Im zweiten Teil beleuchtete Gollnick die Thematik aus der Sicht des Insolvenzverwalters. Er wies darauf hin, dass ein TOA in der Insolvenz des Täters selbst ausscheidet, weil der Verwalters weder Vertreter des Täters noch des Schuldners ist. Anders kann dies aber bei Unternehmensinsolvenzen zu beurteilen sein. Hier stehen regelmäßig mögliche Haftungsansprüche gegenüber dem unredlichen Geschäftsführer bzw. Geschäftsleiter nach den §§ 64 GmbHG, 130a Abs. 2 HGB im Raum. Unabhängig von grundlegenden Fragen der Regresspflicht, etwa dem Nachweis von Handeln trotz und währen Zahlungsunfähigkeit bzw. Überschuldung, Problemen des Haftungsumfangs und der Durchsetzbarkeit von Ansprüchen, sah der Referent keine Probleme, Vergleiche mit potentiellen Tätern bzw. einen TOA mit dem ungetreuen Firmenverantwortlichen mit Sinn und Zweck des Insolvenzverfahrens zu vereinbaren. Er verwies in dem Zusammenhang zudem auf den Schutz, den das Verwendungsverbot des § 97 InsO[29] bei der Gestaltung des kommunikativen Prozesses zwischen Verwalter und betroffenem Unternehmensorgan begründet. Gollnick riet aber dazu, etwaige derartige Vereinbarungen jedenfalls der Gläubigerversammlung zu Genehmigung vorzulegen, schon um etwaige Untreuevorwürfe (§ 266 StGB) zu verhindern. Denn das Einverständnis der Gläubigergesamtheit schließt bereits den Tatbestand der Untreue aus.[30]

Beide Referenten wollten ihre Gedanken, die ebenfalls in Aufsatzform in einer der nächsten ZInsO-Hefte veröffentlicht werden sollen, als Anstoß gewertet sehen, die Frage des TOA im Insolvenzstrafrecht weiter zu erörtern, und dessen Anwendungsmöglichkeiten zu prüfen und verstärkt zu beachten.

VI. Ausblick

Nach den einzelnen Vorträgen ergaben sich umfangreiche – teils durchaus auch kontroverse – Diskussionen zwischen den Anwesenden. Nach Tagungsende wurde die Gespräche bei Fingerfood und Kölsch bis in die Abendstunden fortgesetzt.

Die diesjährigen Organisatoren laden schon jetzt ein zum 6. Kölner Insolvenzstrafrechtstag, der – voraussichtlich – im Mai 2020 stattfinden wird. Ein gleichfalls interessantes und abwechslungsreiches aktuelles Programm ist auch bei dieser Veranstaltung zu erwarten.

---

[29] S. zum Verwendungsverbot des § 97 InsO Püschel, ZInsO 2016, 262, einerseits, Weyand, ZInsO 2015, 1948, andererseits.
[30] S. nur MünchKomm-StGB/Dierlamm, 3. Aufl. 2019, § 266 Rn. 143 m.w.N. S. zur „Entscheidungshoheit der Gläubigergemeinschaft" schon Buchalik/Hiebert, ZInsO 2014, 109, 110.

Rezensionen

Geldwäsche

Oberstaatsanwalt Dr. Marcus Schmitt, Wien

Johanna Grzywotz: Virtuelle Kryptowährungen und Geldwäsche (= Internetrecht und Digitale Gesellschaft Bd 15).

Duncker & Humboldt, Berlin 2019, 372 S., 79,90 €

Die gegenständliche Publikation wurde im Sommersemester 2018 vom Fachbereich Rechtswissenschaft der Friedrich-Alexander-Universität Erlangen-Nürnberg als Dissertation angenommen.

I. Einleitung

Kryptowährungen (insbesondere Bitcoin) und Geldwäsche haben eines gemeinsam: Sie sind ein weltweites Phänomen, das nicht an Landesgrenzen halt macht. Wie alle schnell wachsenden Technologien ziehen auch das Internet und die dort als Zahlungsmittel verwendeten Krypotwährungen, von denen Bitcoin eine herausragende Stellung einnimmt, Menschen an, die die neu eröffneten Möglichkeiten für kriminelle Zwecke zu nutzen suchen. Aufgrund vermeintlicher Anonymität von Bitcoin – eigentlich muss man von Pseudonymität sprechen, da alle Transaktionen auf der Blockchain gespeichert werden – erscheinen diese zum Zwecke der Geldwäsche im Zusammenhang mit Kriminalität im Internet geeigent.

Ziel der Arbeit ist es zu untersuchen, ob das materielle Strafrecht, insbesondere der § 261 StGB, den technischen Herausforderungen, die sich durch Bitcoin stellen, gewachsen ist. Hierbei arbeitet die Autorin heraus, an welchen Stellen es Anpassungen bedarf und zeigt auf, dass neue Technologien nicht nur ein Risiko, sondern auch eine Chance darstellen, vorhandenen Problemen im materiell-rechtlichen Bereich des § 261 StGB zu begegnen.

II. Grundlagen zu Bitcoin

Die Arbeit gliedert sich (neben Einleitung und Zusammenfassung) in vier große Kapitel. Zunächst gibt die Autorin im **zweiten** Kapitel einen umfassenden Überblick über die technischen Parameter und die Erzeugung von Bitcoin durch Mining sowie die Blockchain, welche allen digitalen Währungen zugrunde liegt. Kryptowährungen weichen insbesondere durch ihre dezentrale Struktur, dh das Fehlen von zentralen Autoritäten von herkömmlichen Währungssystemen ab. Bitcoin kann nicht als Bargeld qualifiziert werden, da ihnen zum einen die Körperlichkeit fehlt und zum anderen die Einordnung als gesetzliches Zahlungsmittel. Auch als Buchgeld können sie nicht eingestuft werden, weil Buchgeld das Vorliegen einer Forderung gegenüber einem Kreditinstitut verlangt. Eine zentrale Stelle, gegenüber der die Forderung bestehen kann, existiert im denzentral organisierten System der Blockchain gerade nicht.

Oftmals werden Bitcoin mit E-Geld verwechselt. Bei beiden handelt es sich um digitale Zahlungsmittel. Da aber auch E-Geld (wie Buchgeld) eine Forderung gegenüber einem Emittenten darstelt, können Bitcoin nicht als E-Geld qualifiziert werden, da im Bitcoin-System kein zentraler Emittent existiert, gegenüber dem eine Forderung vorliegen könnte. Als weiterer Unterschied zu E-Geld werden Bitcoin nicht im Austausch gegen gesetzliche Zahlungsmittel geschaffen. Auch wenn Bitcoin als Zahlungsmittel Verwendung finden, so erfüllen sie definitionsgemäß die volkswirtschaftlichen Geldfunktionen von Bar-, Buch- und E-Geld nicht.

III. Grundlagen zu Geldwäsche

Im nächsten **dritten** Kapitel wendet sich die Autorin dem Phänomen der Geldwäsche zu. Sie stellt die Entwicklung und die zahlreichen nachträglichen Änderungen des 1992 in das StGB aufgenommenen § 261 auf dem Hintergrund internationaler rechtlicher Vorgaben dar. Für eine auf Bitcoin abzielende Analyse des § 261 StGB ist die Beantwortung der Frage nach dem Sinn und Zweck der Norm erforderlich.

Der Tatbestand der Geldwäsche wurde vornehmlich im Zusammenhang mit der Bekämpfung der organisierten Kriminalität geschaffen. Er ist aber nicht auf Delikte organisierter Kriminalität eingeschränkt. Anknüpfungspunkt für die Strafverfolgung bilden bei der Bekämpfung der Geldwäsche illegale Erlöse, die in den legalen Finanz- und Wirtschaftskreislauf eingespeist werden sollen. Durch Aufspüren der illegalen Zahlunsflüsse sollen die Profite der kriminellen Organisationen eingezogen und damit diese selbst ihre Existenzgrundlage verlieren. Für die Täter darf sich kriminelles Handeln nicht lohnen. Als geschütztes Rechtsgut des § 261 StGB sieht die Autorin den Schutz der Strafrechtspflege mit ihrer Aufgabe, die Wirkungen von Straftraten zu beseitigen.

Herkömmliche Geldwäschetechniken lassen sich durch das Drei-Phasen-Modell charakterisieren:

- Einspeisung (Placement): Die illegal erlangten Vermögenswerte werden im legalen Finanz- und Wirtschaftskreislauf untergebracht, zB wird Bargeld durch Einzahlung auf

(viele) Konten in Buchgeld umgewandelt oder in Wertgegenstände, welche selbst wieder möglichst einfach zu verkaufen sind.

- Verschleierung (Layering): Die illegale Herkunft des Geldes soll weiter verdeckt werden, um die Papierspur (paper trail) zu verwischen und zu unterbrechen, so dass die Rückverfolgung der illegalen Herkunft der Vermögenswerte nicht mehr möglich ist. Die geschieht insbesondere durch eine Vielzahl von Transaktionen unter Zwischenschaltung unverdächtiger Dritter (Treuhänder). Online Transaktionen vereinfachen die Vernichtung der Papierspur wesentlich.
- Integration: Die illegal erlangten Werte werden in den legalen Finanz- und Wirtschaftskreislauf zurückgeführt. In dieser Phase wird die illegale Verbindung endgültig unterbrochen. Die Vermögenswerte werden nur noch mit legalen Geschäften in Verbindung gebracht. Die einfachste Methode hierfür stellt der Erwerb von Immobilien oder Edelmetallen mit Hilfe der mehrfach verschobenen Vermögenswerte dar. Eine andere Methode bildet die Tilgung eines inländishen Kredites mit ausländischen (inkriminierten) Geldern oder die die Gründung bzw. Erwerb von Unternehmen.

IV. Bitcoin und Geldwäsche – eine Zusammenführung

Im daran anschließenden **vierten** Kapitel untersucht die Autorin das Zusammentreffen beider Phänomene, nämlich die Eignung von Kryptowährungen (Bitcoin) zur Geldwäsche. Neben der Fincancial Action Task Force (FATF) und der Europäischen Bankenaufsicht haben in den vergangenen Jahren auch die EZB und die EU-Kommission auf die Geldwäscherisiken, die sich im Zusammenhang mit Krypotwährungen (Bitcoin) stellen, in verschiedenen Dokumenten hingewiesen. Diese Risiken liegen insbesondere im hohen Grad der Anonymisierung (Pseudonymisierung) und der Dezentralisierung. Neben der Pseudonymität und Dezentralität von Bitcoin sieht die Autorin die Globalität des Bitcoin- Netzwerkes als zentrale Eigenschaften, welche Geldwäscherisiken in sich bergen. Mangels Zentralität gibt es im Bitcoin Netzwerk keine zentrale Stelle, welche verdächtige Transaktionen prüft und meldet. Es gibt keine Banken, die diese Rolle übernehmen könnten. Bitcoin ist zwar kein anonymes Zahlungsmittel, aber ein pseudonymes. Sämtliche Transaktionen sind in der Blockchain verzeichnet. Sie können aber nicht ohne weiteres einer bestimmten Person zugeordnet werden, zumal sich jeder Teilnehmer am Bitcoin-System rasch wechselnd eine Vielzahl von Bitcoin-Adressen zulegen kann. Die Zuordnung der Adressen zu den dahinterstehenden Personen ist denkbar, eine Identifizierung aber nur erschwert möglich. Schließlich sind Transaktionen weltweit ohne Hindernisse möglich, insbesondere auch in und aus Ländern, die keine ausreichende Geldwäscheprävention betreiben. Es gibt keine Kontrollinstanzen. Im Gegensatz zu Bargleld müssen (digitale) Bitcoins nicht über Ländergrenzen hinweg physisch tranportiert werden. Dezentralität, Pseudonymität und Globalität von Bitcoin machen das System grundsätzlich zum Waschen inkriminierter Werte geeignet.

Die drei klassichen Phasen der Einspeisung (Placement), Verschleierung (Layering) und Integragion bei der Geldwäsche sind auch im Falle von Bitcoin anwendbar. Bitcoin stellt hierfür (lediglich) eine neue Technik zur Verfügung. In der Phase der Einspeisung werden entweder (i) inkriminierte Werte (außer Bitcoin), v.a. Fiat-Geld, durch Umtauschtransaktionen im Bitcoin-System platziert oder (ii) inkriminierte Bitcoin-Werte selbst in das System eingespeist.

Umtauschdienstleister unterliegen den Geldwäschepräventionsvorschriften der Länder, in denen sie ansässig sind. Hier ist am ehesten eine Identifierung der Nutzer durch Anwendung des Know-Your-Customer Prinzips möglich. Bitcoins können aber auch direkt aus den Katalogtaten der Geldwäsche erworben werden, zB beim Verkauf von Drogen oder durch Zahlungen nach Erpressungen mit sog. Ransomware (eine durch einen Hacker-Angriff vorgenommene Verschlüsselung von Computernetzwerken in Unternehmen oder Institutionen wird erst nach Zahlung von Lösegeld, typischer Weise in Bitcoin, wieder aufgehoben). Die vom Opfer bezahlten (inkriminierten) Bitcoin befinden sich bereits im System und müssen daher nicht erst noch eingespeist werden.

In der Phase der Verschleierung werden die inkriminierten Bitcoins durch weitere Transaktionen verschoben. Da eine Person eine unendlich große Zahl von Adressen generieren kann, können die transferierten Bitcoins in der Verfügungsmacht derselben Person verbleiben. Die Bitcoins können so leicht von derjenigen Person, die sie ursprünglich ins Netzwerk eingespeist hat, lösgelöst und ohne Aufwand auch über Ländergrenzen hinweg transferiert

werden. Die Spur der Transaktionen bleibt aufgrund der Transparenz der Blockchain nachvollziehbar. Problemtisch ist aber die Identifizierung der Personen, die hinter diesen stehen (Pseudonymität des Systems). Durch Mixing-Dienste kann die Rückverfolgbarkeit erschwert und damit der Grad der Anonymität erhöht werden.

In der Phase der Integration werden Bitcoins in staatliche anerkannte Werte (Fiat-Geld) umgetauscht oder andere Vermögenswerte (zB Immobilien, Edelmetalle etc) mit Bitcoins bezahlt. Der Auszahlungsvorgang kann in ein Land verlegt werden, welches keine oder nur geringe Geldwäschekontrollen anwendet.

Verlustrisikien bilden bei Geldwäsche mit Bitcoin die erheblichen Kursschwanungen. Umgekehrt können diese aber auch dazu genutzt werden, noch weitere Gewinne zu generieren. Nicht zuletzt wäre hier noch zusätzlich zu den von der Autorin genannten Risiken zu erwähnen, dass durch Einspeisung von hohen Fiat-Geldbeträgen in das System (etwa zwei- und dreistellige Millionenbeträge) aufgrund des zum Teil geringen Handelsvolumens auf den verschiedenen Platformen der Kurs allein durch solche Transaktionen negativ beeinflusst werden kann und sohin Verluste im Rahmen der Geldwäsche entstehen.

V. Analyse des § 261 StGB im Hinblick auf Bitcoin

Im **fünften** Kapitel der Arbeit untersucht die Autorin die Anwednbarkeit des § 261 StGB auf Bitcoin. Zunächst geht sie dabei auf die Anwendbarkeit des deutschen Strafrechts ein.

1. Anwendbarkeit des deutschen Strafrechts

Die Tathandlungen des § 261 Abs 1 Var. 1 und 2 (Verbergen und Verschleiern) StGB sowie die Ausführungshandlungen des Abs 2 bilden abstrakte Gefährdungsdelikte. Deutsches Strafrecht kann nur zur Anwendung gelangen, wenn der Ort, von dem der Täter die Geldwäschehandlung mit Bitcoin vornimmt, im Inland belegen ist.

Bei den Tathandlungen des § 261 Abs 1 Var. 3 (Vereiteln) und Var. 4 (Gefährden) StGB handelt es sich um Erfolgsdelikte. Die Anwendbarkeit des deutschen Strafrechts ist gegeben, wenn Anknüpfungspunkte für einen Erfolgseintritt in Deutschland gefunden werden können. Beispielsweise befindet sich der Inhaber der Empfängeradresse oder die Bitcoins selbst aufgrund der Wallet als Belegenheitsort in Deutschland. Auch transaktionsbezogene Anknüpfungspunkte können gefunden werden, wenn die Transaktion mit Hilfe eines deutschen Dienstleisters ausgeführt wird oder durch einen deutschen Bitcoin-Knoten geleitet oder von einem deutschen Miner verarbeitet wird.

2. Rechtswidrige Vortat

Die Anwendbarkeit des Tatbestands der Geldwäsche bedarf einer **rechtswidrigen Vortat**. Die in der Praxis mit Bitcoin begangenen Straftaten können unter die im Katalog des § 261 Abs 1 StGB gelisteten Normen subsumiert werden. Bei betrügerischen oder erpresserischen Handlungen muss die gewerbsmäßige oder bandenmäßige Begehung hinzukommen, damit eine taugliche Vortat für Geldwäsche vorliegt. Die Täter suchen sich in der Regel aber eine Vielzahl von Opfern aus, so dass zumeist eine gewerbsmäßige Begehung zu bejahen ist.

Durch die technische Funktionsweise des Bitcoin-Systems bieten sich für Verbrecher neue Handlungsmöglichkeiten. Bedeutsam sind hier zwei Sachverhalte, nämlich (i) das fremdnützige Bitcoin-Mining und (ii) der Bitcoin-Diebstahl.

Beim (i) fremdnützigen Bitcoin-Mining wird die Rechenleistung nicht selbst aufgebracht, sondern fremde Hardware verwendet, um eigene Strom- und Hardwarekosten zu sparen. Hiezu wird entweder Schadsoftware auf einem Computer oder ohne Zustimmung ein Update installiert, das ohne Wissen und Kenntnis der Berechtigten Miningprozesse durchführt. Die Autorin sieht hierin insbesondere den Tatbestand des § 263a StGB (Computerbetrug) erfüllt, welcher eine taugliche Vortat zur Geldwäsche bildet.

Beim (ii) Bitcoin-Diebstahl werden fremde Bitcoins entwendet. Dies geschieht insbesondere dadurch, dass der Täter den privaten Schlüssel eines Bitcoin-Eigentümers erlangt und mit diesem eine Transaktion auf eine fremde Wallet durchführt. An einen solchen digitalen Schlüssel gelangt man meist durch Phishing- oder Hacking-Attacken. Der Diebstahl im engeren Sinne erfolgt dann durch die Verwendung des Schlüssels im Rahmen der Transakti-

on. In den Fällen des Bitcoin-Diebstahls im engeren Sinne (dh nur Durchführung der Transaktion) sieht die Autorin die Tatbestände der §§ 266 StGB (Untreue, im Falle des Bestehens einer Vermögensbetreuungspflicht), 263a StGB (Computerbetrug), 269 StGB (Fälschung beweiserheblicher Daten), 270 StGB (Täuschung im Rechtsverkehr bei Datenverarbeitung) und 303a StGB (Datenveränderung) erfüllt. Außer § 303a StGB stellen diese Tatbestände, wenn gewerbsmäßig oder bandenmäßig begangen (was in der Praxis häufig der Fall sein wird), taugliche Vortaten zur Geldwäsche dar.

3. Gegenstandsbegriff und Bitcoin

Eine Strafbarkeit wegen Geldwäsche erfordert, dass eine der in § 261 Abs 1 oder 2 StGB genannten Tathandlungen an einem **Gegenstand** vorgenommen wird, der aus einer tauglichen Vortat herrührt. Demzufolge untersucht die Autorin, ob Bitcoins unter den Gegenstandsbegriff der Geldwäsche subsumierbar sind. Vom **klassischen** Gegenstandsbegriff sind bewegliche oder unbewegliche Sachen sowie Rechte an solchen und Forderungen erfasst. Ihnen allen muss ein Vermögenswert zukommen. Damit Bitcoins vom **klassischen** Gegenstandsbegriff umfasst werden, müssen sie eine Sache oder ein Forderungsrecht darstellen. Da Bitcoins jedenfalls keine Köperlichkeit zukommt, ist eine Subsumtion unter den Sachbegriff zu verneinen. Auch die Subsumtion unter ein Forderungsrecht lehnt die Autorin ab, da im dezentralen Bitcoinsystem keine Forderung gegenüber einem Dritten (Emittenten) besteht.

Da Bitcoin vom klassischen Gegenstandsbegriff nicht erfasst werden, gelangt die Autorin nach einer detaillierten Auslegung des Gegenstandsbegriffs auf Grundalgen der grammatischen, historischen, systematischen und teleologieschen Methode zu dem Schluss, dass die klassiche Definition des Gegenstands, die ihn auf Sachen und Forderungsrechte beschränkt, nicht zwingend ist.

Sie entwickelt eine Definintion des Gegenstandsbegriffs anhand der drei Merkmale **Abgrenzbarkeit, Vermögenswert und Ausschlussfunktion**: Ein Gegenstand muss abgrenzbar sein, einen Vermögenswert bilden und andere von der Eigentümerschaft ausschließen. Demzufolge schlägt sie die Aufnahme einer Legaldefinition in § 261 Abs 1 StGB vor, wonach Gegenstand jede abgenzbar, vermögenswerte Position mit Ausschlussfunktion bezeichnet. Unter eine solche Definition des Gegenstandes würden auch virtuelle Güter wie Bitcoin fallen und sohin vom Tatbestand des § 261 Abs 1 StGB erfasst werden.

4. Herrühren

Geldwäsche erfordert weiters das Herrühren des Gegenstandes aus einer rechtswidrigen Vortat. Für den Begriff des Herrührens besteht keine Legaldefinition. Er ist sehr weit gefasst. Es genügt, dass der Gegenstand seinen Ursprung in der Vortat hat. Minimales Erfordernis ist somit Kausalität. Die Autorin analysiert drei Fallgruppen, die auf Bitcoin übertragen werden können: (i) unmittelbar aus der Vortat erlangte Gegenstände; (ii) Surrogate; (iii) Vermischung legaler und illegaler Werte.

Unter (i) fallen Bitcoin, die direkt durch die Straftat erlangt werden (*scelere quaesita*), etwa beim Verkauf von Drogen, aber auch wenn sie aus der Vortat hervorgebracht wurden (*producta seceleris*), etwa beim Mining mittels Schadsoftware. Unter (ii) fallen Tatobjekte, wenn der betroffene Gegenstand als Ersatz aus nachfolgenden Vermögenstransaktionen hervorgeht. Werden Bitcoin im Tausch gegen inkriminiertes Fiat-Geld (Reallgeld) erlangt, bilden sie ein Geldwäschesurrogat. Gleiches gilt, wenn vom inkriminierten Fiat-Geld Mining Hardware angeschafft wird. Die Hardware bildet ein Surrogat, nicht mehr aber die mit der erworbenen Hardware geschürften neuen Bitcoins. Durch (iii) Vermischung legaler und illegaler Werte soll es (im Gegensatz zu Giralgeld) bei Bitcoin nicht zu einer Totalkontamination aller Werte kommen, sondern lediglich zu einer Teilkontamination. Denn in der Blockchain kann jede Transaktion bis zur ersten (illegalen) Transaktion zurückverfolgt werden. Der sog. „Sperrlistenansatz" dient der Prävention von Geldwäsche im Bitcoin-Netzwerk, indem er inkriminierte Transaktionen listet. Die Aufnahme inkriminierter Bitcoins auf die Sperrliste soll dazu führen, dass Umtauschdienstleister gelistete Bitcoins nicht mehr annehmen dürfen und diese damit faktisch entwertet werden. Eine solche Sperrliste ist öffentlich zugänglich.

5. Tathandlungen

An dem Gegenstand, der aus der Straftat herrührt, muss eine taugliche Tathandlung vorgenommen werden. Diese sind in § 261 Abs 1 und 2 StGB definiert. Auf Bitcoin angewendet, ergeben sich folgende Anwendungsbereiche:

Verbergen: Bitcoins als nicht-körperliche Gegenstände können nicht verborgen werden. Dies wäre allerdings bei Hardware, zB USB-Sticks, Paper-Wallets etc, auf denen private Schlüssel gespeichert bzw abgedruckt sind, der Fall.

Verschleiern der Herkunft: Bei einfachen Transkationen ist das Verschleiern aufgrund der Transparenz der Blockchain, die eine Rückverfoglung inkriminierter Tranaktionen bis zum Ursprung zulässt, nicht möglich. Eine Verbindung von Sender- und Emfpängeradresse kann bei einfachen Transaktionen stets hergestellt werden. Anderes gilt aber bei Einschaltung von Mixing-Services. Hier wird die Verbindung von Sendern und Empfängern durch die Zwischenschaltung zahlreicher Transaktionen verwischt, so dass der Tatbestand des Verschleierns erfüllt ist.

Gefährden oder Vereiteln der Herkunftsermittlung oder des Auffindens: Ein Gefährden/Vereiteln der Herkunftsermittlung oder des Auffindens eines inkriminierten Gegenstandes liegt vor, wenn dieses verhindert wird. Bei einer normalen Transaktion im Bitcoin-System ist es stets möglich, durch die Blockchain die Entstehung eines Bitcoins bis zu seinem Ursprung zu ermitteln. Es ist nachvollzihbar, welcher Bitcoin-Adresse die betroffenen Bitcoins zuzuordnen sind. Das Auffinden und die Herkunftsermittlung werden sohin nicht verhindert. Nicht bekannt sind allerdings die Personen, die über die Bitcoin-Adressen verfügen können (Pseudonymität). Der tatsächliche Zugriff auf die Bitcoins wird daher durch eine Transaktion erschwert, da ein Zugriff nur mit Hilfe des privaten Schlüssels möglich ist. An den privaten Schlüssel kann man nur gelangen, wenn man die Person, der die zugehörige Bitcoin-Adresse zuzuordnen ist, ermittelt und identifiziert wird. Da die bloße Identifizierung der Personen noch nicht den Zugriff ermöglicht, sondern hiezu erst der private Schlüssel erlangt werden muss, ist der Zugriff auch bei bekannten Personen jedenfalls im Sinne des § 261 Abs 1 StGB erschwert. Denn das Gefährden bzw Vereiteln der Herkunftsermittlung oder des Auffindes ist deswegen pönalisiert, weil hierdurch der Zugriff gefährdet wird. Mit der Pönalisierung der Geldwäsche soll der Staat aber gerade Zugriff auf die inkriminierten Vermögenswerte erhalten, damit diese dem legalen Finanz- und Wirtschaftskreislauf entzogen werden können. Insoweit ist die Tathandlung des Gefährdens oder Vereitelns der Herkunftsermittlung oder des Auffindens auf Bitcoins anwendbar.

Sich oder einem Dritten verschaffen/Verwahren/Verwenden (§ 261 Abs 2 StGB): Werden inkriminierte Bitcoins, die ein Nutzer von einem anderen erhalten hat, an eine eigene oder dritte Adresse transferiert, so stellt dies ein Sichverschaffen dar. Die Inhaberschaft eines privaten Schlüssels bildet ein Verwahren (Gewahrsame durch Verfügungsmacht). Das Tätigen einer Transaktion ist ein Verwenden. Ein tatbildliches Verwahren oder Verwenden liegt allerdings dann nicht vor, wenn der Täter die illegale Herkunft des Gegenstands zu dem Zeitpunkt, zu dem er ihn erlangt hat, nicht kannte. Ein Verwahren oder Verwenden bein Tätigen einer Transaktion ist nur dann anzunehmen, wenn der Täter im Zeitpunkt des Erhalts der inkriminierten Bitcoins, die er weiter transferiert, deren illegale Herkunft kannte. Dies gilt insbesondere für Mixing-Services, Zahlungsdienstleister und Umtschausdienstleister, die (inkriminierte) Bitcoins entgegennehmen und anschließend weitere Transaktionen durchführen. Bei Umtauschdienstleistern bildet der umgetauschte Gegenstand ein Surrogat.

6. Stellungnahme

Die Autorin legt eine stringent gegliederte und fundierte Studie zur Thematik von virtuellen Währungen (Bitcoins) und Geldwäsche vor. Die Arbeit zeichnet sich nicht nur durch eine tiefgehende und detaillierte Analyse des § 261 StGB im Blick auf Bitcoins aus, sondern auch durch eine Darstellung der technischen Grundlagen des Bitcoin-Netzwerks und einem allgemeinen Überblick über das Phänomen Geldwäsche. Dies erleichtert einem Leser, der möglicherweise noch kein eingehenderes Wissen zu Kryptowährungen (Bitcoins) besitzt, das Verständnis erheblich. Auch wenn die Arbeit als Dissertation eine gründliche wissenschaftliche Analyse der Problematik der Anwendung des Geldwäschestraftatbestandes zum Ziel hat, sind weite Teile auch als Lektüre für den Praktiker, der in der Strafverfolgung oder -verteidigung steht, geeignet, sich eingehendes Wissen zu einem Phänomen anzuei-

genen, das in den letzten Jahren immens an Bedeutung gewonnen hat und weiter gewinnt, da die Blockchaintechnologie unser Leben maßgeblich mit beeinflussen wird. Dies wird grundsätzlich auch für digitale Währungen gelten, mögen sich auch bestimmte einzelne Kryptowährungen nicht durchsetzen. Die Arbeit kann daher jedem mit der Problematik Befassten oder daran Interessierten nachdrücklich empfohlen werden.