„Junges Publizieren“

Seminararbeit von

Halime Erez

Das Schürfen von Bitcoins unter heimlicher Nutzung fremder Computer

Julius-Maximilians-Universität Würzburg
Juristische Fakultät
Prof. Dr. Helmut Baier
Abgabedatum: 14.03.2019

Inhaltsverzeichnis

I. Einführung

Das Internet ist aus dem alltäglichen Leben nicht mehr wegzudenken. Neben seinen Vorteilen hat es auch seine Dunkelfelder: dank umgänglicher technischer Möglichkeiten bietet sich für kriminell anvisierte Personen an, die Vorteile des Internets zu missbrauchen. Der sog. Cybercrime hat sich hieraus entwickelt. Als Cybercrime definiert das Bundeskriminalamt (BKA) „die Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richtet oder die mittels dieser Informaionstechnik begangen werden“.[1] Dabei ist eine stetig wachsende Kriminalitätsentwicklung zu verzeichnen: im Jahre 2017 zeigte sich ein deutlicher Anstieg der begangenen Straftaten von Cybercrime im engeren Sinne. Die Onlinequellen PKS verzeichnet dabei einen Anstieg um 4,0 % gegenüber dem Vorjahr.[2] Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) verzeichnete in einer Studie zudem, dass jeder zweite Internetnutzer Opfer von Cyberattacken wurde.[3] Ein Kriminalitätsphänomen im Bereich des Cybercrimes ist im Zusammenhang mit Umgang von virtuellen Kryptowährungen zu vernehmen. Aufgrund ihrer einfachen Handhabung, der anonym ablaufenden Transaktionen sowie ihrer Unabhängigkeit von einer staatlichen Institution stellen sie ein attraktives digitales Zahlungsmittel für Kriminelle dar. Hochaktutell ist in Deutschland das Schürfen (engl. „mining“ von „mine“ = „Schürfen“) von Bitcoins unter heimlicher Nutzung fremder Computer.[4] Anfang des Jahres 2019 wurden sog. Stromdiebe in Sachsen gefasst, die den Stromverbrauch über fremde Computer abzapften, um mittels technischen Einsatzses Bitcoins zu schürfen und sich diese gutzuschreiben. Bislang gestaltete sich das konventionelle Schürfen von Bitcoins in Deutschland als sehr kostspielig, da damit hohe Rechenleistungen der Computer und auch der hohe Stromverbrauch zusammenhängen. Abhilfe schaffen jedoch neu entwickelte technische Werkzuege, die selbst für Techniklaien relativ leicht zu handhaben sind. So kann der Stromverbrauch auf fremde Rechner abgewälzt und sich der Gewinn geschürfter Bitcoins zu Eigen gemacht werden. Diese Arbeit soll thematisieren, ob das materielle Strafrecht dem neuen technischen Phänomen des Bitcoins und ihrer kriminellen Handhabung gerecht wird. Für eine Auseinandersetzung ist zuächst die Kenntnis des technischen Hintergrunds des Bitcoin-Systems erforderlich. Im Anschluss werden die einschlägigen Straftatbestände bei dem illegalen Bitcoin-Mining in ihrer Reichweite geprüft. Der Fokus liegt hierbei auf dem Einsatz sog. Botnetze, die durch Schadprogramme, wie Trojaner, aufgebaut werden.[5] Je nach Ausgang der strafrechtlichen Erfassung steht die Frage nach gesetzgeberischem Handlunsgbedarf im Raum. Vorschläge, wie der Gesetzesentwurf zu dem sog. digitalen Hausfriedensbruch § 202e StGB, werden eingehend in ihrer Wirkung analysiert. Ferner stellt sich das Problem der anschließenden Handhabung erfasster Bitcoins: unterfallen sie überhaupt der Vermögensabschöpfung im strafprozessualen Verfahren? Schließlich wird im abschließenden Teil der Arbeit auf neue Herausforderungen für die Strafverfolgungsbehörden eingegangen, die sich durch virtuelle Kryptowährungen eröffnet haben. Dabei werden „klassische“ Ermittlungsmaßnahmen, wie die Beschlagnahme und Durchsuchung, durch die Pseudonymität der Bitcoin-Nutzer schnell an ihre Grenzen gebracht. In dem Sinne werden einige Präventionsmaßnahmen angeschnitten. Zum Schluss wird auf die Bedeutung virtueller Kryptowährungen und ihrer strafrechtlich zu erwartenden Entwicklung eingegangen.

---

1 https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Internetkriminalität/internetkriminali-taet_node.html (zuletzt abgerufen am 5.3.19).

2 BKA-cybercrime, Bundeslagebild 2017, abrufbar unter: https://www.google.com/search?client=sa-fari&rls=en&q=bka+cybercrime+bun-deslage.bild+2017&ie=UTF-8&oe=UTF-8 (zuletzt abgerufen am 5.3.19).

3 https://www.bitkom.org/Presse/Presseinformation/Cybercrime-Jeder-zweite-Internetnutzer-wurde-Opfer.html (zuletzt abgerufen am 5.3.19).

4 https://deutsche-wirtschafts-nachrichten.de/2019/02/07/sachsen-razzien-gegen-stromdiebe-zum-bitcoin-mining/; https://coinkurier.de/stromraub-gestoppt/ (zuletzt abgerufen am 5.3.19).

5 *Werner*, Verkehrspflichten privater IT-Nutzer in Bezug auf die Verbreitung von Schadsoftware, 2010, S. 57.

II. Das Phänomen virtueller Währungen

1. Definitionsversuch

Virtuelle Währungen exisitieren in Form von Daten, die kryptographisch eine eigenständige Existenz gewinnen. Von der Europäischen Bankenaufsichtsbehörde (EBA) werden virtuelle Währungen als „digitale Abbilund von Wert, der nicht von einer Zentralbank oder Behörde geschaffen wird und auch keine Verbindung zu gesetzlichen Zahlungsmitteln haben muss“ definiert.[6] Hieraus leiten sich die Kryptowährungen ab.[7] Kryptowährungen sind verschlüsselte Ersatzwährungen, die auf der Idee einer nichtstaatlichen Konstruktion basieren.[8] Zudem ist die Geldmenge bei den meisten Kryptowährungen begrenzt.[9] Derzeit existieren ca. 1990 Kryptowährungen. Die bekannteste von ihnen ist Bitcoin (Einheit: BTC).[10]

2. Was ist Bitcoin?

Bitcoins sind im Grunde als digitale, nicht-staatliche Währungen zu verstehen.[11] Sie werden definiert als „ein konsensorientiertes Netzwerk, welches ein neues Zahlungssystem und vollständig digitales Geld möglich macht“. Als Kryptowährung wird das Netzwerk nur von den Nutzern und ohne zentrale Stelle betrieben.[12] Bitcoin wurde erstmals am 1.November 2008 in der Veröffentlichung des Arbeitspapiers mit dem Titel „Bitcoin: A Peer-to- Peer Electronic Cash System“ unter dem Pseudonym „Satoshi Nakamoto“ über eine Krypto-Mailingliste erwähnt. Die Bitcoin-Software war schließlich ab Januar 2009 erstmals verfügbar.[13]

a) Funktionsweise von Bitcoins

Das von Nakamoto erstellte System der Bitcoins ist die einer Open-Source-Software.[14] Dies ist eine quellenoffene Software, die öffentlich zugänglich ist.[15] Alle Geräte, die hierdurch miteinander verbunden sind, bilden das Netzwerk, in dem Bitcoins erworben, verwaltet und übertragen werden. Daher ist von einem sog. Peer-to-Peer-Netzwerk die Rede. „Peer-to-peer“ (P2P) ist die Akkumulation für Netzwerke mit gleichberechtigten Nutzern („peers“) ohne übergeordnete Instanz.[16]

aa) Bitcoin-Transaktionen

Bitcoins sind eine Kette digitaler Signaturen.[17] Innerhalb des Bitcoin-Systems werden nicht Münzen, sondern Werteinheiten durch Änderung wertzuweisender Informationen übertragen.[18] Für die Zuordnung der Werte wird

---

6 EBA-European Banking Authority, EBA Opinion on „virtual currencies“, 4.7.2014, S. 11, abrufbar unter: https://eba.europa.eu/sites/default/documents/files/documents/10180/657547/81409b94-4222-45d7-ba3b-7deb5863ab57/EBA-Op-2014-08%20Opinion%20on%20Virtual%20Currencies.pdf?retry=1 (zuletzt abgerufen am 13.2.2019).
7 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, 2019, S. 27.
8 *Schlund/Pongratz*, DStR 2018, 598 (600).
9 *Grzywotz*, S. 27.
10 *Heine*, NStZ 2016, 441 (442).
11 https://www.heise.de/newsticker/meldung/Bankraub-und-Erpressung-mit-Bitcoins-1702157.html (zuletzt abgerufen am 10.3.19).
12 https://bitcoin.org/de/faq#allgemein (zuletzt abgerufen am 17.2.19).
13 https://bitcoin.org/de/faq#wer-hat-bitcoin-erfunden (zuletzt abgerufen am 13.2.19).
14 *Vogel*, Relevanz & Risiken von virtuellen Währungen am Beispiel von Bitcoin, 2016, S. 21.
15 *Kochheim*, Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik, 1. Aufl. (2015), S. 619.
16 *Bittner*, BLJ 2017, 63, abrufbar unter: https://law-journal.de/archiv/jahrgang-2017/heft-1/bitcoin/ (zuletzt abgerufen am 14.2.19).
17 *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, S. 2, abrufbar unter: https://bitcoin.org/bitcoin.pdf (zuletzt abgerufen am 20.2.2019); *Pesch/Böhme*, DuD 2017, 93 (94).
18 *Safferling/Rückert*, MMR 2015, 788 (790).

ein digitales Signaturverfahren, welches auf asymmetrischer Kryptographie basiert, verwendet.[19] Es werden Schlüsselpaare, bestehend aus jeweils einem öffentlich sowie privaten Schlüssel, erzeugt. Der private Schlüssel ist nur dem Inhaber bekannt und dient der Signatur vorgenommener Transaktionen von Bitcoins. Damit werden Authentizität und Integrität sowie der Schutz gegen Verfügungen durch Unbefugte sichergestellt.[20] Der öffentlich Schlüssel ist jedem Nutzer in dem System bekannt und dient dem Empfang von Transaktionen. Dementsprechend kann der öffentliche Schlüssel als die Bitcoin-Adresse bezeichnet werden. Diese ist vergleichbar mit einer Kontonummer bei geläufigen Geldtransaktionen.[21] Die Verwaltung der Schlüsselpaare findet in den „Wallets" statt, eine Art elektronische Brieftasche.[22] Mit Hilfe der Wallet-Software kann sich jeder Nutzer beliebig viele Schlüsselpaare erzeugen.[23]

bb) Zuordnung von Bitcoins durch die Blockchain

Bitcoins unterscheiden sich von staatlich anerkannten Währungen insbesondere durch ihre Dezentralität; es fehlt an einer zentralen Instanz, wie eine Bank, die für die Abwicklung der Übertragung von Bitcoins zuständig ist und garantiert, dass der Kunde das Geld hat. Es besteht daher der Bedarf einer „Ersatz-Institution".[24] Für das Bitcoin-System wird diese Funktion von der „Blockchain" übernommen. Sie bildet die gesamte Transaktionshistorie ab, indem sie mehrere Datenblöcke darstellt, die jede einzelne jemals durchgeführte Transaktion enthält.[25] Nur die hier aufgelisteten Transaktionen gelten als durchgeführt und bestätigt.[26] So lässt sich jeder Bitcoin-Betrag zurückverfolgen.[27]

cc) Ergänzung der Blockchain durch das Bitcoin-Mining

Neben dieser Verifikationsfunktion ist die Blockchain auch Quelle neuer Bitcouns durch jede neue Transaktion.[28] Damit Transaktionen bewerkstelligt und an die vorhandenen Blöcke angehängt werden können, muss ausreichend Rechenleistung zur Verfügung stehen und von den Teilnehmern beigesteuert werden (sog. Distributed Ledger Technology).[29] Zur Absicheurng dieses Prozesses muss ein Arbeitsnachweis („Proof of work") erbracht werden, indem sof. „mathematische Rätsel" gelöst werden.[30] Mit jedem neuen Block entsteht wachsender Rechenaufwand, der es immer schwieriger macht, einen gültigen Block rückgängig zu machen und somit die gesamte Blockchain zu manipulieren.[31] Hierfür müssen enorme Ressourcen aufgewendet werden, wie der Stromverbrauch und die Abschreibung der Hardware.[32] Da das Mining eine kostspielige Angelegenheit ist, bedarf es eines gewissen Anreizes. Der Miner wird durch Ausschüttung neuer Bitcoins belohnt. Daneben können auf freiwilliger Basis die Transaktionsgebühren dem Miner gutgeschrieben werden.[33] Diese Belohnung wird alle 210.000-Miningvorgänge halbiert. Hierdurch wird die Bitcoin-Menge auf 21 Millionen begrenzt. Denkt man die Halbierung weiter, so

19 *Kütük/Sorge*, MMR 2014, 643.
20 *Grzywotz/Köhler/Rückert*, StV 2016, 753 (754).
21 *Sorge/Krohn-Grimberghe*, DuD 2012, 479.
22 *Spindler/Bille*, WM 2014, 1357; *Heine*, NStZ 2016, 441 (442).
23 *Kütük/Sorge*, MMR 2014, 643.
24 *Grzywotz*, S. 41; *Kaplanov*, Nerdy Money: Bitcoin, the Private Digital Currency, and the Case Against its Regulation, Consumer Law Review 2012, 111 (118), abrufbar unter: https://lawecommons.luc.edu/cgi/viewcontent.cgi?article=1920&context=lclr (zuletzt abgerufen am 13.10.2020).
25 *Boehm/Pesch*, MMR 2014, 75 (76); *Dinesh/Erlich/Gilfoyle/Jared/Richard/Pouwelse*, Operational Distributed Regulation for Bitcoin, abrufbar unter: https://arxiv.org/pdf/1406.5440.pdf (zuletzt abgerufen am 8.10.2020), S. 2.
26 *Ammann*, CR 2018, 379; *Möser/Böhme/Breuker*, An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem, abrufbar unter: https://maltemoeser.de/paper/money-laundering.pdf (zuletzt abgerufen am 8.10.2020), S. 2.
27 *Pesch/Böhme*, DuD 2017, 93 (94).
28 Vgl. *Grzywotz*, S. 42.
29 *Ammann*, CR 2018, 379; *Grzywotz*, S. 42.
30 *Beck*, NJW 2015, 580; *Nakamoto*, S. 3.
31 *v. Hauff*, Illegales Crypto-Mining, abrufbar unter: http://rechtundnetz.com/illegales-crypto-mining/ (zuletzt abgerufen am 21.2.19).
32 *Vogel*, S. 23.
33 *Grzywotz/Köhler/Rückert*, StV 2016, 753.

werden nach dem Jahre 2140 keine weiteren Bitcoins mehr ausgegeben.[34]

b) Versuch rechtlicher Einordnung von Bitcoins

aa) Einordnung als Geld

Bislang existiert keine gesetzliche Definition des Begriffes des Geldes.[35] Allerdings steht fest, dass Banknoren und Münzen als einzige gesetzliche Zahlungsmittel anerkannt sind nach Art. 123 Abs. 1 S. 3 AEUV, Art. 88 Abs. 1 GG, § 14 Abs. 1 S. 2 BbankG. Da es bei Bitcoins an der Anerkennung als gesetzliches Zahlungsmittel und der Körperlichkeit fehlt, scheidet die Einordnung als Geld aus.[36] Weiterhin wäre an die Einordnung als Buchgeld zu denken. Dabei ist das Vorliegen einer Forderung und somit eine zentrale Stelle, über welche die Transaktion erfolgen soll, erforderlich. Außerdem enthält das Buchgeld eine Forderung auf gesetzliche Zahlungsmittel. Mangels Zentralität im Bitcoin-Netzwerk und einer Drittperson, von der aus die Forderung ausgeht, sind Bitcoins nicht als Buchgeld einzuordnen. In Betracht kommt ferner die Zuordnung als E-Geld, welche ebenfalls ein digitales Zahlungsmittel ist. Gem. § 1a Abs. 3 ZAG ist E-Geld jeder elektronisch gespeicherte monetäre Wert in Form einer Forderung gegenüber dem Emittenten, der gegen Zahlung eines Geldbetrages ausgestellt wird, um Zahlungsvorgänge i.S.d. § 675f Abs. 3 S. 1 BGB durchzuführen. Jedoch ist hier ebenfalls wegen des Grundgedankens des Bitcoin-Systems eine Einordnung als E-Geld wenig sinnvoll.[37] Somit sind Bitcoins nicht als Bar-, Buch- sowie E-Geld einzuordnen.

bb) Einordnung als Rechnungseinheit i.S.d. KWG

Die BaFin qualifiziert Bitcoins als Finanzinstrumente in Form von Rechnungseinheiten nach § 1 Abs. 11 S. 1 Nr. 7 Alt. 2 KWG.[38] Danach unterliegt derjenige, der gewerbsmäßig im eigenen Namen für fremde Rechnung an- und verkauft und demnach ein erlaubnispflichtiges Finanzkommissionsgeschäft tätigt, der bankenrechtlichen Kontrolle.[39] Die Zuordnung von Bitcoins als Rechnungseinheiten beschert jedoch Einwände. Das *KG* in Berlin verneinte in einer Entscheidung die Qualifikation von Bitcoins als Finanzinstrumente und demnach als Rechnungseinheiten.[40] Begründet wird die Entscheidung damit, der Gesetzgeber habe es bei der Umsetzung des Gesetzes von EG-Richtlinien für notwendig erachtet, Rechnungseinheiten unter die Bankenaufsicht fallen zu lassen. Demnach sollen die gemeinsame Erfassung von Devisen und vergleichbaren Rechnungseinheiten internationalem Standard entsprechen.[41] Es sei allerdings nicht anzunehmen, dass der Gesetzgeber bei Gesetzeserlassung virtuelle Währungen, insb. Bitcoins in seine Betrachtung miteinfließen lassen wolle, da Bitcoins erst im Jahre 2008/09 bekannt wurden. Zudem scheitere eine Auslegung der Erfassung von Bitcoins an fehlender Wertbeständigkeit; es mangele an einer zentralen Stelle, die den Wert von Bitcoins feststelle. Stattdessen bestimmen die Teilnehmer des Bitcoin-Netzwerkes den Preis von Bitcoins individuell.[42]

cc) Steuerrechtliche Handhabung

---

34 *Grzywotz/Köhler/Rückert*, StV 2016, 753; *Bonneau/Miller/Clark/Narayanan/Kroll/Felten*, SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies, abrufbar unter: https://www.ieee-security.org/TC/SP2015/papers-archived/6949a104.pdf (zuletzt abgerufen am 8.10.2020), S. 105.

35 *Spindler/Bille*, WM 2014, 1357; *Beck*, NJW 2015, 580 (581).

36 *Beck*, NJW 2015, 580; *Schlund/Pongratz*, DStR 2018, 598 (599).

37 *Sorge/Krohn-Grimberghe*, DuD 2012, 479 (483); *Grzywotz*, S. 56.

38 BaFin, Merkblatt Finanzinstrumente, abrufbar unter: https://www.bafin.de/DE/Aufsicht/FinTech/VirtualCurrency/virtual_currency_node.html#doc7906358bodyText3, (zuletzt abgerufen am 13.2.19).

39 BaFin Merkblatt, abrufbar unter: https://www.bafin.de/DE/Aufsicht/FinTech/VirtualCurrency/virtual_currency_node.html (zuletzt abgerufen am 15.2.19); *Börner*, NZWiSt 2018, 48.

40 *KG Berlin*, NJW 2018, 3734.

41 BT-Drs. 13/7142, S. 69.

42 *Auffenberg*, NVwZ 2015, 1184.

Der *EuGH* hat entschieden, dass es sich bei einem Umtausch eines Bitcoins in ein konventionelles Zahlungsmittel um einen von der Mehrwertsteuer befreiten Umtausch handele, nach Art. 2 der Richtlinie 2006/112, sofern es von den handelnden Parteien als alternatives Zahlungsmittel akzeptiert werde.[43] Art. 135 Abs. 1 lit. e MwStSystRL sehe nämlich vor, dass sich Umsätze, die sich „auf Devisen, Banknoten und Münzen beziehen, die gesetzliches Zahlungsmittel sind" von der Steuer befreit seien. Demnach dienen Bitcoins keinem anderen Zweck als dem des Zahlungsmittels.[44]

dd) Konsequenz

Die Auffassung von Bitcoins als Rechnungseinheit entspricht zumindest der steuerrechtlichen Beurteilung des *EuGH*. Zudem bringt sie eine gewisse rechtliche Anerkennung mit sich. Dennoch beruht diese Entscheidung nicht auf einer eigenständigen Rechtseinordnung von Kryptowährungen, da sie „lediglich die Konsequenz einer Auslegung der Mehrwertsteuerrichtlinie" ist.[45] Es bedarf daher nach einhelliger Auffassung alsbald einer gesetzlichen Regulierung zur allgemeinen Handhabung und Einordnung von Kryptowährungen.[46]

III. Strafrechtliche Einordnung des fremdnützigen Schürfens von Bitcoins

1. Fremdnütziges Bitcoin-Mining

Der Miningprozess als solcher rentiert sich, sofern es zur „Belohnung" kommt. Belohnt wird jedoch erst dann, wenn die mathematischen Aufgaben gelöst werden. Die Wahrscheinlichkeit, die passende Lösung zu finden, verhält sich dabei proportional zur investierten Rechenleistung. Aufgrund gestiegener technischer Anforderungen ist das Mining kaum noch gewinnbringend, weshalb der Einsatz von Ressourcen notwendig ist. [47] Im Zuge dessen entwickelte sich eine kriminelle Ausprägung des Minings.[48] Fraglich ist, wie das heimliche Schürfen von Bitcoins unter Nutzung fremder Computer nach dem bisher geltenden Strafrecht zu erfassen ist.

2. Strafrechtliche Würdigung des Bitcoin-Minings

a) Bitcoin-Mining mittels Schadsoftware

2015 sah sich der *BGH* erstmals dem Fall des illegalen Bitcoin-Minings konfrontiert:[49] die zwei Angeklagten stellten eine Schadsoftware in Form eines Trojaners her, welches sie auf einer Internetplattform zum Download, getarnt als Musikdatei/Videodatei, verfügbar machten. Die vielfache Installation unwissender Nutzer ermöglichte den Aufbau eines sog. Botnetzes. Dieses verhalf den Tätern das Rechensystem und seiner Rechenleistung zu Eigen zu machen. Nach 120 Sekunden wurde die Schadsoftware selbsttätig und setzte sich mit dem Command & Control-Server in Verbindung, über den sie Rechenaufgaben löste. Somit verschafften sich die Täter den erforderlichen

43 *EuGH*, DStR 2015, 2433.
44 *EuGH*, DStR 2015, 2433 (2437).
45 bank und markt, 3/2018, 20.
46 *Grzywotz*, S. 57; *Börner*, NZWiSt 2018, 48 (50); *Schlund/Pongratz*, DStR 2018, 598; *Rauer*, Beitrag LTO, abrufbar unter: https://www.lto.de/recht/hintergruende/h/kg-161ss2818-bitcoins-rechtliche-einordnung-kein-e-geld-rechnungseinheit/ (zuletzt abgerufen am 23.2.2019); *Dietsch*, MwStR 2018, 250.
47 *V. Hauff*, S. 1.
48 Manager Magazin, abrufbar unter: https://www.manager-magazin.de/digitales/it/computer-betrug-cyberkriminelle-setzen-auf-schuerfen-statt-erpressen-a-1232778.html (zuletzt abgerufen am 23.2.19); *Heine*, NStZ 2016, 441.
49 *BGH*, Beschl. v. 27.7.2017 – 1 StR 412/16.

Ressourceneinsatz für das Schürfen von Bitcoins ohne selbst über die Rechenleistung und Hardware verfügen zu müssen. Damit gewannen sie neu entstandene Bitcoins, die ihrem Guthaben gutgeschrieben wurden.[50] Es folgte eine Verurteilung wegen Ausspähens von Daten in Tateinheit mit Datenveränderung, §§ 202a, 303a, 52 StGB.

aa) Technischer Hintergrund

Zum besseren Verständnis der Strafbarkeit des illegalen Minings mittels Schadsoftware werden vorab einige wichtige technische Begriffe erläutert.

(1) Botnetz

Botnetze sind im Bereich der Cyberkriminalität eines der wichtigsten Täterinstrumente: sie werden zeitweise als das „mächtigste Werkzeug" bezeichnet.[51] Ein Botnetz ist ein Zusammenschluss von Computern, die mit einem Schadprogramm infiziert sind.[52] Der Einsatz eines Botnetzes ermöglicht Cyberkriminellen die unbemerkte Fernsteuerung befallener Rechner.[53] Durch den Betrieb wird das Netzwerk von der Bot Ware in seiner Integrität beeinträchtigt und entzieht Rechenkapazität.[54] Die zentrale Steuerung des Botnetzes erfolgt durch den Command & Control-Server (C&C- Server).[55] Dieser überwacht die „Zombies" (befallene Rechner), versorgt sie mit Updates und versieht sie mit Aufträgen, wie das Schürfen von Bitcoins.[56] Die Verbreitung von Bot Programmen erfolgt meist ohne Einverständnis des betroffenen Nutzers. Bot Programme werden entweder durch die Installation einer Schadsoftware (Trojaner) oder durch den Aufruf einer manipulierten Website verbreitet.[57]

(2) Trojaner

Ein Trojanisches Pferd, kurz Trojaner, ist eine Software, die sich als harmloses Programm tarnt (E-Mail, zum Download angebotene Datei)[58] , aber eigentlich eine Malware (Bot-Programm) in das informationstechnische System (itS) einschleust und unerwünschte Aktionen ausführt. Die Aktionen erfolgen meist im Hintergrund und ohne Kenntnis des Betroffenen. Die eigentliche Funktion eines Trojaners ist die Übernahme eines Computersystems.[59]

(3) Angriffsgeschehen beim Einsatz von Botnetzen

Das Angriffsgeschehen beim Einsatz eines Botnetzes lässt sich in vier Phasen unterteilen. In der ersten Phase wird die später ausgeführte Schadsoftware programmiert. Die Infektion (mittels Trojaner) der itS erfolgt im zweiten Schritt. Danach verknüpfen sich die Bots mit dem C&C-Server, um mit Aufträgen versehen zu werden. Im letzten Schritt und damit der vierten Phase attackiert das Botnetz auf Befehl des C&C-Server. In unserem Fall äußert sich der Befehl in der Nutzung der Rechenleistung, um später Bitcoins zu schöpfen.

bb) § 248c StGB – Entziehung elektrischer Energie – „Der Diebstahl von Rechenleistung"[60]

Durch die unberechtigte Nutzung der Rechenkapazität der Computer und des Stromverbrauchs kommt zunächst

50 *LG Kempten*, Urt. v. 29.10.2014 – 6 KLs 223 Js 7897/13.
51 *Kochheim*, Rn. 210.
52 *Kochheim*, Rn. 683.
53 *Kochheim*, Rn.683; *Namestnikov*, Schattenwirtschaft Botnetz – ein Millionengeschäft für Cybercriminelle, S. 3., abrufbar unter: https://media.kasperskycontenthub.com/wp-content/uploads/sites/62/2009/07/12143924/ynam_botnets_0907_de.pdf (zuletzt abgerufen am: 6.10.2020).
54 *Kochheim*, Rn. 684.
55 *Kochheim*, Rn. 691.
56 *Kochheim*, Rn. 683.
57 *v. Hauff*, S. 2.
58 *Stam*, ZIS 2017, 547 (548).
59 *Werner*, S. 62.
60 *Grzywotz*, S. 157.

die Strafbarkeit wegen Entziehung elektrischer Energie nach § 248c StGB in Betracht. Am 4. August 1953 wurde der § 248c in das StGB eingeführt. Der Gesetzgeber konnte daher bei Gesetzeserlass keine Konstellation wie das Bitcoin-Mining erfassen wollen.[61] Dennoch könnte eine Strafbarkeit gegeben sein.

(1) Fremde elektrische Energie

Tatobjekt ist die fremde elektrische Energie. Der Begriff der Energie richtet sich nach physikalisch-naturwissenschaftlichen Kriterien.[62] Sie ist fremd, wenn an ihr kein Eigentum im zivilrechtlichen Sinne begründet werden kann, dem Täter also keine Befugnis zur Entziehung zusteht.[63] Vorliegend wird für die Berechnung Stromverbrauch genutzt, der unzweifelhaft Gegenstand elektrischer Energie ist. Zudem sind die Täter nicht zum Verbrauch des Stroms befugt – die Fremdheit ist zu bejahen.

(2) Entziehen

Entziehen ist die einseitig bewirkte Minderung des Energievorrats durch Entnahme von Energie aus einer elektrischen Anlage oder Einrichtung mittels eines Leiters.[64] Leiter ist jeder physikalisch geeignete Stromleiter[65], insbesondere Kabel oder sonstige Metalle.[66] Jedoch übermittelt die Schadsoftware nicht wie ein Kabel die Elektrizität auf und überträgt sie auf einen anderen Ort. Sie ist daher kein Leiter i.S.d. § 248c StGB. Die Strafbarkeit nach § 248c StGB wegen Entziehung elektrischer Energie scheidet somit aus.[67]

cc) § 202a StGB – Ausspähen von Daten

Durch den Einsatz eines Botnetzes ermöglichten sich die Täter den Zugriff auf die infizierten Computer und auf die dort gespeicherten Daten. Insofern kommt eine Strafbarkeit nach § 202a StGB wegen des Ausspähens von Daten in Betracht. Danach macht sich derjenige strafbar, der sich oder einem anderen unbefugt Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft.

(1) Zugangssicherung

Gegen den unberechtigten Zugang sind die Daten gesichert, wenn eine besondere Zugangssicherung vorliegt, der Betroffene damit sein „Interesse an der Geheimhaltung“ dokumentiert[68] und der Zugriff so ausgeschlossen oder erheblich erschwert wird.[69]

An den Sicherungsgrad des Zugangs werden keine hohen Anforderungen gestellt.[70] Umstritten ist hier, ob lediglich irgendeine Sicherung des Geheimhaltungsinteresses oder ob sich diese gegen die spezifische Angriffsart richten muss.[71] Nach überwiegender Auffassung, muss sich der Sicherungszweck zumindest gleichrangiges Ziel des Motivs für den Betroffenen sein. Verlangt wird teilweise, dass der Sicherungszweck dominierendes Ziel sein soll,

61 *Grzywotz*, S. 157.
62 *Wittig*, in: BeckOK-StGB, 41. Ed. (Stand: 1.2.2019), § 248c Rn. 2.
63 *OLG Celle*, MDR 1969, 597; *Wittig*, in: BeckOK-StGB, § 248c Rn. 2.
64 *Kindhäuser*, in: Kindhäuser/Neumann/Paeffgen, Strafgesetzbuch, 4. Aufl. (2013), § 248c Rn. 4.
65 *Fischer*, StGB, 66. Aufl. (2019), § 248c Rn. 3.
66 *Kindhäuser*, in: Kindhäuser/Neumann/Paeffgen, Strafgesetzbuch, 5. Aufl. (2017), § 248c Rn. 5.; *Wittig*, in: BeckOK-StGB, § 248c Rn. 2.
67 Vgl. *Heine*, NStZ 2016, 441.
68 *Eisele*, in: Schönke/Schröder, Strafgesetzbuch, 30. Aufl. (2019), § 202a Rn. 7; BT-Drs. 10/5058, S. 29; *BGH*, NStZ 2018, 401; *Hilgendorf/Valerius*, Computer- und Internetstrafrecht: ein Grundriss, 2. Aufl. (2012), Rn. 546.
69 *Gercke*, in: Gercke/Brunst, Praxishandbuch Internetstrafrecht, 2009, Rn. 94; *BGH*, Beschl. v. 14.1.2010 – 4 StR 93/09, S. 4.
70 *Fischer*, StGB, § 202a Rn. 2.
71 *Stam*, ZIS 2017, 547 (549).

denn wenn nun jede Sicherungsmaßnahme ausreichend wäre, könnte sich der geschützte Bereich zu weit ausdehnen und es könnte zu Kollisionen mit Schutzbereichen anderer Normen kommen.[72] Einigkeit besteht zumindest darüber, dass es nicht ausreichend ist, wenn die Sicherungsmaßnahme von untergeordneter Bedeutung oder ein Nebeneffekt ist.[73]

Im vorliegenden Fall umgehen die Täter mittels Trojaner eine Firewall. Fraglich ist, ob diese eine Zugangssicherung i.S.d. § 202a StGB ist. Mit dem Einsatz einer Firewall wird signalisiert, dass der Berechtigte Daten hinter dieser Firewall schützen will.[74] Eine Firewall übernimmt die Funktion eines „Torwächters", der den Datenverkehr zwischen einem Netzwerk und dem Internet überwacht.[75] Dabei kann er die Installation selbst nicht verhindern, da nicht der Inhalt der Daten überprüft wird. Anders wäre es, wenn eine Firewall mit einem Antiviren-Programm kombiniert wird und dadurch alle transportierten Daten untersucht.[76] Den Schutz gewährt hier jedoch in erster Linie das Antivirenprogramm und nicht die Firewall selbst.[77] Bei einer Firewall handelt es sich demnach erst dann um eine Zugangssicherung, soweit diese gerade vor unbefugtem Zugang durch Trojaner schützen soll.[78] In ihrer Erstentscheidung kritisierte der *BGH* die unzureichenden Feststellungen zur Frage der Überwindung besonderer Schutzvorkehrungen[79] , die das *LG Kempten* nicht getroffen habe und verneinte den Tatbestand des § 202a StGB; der alleinige Verweis auf den Bestand einer Sicherung zeuge daher nicht von einer „besonderen Sicherung" i.S.d. § 202a StGB.[80] In der Revisionsentscheidung von 2017 wurde die Qualifikation der Firewalls als „besondere Sicherung" damit begründet, dass diese gerade der Verhinderung eines unberechtigten Eindringens in das Netzwerk von außen und des Zugriffs auf Rechnerdaten innerhalb des Netzes dienen soll. Damit wollten die Verfügungsberechtigten erkennbar den Zugang mittels Firewall verhindern.[81]

(2) Zugang verschaffen

Der Täter müsste sich unter Überwindung einer Schutzmaßnahme unberechtigt Zugang zu Daten verschafft haben. Damit wird das Geheimhaltungsinteresse des Verfügungsberechtigten geschützt.[82] Vorliegend verschaffen sich die Täter den Zugang, indem sie die Sicherung mittels Trojaner umgehen. Ohne Tarnung des Trojaners als harmlose Programmdatei und damit der Täuschung wäre der Zugriff verhindert.[83]

dd) § 303a StGB – Datenveränderung

Ferner kommt eine Strafbarkeit wegen Datenveränderung gem. § 303a StGB in Betracht. Danach macht sich strafbar, wer rechtswidrig Daten löscht, unterdrückt, unbrauchbar macht oder verändert. Schutzgut ist das Interesse des Betroffenen an der unversehrten Verwendbarkeit der Daten.[84]

(1) Daten

---

72 *Leicht*, IuR 1987, 45 (47), abrufbar unter: https://www.jurpc.de/jurpc/show?id=iur_1987_0000_0002_0003_0011&page=1 (zuletzt abgerufen am 8.10.2020).
73 *Eisele*, in: Schönke/Schröder, § 202a Rn. 14.; *Gercke*, in: Gercke/Brunst, Rn. 94.; *Hilgendorf/Valerius*, Rn. 546.
74 *Koch*, Strafrechtliche Probleme des Angriffs und der Verteidigung in Computernetzen, 2006, S. 48.
75 *Werner*, S. 80.
76 *Werner*, S. 86.
77 *Stam*, ZIS 2017, 547 (549); *Kochheim*, S. 597; *Koch*, S. 49.
78 *Eisele*, in: Schönke/Schröder, § 202a Rn. 14; *Stam*, ZIS 2017, 547 (549).
79 *BGH*, Beschl. v. 21.7.2015 – 1 StR 16/15.
80 BeckRS 2014, 123570.
81 *BGH*, NStZ 2018, 401.
82 *BGH*, NStZ 2018, 401.
83 *BGH*, Beschl. v. 27.7.2017 – 1 StR 412/16.
84 *Hilgendorf*, in: SSW-StGB, 2. Aufl. (2014), § 303a Rn. 3.

Vor dem Hintergrund der Definition des Datenbegriffs nach Art. 2 lit. b der Richtlinie 2013/40/EU sind „Computerdaten“ als jede Darstellung von Tatsachen, Informationen oder Konzepten in einer für die Verarbeitung in einem Informationssystem geeigneten Form zu verstehen. Die Definition ist auch für das nationale Recht maßgeblich.[85] Die in der Registry enthaltenen Informationen sind unzweifelhaft Daten i.S.d. § 303a bzw. § 202a StGB.

(2) Tathandlung

Fraglich ist, welche Tathandlung in Betracht kommt. Tathandlungen des § 303a StGB sind das Löschen, Unterdrücken, Unbrauchbarmachen und Verändern von Daten. Keine Tathandlungen sind welche, durch die Manipulation keine Daten betroffen werden.[86] Ein Löschen scheidet aus, da lediglich neue Daten hinzugefügt werden. Fraglich ist, inwieweit sich das Verändern im vorliegenden Fall auswirkt. Ein Verändern ist die inhaltliche Umgestaltung gespeicherter personenbezogener Daten nach § 3 Abs. 4 Nr. 2 BDSG. Ein neutrales Hinzufügen einer Datei ohne Einfluss auf den Steuerungsvorgang und den inhaltlichen Aussagewert ist demnach nicht strafbar. Die Eingabe von Dateien müsste die Datenverarbeitungsfunktion, wie den Speicherplatz oder Prozessorleistung, beeinträchtigen.[87] Im vorliegenden Fall handelt es sich bei dem Betriebssystem des Microsoft Windows um eine Datenbank der „Registry“. Bei Eingabe einer Datei wird lediglich die Veränderung der Datenbank bewirkt. Die Registry ist nicht Teil des eigentlichen Programms. Daher ist durch den zusätzlichen Eintrag der Registry nicht bereits das Verändern gegeben; die Datenbank wird lediglich vergrößert und vorhandene Einträge werden nicht beeinträchtigt.[88] Ein Verändern würde ausscheiden.[89] Allerdings muss die Schadsoftware gestartet werden.[90] Bereits hier ist eine inhaltliche Änderung des Programms gegeben, denn der Start einer zusätzlichen Anwendung der Schadsoftware und des Programmbefehls des späteren Bitcoin-Minings ist nicht vorgesehen. Das Programm wird verändert. Der Tatbestand des § 303a StGB wäre demnach erfüllt.

ee) § 263a StGB

Wegen der Infizierung des Computers mit dem Trojaner kommt eine Strafbarkeit nach § 263a StGB wegen Computerbetrugs in Form der „unrichtigen Gestaltung des Programms“ in Betracht. Mit § 263a StGB wird das Vermögen im Rechtsverkehr geschützt.[91]

(1) Unrichtige Gestaltung des Programms

Die Schadsoftware heftet sich zunächst an die Registry an. Bei dieser müsste es sich um ein Programm handeln. Ein Programm ist jede aus einer Folge von Einzelbefehlen bestehende Anweisung an den Computer.[92] Die Registry ist die „zentrale hierarchische Konfigurationsdatenbank des Windows-Betriebssystems“. Hier erfolgt die Verwaltung von Computerprogrammen.[93] Die Registry ist daher ein Programm. Ferner ist zu prüfen, ob die Re-

85 *Heine*, NStZ 2016, 441.
86 *Heine*, NStZ 2016, 441; *Wolf*, in: LK-StGB, 12. Aufl. (2008), § 303a Rn. 27.
87 *Heine*, NStZ 2016, 441.
88 *Heine*, NStZ 2016, 441.
89 *Heckmann*, in: juris PraxisKommentar Internetrecht, 4. Aufl. (2014), Kap. 8 Rn. 116.
90 *Grzywotz*, S. 166; *Heckmann*, in: juris PraxisKommentar Internetrecht, Kap. 8 Rn. 116.
91 *Kochheim*, Rn. 528; *Wohlers/Mühlbauer*, in: MüKo-StGB, 3. Aufl. (2019), § 263a Rn. 20.
92 *Wohlers/Mühlbauer*, in: MüKo-StGB, § 263a Rn. 20.
93 Vgl. *Grzywotz*, S. 159; *Schulz/Vahldiek*, Die Windows-Registry – Antworten auf die häufigsten Fragen, abrufbar unter: https://www.heise.de/select/ct/2017/04/1487005733139460 (zuletzt abgerufen am 8.3.19); *Heine*, NStZ 2016, 441.

gistry gestaltet wurde. Gestalten ist das Hinzufügen, die Veränderung oder das Löschen von Programmablaufschritten und den Einbau sonstiger falscher Funktionen.[94] Dieses wird ebenfalls als Programmmanipulation bezeichnet. Sie ist die innere, datenverarbeitende Logik, die vom Betriebssystem zur Verfügung gestellt wird.[95] Es ist zwischen systemkonträr und systemkonformer Manipulation zu unterscheiden.[96] Ersteres ist das Hinzufügen zusätzlicher Programmablaufschritte oder deren Löschung oder das Umgehen durch elektronische Verzweigungen. Bei der systemkonträren Programmmanipulation werden die vorhandenen Programmablaufschritte durch neue, nicht vorgesehene überlagert.[97] Vorliegend werden durch die Schadsoftware vorhandene Programmabläufe nicht beeinflusst, aber neue Arbeitsanweisungen eingetragen: dies äußert sich in dem automatischen Start des Miningprozesses nach 120 Sekunden Inaktivität des jeweiligen Nutzers. Systemkonträre Programmmanipulation und damit eine Gestaltung liegen vor.

Unrichtig ist das Programm, wenn es dem Willen und den Vorstellungen des Verfügungsberechtigten nicht entspricht.[98] Nach objektiver Auslegung des Unrichtigkeitsbegriffs ist die Programmgestaltung unrichtig, wenn der Datenverarbeitungsvorgang (DV) zu einem fehlerhaften Ergebnis führt und so die zu ermittelnde Aufgabenstellung unzutreffend bewältigt.[99]

(2) Beeinflussung des Ergebnisses des Datenverarbeitungsvorgangs und daraus resultierender Vermögensschaden

Das Ergebnis des DV müsste beeinflusst worden sein. Ein DV umfasst alle Vorgänge, bei denen durch Aufnahme von Daten und durch ihre Verknüpfung Arbeitsergebnisse erzielt werden. Daten sind kodierte Zeichen.[100] Die Registry ist unzweifelhaft ein kodiertes Zeichen und damit unterfällt es dem Begriff der Daten. Die Daten werden beim Start des Computers auch automatisch verarbeitet – ein DV liegt vor. Die Beeinflussung äußert sich in dem unbemerkten Start der Schadsoftware und stellt ein Ergebnis dar.[101] Taterfolg ist der Eintritt eines Vermögensschadens als unmittelbare Folge des Ergebnisses des DV. Vorliegend wäre an die abgezapfte Rechenleistung der betroffenen Computer zu denken. Die Rechenleistung wird durch den Stromverbrauch und der Nutzung der Hardware bereitgestellt. Fraglich ist daher, ob der Stromverbrauch als solcher unter den Begriff des Vermögens zu subsumieren ist. Vorherrschend ist die Auffassung des ökonomisch-juristischen Vermögensbegriffs.[102] Danach ist das Vermögen die Summe der wirtschaftlichen Güter einer Person, soweit sie ihr unter dem Schutz der Rechtsordnung oder wenigstens ohne deren Missbilligung zustehen.[103] Dem Stromverbrauch kommt ein Marktwert zu. Von § 248c StGB wird ihr eine gewisse wirtschaftliche Position zugesprochen. Somit liegt im Ergebnis eine Beeinflussung des DV vor, welche wegen der genutzten Rechenleistung mit einem Vermögensschaden der Nutzer einhergeht.

ff) Weitere Tatbestände

94 *Joecks*, in: MüKo-StGB, § 263a Rn. 10.
95 *Kochheim*, Rn. 531.
96 BeckRS 2016, 17444, Rn. 20 f.; *Perron*, in: Schönke/Schröder, § 263a Rn. 5.
97 *Perron*, in: Schönke/Schröder, § 263a Rn. 5; *Fischer*, StGB, § 263a Rn. 6; vgl. *Kochheim*, Rn. 587.
98 *Perron*, in: Schönke/Schröder, § 263a Rn. 5.
99 *Gercke*, in: *Gercke/Brunst*, Rn. 178; *Tiedemann/Valerius*, in: LK-StGB, § 263a Rn. 30; *Eisele*, in: Schönke/Schröder, § 40 Kap. 8 Rn. 28; *v. Heintschel-Heinegg*, in: BeckOK-StGB, § 263a Rn. 13; *Hilgendorf*, JuS 1997, 130 (131); *Fischer*, StGB, § 263a Rn. 6.
100 *Mühlbauer*, in: MüKo-StGB, § 263a Rn. 13 f.
101 Vgl. *Grzywotz*, S. 161.
102 *Fischer*, StGB, § 263 Rn. 90.
103 *Dierlamm*, in: MüKo-StGB, § 263 Rn. 205; *BGH*, Urt. v. 16.8.2017 – 2 StR 335/15.

(1) §303b StGB- Computersabotage- Angriffsaktivität des Botnetzes

Schutzgut des § 303b StG0B ist das „Interesse der Betreiber und Nutzer von Datenverarbeitungen an deren ordnungsgemäßer Funktionsweise“. Damit stellt der § 303b StGB eine Qualifikation zum § 303a StGB dar.[104] Von wesentlicher Bedeutung ist die Datenverarbeitung, wenn die Tätigkeit des Betroffenen durch eine Störung gefährdet ist.[105] Die bloße Gefährdung reicht für die Bejahung einer Störung nicht aus.[106] Bei Privatpersonen soll auf die Bedeutung der Datenverarbeitungsanlage für die Lebensgestaltung abgestellt werden.[107] Sofern es also durch das Mining zu einer offensichtlichen Überlastung kommt, ist der Tatbestand erfüllt.[108] Im vorliegenden Fall öffnet sich, von den Betroffenen unbemerkt, die Installation der Schadsoftware. Insofern scheidet eine Strafbarkeit nach § 303b StGB aus.

(2) § 265a StGB – Erschleichen von Leistungen

Die Täter nutzten den Strom und die Hardware der Rechner, ohne i.S.d. § 265a StGB ein Entgelt zu entrichten- die Strafbarkeit nach § 265a StGB wegen Erschleichen von Leistungen könnte gegeben sein. Automat i.S.d. § 265a StGB jedes technische Gerät, das dadurch, dass mit der Entrichtung des vorgesehenen Entgelts ein Mechanismus oder ein elektronisches Steuerungssystem in Funktion gesetzt wird, selbsttätig bestimmte Gegenstände abgibt oder sonstige Leistungen erbringt.[109] Ein Computer könnte ein Leistungsautomat sein.[110] Allerdings wird die Leistung des Computers nicht gegen die Entrichtung eines Entgelts herausgegeben.[111] Eine Strafbarkeit nach § 265a StGB scheidet ebenfalls aus.

(3) § 303 StGB – Sachbeschädigung

Möglicherweise wurde die Festplatte und der Prozesslüfter aus der Überlastung der Grafikkarte den Tatbestand des § 303 StGB wegen Sachbeschädigung erfüllen.[112] Der Prozesslüfter und die Festplatte sind unzweifelhaft körperlich zu erfassen.[113] Die Beschädigungshandlung äußert sich in einer verletzenden Handlung, die die Sache in ihrer Substanz nicht unerheblich verletzt und dadurch ihre stoffliche Zusammensetzung verändert oder ihre Unversehrtheit derart beeinträchtigt wird, sodass die bestimmungsgemäß Gebrauchsfähigkeit gemindert ist.[114] Ob die vorliegenden Gegenstände tatsächlich nicht unerheblich verletzt wurden, ist nach den jeweiligen Umständen zu ermitteln.[115]

(4) Vorbereitungshandlungen

Stellt der Täter ein Computerprogramm her, wie hier eine Schadsoftware, wäre der Tatbestand des § 202a StGB wegen der Vorbereitung des Ausspähens und Abfangens von Daten erfüllt.

b) Weitere Konstellationen des Bitcoin-Minings

---

104 *Eisele*, in: Schönke/Schröder, § 10 Kap. 4 Rn. 79; BT-Drs. 16/3656 S. 13.
105 *Gercke*, in: Gercke/Brunst, Rn. 138; *Fischer*, StGB, § 303b Rn. 6.
106 *Gercke*, in: Gercke/Brunst, Rn. 136; BT-Drs. 10/5058, S. 35.
107 *Hilgendorf*, in: SSW-StGB, § 303b Rn. 6.
108 *Grzywotz*, S. 167.
109 *Perron*, in: Schönke/Schröder, § 266a Rn. 4.
110 *Hefendehl*, in: MüKo-StGB, § 265a Rn. 30.
111 *Koch*, S. 121.
112 *Grzywotz*, S. 168.
113 *Stree/Hecker*, in: Schönke/Schröder, § 303 Rn. 3.
114 *Stree/Hecker*, in: Schönke/Schröder, § 303 Rn. 8; *Weidemann*, in: BeckOK-StGB, § 303 Rn. 8.
115 *Grzywotz*, S. 168.

Im Folgenden wird die Strafbarkeit weiterer Konstellationen des Bitcoin-Mining angeprüft.

aa) Bitcoin Mining mittels Software-Update ohne Zustimmung[116]

Weitere Methode ist der automatische Start des Mining-Prozesses getarnt als Software-Update. Stimmt der Betroffene nicht dem Software-Update und damit dem Schürfen zu, so ergibt sich die Strafbarkeit nachfolgenden Vorschriften:

(1) § 303a StGB – Datenveränderung

Die eigentümerähnliche Verfügungsbefugnis könnte bei demjenigen, der die Daten abgespeichert hat, vorliegen.[117]

(2) § 202a StGB – Ausspähen von Daten

Im Rahmen des § 202a StGB könnte es an dem Tatbestandsmerkmal „nicht für den Täter bestimmt" scheitern. Denn durch die automatische Verknüpfung der Mining- Komponente mit dem Update der Software könnten für die Entwickler der vorliegenden Software die Daten bestimmt sein. Hiergegen ist jedoch einzuwenden, dass es für ein Update einer Software der Zustimmung der Nutzer bedarf. Demnach sind die Daten nicht für die Softwareentwickler bestimmt. Die Zustimmung ist in Bezug auf das parallel ablaufende Mining nicht anzunehmen. Die Daten sind nicht den Softwareentwicklern als Täter bestimmt. Der Tatbestand des § 202a StGB liege vor.

(3) § 202c StGB – Vorbereiten des Ausspähens von Daten und Abfangens von Daten

Der Tatbestand des § 202c Abs. 1 Nr. 2 StGB wäre erfüllt, sofern der Täter ein Computerprogramm zum Zweck der Begehung einer in § 202c Abs. 1 StGB aufgezählten Tat hat. Eine objektivierte Zweckbestimmung des Programms muss möglich sein. Dafür muss sich die Absicht des Programmherstellers manifestiert haben.[118] In einem Vorfall des ESEA aus dem Jahr 2013 haben die Entwickler beteuert, sie hätten bloß Testgänge zum Mining durchgeführt und daher vor den Nutzern nicht bekanntgegeben.[119] Von § 202c StGB nicht erfasste Fälle sind die der sog. „Dual-Use-Tools". Diese sind Instrumente sowohl für legale als auch für illegale Zwecke.[120] Im erwähnten Fall ist gerade die Intention des illegalen Zwecks nicht zu entnehmen. Daher würde eine Strafbarkeit nach § 202c StGB ausscheiden.

bb) Bitcoin Mining mittels Software-Update mit Zustimmung[121]

Aufgrund der Zustimmung zum Mining Prozess scheiden Strafbarkeiten nach §§ 202a, 303a sowie 263a StGB aus. Allerdings könnte eine Strafbarkeit wegen Sachbeschädigung nach § 303 StGB in Betracht kommen, sofern der Mining Prozess zu die Hardware überlastet und daher beschädigt.[122]

cc) Bitcoin Mining mittels Nutzung fremder Rechner

116 *Grzywotz*, S. 169.
117 *Grzywotz*, S. 170.
118 *Eisele*, in: Schönke/Schröder, § 202c Rn. 4.
119 https://www.theregister.co.uk/2013711/20/esea_gaming_bitcoin_fine/ (zuletzt abgerufen am 8.3.19).
120 *BVerfG*, Beschl. v. 18.5.2009 – 2 BvR 2233/07, 2 BvR 11515/08.
121 Vgl. *Grzywotz*, S. 169.
122 *Grzywotz*, S. 173.

Mit dieser Konstellation ist das wortwörtliche Nutzen fremder Rechner bspw. auf dem Arbeitsplatz gemeint.[123] Eine Strafbarkeit nach § 248c StGB ist hier zu verneinen: dieser käme nur bei Vorlage einer unbefugten Stromentnahme durch einen nicht zur ordnungsgemäßen Energieentnahme bestimmten Leiter in Betracht.[124] Mit „unbefugt" ist nicht das einfache Einschalten und die Entziehung von Energie gemeint.[125] I.S.d. § 263a StGB wäre eine unbefugte Verwendung von Daten gegeben, wenn hierdurch der DV beeinflusst werden würde. Dessen Ergebnis müsste vermögensrelevant sein.[126] Im vorliegenden Fall wird durch die unbefugte Verwendung von Kennungsdaten nicht bereits ein vermögensrelevantes Ergebnis erzeugt, sondern erst durch das Starten des Mining-Vorgangs. Insofern wäre die Strafbarkeit nach § 263a StGB ebenfalls zu verneinen.[127]

3. Fazit

Zusammenfassend lässt sich sagen, dass das illegale Bitcoin-Minings über ihre verschiedenen Methoden weitestgehend unter Strafe stehen. Der Bundesrat sieht dies aber anders: auf Initiative Hessens aus dem Jahre 2016 hat er einen Gesetzesentwurf zur „Strafbarkeit der unbefugten Benutzung informationstechnischer Systeme" nach § 202e StGB angenommen.[128] Ziel der Einführung des § 202e StGB ist es, Infektionen und allgemein Angriffe aus Bot Programmen strafrechtlich zu schützen und die damit einhergehende Beeinträchtigung des IT-Grundrechts auf Vertraulichkeit und Integrität informationstechnischer Systeme zu gewährleisten.[129] Die Bundesregierung bezweifelt hingegen das Bestehen von Strafbarkeitslücken und kritisiert den Entwurf zu § 202e StGB.[130]

a) Gesetzgeberischer Handlungsbedarf

Die Frage nach gesetzgeberischem Handlungsbedarf kann bejaht werden, sofern Schutzlücken hinsichtlich der Erfassung der Botnetzkriminalität bestehen.

aa) Schutzlücke de lege lata

Nach Auffassung der Bundesregierung unterfällt jede Aktivität im Zusammenhang mit einem Botnetz bereits dem Schutz des bestehenden Strafrechts.[131]

(1) Materiell-rechtliche Erfassung

In der Entwurfsbegründung werden die Gefahren der Infektion, der dritten Phase des Angriffsgeschehens, geschildert. Es wird bereits die strafrechtliche Erfassung des Botnetzaufbaus, der zweiten Phase, und der anschließenden Infektion der Schadsoftware erfordert, denn genau hier liege die eigentliche Gefahr des „digitalen Hausfriedensbruchs" und damit die Beeinträchtigung des IT-Grundrechts.[132]

Die Infektion der Bots mittels Schadsoftware ist nach gegenwärtigem Strafrecht jedoch ausreichend geschützt.

[123] https://www.zeit.de/gesellschaft/zeitgeschehen/2018-02/russland-bitcoin-festnahme-mining-super-computer; https://www.Pressetext.com/news/20140611013 (zuletzt abgerufen am 28.2.19); vgl. *Grzywotz*, S. 180.
[124] *Kindhäuser*, in: Kindhäuser/Neumann/Paeffgen, StGB, § 248c Rn. 7.
[125] *Eser/Bosch*, in: Schönke/Schröder, § 248c Rn. 11.
[126] *Perron*, in: Schönke/Schröder, § 263a Rn. 19 ff.
[127] Vgl. *Grzywotz*, S. 182.
[128] BT-Drs. 19/1716, S. 3 ff.; BR-Drs. 338/16, S. 7.
[129] BT-Drs. 18/10182, S. 3.
[130] BT-Drs. 18/10182, S. 19.
[131] BT-Drs. 18/10182, S. 19.
[132] BT-Drs. 18/10182, S. 3.

Die Normüberschrift „digitaler Hausfriedensbruch“ findet in dem rechtswidrigen Zugang zu einem IT-System Geltung: bereits der Zugang zu einem System und nicht erst die Zugangsverschaffung auf Daten, die § 202a StGB sanktioniert, soll danach unter Strafe stehen. Den Zugang verschafft sich der Täter nach § 202e StGB, „wenn das System infiltriert, also eine etwaige Sperre überwunden und er in der Lage ist, Eingaben unmittelbar vorzunehmen.“ Bei der Überwindung einer Sperre fordert der Bundesrat keine Strafbarkeitsvoraussetzung, wie dies bei § 202a StGB mit der Zugangssicherung der Fall ist. Die Übernahme der „besonderen Zugangssicherung“ steht nicht im Einklang mit der „lückenlosen Strafbarkeit“.[133] So sei der strafrechtliche Schutz allein vom Opferverhalten abhängig und für die Strafbarkeit nach § 202a StGB hänge es letztlich davon ab, ob die Sicherung gegen die spezifische Angriffsart gesichert ist oder nicht.[134] Daher werden bereits der vorverlagerte Datenschutz sowie der Schutz der betroffenen Systeme erfasst, mit der Begründung, durch technische Möglichkeiten können Spuren verwischt und daher ein Fehlschlag forensischer Ermittlungen fehlschlagen. Der Entwurf verweist hierbei auf die *BGH*-Entscheidung, die ebenfalls den § 202a StGB als nicht einschlägig ansah aufgrund faktisch fehlender Feststellungen der Zugangssicherung und ihrer Überwindung. Allerdings war dies nicht der Grund für die Aufhebung. Der *BGH* zweifelte lediglich die unzureichende Feststellung in einem schlecht ermittelten Verfahren des *LG Kempten*.[135] Die Bagatellklausel in Satz 2 hilft hierbei ebenfalls nicht weiter, da sie sich nur einen Einzelfall bezieht („wenn sie geeignet ist, berechtigte Interessen eines anderen zu beeinträchtigen“).[136]

Der Bundesrat zweifelt außerdem an der Gewährleistung ausreichenden Schutzes durch § 303a StGB. Hierbei verweist er auf die Fälle der „fileless maleware“, eine neu entwickelte Schadsoftware, die keine Veränderung an gespeicherten Daten ausführt.[137] Mit dieser Schadsoftware sei eine Strafbarkeitslücke gegeben. Doch auch hiergegen ist einzuwenden, dass allein zur Aktivierung der „fileless malware“ eine Veränderung der Daten im itS und der Daten in der Registry erforderlich ist. Der Schutz des § 303a StGB wäre jedenfalls dann nicht gegeben, wenn bloße Daten hinzugefügt werden würden. Anders wäre der Fall zu beurteilen, dass mit dem Zugriff auf das itS eine Veränderung des inhaltlichen Aussagegehalts einhergeht – der Tatbestand des § 303a StGB liegt vor. Da § 303a StGB keine dauerhafte Veränderung verlangt, unterfällt bereits jede Aktion im Aufbaustadium der „Veränderung“. Handelt es sich bei den betroffenen Daten zudem um personenbezogene nach § 3 Abs. 1 BDSG, so kommt eine Strafbarkeit nach dem einschlägigen Gesetz in Betracht.[138]

(2) Praktische Probleme in der Strafverfolgung

Laut Gesetzentwurf bestehen Probleme bei der Strafverfolgung von IuK-Kriminalität. Die Strafverfolgung im Bereich des Cybercrimes begegnet tatsächlich regelmäßig Hindernissen: der Betrieb eines Botnetzes erfolgt meist unbemerkt. Mangels Verdachtsannahme kann auch die Strafverfolgungsbehörde nicht umgehend Kenntnis von der Tatbestandsverwirklichung erlangen. Hinzu kommt, dass sich die Identifikation der Täter schwierig gestaltet – mittels Verschleierungstechniken arbeitet der Großteil der Täter im Internet anonym.[139] Komplizierter wird es,

133 BT-Drs. 18/10182, S. 12.
134 Vgl. a.a.O., S. 12 f.
135 *Kühne*, Die Entwicklung des Internetstrafrechts: unter Berücksichtigung der §§ 202a-202c StGB sowie § 303a und § 303b StGB, 2018, S. 375 ff.
136 *Kahler/Hoffmann-Holland*, KriPoZ 2018, 267 (268); *Tassi*, DuD 2017, 176 (178).
137 BKA Herbsttagung 2018, „Sicherheit einer offenen und digitalen Gesellschaft“, S. 5 f.
138 *Kühne*, S. 379.
139 *Dalby*, Grundlagen der Strafverfolgung im Internet und der Cloud – Möglichkeiten, Herausforderungen und Chancen, 2016, S. 234 ff.

wenn die Täter Botnetze aus dem Ausland betreiben. Mangels ausreichender Ressourcen für die erfolgreiche Strafverfolgung, könnten diese nur schwer oder nicht aufgespürt werden.[140] Durch Schaffung eines neuen Tatbestands bleiben die beschriebenen Probleme jedoch ungelöst.[141] Vielmehr erweist sich der Vorschlag der besseren Ausstattung der Ermittlungstätigkeiten mittels Einsatz technischen Equipments und der Aneignung von IT-Kompetenzen als sinnvoller.[142]

bb) Zwischenergebnis

Zusammenfassend lässt sich feststellen, dass die Botnetzkriminalität nach den Regelungen der §§ 202a, 303a StGB u.U. denen des BDSG ausreichenden Schutz genießt. Damit geht auch der Strafrechtsschutz der Entwicklung der Schadsoftware in der ersten Phase einher, § 202c StGB. Es bestehen daher keine Schutzlücken im bestehenden Strafrecht. Die Probleme der Strafverfolgung können durch Schaffung eines neuen Tatbestands eher weniger gelöst werden.

b) Strafrechtsschutz de lege ferenda durch § 202e StGB

Mit § 202e StGB hat sich der Bundesrat zum Ziel gesetzt, die vermeintlichen Schutzlücken der §§ 202a, 303a StGB durch die Strafbarkeit des „digitalen Hausfriedensbruch“ zu schließen. Mit Verweis auf den Paralleltatbestand des „unbefugten Gebrauchs eines Fahrzeugs“ gem. § 248b StGB begründet der Bundesrat das Gebrauchsrecht damit, dass ein Fahrrad nicht besser geschützt sein könne als Computer mit höchstpersönlichen Daten.[143] Bedenken bestehen jedoch bei der Heranziehung des § 248b StGB als Beispiel, da dieses als furtum usus ein unteilbares Gebrauchsrecht ist, wohingegen dieses bei den Rechenkapazitäten von IT-Systemen durchaus teilbar ist.[144] Der Rechtsgedanke des § 248b StGB kann den Schutzbereich des § 202e StGB daher nicht präzise wiedergeben.[145] Mit der Anordnung eines Beeinflussens oder mit einer Ingangsetzung nach § 202e Abs. 1 S. 1 Nr. 2 StGB soll der Strafrechtsschutz weiter greifen als bei der Voraussetzung eines DV i.S.d. §§ 303a, 303b StGB. Um auch elektronisch fernsteuernde Anlagen und Einrichtung zu schützen, wurde der Begriff des „informationstechnischen Ablaufs“ aufgenommen“. Die Ausuferung wird mit der Definition des informationstechnischen Ablaufs nach § 2 des BSI-Gesetzes begründet: „jede Verbreitung oder Übertragung von Informationen durch technische Mittel“.[146] Doch danach würden bereits alltägliche Handlungsweisen unter Strafe stehen.[147] Aufgrund der Digitalisierung des Alltags wäre der Anwendungsbereich unüberschaubar weit ausgelegt.[148] Auch die Herleitung des Schutzguts des § 123 StGB für den Schutz des in § 202e StGB verankerten IT-Grundrechts verbietet sich: es wird das Recht geschützt, zu entscheiden, wer sich in einer räumlichen Sphäre aufhalten darf. Die Bestimmung des Schutzbereichs ist jedoch mangels körperlicher Umgrenzung im digitalen Raum schwierig. Die Begrenzung des Berechtigten auf den rechtmäßigen Dateninhaber hat die Begrenzung auf dessen formelles Geheimhaltungsinteresse zur Folge. Dieses wird bereits von § 202a StGB ausreichend geschützt. In dem Sinne kann das IT-Grundrecht nicht mit Herleitung des Haus- sowie Gebrauchsrechts aus §§ 123, 248b StGB hergeleitet und demnach geschützt

[140] *Johannsen*, Der digitale Hausfriedensbruch nach § 202e StGB-E, abrufbar unter: http://rechtundnetz.com/digitaler-hausfriedensbruch/ (zuletzt abgerufen am 1.3.19), S. 6.
[141] *Stam*, ZIS 2017, 547 (551).
[142] *Kühne*, S. 381.
[143] BT-Drs.18/10182, S. 5.
[144] *Kahler/Hoffmann-Holland*, KriPoZ 2018, 267 (268); *Tassi*, DuD 2017, 176 (178).
[145] *Kühne*, S. 386.
[146] BT-Drs.18/10182, S. 16.
[147] *Johannsen*, S. 6.
[148] *v. Hauff*, S. 3; *Tassi*, DuD 2017, 176.

werden.

c) Zwischenergebnis

Das Ziel, eine umfassendere Strafbarkeit der Botnetzkriminalität durch strafrechtliche Anerkennung des IT-Grundrechts erreichen zu wollen, ist legitim. Allerdings bestehen hierfür keine bedeutenden Schutzlücken, die die Anerkennung des § 202e StGB begründen würden. Die Botnetzkriminalität wird bereits ausreichend vom geltenden Strafrecht erfasst. Wegen der Ausuferung des Anwendungsbereichs des § 202e StGB und der Unklarheiten innerhalb der Tatbestandsmerkmale kann das Ziel nicht effektiv erreicht werden.

d) Alternativen

Gegen das nach Auffassung des Bundesrats ergebende Problem können durchaus weniger eingriffsintensive Lösungsvorschläge entgegengehalten werden. Dies gebietet ebenfalls der Ultima ratio-Grundsatz im Strafrecht.[149] Eine Möglichkeit wäre die Infektion eines itS zur Vorbereitung einer weiteren Straftat selbständig in § 202c Abs. 1 S. 2 StGB unter Strafe zu stellen. Problematisch wäre in diesem Zusammenhang jedoch, dass die Absicht des Täters in der Regel nicht in der Vorbereitung der Tat liegt, sondern beim Betrieb des Botnetzes zur Generierung von Bitcoins. Außerdem geht es bei § 202c StGB nicht primär um den Schutz des persönlichen Lebens- und Geheimbereichs, sondern um den Missbrauch der Rechenleistungen und Ressourcen der Systeme. Vorzugswürdig ist die Ausweitung des Tatbestands der Computersabotage nach § 303b StGB.[150] Wie oben festgestellt, ist im Zusammenhang mit Botnetzangriffen keine „wesentliche Bedeutung“ gegeben. Doch könnte dies durch die Anerkennung der erheblichen Störung für den einzelnen Betroffen in der Ausnutzung seiner bereitgestellten Rechenleistung bejaht werden. Hierfür bietet sich die Erweiterung um ein Tatbestandserfolg an: durch die einfache Ausdehnung des § 303b StGB auf Hacking-Handlungen würde dem Anliegen des Bundesrates gerecht, ohne jegliche Alltagstätigkeit zu pönalisieren. Resümierend ist festzuhalten, dass es am ausreichenden Schutz des Internets gegen Botnetze jedenfalls nicht an den Lücken im geltenden Strafrecht mangelt, sondern eher an der Anonymität der Täter, die sich hinter den komplexen Techniken verstecken sowie die schwierige Erkennung der Opferstellungen.

IV. Die strafrechtliche Vermögensabschöpfung von Bitcoins

Ferner bestehen Schwierigkeiten bei der strafrechtlichen Vermögensabschöpfung von Bitcoins nach §§ 73 ff. StGB. Zweck des Verfalls des § 73 StGB ist die „Abschöpfung unrechtmäßig erlangten Vermögenszuwachses“.[151] Der Verfall ist eine Rechtsfolge eigener Art einer rechtswidrigen Tat und stellt eine öffentlich-rechtliche Abschöpfung zu Gunsten des Staates dar.[152] § 74 StGB, der die Einziehung von Tatprodukten, Tatmitteln und Tatobjekten vorsieht, ist hingegen kein einheitliches Rechtsinstitut.[153] Im Falle der möglichen Einziehung von Bitcoins ist der Verfall nach § 73 StGB besonders in Augenschein zu nehmen, da nur wenige Fälle denkbar sind, bei denen Bitcoins durch die „begangene“ Straftat i.S.d. § 74 StGB hervorgebracht werden.[154] Im anschließenden Ermittlungsverfahren werden die Gegenstände durch die Beschlagnahme sichergestellt gem. §§ 111b, 111c StPO.

149 *Roxin*, Strafrecht Allgemeiner Teil Band I, 4. Aufl. (2006), § 2 Rn. 28 ff.
150 *Kahler/Hoffmann-Holland*, KriPoZ, 2018, 267 (272).
151 *Heger*, in: *Lackner/Kühl*, StGB, 29. Aufl. (2018), § 73 Rn. 1; BGHSt 31, 145 = NJW 2002, 2257.
152 *Schmidt*, in: LK-StGB, § 73 Rn. 8.
153 *Heger*, in: *Lackner/Kühl*, StGB, § 74 Rn. 2.
154 *BGH*, NStZ-RR 1997, 318; *Rückert*, MMR 2016, 295.

1. Bitcoins als Gegenstand von Verfall, § 73 StGB

a) Vorbemerkung zur Reform der §§ 73 ff. StGB

Im Folgenden wird der Verfall anhand der bereits oben geschilderten Entscheidung durch den *BGH* erläutert. Wird über die Anordnung der Einziehung eines Tatertrags oder des Wertes des Tatertrags einer Tat, die vor dem 1. Juli 2017 entschieden worden ist, erst danach entschieden, sind die hier einschlägigen Vorschriften in der neuen Fassung des StGB bzgl. der Vermögensabschöpfung vom 13. April 2017 anzuwenden, Art. 316h EGStGB. Für den vorliegenden Fall bedeutet dies, dass die alten Regelungen zur Vermögensabschöpfung anzuwenden sind, da die Verfallsanordnung vor dem 1. Juli 2017 ergangen ist.

b) „Etwas erlangt"

Fraglich ist, ob Bitcoins tauglicher Gegenstand der Verfallsvorschrift der §§ 73 ff. StGB sind. I.S.d. § 73 Abs. 1 StGB erstreckt sich der Verfall grundsätzlich nur auf das unmittelbar erlangte Etwas.[155] Das Erlangte ist die Gesamtheit der aus oder für die Tat erlangten wirtschaftlichen messbaren Vorteile, wie Rechte.[156] Damit wird jeglicher Vermögenszuwachs erfasst.[157] Wegen ihres ermittelbaren Marktwerts sind Bitcoins realisierbarer Vermögenswert.[158] Sie sind „etwas Erlangtes". Der in der Literatur verbreiteten Auffassung, Bitcoins seien nicht etwas Erlangtes ist nicht zuzustimmen, da der Wortlaut des § 73 StGB keine Ansätze dafür gibt, Einschränkungen vorzunehmen.[159]

c) „Aus der Tat"

„Aus der Tat erlangt" ist der Vermögenszuwachs, der dem Täter unmittelbar aus der Tatbestandsverwirklichung in einer Phase des Tatablaufs zugeflossen ist.[160] Im Falle des Bitcoin-Minings mittels Einsatz von Botnetzen, bei dem das *LG Kempten* und der *BGH* entschieden haben, ist bereits die Nutzung von Botnetzen Anknüpfungspunkt: durch die Datenveränderung wird eine Verbindung zum C&C- Server über das Internet hergestellt. Mit Hilfe dieser Internetverbindung eröffnet sich der Zugriff auf die Rechenleistung. Die im Anschluss generierten Bitcoins fließen dem Täter ohne jeden weiteren Zwischenschritt,[161] mithin unmittelbar zu: nach 120 Sekunden Inaktivität durch den Nutzer wird automatisch mit dem erforderlichen Rechenprozess begonnen.[162] Die Bitcoins sind somit „aus der Tat" erlangt.

2. Der Verfall und Wertersatz des Verfalls

a) Der Wertersatz des Verfalls, § 73a a.F. StGB

155 *Schmidt*, in LK-StGB, § 73 Rn. 17.
156 *Heuchemer*, in: BeckOK-StGB, § 73 Rn. 10; *Fischer*, StGB, § 73 Rn. 8; *Saliger*, in: Kindhäuser/Neumann/Paeffgen, StGB, § 73 Rn. 3.
157 *Heger*, in: Lackner/Kühl, StGB, § 73, Rn. 3.
158 *Achenbach*, NStZ 2018, 698; vgl. *BGH*, Beschl. v. 27.7.2017 – 1 StR 412/16, S. 9.
159 S. auch: *BGH*, Beschl. v. 27.7.2017 – 1 StR 412/16, S. 9.
160 *Saliger*, in: Kindhäuser/Neumann/Paeffgen, StGB, § 73 Rn. 6; BGHSt 53, 179 (180).
161 *Saliger*, in: Kindhäuser/Neumann/Paeffgen, StGB, § 73 Rn. 6a.
162 Vgl. *BGH*, Beschl. v. 27.7.2017 – 1 StR 412/16, S. 9; *Heine*, NStZ 2016, 441.

Sind die Voraussetzungen des § 73 StGB erfüllt, so ergibt sich die Grundlage für den Verfallsanspruch. Ist die Einziehung allerdings aufgrund der Beschaffenheit oder aus anderem Grund nicht möglich, so erfolgt durch Anordnung des Gerichts der Verfall vom Wertersatz, § 73a StGB a.F. Aufgrund ihrer Beschaffenheit sind Bitcoins dem Verfall von Wertersatz unterworfen, § 73a StGB a.F.[163] Hat der Täter aber noch Zugriff auf seine Bitcoins über die Wallet und kann über diese durch den privaten Schlüssel verfügen, so kommt kein Verfall des Wertersatzes, sondern die Verfallsanordnung der Bitcoins selbst in Betracht.[164]

b) Der Verfall nach § 73 StGB

Das *LG Kempten* entschied für Bitcoins, deren private Schlüssel sich unverschlüsselt auf einem Datenträger befanden, den Verfall nach § 73 StGB a.F. Für den weiteren Anteil an Bitcoins, welche verschlüsselte private Schlüssel hatten, wurde der Verfall des Wertersatzes erklärt.[165] Dabei ist die Kenntnis des privaten Schlüssels für die Vollstreckung der Verfallsentscheidung entscheidend, aber nicht für die Bestimmung des Verfallsgegenstands, da der private Schlüssel lediglich die Zugriffsmöglichkeit regelt.[166]

3. Die strafprozessuale Sicherung von Bitcoins auf Grundlage der §§ 111a ff. StPO und deren Vollzug

a) Die Sicherstellung bei Verfall vom Wertersatz, § 111d StPO

Wird der Verfall von Wertersatz angeordnet, so käme der „dingliche Arrest“ nach § 111d StPO (a.F.) in Betracht. Dieser kann nur bei Vorlage eines Arrestgrundes angeordnet werden.[167] Zuständig für die Anordnung ist der Richter, bei Gefahr im Verzug die Staatsanwaltschaft.[168] Die Durchführung regelt der § 111d Abs. 2 StPO: für bewegliches Vermögen gilt die Pfändung, ebenso für Forderungen gem. § 930 Abs. 1 S. 3 ZPO. Bei Grundstücken erfolgt die Eintragung einer Sicherungshypothek ins Grundbuch. Fraglich ist, in welche Kategorie der §§ 930 ff. ZPO Bitcoins fallen. In Betracht kommen der Vollzug nach den Grundsätzen der Forderungspfändung, § 930 Abs. 1 S. 2 ZPO i.V.m. §§ 828 ff. ZPO oder die Regelungen für sonstige Vermögensrechte nach § 930 Abs. 1 S. 2 ZPO i.V.m. § 857 ZPO i.V.m. §§ 828 ff. ZPO. Nach dem Wortlaut passt keine der genannten Möglichkeiten. *Rückert* zieht daher die Analogie der §§ 808 ff. ZPO vor; die fehlende Sachqualität von Bitcoins könnte sich in der Auffassung vieler Stimmen, wonach Daten, die auf einem Datenträger gespeichert waren, ebenfalls hierunter zu fassen wären, wiederfinden.[169] Die vergleichbare Interessenlage wäre über die Sachqualität ebenfalls zu bejahen. Problematisch ist allerdings, dass es für den Pfändungsbeschluss an einem Schuldner fehlt, § 829 Abs. 2, 3 ZPO. Nach *Rückert* könne dieser Umstand über den § 857 Abs. 2 ZPO, die Zwangsvollstreckung in andere Vermögensrecht, überwunden werden, allerdings merkt er an, dass es hier an den Merkmalen „Recht“ und „Verfügung“ mangelt, da es sich bei Bitcoins nicht um ein Recht handelt und eine Bitcoin-Transaktion nicht mit einem Rechtsgeschäft in Form einer Verfügung vergleichbar ist. Dadurch würde nicht die gewünschte Sicherungswirkung entfaltet werden. Für diesen Fall schlägt *Rückert* die „virtuelle Inbesitznahme“ i.S.d. § 808 ZPO analog vor; danach sollen

[163] *Heuchemer*, in: BeckOK-StGB, § 73c Rn. 4; *Rückert*, MMR 2016, 296.
[164] *Heine*, NStZ 2016, 441 (445).
[165] *LG Kempten*, Urt. v. 29.10.2014 – 6 KLs 223 Js 7897/17.
[166] *Heine*, NStZ 2016, 441 (445).
[167] *Huber*, in: Graf, StPO mit GVG und Nebengesetzen, 12. Aufl. (2012), § 111d Rn. 7.
[168] *Rückert*, MMR 2016, 295 (297).
[169] *Rückert*, MMR 2016, 295 (297); *BGH*, NJW 1993, 2436 (2436 f.); *König*, NJW 1993, 3121 (3124).

private Schlüssel als abgrenzbare Datenmenge weggenommen werden können, wie durch das Kopieren der privaten Schlüssel auf behördeneigene Datenträger oder Löschung der Daten. Nach der Wegnahme könnte eine Transaktion auf einen behördeneigenen öffentlichen Schlüssel übertragen werden. So sei die erforderliche Sicherungswirkung gegeben.[170] *Goger* überwindet dieses Problem, indem dem Beschuldigten selbst der Pfändungsbeschluss mit dem Verfügungsverbot zugestellt werden soll nach den Vorschriften §§ 111c Abs. 3 S. 2 StPO i.V.m. § 857 Abs. 2 ZPO.[171]

b) Die Sicherstellung des Verfalls, §§ 111b f. StPO

Im Folgenden ist kurz darzustellen, wie sich die Annahme des *LG Kempten* bzgl. des Verfalls auf die Sicherstellung auswirkt. Das *LG Kempten* subsumiert den Verfall von Bitcoins unter die §§ 111b, 111c StPO. Eine direkte Anwendung des § 111c StPO scheidet hier aus.[172] In Betracht kommt nur eine analoge Anwendung der Vorschrift. Dabei wird mit der h.M. von der generellen Analogiefähigkeit strafprozessualer Normen ausgegangen. Anderer Ansicht ist *Goger*, der Bitcoins als „andere Vermögensrechte" zu subsumieren vermag.[173] Dies spricht allerdings gegen den Wortlaut des § 111c Abs. 2 S. 1 Alt. 2 StPO. Nach Auffassung von *Rückert* kann die „Ingewahrsamnahme" i.S.d. § 111c StPO durch Kopie des Schlüssels auf behördeneigenen Datenträger und die anschließende Löschung auf dem Datenträger des Betroffenen erfolgen. Die „maximale Sicherung" soll durch die Transaktion hergestellt werden.[174] *Goger* begegnet der Analogie mit Kritik: die Ingewahrsamnahme, welche nach außen deutlich hervortreten muss, kann nicht durch die oben beschriebene Transaktion des Schlüssels auf einen behördeneigenen Datenträger bezweckt werden. Der Beschuldigte kann seinen privaten Schlüssel nämlich auf mehreren Datenträgern gespeichert haben, die den Ermittlungsbehörden nicht bekannt sind.[175]

c) Notveräußerung

Nach Sicherstellung der Bitcoins besteht die Gefahr für die Ermittlungsbehörden/Tatverdächtigen, dass diese während des vorläufigen Verfahrens der Beschlagnahme einem starken Wertverlust unterliegen.[176] Hierfür bietet sich die Notveräußerung nach § 111l StPO a.F. (§ 111p StPO n.F.) als Lösung an. § 111l Abs. 1 S. 1 StPO a.F. gibt den Veräußerungsgrund des erheblichen Wertverlusts an. Aufgrund des bestimmbaren Marktwerts von Bitcoins, sind diese i.S.d. § 111l StPO als „Vermögenswerte" zu erfassen.[177] Die Notveräußerung von Bitcoins ist daher möglich.[178]

d) Fazit

Trotz ausreichend deckender Regelungen zur Vermögensabschöpfung von Bitcoins, besteht durchaus noch Klärungsbedarf, wie die verschiedenen Auffassungen und auch die Tatsache, dass kaum Äußerungen hierzu in der

170 *Rückert*, MMR 2016, 295 (298); *Grzywotz*, S. 270.
171 *Goger*, MMR 2016, 431 (433).
172 *Rückert*, MMR 2016, 295 (298).
173 *Goger*, MMR 2016, 431 (432 f.).
174 *Rückert*, MMR 2016, 295 (299).
175 *Goger*, MMR 2016, 431 (433).
176 *Goger*, MMR 2016, 431 (434).
177 *Bittmann*, in: MüKo-StPO, § 111l Rn. 2; *Rückert*, MMR 2016, 295 (299).
178 Pressemitteilung, abrufbar unter: https://www.justiz.bayern.de/gerichte-und-behoerden/generalstaatsanwaltschaft/bamberg/presse/2018/10.php; *Giese*, Artikel BTC-Echo, abrufbar unter: https://www.btc-echo.de/lul-to-bayern-verkauft-kryptos-im-wert-von-12-millionen-euro (zuletzt abgerufen am 3.3.19).

Literatur vorliegen, aufzeigen. Das neu gestaltete Recht zur Vermögensabschöpfung bietet hier ebenfalls keine Aufklärung zur Handhabung bei virtuellen Währungen.[179]

V. Herausforderung der Bekämpfung von Bitcoin-Straftaten

Besonders in der Praxis des Strafverfahrensrechts verdeutlichen sich die Probleme des Cybercrimes für Strafverfolgungsbehörden. Im Zusammenhang Bitcoin-bezogener Straftaten stellen insbesondere die Merkmale des Bitcoin-Systems Hindernisse für eine erfolgreiche Strafermittlung dar.

1. Herausforderungen für die Strafverfolgung

Die Vorschriften für die IT-forensische Sicherung und Analyse von Daten aus IT- Systemen nach den Regelungen der Beschlagnahme und Durchsuchung gem. §§ 94 ff. und §§ 102 ff. StPO sind durchaus für die Fälle im Bereich des Cybercrimes anwendbar. Allerdings werden die Ermächtigungsvorschriften neuen Anforderungen, die mit der entwickelten Technik einhergehen, nicht gerecht.[180] Es ist bislang noch ungeklärt, inwieweit deren Anwendungsbereich auf den Bereich des Cybercrimes im Allgemeinen zu beziehen sind und ob nicht doch eine Neugestaltung strafprozessualer Vorschriften notwendig ist.[181]

a) Faktische Herausforderungen

Für einen erfolgreichen Ablauf der Ermittlungen sind organisatorische Spezialisierung und Besetzung mit IT-Spezialisten sowie einer optimalen Ausstattung erforderlich. Die Eigenschaften des Bitcoin-Systems erschweren jedoch die Ermittlungstätigkeit.[182]

aa) Dezentralität

Gerade das Merkmal der Dezentralität des Bitcoin-Systems lässt die klassischen Ermittlungstätigkeiten, wie das Auskunftsersuchen bei Banken nach §§ 161, 95 StPO sowie die für die Ermittlung erforderlichen Werkzeuge der Durchsuchung und Beschlagnahme, §§ 94 ff. StPO, ins Leere laufen.[183] Grund hierfür ist die fehlende zentraler Instanz.[184]

bb) Anonymität und Pseudonymität

Für den Ausfall der Ermittlungsinstrumente könnte die Analyse der öffentlich einsehbaren Blockchain und damit die Zurückverfolgung der Transaktionen in Betracht kommen.[185] Doch darauf folgt ein weiteres Hindernis: die Pseudonymität innerhalb der Blockchain. Die Entdeckung strafrechtlicher Handlungen im Internet ist in der Regel bereits aufgrund des wachsenden Datenvolumens unwahrscheinlich. Doch selbst wenn die Delikte von den zuständigen Behörden wahrgenommen werden, bleiben die Täter meist anonym.[186] Das Blockchain-System selbst

179 siehe BT-Drs. 18/11640.
180 *Heinson*, IT-Forensik, 2015, S. 90.
181 *Pesch/Böhme*, DuD 2017, 93 (95).
182 *Grzywotz/Köhler/Rückert*, StV 2016, 753 (758).
183 *Michels*, Straftaten und Strafverfolgung im Internet, 2003, S. 19 ff.
184 *Grzywotz/Köhler/Rückert*, StV 2016, S. 753 (758).
185 *Pesch/Böhme*, DuD 2017, 93 (96).
186 *Hilgendorf/Valerius*, Rn. 759.

besteht auf Grundlage der Pseudonymität der Nutzer. Insbesondere bei der Ausübung von Bitcoin-Straftaten stellen viele Täter beliebig viele Adressen her, um ihre Identität zu verschleiern.[187] An der Pseudonymität scheitert schließlich die weitere Verfolgung in den meisten Fällen.[188]

2. Lösungsansätze zur Bewältigung der Herausforderungen

a) Datenanalyse und Datenverknüpfung

Einen Anknüpfungspunkt für die Ermittlungstätigkeiten stellen die öffentlich einsehbaren Transaktionsdaten dar, die in der Blockchain gesammelt sind.[189] Mithilfe von Datenverarbeitungsmethoden können diese Transaktionen mit anderen Datensätzen verknüpft werden, um die Adressen den jeweiligen Personen zuordnen zu können.[190] Ein Beispiel hierfür sind Datensätze aus Informationen über Online-Geschäfte, bei denen eine Entrichtung eines bestimmten Betrags an eine bestimmte Bitcoin-Adresse übertragen wird.[191] Die Frage, ob in diesen Fällen auf die bereits bestehenden Befugnisse aus der StPO zurückzugreifen ist oder ob lediglich die Grenzen der Ermittlungsklauseln, die einzuhaltende nicht intensive Grundrechtsbeeinträchtigung, eingehalten werden können, wurde bislang nicht beantwortet.[192] Kämen beide Alternativen nicht in Betracht, müsste sich der Gesetzgeber mit neuen Ermächtigungsnormen befassen.

b) „Technische Prävention"

Das österreichisch-deutsche Forschungsprojekt BITCRIME hat sich die Entwicklung von Regulierungsansätzen zur Prävention der Kriminalisierung virtueller Kryptowährungen zur Aufgabe gemacht.[193] Aufgrund der mit einem Totalvorbehalt einhergehenden intensiven Grundrechtseingriffe wird eine solche Maßnahme abgelehnt.[194] Als besonders vielversprechender Ansatz hat sich das sog. „Blacklisting" herausgestellt.

aa) „Blacklisting"

Das sog. „Blacklisting" ist als eine Sperrliste zu verstehen. Nach Feststellung des kriminellen Bezugs der Transaktionen, würden diese in der Sperrliste aufgenommen werden. Hierdurch könnte der Tausch illegal erworbener Bitcoins in Realwährungen verhindert werden und präventiv würde es die Nutzer dazu verleiten, auf illegalem Wege erworbene Bitcoins nicht mehr anzunehmen, da sie diese nicht mehr in Realwährungen umtauschen könnten.[195] Alternativer Anknüpfungspunkt sind Adressen. Hier könnten Dienstanbietern, welche gewerblich einen Tausch von Bitcoins in Realwährungen oder Waren anbieten, die Pflicht auferlegt werden, mit Adressen kriminellen Bezugs keine Verträge zu schließen bzw. Coins der aufgelisteten Konten nicht als Leistung zu akzeptieren. Dabei würden die Bitcoins aus der kriminell assoziierten Transaktion als wertlos oder teilentwertet erklärt

187 *Möser/Böhme/Breuker*, An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem, S. 3 f.
188 *Pesch/Böhme*, DuD 2017, 93 (96); Blogbeitrag, abrufbar unter: https://blogs.fau.de/cybercrime/category/cybercrine-strafverfolgung/ (zuletzt abgerufen am 3.3.19).
189 *Erbguth*, Tracking von Bitcoin-Zahlungen, S. 12, abrufbar unter: https://erbguth.ch/slides/Tracking%20von%20Bitcoin-Zahlungen.pdf (zuletzt abgerufen am 8.3.19).
190 *Grzywotz/Köhler/Rückert*, StV 2016, 753 (758).
191 *Pesch/Böhme*, DuD 2017, 93 (95).
192 Vgl. *Grzywotz/Köhler/Rückert*, StV 2016, 753 (758).
193 Projekt BITCRIME, „Präventionen von Straftaten mit Bitcoins und Alt-Coins", S. 1, abrufbar unter: https://www.bit- crime.de/presse-publikationen/pdf/BITCRIME-RegulRep.pdf (zuletzt ab gerufen am 8.3.19)
194 Projekt BITCRIME, „Präventionen von Straftaten mit Bitcoins und Alt-Coins", S. 8, abrufbar unter: https://www.bit- crime.de/presse-publikationen/pdf/BITCRIME-RegulRep.pdf (zuletzt ab gerufen am 8.3.19).
195 *Grzywotz/Köhler/Rückert*, StV 2016, 753 (759); *Pesch/Böhme*, DuD 2017, 93 (97).

werden.[196] Gegen die Geeignetheit von Adressen spricht indes, dass Bitcoin-Adressen durch jedermann beliebig oft hergestellt werden können. Damit könnten Kriminelle ohne großen Aufwand durch Erzeugung neuer Adressen die Listung umgehen und die Bitcoins auf die neuen Adressen übertragen. Hingegen spricht für die Auflistung von Transaktionen, dass diese die Erfassung von Folgetransaktionen ermöglichen. Damit kann die Regulierung von Sperrlisten nicht umgangen werden. Mit Transaktionssperrlisten wären die geringsten Nachteile für legale Nutzer verbunden und damit die Verhältnismäßigkeit gewahrt.[197]

bb) Fazit

Die Transparenz des Bitcoin-Systems, in der bislang jede Transaktion von Bitcoins erfasst ist und die einsehbar ist, gebietet sich als bedeutende Möglichkeit in der Strafverfolgung und Prävention Bitcoin-bezogener Straftaten. Die Identifikation der Nutzer birgt jedoch den Nachteil, dass legalen Nutzern die Pseudonymität verwehrt wird. Die Systematik der Transaktionssperrlisten bietet sich daher hierfür an; mit ihr wird an die Transparenz des Bitcoin-Systems angeknüpft, ohne auf die Identifikation der Nutzer zugreifen zu müssen.

VI. Zusammenfassung und Ausblick

Im Umgang mit Bitcoins ist vieles noch ungeklärt: Bitcoins bedürfen einer Einordnung im deutschen Rechtssystem und weisen im Falle ihrer Vermögensabschöpfung Unklarheiten auf, die gegebenenfalls nur über die Analogie einschlägiger Normen gelöst werden können. Die strafrechtliche Würdigung hinsichtlich des Einsatzes eines Botnetzes zum heimlichen Schürfen von Bitcoins ist im Grunde ausreichend erfasst nach §§ 202a, 303a StGB. Die steigende Komplexität technischer Möglichkeiten birgt jedoch die Gefahr der Entwicklung weiterer Methoden des heimlichen Schürfens, die bislang entweder unentdeckt sind oder in ihrer strafrechtlichen Erfassung der Aufklärung bedürfen. Hierzu verhilft der Gesetzesentwurf zum Schutz des „Digitalen Hausfriedensbruchs“ nach § 202e StGB eher weniger. Dass die Norm „technikoffen“ ausgelegt ist, stellt vielmehr eine weitere Herausforderung für die Entdeckung versteckter Technikinstrumente dar und stellt alltägliche Handlungen unter Strafe. Die vertretene Ansicht der Ausweitung des § 303b StGB scheint insofern vorzugswürdig, als dass der in der Praxis bedeutsam gewordene Anstieg der Stromrechnung dadurch strafrechtlich erfasst werden kann. Mit dieser Neufassung würde das Anliegen des Bundesrats hinsichtlich der ausreichenden Gewährleistung des IT-Grundrechts aufgenommen werden, ohne Alltagskriminalität zu erschaffen. Im Ergebnis stellt das Strafrecht somit grundsätzlich ein geeignetes Regelungsinstrument dar, um den Erscheinungsformen des Cybercrimes entgegen zu wirken. Im Lichte des Ultima-ratio Grundsatzes sind bei der Bekämpfung der Kriminalität im Internet jedoch zunächst außerstrafrechtliche Präventionsmaßnahmen zu ergreifen. So könnte dem in erster Linie bestehenden Aufklärungsbedarf über die Gefahren und Risiken des Internets sowie über die technischen Schutzmöglichkeiten, wie Virenscanner, Firewalls und Verschlüsselungssysteme, zunächst Rechnung getragen werden.[198] Ermittlungen von Bitcoin-Straftaten stellen sich den Herausforderungen des dezentral ausgelegten Bitcoin-Systems und des pseudonymen Auftritts der Nutzer. Die technische Präventionsmaßnahme des sog. Blacklistings erscheint zudem als erforderlich, da ein anderes, milderes aber gleich effektives Mittel nicht ersichtlich ist. Der Bekämpfung und Prävention der Inter-

196 *Pesch/Böhme*, DuD 2017, 93 (97).
197 Projekt BITCRIME, „Präventionen von Straftaten mit Bitcoins und Alt-Coins“, S. 9, abrufbar unter: https://www.bit- crime.de/presse-publikationen/pdf/BITCRIME-RegulRep.pdf (zuletzt abgerufen am 8.3.19).
198 So auch *Beukelmann*, Prävention von Computerkriminalität, 2001, S. 100.

netkriminalität hat sich das BKA bereits in Kooperation mit nationalen und internationalen Konstitutionen (Europol, Interpol) angenommen.[199] Dennoch stiegen die Fallzahlen im Bereich der Cyberkriminalität seit 2017 an. Die hohe Dunkelziffer lässt darüber hinaus auf ein großes Gefährdungspotenzial dieses Deliktsfeldes schließen.[200] Auch der Betrieb von Botnetzen wird immer attraktiver. Das Interesse krimineller Akteure am illegalen Krypto-Mining hat besonders im Jahre 2017 stark zugenommen. Wegen der einfachen Handhabung und der Vielschichtigkeit, die das System von Kryptowährungen bietet, ist ein Rückgang der Zahlen Betroffener nicht anzunehmen.[201]

[199] https://www.bka.de/DE/DasBKA/OrganisationAufbau/Fachabteilungen/SchwereOrganisierteKriminalitaet/schwereorganisiertekriminalitaet_node.html (zuletzt abgerufen am 10.3.19)

[200] BKA-Bundeslagebild Cybercrime 2017, abrufbar unter: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/Cybercrime/cybercrimeBundeslagebild2017.html (zuletzt abgerufen am 10.3.19).

[201] BSI, Die Lage der IT-Sicherheit in Deutschland 2018, S. 91 f, abrufbar unter: https://www.bsi.bund.de/Shared-Docs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2018.pdf?__blob=publication-File&v=5 (zuletzt abgerufen am 10.3.19).