelle. Um am Netzwerk teilzunehmen ist keine Identifizierung in der Realwelt[52] – wie dies z.B. bei der Eröffnung eines Kontos erforderlich ist – von Nöten (kein sog. »know your customer« Prinzip – KYC).[53] Entscheidend im Zusammenhang mit der Geldwäsche ist zudem die hindernislose Grenzüberschreitung. Der Eintausch von Bitcoins in gesetzliche Zahlungsmittel ist weltweit über Plattformen möglich und kann auch über Netzwerke wie »local bitcoins«[54] unproblematisch zwischen Privatleuten gegen Bargeld erfolgen. Die Attraktivität des Bitcoin-Systems zum Waschen inkriminierter Gelder ist demnach nicht von der Hand zu weisen.

2. Probleme im Zusammenhang mit § 261 StGB

Im Zusammenhang mit § 261 StGB stellen sich im Bereich von Bitcoins mehrere Fragen. Bereits bei der Problematik, ob sie überhaupt unter den Gegenstandsbegriff des § 261 StGB zu subsumieren sind, wird deutlich, dass es sich bei virtuellen Währungen um ein neuartiges Phänomen handelt, das mit den klassischen Rechtsbegriffen nur schwer zu fassen ist. Geläufig wird der Gegenstand im Sinne des § 261 StGB als Sache oder Recht definiert.[55] Mangels Körperlichkeit lassen sich Bitcoins nicht unter den Sachbegriff subsumieren.[56] Das Fehlen einer zentralen Instanz hat darüber hinaus den Effekt, dass sie auch nicht – anders als das beim Buchgeld der Fall ist – als Forderungsrecht bezeichnet werden können.[57] Anhand einer umfassenden Auslegung muss geprüft werden, ob Bitcoins dennoch Gegenstand und damit taugliches Tatobjekt einer Geldwäsche darstellen. Daneben ist die im Rahmen des § 261 StGB seit jeher umstrittene Frage

43 Vgl. *Goger* MMR 2016, 431.
44 BGH, Beschl. v. 21.07.2015 – 1 StR 16/15, juris; LG Kempten, 6 KLs 223 Js 7897-13 jug sowie nun die erneute Entscheidung des LG Kempten, 2 KLs 223 Js 7897/13 (3).
45 Neben dem Bitcoin Mining wie hier mittels Schadsoftware, kommt dieses auch noch im Rahmen von Cloud-Computing, vgl. http://www.wired.com/2014/07/how-hackers-hid-a-money-mining-botnet-in-amazons-cloud/ oder mittels Nutzung fremder Rechner, vgl. http://www.pressetext.com/news/20140611013, vor.
46 *Fischer* (Fn. 27), § 248c Rn. 1.
47 So auch der BGH, Beschl. v. 21.07.2015 – 1 StR 16/15, juris Rn. 17.
48 http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf (zuletzt abgerufen am 16.06.2016); https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf (zuletzt abgerufen am 16.06.2016).
49 Insbesondere im Zusammenhang mit Silk Road: http://www.spiegel.de/netzwelt/netzpolitik/silk-road-vier-jahre-gefaengnis-fuer-bitcoin-haendler-a-1014228.html.
50 Jeder Client kann beliebig viele Schlüssel erzeugen, vgl. *Boehm/Pesch* MMR 2014, 75 (76).
51 Eine Untersuchung solcher Dienste befindet sich bei: *Möser/Böhme/Breuker* (Fn. 18).
52 *Bollen* JBFLP 2013 (v. 01.05.2013), 1 (7); *Boehm/Pesch* MMR 2014, 75 (76).
53 *Safferling/Rückert* MMR 2015, 788 (790).
54 https://localbitcoins.com/. Von Deutschland aus ist die Seite jedoch nicht mehr erreichbar, vgl. hierzu: http://bitcoinblog.de/2014/12/08/localbitcoins-aus-grunden-der-regulierung-nicht-mehr-in-deutschland-verfugbar/ (zuletzt abgerufen am 16.06.2016).
55 BT-Drs. 12/989, S. 27; *Burr*, Geldwäsche, 1995, S. 55; *Körner/Dach*, Geldwäsche, 1994, Rn. 12; *Leip*, Der Straftatbestand der Geldwäsche, 2. Aufl. 1999, S. 65; *Voß*, Das Tatobjekt der Geldwäsche, 2007, S. 16 f.
56 Siehe dazu schon unter **C.II**; vgl. auch *Rückert* MMR 2016, 295 (296); *Goger* MMR 2016, 431 (432).
57 So auch: *Kütük/Sorge* MMR 2014, 643 (644); *Rückert* MMR 2016, 295 (296); *Goger* MMR 2016, 431 (432).

des Umgangs mit »Mischkonstellationen« zu untersuchen.[58] Die neueste Rechtsprechung des *BGH* zu dieser Problematik im Rahmen der Zusammenführung von illegalen und legalen Geldern auf einem Konto,[59] die im Rahmen des Tatbestandsmerkmals »herrühren« relevant wird, wirft zum einen die Frage auf, ob und wenn ja wann, eine solche Vermischung bei Bitcoin vorliegt. Auch im Bereich der Tathandlungen des § 261 Abs. 1 und Abs. 2 StGB ergeben sich zahlreiche Fragestellungen. Dabei ist zu untersuchen, ob das Tätigen einer Transaktion stets unter eine solche zu subsumieren ist. Insbesondere das Verwenden im Sinne von § 261 Abs. 2 Nr. 2 StGB, das als jeder bestimmungsgemäße Gebrauch zu definieren ist,[60] wird regelmäßig gegeben sein.[61] Dabei ist § 261 Abs. 6 StGB, der dem gutgläubigen Erwerber eines inkriminierten Gegenstandes ermöglichen will, diesen unbeeinträchtigt von Abs. 2 veräußern zu können, zu beachten.[62] Da sich die Norm explizit nur auf Abs. 2 beschränkt, stellt sich die Frage, ob sie nicht ins Leere läuft, sofern durch das Tätigen einer Transaktion auch stets eine Tathandlung des Abs. 1 vorliegt. Ein besonderes Augenmerk wird dabei auf den Varianten des Gefährdens der Herkunftsermittlung bzw. des Auffindens liegen. Im Rahmen des Vorsatzes und der Leichtfertigkeit sind die Auswirkungen eines Transaktionsblacklistings zu untersuchen.[63]

D. Neue Herausforderungen für die Strafverfolgung

Neue Herausforderungen für die Strafverfolgung ergeben sich in juristischer Hinsicht aus den besonderen technischen Gegebenheiten des Bitcoin-Netzwerks, welche die Ermittlungstätigkeit erschweren.

I. Erschwerung der Ermittlungstätigkeit durch Dezentralität und Pseudonymität

Ermittlungen im Bereich virtueller Kryptowährungen werden vor allem durch die Dezentralität des Bitcoin-Netzwerks und die Pseudonymität der Bitcoin-Nutzer erschwert. Ersteres führt dazu, dass die »klassischen« Ermittlungsmethoden bei Verfolgung von Geldströmen nicht anwendbar sind. Mangels zentraler, verwaltender Stelle (Bank) ist kein Adressat vorhanden, an den ein Auskunftsersuchen nach §§ 161, 95 StPO[64] gerichtet werden könnte. Auch eine Durchsuchung und Beschlagnahme von Bankunterlagen gem. §§ 94 ff. StPO ist deshalb nicht möglich. Mangels Bearbeitung der Vorgänge im Bitcoin-Netzwerk durch Bankmitarbeiter können diese auch nicht als Zeugen vernommen werden.[65] Als Ausgleich für den Wegfall dieser Instrumente kommt eigentlich nur eine Analyse der öffentlich einsehbaren Blockchain in Betracht. In ihr lässt sich die Spur von Bitcoins über sämtliche Transaktionen hinweg bis zu deren Entstehung durch Mining[66] zurückverfolgen. Allerdings ist zunächst nur eine Verfolgung der Bitcoins über die verschiedenen Bitcoin-Adressen (öffentliche Schlüssel) möglich.[67] Diese können jedoch von jedem Bitcoin-Nutzer selbst in beliebiger Zahl erstellt werden,[68] ohne dass hierfür eine verwaltende Instanz notwendig ist, welche eine Identitätsprüfung vornehmen könnte (wie z.B. bei der Eröffnung eines Girokontos, vgl. § 24c Abs. 1 KWG). Dies führt zu einem weiteren Hindernis für Ermittler: Die Verfolgung der »Geldspur« führt – anders als bei Buchgeld – nicht unmittelbar zur Identifikation der beteiligten Personen.

II. Mögliche Lösung: Datenanalyse und Datenverknüpfung

Einen möglichen Ausweg bieten dabei die öffentlich einsehbaren Transaktionsdaten in der Blockchain.[69] Diese können mittels moderner Datenerhebungs- und Datenverarbeitungsmethoden mit anderen Datensätzen, z.B. aus anderen Bereichen des Internets, verknüpft werden, um Bitcoin-Adressen bestimmten natürlichen oder juristischen Personen oder Personengruppen (z.B. kriminelle, oder terroristische Vereinigungen) zuordnen zu können.[70] Für den Rechtsanwender (z.B. die anordnende Staatsanwaltschaft) stellt sich hierbei die Frage, ob der Einsatz einer solchen Datenerhebungs- und Datenverknüpfungssoftware auf bereits bestehende Standardbefugnisse – wie z.B. §§ 100a,[71] 98a, 100g, 110 Abs. 3 StPO – gestützt werden kann oder ob zumindest die Grenzen der Ermittlungsgeneralklauseln (§§ 161, 163 StPO) – also vor allem eine nur »geringfügige« Grundrechtsbeeinträchtigung[72] – eingehalten werden können. Für den Fall, dass für bestimmte Anwendungsfälle (zu denken ist hier vor allem an die besonders eingriffsintensive automatisierte Gewinnung von Rasterdaten[73]) beides nicht in Betracht kommt, müssen für den Software-Einsatz neue Ermächtigungsnormen durch den Gesetzgeber geschaffen werden.

E. Prävention durch Transaktionsblacklisting – ein Problemanriss

Die bestehenden Schwierigkeiten der Strafverfolgung könnten durch eine wirksame Präventionsstrategie abgemildert werden. Ziel muss es dabei sein, die Verwendung virtueller Kryptowährungen für Kriminelle so unattraktiv wie möglich zu machen, ohne dabei zu stark in die Freiheit der legitimen Nutzer von Bitcoin & Co einzugreifen.

---

58 Siehe dazu z.B. nur die Ausführungen bei *Bischofberger,* Zur Auslegung des Tatbestandsmerkmals »Herrühren« im Rahmen des Straftatbestandes § 261 StGB, S. 141 ff.; *Fischer* (Fn. 27), § 261 Rn. 8; MüKo-StGB/*Neuheuser* (Fn. 28), § 261 Rn. 53 ff.

59 BGH StV 2016, 19.

60 *Fischer* (Fn. 27), § 261 Rn. 26; MüKo-StGB/*Neuheuser* (Fn. 28), § 261 Rn. 69, a.A: NK-StGB/*Altenhain* (Fn. 25), § 261 Rn. 116, der das Gebrauchen zu eigenen oder fremden Zwecken ausreichen lässt.

61 Bei gesetzlicher Währung sind von dieser Tathandlungsvariante vielfältige Geldgeschäfte erfasst, vgl. BT-Drs. 12/989, S. 27; LK-StGB/*Schmidt/Krause,* 12. Aufl. 2010, § 261 Rn. 21.

62 BT-Drs. 12/3533, S. 14.

63 Dazu siehe unter E.

64 Vgl. hierzu: *Meyer-Goßner/Schmitt*-StPO, 58. Aufl. 2015, § 95 Rn. 1 f.; *Singelnstein* NStZ 2012, 593 (603).

65 Zum Ganzen *Safferling/Rückert* MMR 2015, 788 (791).

66 Zum Prozess des Minings, bei dem neue Bitcoins generiert werden, vgl. C.III.

67 Zu einer solchen Blockchain-Analyse: *Ober/Katzenbeisser/Hamacher,* Future Internet 2013, Vol. 5, S. 237 ff.

68 Vgl. *Spindler/Bille* WM 2014, 1357 (1358).

69 Bspw. einsehbar unter: www.blockchain.info.

70 Vgl. *Reid/Harrigan,* in: Altshuler/Elovici/Cremers/Aharony/Pentland (Hrsg.), Security and Privacy in Social Networks, S. 197, S. 210 ff.; sowie *Sadeghi/Ron/Shamir,* Financial Cryptography and Data Security, 2013, S. 6; *Meiklejohn* et al, in: Proceedings of the 2013 conference on Internet measurement conference, S. 127; eine forensische Analyse der Blockchain bieten zum Beispiel Dienstleister wie www.walletexplorer.com, www.blockchain.info oder www.chainalysis.com an.

71 Hierzu *Safferling/Rückert* MMR 2015, 788.

72 Hierzu BGHSt 51, 211 (218) = StV 2007, 115; *Meyer-Goßner/Schmitt*-StPO (Fn. 64), § 161 Rn. 1.

73 Zum Begriff der Rasterdaten: *Klever,* Rasterfahndung nach § 98a StPO, 2003, S. 163 (165 f. m.w.N.).

I. Die Idee des Transaktionsblacklistings

Ein Ansatz kann dabei in einer Transaktions-Sperrliste (folgend: Blacklisting) liegen.[74] Dienstleistern, welche gewerblich einen Tausch von Bitcoins in Realwährung oder Waren (und umgekehrt) anbieten, wäre es gesetzlich verboten, Bitcoins in Realwährung zu wechseln oder als Zahlungsmittel zu akzeptieren, wenn sich diese bis zu einer gesperrten Transaktion im Bitcoin-System zurückverfolgen lassen würden.[75] In die Sperrliste aufgenommen würden Transaktionen, wenn bspw. durch ein gerichtliches Verfahren feststeht, dass die Bitcoins durch eine Straftat erworben oder hervorgebracht wurden. Hierdurch könnte zum einen verhindert werden, dass die Kriminellen selbst ihre »illegal« erworbenen Bitcoins in Realwährung tauschen. Zum anderen würden auch legitime Nutzer dazu angehalten, solche Bitcoins nicht mehr als Erfüllung von Geschäften anzunehmen, weil sie diese Bitcoins dann ebenfalls nicht mehr in eine Realwährung eintauschen könnten.[76]

So kompliziert dieser Ansatz auf den ersten Blick erscheinen mag, er weist gegenüber anderen, klassischeren Präventionsmaßnahmen erhebliche Vorteile auf. Die Implementierung eines Know-Your-Customer-Prinzips (vgl. § 24c Abs. 1 KWG) bei Bitcoin-Dienstleistern[77] ist beispielsweise deshalb nicht effektiv, weil die (kriminellen) Bitcoin-Nutzer wegen der Dezentralität des Bitcoin-Netzwerks nicht auf die Inanspruchnahme der Dienstleister zur Abwicklung ihrer Geschäfte angewiesen sind.[78]

II. Herausforderungen für den Gesetzgeber

Den Gesetzgeber – der ein Blacklisting-System implementieren müsste – stellt ein so neuartiges Präventionskonzept wie das Transaktions-Blacklisting vor mannigfaltige juristische Herausforderungen. So stellt die faktische Entwertung der Bitcoins, die auch einen an den Straftaten völlig Unbeteiligten treffen kann, wenn der Sperrlisteneintrag zu einem Zeitpunkt erfolgt, an dem die Bitcoins bereits an einen Unbeteiligten weiter transferiert wurden,[79] einen schwerwiegenden Eingriff in Art. 14 Abs. 1 GG dar (in dessen entwicklungsoffenen Schutzbereich virtuelle Kryptowährungen durchaus fallen können).[80] Dieser Eingriff kann nur unter strenger Beachtung des Verhältnismäßigkeitsprinzips, z.B. durch Normierung von Härtefall-, Entschädigungs- und Rechtsschutzvorschriften erfolgen. Auch für den Fall der Vermischung von »legalen« und »illegalen« Bitcoins durch Zusammenfassung in Transaktionen müsste eine Regelung für eine anteilige[81] »Vergiftung« der vermischten Bitcoins gefunden werden.[82] Das Verhältnis einer solchen Sperrliste zu den bestehenden Vorschriften der Vermögensabschöpfung des StGB[83] müsste geklärt werden, um eine doppelte Abschöpfung (durch Sperrlisteneintrag und Einziehung oder Verfall) zu vermeiden. Das Risiko für Nicht-Tatbeteiligte, ihre (ohne ihre Kenntnis) von einem Kriminellen erhaltenen Bitcoins durch einen Sperrlisteneintrag nicht mehr eintauschen zu können, müsste durch eine Einsehbarkeit der Sperrliste und einen Risikobewertungsdienst[84] für Bitcoin-Nutzer abgemildert werden.

III. Verhältnis zur Geldwäschestrafbarkeit

Diese Maßnahmen werfen allerdings ihrerseits Fragen im Verhältnis zur Geldwäschestrafbarkeit nach § 261 StGB auf,[85] da in solch einem Fall das Wissen um die illegale Herkunft dieser Bitcoins bei deren Benutzung Vorsatz begründen kann. Bei Bitcoin handelt es sich trotz der Pseudonymität um ein äußerst transparentes System. In der für jedermann einsehbaren Blockchain ist eine komplette Rückverfolgbarkeit des »Geldweges« anders als bei Bar- und Buchgeld möglich. Diesen Umstand nutzt das hier erläuterte Modell des Blacklistings. Die Auswirkungen eines solchen Systems auf die Geldwäsche sind jedoch nicht nur beim Vorsatz, sondern auch beim Leichtfertigkeitstatbestand des § 261 Abs. 5 StGB zu untersuchen, weil der Bitcoin-Nutzer dann vor Annahme der Bitcoins die Möglichkeit hat, deren kriminelle Herkunft (oder zumindest eine gewisse Wahrscheinlichkeit für eine kriminelle Herkunft) zu prüfen. Hierbei ist insbesondere zu untersuchen, welche Rolle Risikobewertungsdienste spielen, welche die Wahrscheinlichkeit berechnen, dass sich eine Transaktion in Zukunft auf einer Sperrliste befinden wird.[86]

---

74 Vgl. *Möser/Böhme/Breuker* (Fn. 18); *Möser/Böhme/Breuker* (Fn. 11), S. 16 ff.
75 Vgl. *Möser/Böhme/Breuker* (Fn. 11), S. 16.
76 Vgl. *Möser/Böhme/Breuker* (Fn. 11), S. 16 (22 f.).
77 Ein solches Konzept wird z.B. bereits von www.bitcoin.de verwendet.
78 Vgl. *Möser/Böhme/Breuker* (Fn. 11), S. 16 (19).
79 Hierzu: *Möser/Böhme/Breuker* (Fn. 11), S. 16 (21).
80 Zur Offenheit des grundgesetzlichen Eigentumsbegriffs: BVerfGE 83, 201 (209); 101, 239; BVerfG NJW 2005, 589 (Internet-Domain); allgemein: Maunz/Dürig-GG/*Papier*, 75. EL 09/2015, Art. 14 GG Rn. 8 ff., 55 ff.
81 Eine Totalkontamination (vgl. BGH NStZ 2015, 703 = StV 2016, 19 zur Geldwäsche bei Buchgeld) wäre bei Bitcoins (wohl) wegen der vollständigen Nachverfolgbarkeit der Transaktionskette und des Verweises auf bestimmte Transaktionsoutputs unverhältnismäßig.
82 Zu sog. Haircut- und FIFO-Modellen: *Möser/Böhme/Breuker* (Fn. 11), S. 16 (21 f.).
83 Zur Anwendbarkeit der §§ 73 ff. StGB auf Bitcoin: *Rückert* MMR 2016, 295; *Goger* MMR 2016, 431.
84 Vgl. *Möser/Böhme/Breuker* (Fn. 11), S. 16 (22 ff.).
85 Vgl. dazu schon unter **C.IV.**
86 Zu der Einführung solcher Risikobewertungsdienste siehe: *Möser/Böhme/Breuker* (Fn. 11), S. 16 (17).