



## Beschlagnahme von Kryptowährungen im Strafverfahren

MONIKA SIMMLER\*

SINE SELMAN\*\*



DANIEL BURGERMEISTER\*\*\*

Die unklare Rechtsnatur von Kryptowährungen stellt die Strafverfolgungsbehörden bei der strafprozessualen Beschlagnahme von Bitcoin, Ethereum, Ripple und Co. vor neue Herausforderungen, welchen sich dieser Beitrag annimmt. Es wird festgestellt, dass Kryptowährungen als Daten mit Vermögenswert sui generis zu klassifizieren sind. Somit sind sie zu Einziehungs-, Restitutions- und Kostendeckungszwecken beschlagnahmefähig, wobei eine Sicherstellung nur durch eine Übertragung des Wertes der Kryptowährungen auf eine staatliche Wallet gelingt. Aufgrund der Volatilität von Kryptowährungen kann eine vorzeitige Verwertung geboten sein. Der vorliegende Beitrag identifiziert die rechtlichen Unklarheiten hinsichtlich der Beschlagnahme von Daten als unbefriedigende Ausgangslage für die Praxis. Insgesamt bietet der Beitrag einen umfassenden Überblick über die gesetzlichen Grundlagen der Beschlagnahme von Kryptowährungen und schliesst mit konkreten Handlungsempfehlungen an die Praxis.

La nature juridique peu claire des cryptomonnaies pose de nouveaux défis aux autorités de poursuite pénale pour la saisie de Bitcoin, Ethereum, Ripple etc., dont traite le présent document. L'article constate que les cryptomonnaies doivent être qualifiées de données disposant d'une valeur patrimoniale sui generis. Elles peuvent donc être saisies à des fins de recouvrement, de restitution et de couverture de frais ; la sûreté ne pouvant être obtenue que par le transfert de la valeur des cryptomonnaies dans un wallet étatique. En raison de la volatilité des cryptomonnaies, une réalisation anticipée peut s'avérer nécessaire. Cet article considère néanmoins les ambiguïtés juridiques concernant la confiscation des données comme une situation initiale insatisfaisante dans la pratique. Dans l'ensemble, l'article donne un aperçu complet des bases légales relatives à la confiscation des cryptomonnaies et se termine par des recommandations concrètes d'action dans la pratique.

### Inhaltsübersicht

- I. Einleitung
- II. Kryptowährungen: Grundlagen und strafprozessuale Ausgangslage
  - A. Was sind Kryptowährungen?
    1. Technische Grundlagen
    2. Pseudoanonymität, Darknet und Schattenwirtschaft
    3. Aufbewahrungsmöglichkeiten: Hot & Cold Storages
  - B. Ausgangslage: Rechtsnatur von Kryptowährungen
    1. Allgemeine rechtliche Einordnung
    2. Qualifikation als Sache, Daten oder Vermögenswert?
    3. Kryptowährungen als Daten mit Vermögenswert sui generis
- III. Beschlagnahme von Kryptowährungen nach Art. 263 ff. StPO
  - A. Grundlagen der Beschlagnahme
    1. Zweck und Wesen

2. Beschlagnahmearten
- B. Eignung von Kryptowährungen als Beschlagnahmeobjekt
  1. ... als «Gegenstand»?
  2. ... als «Daten»?
  3. ... als «Vermögenswert»?
  4. Zwischenfazit
- C. Beschlagnahme durch Übertragung auf staatliche Wallets
  1. Rechtliche Grundlage
  2. Durchführung der Beschlagnahme in der Praxis
  3. Herausgabepflicht
  4. Einrichtung einer staatlichen Wallet
- D. Veräusserung beschlagnahmter Vermögenswerte
  1. Volatilität und vorzeitige Verwertung von Kryptowährungen
  2. Voraussetzungen und Umsetzung einer Veräusserung
- IV. Fazit

\* MONIKA SIMMLER, Dr. iur., Postdoctoral Fellow für Strafrecht, Strafprozessrecht und Kriminologie an der Universität St. Gallen.

\*\* SINE SELMAN, M.A. HSG in Law, a.o. Gerichtsschreiberin am Kreisgericht Rorschach.

\*\*\* DANIEL BURGERMEISTER, MLaw, RA, MAS Forensics, Staatsanwalt bei der Staatsanwaltschaft St. Gallen.

### I. Einleitung

Kryptowährungen sind in aller Munde. Das im Zuge der weltweiten Finanzkrise 2008 vorgestellte Protokoll für ein

Peer-to-Peer-Zahlungssystem «Bitcoin»<sup>1</sup> und die mittlerweile mehr als 1500 weiteren Kryptowährungen mit einer Marktkapitalisierung von über 320 Mia. USD<sup>2</sup> haben den Finanzmarkt ordentlich in Unruhe versetzt. Auch bei der Begehung von Straftaten nimmt die Relevanz von derartigen virtuellen Währungen stetig zu. So sei gerade *Bitcoin* mittlerweile die «*Currency of Choice*» für Cyberkriminelle.<sup>3</sup> Kryptowährungen haben deshalb in der jüngeren Vergangenheit vermehrt (straf-)rechtswissenschaftliche Aufmerksamkeit erhalten.<sup>4</sup> Dabei stand bis anhin primär die materiell-rechtliche Erfassung und Behandlung dieser neuen Finanzinstrumente im Zentrum. Virtuelle Währungen und die zugrundeliegende *Blockchain*-Technologie stellen jedoch insbesondere Strafverfolgungsbehörden vor neue Herausforderungen,<sup>5</sup> womit auch strafprozessrechtliche Fragen in den Vordergrund rücken.<sup>6</sup>

In Anbetracht der wachsenden Bedeutung dieser «virtuellen Vermögenswerte» bei verschiedenen kriminellen Verhaltensweisen erweist sich gerade hinsichtlich der Beschlagnahme die ungeklärte Rechtsnatur von Kryptowährungen als problematisch. Auch wenn die Beschlagnahme von Kryptowährungen bzw. vor allem die spätere Ver-

ässerung mit Millionengewinnen z.B. in Deutschland bereits Schlagzeilen machte,<sup>7</sup> verbleiben für das hiesige Strafprozessrecht Unklarheiten in Bezug auf die relevanten rechtlichen Grundlagen. Um eine konsequente Strafverfolgung sicherzustellen, müssen sowohl diese rechtlichen Unklarheiten als auch die praktischen Probleme im Umgang mit der Sicherstellung und Beschlagnahme von Kryptowährungen geklärt werden.<sup>8</sup> Dieser Aufgabe widmet sich der vorliegende Beitrag. Zu diesem Zweck werden zunächst kurz die für die vorliegende Forschungsfrage relevanten technischen Grundlagen eingeführt und die speziellen Charakteristiken diskutiert, welche zur kriminalpolitischen Relevanz der Kryptowährungen geführt haben. Ebenso gilt es, sich gleichsam einführend der rechtlichen Natur der virtuellen Währungen zu widmen, da für die Anwendbarkeit der relevanten Bestimmungen eine Einordnung in bestehende Rechtsbegrifflichkeiten vonnöten ist. In der Folge werden die allgemeinen Voraussetzungen der Beschlagnahmearten erörtert, bevor geprüft wird, ob Kryptowährungen als Gegenstände, Daten oder Vermögenswerte unter Art. 263 ff. StPO subsumiert werden und damit taugliche Beschlagnahmeobjekte darstellen können. Da sich sowohl bei der Sicherstellung als auch bei der Aufbewahrung, Herausgabe oder Veräusserung von Kryptowährungen praktische Schwierigkeiten ergeben, z.B. Zugangsschranken oder die Notwendigkeit der Übertragung der Werte zum Staat, widmet sich der Beitrag im Anschluss auch detailliert der konkreten Umsetzung dieser strafprozessualen Massnahme. In seiner Gesamtheit bietet dieser Artikel einen umfassenden Überblick über die gesetzlichen Grundlagen und die praktische Umsetzung der Beschlagnahme von Kryptowährungen.

## II. Kryptowährungen: Grundlagen und strafprozessuale Ausgangslage

### A. Was sind Kryptowährungen?

#### 1. Technische Grundlagen

Die Funktionsweise der Kryptowährungen bzw. der ihnen zugrunde gelegten Technologie ist komplex und der

<sup>1</sup> SATOSHI NAKAMOTO, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, Internet: <https://bitcoin.org/bitcoin.pdf> (Abruf 9.7.2018); DON TAPSCOTT/ALEX TAPSCOTT, Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World, New York 2016, 5.

<sup>2</sup> Gemäss <https://coinmarketcap.com/> (Abruf 9.7.2018).

<sup>3</sup> So STEVEN D. BROWN, Cryptocurrency and criminality: The Bitcoin opportunity, *The Police Journal: Theory, Practice and Principles*, Vol. 89 (4), 2016, 327 ff., 327.

<sup>4</sup> Siehe für die Schweiz z.B. DANIEL STOLL, Le bitcoin et les aspects pénaux des monnaies virtuelles, *forumpenale* 2015, 99 ff.; JEAN-DANIEL SCHMID/ALEXANDER SCHMID, Bitcoin – eine Einführung in die Funktionsweise sowie eine Auslegeordnung und erste Analyse möglicher rechtlicher Fragestellungen, *Jusletter* vom 4.6.2012; LUKAS MÜLLER/THOMAS STOLTZ/TOBIAS A. KALLENBACH, Liberierung des Aktienkapitals mittels Kryptowährung, *AJP* 2017, 1318 ff.; NICOLAS JACQUEMART/STEPHAN D. MEYER, Der Bitcoin-/Bitcoin-Cash-Hardfork, *GesKR* 2017, 469 ff.; FRANÇOIS PILLER, Virtuelle Währungen – Reale Rechtsprobleme?, *AJP* 2017, 1426 ff.

<sup>5</sup> Zu diesen Herausforderungen der Ermittlung z.B. CHRISTOPH SAFERLING/CHRISTIAN RÜCKERT, Telekommunikationsüberwachung bei Bitcoins, *MMR* 2015, 788 ff.; ANDREAS EUGSTER, Kryptowährung Bitcoin, Funktionsweise und künftige Herausforderungen für Ermittlungsbehörden, *Kriminalistik* 2018, 40 ff.; vgl. United Nations Office on Drugs and Crime (UNODC), Basic Manual on the Detection and Investigation of the Laundering of Crime Proceeds Using Virtual Currencies, Juni 2014, Internet: [https://www.imolin.org/pdf/imolin/FULL10-UNODCVirtualCurrencies\\_final.pdf](https://www.imolin.org/pdf/imolin/FULL10-UNODCVirtualCurrencies_final.pdf) (Abruf 9.7.2018).

<sup>6</sup> Vgl. für das deutsche Recht z.B. CHRISTIAN RÜCKERT, Vermögensabschöpfung und Sicherstellung bei Bitcoins, *MMR* 2015, 295 ff., 295.

<sup>7</sup> Siehe z.B. <http://www.spiegel.de/wirtschaft/unternehmen/bitcoin-beschlagnahmt-berliner-justiz-kann-auf-riesigen-gewinn-hoffen-a-1187474.html> (Abruf 9.7.2018); <http://www.rp-online.de/wirtschaft/finanzen/beschlagnahmt-kryptowaehrung-hessen-hofft-auf-millionen-durch-bitcoin-verkauf-aid-1.7270734> (Abruf 9.7.2018).

<sup>8</sup> Vgl. auch THOMAS GÖGER, Bitcoins im Strafverfahren: Virtuelle Währung und reale Strafverfolgung, *MMR* 2016, 431 ff., 431.

strafprozessuale Umgang damit erfordert Spezialwissen.<sup>9</sup> Auch wenn *Bitcoin* die erste eigentliche Kryptowährung war, gibt es mittlerweile zahlreiche Alternativen, sog. *Altcoins*, welche sich in ihren Anwendungen und Protokollen auch deutlich voneinander unterscheiden können.<sup>10</sup> Dennoch lohnt sich eine gemeinsame Betrachtung, denn ein Fokus einzig auf *Bitcoin* wäre in Anbetracht der Vielfalt dieser Anwendungen und der wachsenden Bedeutung von Alternativen nicht mehr angebracht. Dies befreit allerdings nicht davon, Eigenheiten im Einzelfall zu berücksichtigen. Allen Kryptowährungen ist gemeinsam, dass sie auf der *Blockchain*-Technologie basieren, d.h. auf digitalen «Grundbüchern». Dieses öffentliche Protokoll, in welchem jede Transaktion vermerkt wird und welches es erlaubt, alle Transaktionen theoretisch endlos zurückzuverfolgen, schafft das «dezentrale Vertrauen», auf welchem die Währungen aufbauen.<sup>11</sup> Es handelt sich dabei um ein Paradigma basierend auf einer Kombination von Kryptographie und einem digitalen, dezentralen Netzwerk.<sup>12</sup> Das *Peer-to-Peer*-Prinzip impliziert dabei, dass alle zum Netzwerk gehörenden Informationen dezentral auf allen vernetzten Endgeräten der Nutzer gespeichert sind und kein zentraler Server existiert.<sup>13</sup> Diese sog. *Distributed Public Ledgers*, d.h. «verteilte öffentliche Hauptbücher», sind einsehbar, auf denen zwar jeder etwas Neues eintragen, aber niemand einen Eintrag wieder löschen kann.<sup>14</sup>

Kryptowährungen zeichnen sich dadurch aus, dass sie im Gegensatz zu herkömmlichen Fiatwährungen nicht von Staaten eingeführt<sup>15</sup> und kontrolliert werden.<sup>16</sup> Es mangelt demzufolge an einer zentralen Instanz. Des Weiteren finden die Finanztransaktionen aufgrund der technischen Ausgestaltung nicht zwischen verschiedenen

Individuen direkt statt, sondern zwischen «Adressen».<sup>17</sup> Bei den meisten Kryptowährungen, so z.B. bei *Bitcoin*, ersetzen kryptografische Schlüsselpaare die Funktion herkömmlicher Bankkonten. Diese *Keys* beinhalten einen sehr langen Code bestehend aus Nummern und Buchstaben, wobei jedem Nutzer ein *Private Key*, ein nur ihm bekannter Code, und ein *Public Key*, eine Art öffentliche Kontonummer, zukommt. Nur wer über beide Schlüssel verfügt, kann *Bitcoins* transferieren.<sup>18</sup> Bei den meisten dezentralen Kryptowährungen werden die Transaktionen mittels eines kryptographischen «Puzzles» gesichert bzw. bestätigt (sog. *Proof-of-Work*), wobei sich mittlerweile auch andere Validierungsmethoden etabliert haben.<sup>19</sup> Der erste Computer, der dieses Rätsel löst und damit die Transaktion verifiziert, wird mit neu kreierten *Coins* bezahlt. Diesen kompetitiven Prozess nennt man *Mining*. Er dient dem Erzeugen von neuen Einheiten, welche folglich mit dem Zurverfügungstellen von Rechenleistung «bezahlt» werden.<sup>20</sup> Dennoch dient das *Mining* nicht in erster Linie der Generierung neuer Einheiten, sondern letztlich der Verarbeitung und Bestätigung von Transaktionen durch das Netzwerk.<sup>21</sup> Wenn 51 % der Akteure im Netzwerk die Transaktion bestätigt haben, findet sie Eingang in die *Blockchain*.<sup>22</sup> Da sämtliche Bewegungen in die *Blockchain* eingetragen werden und diese öffentlich ist, hat diese eine Publizitätsfunktion.<sup>23</sup> Durch dieses Verfahren wird sichergestellt, dass niemand sein virtuell verfügbares Guthaben mehrfach ausgeben kann (Vermeidung des sog. *Double Spending*).<sup>24</sup>

## 2. Pseudoanonymität, Darknet und Schattenwirtschaft

Die kriminellen Möglichkeiten, welche sich durch Kryptowährungen ergeben, sind vielseitig. Kryptowährungen spielen vor allem bei denjenigen Delikten eine Rolle, bei denen sie als Zahlungsmittel eingesetzt werden.<sup>25</sup> Dort nehmen sie eine «Geldersatzfunktion» ein.<sup>26</sup> Es stehen

<sup>9</sup> EUGSTER (FN 5), 40.

<sup>10</sup> SANDER DUIVESTEIN ET AL., *Blockchain: Cryptoplattform for a Frictionless Economy, Design to Disrupt*, 2015, 8; dazu auch European Central Bank, *Virtual currency schemes – a further analysis*, Februar 2015 (zit. ECB, Analysis), 9 ff.

<sup>11</sup> Siehe dazu z.B. ANDY EXTANCE, *The future of cryptocurrencies: Bitcoin and beyond*, *Nature*, Vol. 526 (7571), 2015, 21 ff.

<sup>12</sup> EUGSTER (FN 5), 40.

<sup>13</sup> ANDREAS JÄNKE, «Bitcoins» – Was sie sind, wie sie funktionieren und weshalb sie für Kriminelle interessant sind, *Kriminalistik* 2016, 63 ff., 64.

<sup>14</sup> CHRISTIAN RÜCKERT, *Die Blockchain-Technologie – Digitaler Konsens statt Bürokratie?*, *Nuernberg Web Week Magazin* 2017, 22 ff., 22.

<sup>15</sup> Eine Ausnahme könnte Venezuela darstellen, denn dort hat die Regierung die staatliche Kryptowährung «Petro» ausgegeben, wobei umstritten ist, ob es sich dabei wirklich um eine Kryptowährung handelt (DIETER BACHMANN, *Venezuela führt die neue Kryptowährung «Petro» ein*, *NZZ-Online* vom 3.12.2017).

<sup>16</sup> TAPSCOTT/TAPSCOTT (FN 1), 5.

<sup>17</sup> DUIVESTEIN ET AL. (FN 10), 9.

<sup>18</sup> RÜCKERT (FN 14), 24.

<sup>19</sup> RÜCKERT (FN 14), 22; ECB, Analysis (FN 10), 10.

<sup>20</sup> EUGSTER (FN 5), 42.

<sup>21</sup> JÄNKE (FN 13), 64.

<sup>22</sup> DUIVESTEIN ET AL. (FN 10), 5 und 10 ff.

<sup>23</sup> FRANZISKA BOEHM/PAULINA PESCH, *Bitcoins: Rechtliche Herausforderungen einer virtuellen Währung*, *Eine erste juristische Einordnung*, *MMR* 2014, 75 ff., 76.

<sup>24</sup> DUIVESTEIN ET AL. (FN 10), 9.

<sup>25</sup> So auch BOEHM/PESCH (FN 23), 77.

<sup>26</sup> JOHANNA GRZYWOTZ/OLAF M. KÖHLER/CHRISTIAN RÜCKERT, *Cybercrime mit Bitcoins – Straftaten mit virtuellen Währungen, deren Verfolgung und Prävention*, *StV* 2016, 753 ff., 756.

folglich Geldwäschereirisiken und die Nutzung der virtuellen Währungen für den Handel mit illegalen Gütern und Dienstleistungen im Zentrum.<sup>27</sup> Gerade der weitbekannte Fall der Schwarzmarktplattform *Silkroad*<sup>28</sup> hat dazu geführt, dass Kryptowährungen regelmässig mit der Schattenwirtschaft in Verbindung gebracht werden.<sup>29</sup> So ist es denn auch kein Zufall, dass Kryptowährungen – dabei vor allem *Bitcoin* – mittlerweile im *Darknet* vorherrschendes Zahlungsmittel sind und auch fast alle heutigen *Ransomware*- oder «*Distributed Denial of Service*»-Angriffen (DDoS) mittels Kryptowährungen abgewickelt werden.<sup>30</sup> Virtuelle Währungen werden jedoch nicht nur als Hilfsmittel bei illegalem Handel oder z.B. bei Erpressungen relevant. Aufgrund ihres Vermögenswerts können sie vielmehr auch selbst Gegenstand krimineller Handlungen, z.B. des weiten Spektrums an Vermögensdelikten, werden.<sup>31</sup> Schlagzeilen über «Diebstähle» von Kryptowährungen oder über Hacking- oder Trojanerangriffe auf *Bitcoin*-Speicherplätze, Handelsbörsen oder *Wallet*-Betreiber sind mittlerweile an der Tagesordnung.<sup>32</sup>

Die Popularität der Kryptowährungen in Schwarzmarkt und Schattenwirtschaft, aber auch die Attraktivität derselben für Hacking-Angriffe ist primär der technischen Ausgestaltung der virtuellen Währungen, welche im Vergleich zu herkömmlichen Bankkonten eine erhöhte Anonymität erlaubt, und der Abwesenheit einer zentralen oder staatlichen Kontrollinstanz zuzuschreiben. Auch wenn das den Kryptowährungen zugrundeliegende *Blockchain*-Protokoll öffentlich ist, so ist das Netzwerk selbst «pseudoanonym», u.a. weil jeder Nutzer grundsätzlich eine unendliche Anzahl an unabhängigen öffentlichen Schlüsseln generieren kann.<sup>33</sup> Dieser *Public Key* wird dann zu

einer Art «Pseudonym», den zwar jeder einsehen und nachverfolgen kann, der aber im Allgemeinen nicht mit der Identität des Besitzers direkt in Verbindung gebracht werden kann. Dadurch wird die Identitätsaufklärung für Dritte deutlich erschwert.<sup>34</sup> Auch wenn in der *Blockchain* alle Transaktionen nachvollziehbar sind, können die öffentlichen Adressen dem Nutzer also oft nicht eindeutig zugeordnet werden.<sup>35</sup> Gerade der Einsatz sog. *Mixer*, die Kryptowährungen verschiedener Nutzer automatisiert vermischen und an neue Adressen auszahlen, erleichtern die Verschleierung.<sup>36</sup> Diese Anonymität, oder eben «Pseudoanonymität», gilt als gefahren erhöhend und steht im Verdacht, kriminellen Aktivitäten Vorschub zu leisten und Ermittlungen zu erschweren.<sup>37</sup>

Dennoch kann nicht geleugnet werden, dass sich durch die öffentliche Einsehbarkeit der *Blockchain* auch neue Chancen im Bereich der Strafverfolgung ergeben.<sup>38</sup> So erlaubt die Technologie die Zurückverfolgung des Geldweges und damit eine einfachere Beweissicherung in Hinblick auf die illegale Herkunft von Vermögenswerten. Mittels sog. *Data Mining*, d.h. mit modernen Datenerhebungs- und Datenverarbeitungsmethoden bzw. mit der Verknüpfung der *Blockchain*-Daten mit anderen Datenbanken, lässt sich ferner der Pseudoanonymität durchaus entgegenwirken. Viele Adressen lassen sich dadurch Personen zuordnen.<sup>39</sup> Obwohl mittlerweile verschiedene derartige «Deanonymisierungsmethoden» bestehen, bleibt die Ermittlung durch die Dezentralität allerdings dennoch erschwert.<sup>40</sup>

### 3. Aufbewahrungsmöglichkeiten: Hot & Cold Storages

Strafverfolgungsbehörden benötigen im Zusammenhang mit Kryptowährungen ein Verständnis für die grundlegende Funktionsweise der *Blockchain*-Technologie und des Kryptowährungsmarktes. Für die Sicherstellung virtuel-

<sup>27</sup> Vgl. Bericht des Bundesrates vom 25. Juni 2014 zu virtuellen Währungen in Beantwortung der Postulate Schwaab (13.3687) und Weibel (13.4070) (zit. Bericht des Bundesrates), 20 ff.; siehe auch BOEHM/PESCH (FN 23), 75.

<sup>28</sup> Siehe zu diesem Fall aus kriminologischer Sicht z.B. JUDITH ALDRIDGE/DAVID DECARY-HETU, Not an «eBay for Drugs»: The Cryptomarket «Silk Road» as a Paradigm Shifting Criminal Innovation, Mai 2014, SSRN: <https://dx.doi.org/10.2139/ssrn.2436643> (Abruf 9.7.2018).

<sup>29</sup> Siehe z.B. KEVIN F. K. LOW/ERNIE G. S. TEO, Bitcoins and other cryptocurrencies as property?, *Law, Innovation and Technology*, Vol. 9 (2), 2017, 235 ff., 238 f.; SETH LITWACK, Currency or Fool's Gold: A Comparative Analysis of the Legal Classification of Bitcoin, *Temple Int'l & Comp. L. J.*, Vol. 29, 2015, 309 ff., 315 f.

<sup>30</sup> Europol, Internet Organised Crime Threat Assessment, 2017, 60 f.

<sup>31</sup> So auch BOEHM/PESCH (FN 23), 77.

<sup>32</sup> Vgl. HELGO EBERWEIN/ARTHUR STADLER/ANNA-ZOE STEINER, Bitcoins – Rechtliche Aspekte einer virtuellen Währung, *Jusletter IT* vom 20.2.2014, N 17.

<sup>33</sup> Anstatt vieler z.B. CHRISTIAN RÜCKERT, Virtual Currencies and Fundamental Rights, August 2016, 8, SSRN: <https://dx.doi.org/10.2139/ssrn.2820634> (Abruf 9.7.2018).

org/10.2139/ssrn.2820634 (Abruf 9.7.2018).

<sup>34</sup> Vgl. SABINE GLESS/PETER KUGLER/DARIO STAGNO, Was ist Geld? Und warum schützt man es?, *recht* 2015, 82 ff., 87.

<sup>35</sup> Bericht des Bundesrates (FN 27), 19.

<sup>36</sup> GRZYWOTZ/KÖHLER/RÜCKERT (FN 26), 755.

<sup>37</sup> EXTANCE (FN 11), 22 f.; SAFFERLING/RÜCKERT (FN 5), 291; EBERWEIN/STADLER/STEINER (FN 32), N 16; BOEHM/PESCH (FN 23), 75; BROWN (FN 3), 327; zu den Herausforderungen im Bereich der Ermittlungstätigkeit siehe auch JASON LUU/EDWARD J. IMWINKELRIED, The Challenge of Bitcoin Pseudo-Anonymity To Computer Forensic, Oktober 2015, SSRN: <https://ssrn.com/abstract=2671921> (Abruf 9.7.2018).

<sup>38</sup> So GRZYWOTZ/KÖHLER/RÜCKERT (FN 26), 754 f.

<sup>39</sup> GRZYWOTZ/KÖHLER/RÜCKERT (FN 26), 758.

<sup>40</sup> Vgl. RÜCKERT (FN 33), 14.

ler Währungen ist es zentral, auch Kenntnisse darüber zu erlangen, wie diese Währungen aufbewahrt, gespeichert und weitertransferiert werden. Um virtuelle Währungen aufzubewahren und zu verwalten, müssen Nutzer im Regelfall über eine sog. *Wallet* verfügen, wobei diese eine oder mehrere Adressen beinhaltet, d.h. *Keys*, auf welche ein Guthaben transferiert werden kann.<sup>41</sup> Dabei ist zwischen *Paper*-, *Web*- und *Hardware-Wallets* zu unterscheiden. Bei den sog. *Paper-Wallets* werden Ausdrücke des privaten Schlüssels an einem sicheren Ort aufbewahrt. An die virtuelle Währung gelangt man, wenn man den ausgedruckten Code in eine *Wallet*-Software einliest, indem man den QR-Code<sup>42</sup> einscannt oder den Schlüssel manuell eingibt. Es ist auch möglich, anstelle des gesamten hochsensiblen privaten Schlüssels einen sog. *Seed-Key* auszudrucken, der die Berechnung des privaten Schlüssels ermöglicht.<sup>43</sup> Solche analogen Speicherungsverfahren haben den Vorteil, dass sie gegen Cyberattacken resistent sind. Falls der private Schlüssel aber nur in einer *Paper-Wallet* gespeichert ist und er verloren geht, ist eine Authentifizierung nicht mehr möglich und der Zugriff auf die Kryptowährungen wird verunmöglicht. Auch wenn es somit also denkbar ist, die Codes auch «analog» auf Papier aufzubewahren, werden die privaten Schlüssel i.d.R. von Nutzern mittels spezieller Software in digitalen *Wallets* aufbewahrt.<sup>44</sup> Die Aufbewahrung und Verwaltung des privaten Schlüssels sowie die Anzeige der Währungseinheiten auf dem Computer oder dem Smartphone ist mit einer derartigen Software möglich.<sup>45</sup> Man unterscheidet dabei zwischen sog. *Cold Storages* (*Hardware-Wallets*) und *Hot Storages* (*Web-Wallets*), wobei bei beiden Varianten wiederum verschiedene Verschlüsselungstechnologien zum Einsatz kommen können, welche das Hacken oder Entwenden der *Keys* erschweren.<sup>46</sup> Die Möglichkeiten, Kryptowährungen aufzubewahren, sind entsprechend vielseitig, wobei auch Kombinationen von verschiedenen Speicherarten denkbar sind. Bei der Speicherung des Schlüsselmaterials im Rahmen von *Cold Storages* wird

der private Schlüssel auf einem Gerät aufbewahrt, das keine Verbindung zum Internet hat. Mithilfe dieses Geräts, z.B. eines speziellen USB-Sticks, können Transaktionen erst durch Anschluss des Datenträgers am Computer und unter Verwendung von der spezifischen Software durchgeführt werden. *Hot Storages* hingegen erlauben dem Benutzer, von überall her auf sein Vermögen zuzugreifen.<sup>47</sup> So befinden sich die Schlüssel z.B. auf Computern, Mobiltelefonen (*Mobile-Wallets*) oder in online-basierten Clouddiensten (z.B. *Web-Wallets* auf Trading-Plattformen, *Hybrid-Wallets* oder *In-Browser-Wallets*).<sup>48</sup> Bei den *Web-Wallets* wird sowohl der öffentliche als auch der private Schlüssel auf dem Server des Anbieters gespeichert. Über eine Applikation auf dem Smartphone oder dem Computer erlangt man mit der Eingabe des Benutzernamens und des Passworts Zugriff und kann Transaktionen tätigen.

Aufgrund der Abwesenheit einer zentralen Instanz ist der Besitzer dafür verantwortlich, seine Schlüssel sicher aufzubewahren, was indessen einen Zugriff von Behörden und eine erfolgreiche Sicherstellung – gerade im Falle nicht vorhandener Kooperation – bei technisch versierten Besitzern deutlich verkompliziert. Für Ermittlungsbehörden ist das Verständnis der «*Wallet*-Vielfalt» und damit der «Kryptolandschaft» deshalb von grosser Bedeutung. Einerseits wird nur so klar, was überhaupt für eine Beschlagnahme infrage kommt und auf was sich eine allfällige Herausgabepflicht bezieht. Andererseits kann nur auf diese Weise adäquat beurteilt werden, wie eine Beschlagnahme praktisch vonstattengehen muss, ob sie überhaupt ausreicht oder ob nicht vielmehr noch andere Massnahmen zu ergreifen sind. Diese könnten z.B. in der Ergreifung eines Rechtshilfeersuchens für die umgehende Sicherung von bzw. den Zugriff auf Computerdaten nach Art. 29 ff. des Übereinkommens über die Cyberkriminalität<sup>49</sup> bestehen. Aber auch eine allfällige Übertragung von entdeckten Guthaben auf staatliche *Wallets* bedarf, neben der noch zu diskutierenden Frage nach der gesetzlichen Grundlage, eines Verständnisses für die Aufbewahrungs- und Sicherstellungsfunktionalismen.

## B. Ausgangslage: Rechtsnatur von Kryptowährungen

### 1. Allgemeine rechtliche Einordnung

<sup>41</sup> Bericht des Bundesrates (FN 27), 8.

<sup>42</sup> Der QR-Code ist eine computerlesbare visuelle Darstellung z.B. einer Bitcoin-Adresse (vgl. AARON KOENIG, Bitcoin, Geld ohne Staat, Die digitale Währung aus Sicht der Wiener Schule der Volkswirtschaft, München 2018, 125).

<sup>43</sup> KOENIG (FN 42), 95.

<sup>44</sup> RÜCKERT (FN 14), 24.

<sup>45</sup> BENEDIKT SEILER/DANIEL SEILER, Sind Kryptowährungen wie Bitcoin (BTC), Ethereum (ETH), Ripple (XRP) und Co. als Sachen im Sinne des ZGB zu behandeln?, *sui-generis* 2018, 149 ff., 153; JACQUEMART/MEYER (FN 4), 469.

<sup>46</sup> MARIA LETIZIA PERUGINI/CESARE MAIOLI, Bitcoin: between digital currency and financial commodity, *Mai* 2015, 5, SSRN: <https://dx.doi.org/10.2139/ssrn.2526472> (Abruf 9.7.2018).

<sup>47</sup> EUGSTER (FN 5), 42.

<sup>48</sup> ECB, Analysis (FN 10), 8; siehe die Übersicht bei EUGSTER (FN 5), 43.

<sup>49</sup> Übereinkommen vom 23. November 2001 über die Cyberkriminalität (SR 0.311.43).

In vielen Rechtsordnungen gestaltet es sich als schwer, die Natur der Kryptowährungen zu definieren.<sup>50</sup> Bis heute haben Kryptowährungen im Schweizer Recht noch keine explizite Reglementierung erfahren.<sup>51</sup> Kryptowährungen wird die Geldeigenschaft abgesprochen,<sup>52</sup> da diese gemäss h.L. nur den von anerkannten Staaten herausgegebenen Zahlungsmitteln zukommt.<sup>53</sup> Auch wenn virtuelle Währungen als Tauschmittel fungieren, haben sie bis anhin in keiner Rechtsordnung den Status als offizielles, staatliches Zahlungsmittel.<sup>54</sup> Dennoch bewegen sich Kryptowährungen nicht im rechtsfreien Raum.<sup>55</sup>

Für die Anwendbarkeit strafprozessrechtlicher Normen ist es essentiell, die Rechtsnatur von Kryptowährungen einzugrenzen und zu klären, ob Kryptowährungen mit den bestehenden Rechtsbegriffen erfasst werden können. Nur so kann ausgemacht werden, welche Bestimmungen Anwendung finden und unter welche Begrifflichkeiten Kryptowährungen subsumiert werden können. So ist aufgrund der Ausgestaltung dieser virtuellen Währungen auf Anhieb keineswegs eindeutig, ob es sich bei ihnen um «Sachen», «Gegenstände», «Vermögenswerte» oder «Daten» handelt und ob diese folglich ohne Weiteres den entsprechenden Bestimmungen unterliegen. Diese Frage der rechtlichen Klassifikation von Kryptowährungen ist für die gesamte Rechtsordnung relevant,<sup>56</sup> z.B. auch für das Vermögens- und Finanzmarktstrafrecht. Für die vorliegende Forschungsfrage erhält sie besondere Bedeutung, da die Bestimmungen von Art. 263 ff. StPO und Art. 69 ff. StGB sich auf eine derartige Eignung stützen. Die Frage, ob Kryptowährungen als Gegenstände, Vermögenswerte oder Daten (und ggf. was für Daten) zu begreifen sind, kann als straf- und strafprozessrechtlich ungeklärtes Terrain bezeichnet werden, was in Anbetracht der zunehmen-

den Relevanz dieses Phänomens in Bezug auf kriminelle Verhaltensweisen unbefriedigend ist. Entsprechend soll in der Folge an einer Klärung gearbeitet werden.

## 2. Qualifikation als Sache, Daten oder Vermögenswert?

Gemäss Bundesrat handelt es sich bei einer «virtuellen Währung» um die «digitale Darstellung eines Wertes, welche im Internet handelbar» ist und die «Funktionen von Geld übernimmt».<sup>57</sup> Auch die *Europäische Zentralbank* definiert Kryptowährungen als «digitale Repräsentation eines Wertes».<sup>58</sup> Kryptowährungen stellen damit ein immaterielles, d.h. virtuelles Gut dar.<sup>59</sup> Sie existieren folglich zunächst einmal nur als digitaler Code, der auf die eine oder andere Weise in einer *Wallet* gespeichert ist. Es handelt sich also nicht um einen körperlichen Gegenstand, sondern um «verschlüsselte, maschinenlesbare Informationen», d.h. um Daten.<sup>60</sup> Als Daten gelten «sämtliche Informationen, das heisst Buchstaben, Wörter, Zahlen, Abbildungen, die irgendeinen Sinn ergeben und aus diesem Grund weitergegeben oder aufbewahrt werden».<sup>61</sup> Kryptowährungen können unter diesen Datenbegriff subsumiert werden. Ein Spezialfall stellt allenfalls die «analoge» Speicherung des Schlüssels und damit der Daten in einem *Paper* oder einer *Cold Wallet* dar. Hierbei ist der Datenträger zumindest verkörpert. Dennoch lassen sich Kryptowährungen eigens nicht unter den Sachbegriff subsumieren.<sup>62</sup>

Aufgrund ihrer Handelbarkeit wird Kryptowährungen, d.h. den spezifischen digitalen Codes, ein Vermögenswert

<sup>50</sup> Vgl. auch LITWACK (FN 29).

<sup>51</sup> SÉBASTIEN GOBAT, Les monnaies virtuelles à l'épreuve de la LP, AJP 2016, 1095 ff., 1097.

<sup>52</sup> Vgl. für das deutsche Recht z.B. MORITZ SCHROEDER, Bitcoin: Virtuelle Währung – reelle Problemstellungen, JurPC Web-Dok. 2014, Abs. 1 ff., Abs. 117.

<sup>53</sup> GLESS/KUGLER/STAGNO (FN 34), 82 mit den entsprechenden Nachweisen.

<sup>54</sup> BROWN (FN 3), 330 mit Verweis auf einen Bericht der amerikanischen Financial Actions Taskforce (FATF) von 2015; für die Schweiz LUKAS MÜLLER/MILENA REUTLINGER/PHILIPPE J.A. KAISER, Entwicklungen in der Regulierung von virtuellen Währungen in der Schweiz und der Europäischen Union, EuZ 2018, 80 ff., 86 mit Verweis auf Art. 2 des Bundesgesetzes vom 22. Dezember 1999 über die Währung und die Zahlungsmittel (WZG; SR 941.10).

<sup>55</sup> Bericht des Bundesrates (FN 27), 3.

<sup>56</sup> Zur Frage der Rechtsnatur virtueller Währungen im Zivil-, Steuer- und Finanzmarktrecht siehe z.B. MÜLLER/REUTLINGER/KAISER (FN 54), 86 ff.

<sup>57</sup> Bericht des Bundesrates (FN 27), 7 f.

<sup>58</sup> ECB, Analysis (FN 10), 4.

<sup>59</sup> BOEHM/PESCH (FN 23), 77.

<sup>60</sup> So GLESS/KUGLER/STAGNO (FN 34), 89 mit Verweis auf GÜNTER STRATENWERTH/GUIDO JENNY/FELIX BOMMER, Schweizerisches Strafrecht, BT I, 7. A., Bern 2010, § 14 N 24 f.

<sup>61</sup> STEFAN HEIMGARTNER, Strafprozessuale Beschlagnahme – Wesen, Arten und Wirkungen, Zürich 2011, 87 in Anschluss an NIKLAUS SCHMID, Zu den Begriffen der Daten, Datenverarbeitung und Datenverarbeitungsanlage im neuen Vermögens- und Urkundenstrafrecht, Aktuelle Probleme der Kriminalitätsbekämpfung, ZStrR 1992, 315 ff., 317.

<sup>62</sup> So für das deutsche Recht z.B. SCHROEDER (FN 52), Abs. 118; GRZYWOTZ/KÖHLER/RÜCKERT (FN 26), 757; MERIH ERDEM KÜTÜK/CHRISTOPH SORGE, Bitcoin im deutschen Vollstreckungsrecht, MMR 2014, 643 ff., 644; RÜCKERT (FN 6), 296; für das österreichische Recht SEVERIN GLASER, Bitcoins aus strafrechtlicher Sicht, in: Helgo Eberwein/Anna-Zoe Steiner (Hrsg.), Bitcoins, Wien 2014, 127 ff., 128; a.M. für das schweizerische Recht aus zivilrechtlicher Sicht SEILER/SEILER (FN 45), 160; MÜLLER/REUTLINGER/KAISER (FN 54), 87.

zugemessen.<sup>63</sup> Der Wert der virtuellen Währungen liegt im Allgemeinen im Netzwerk begründet, d.h. darin, dass andere Marktteilnehmer auf die Akzeptanz als Zahlungsmittel vertrauen.<sup>64</sup> Da virtuelle Währungen keinen realen Gegenwert i.S. einer Münze oder dergleichen aufweisen, bestimmt sich ihr Vermögenswert ausschliesslich in Form dieses Marktwertes.<sup>65</sup> Da es zudem im dezentralen Netzwerk keinen Schuldner und keinen Emittenten gibt, entsteht kein Zahlungsverprechen im herkömmlichen Sinne – weder gegen die *Blockchain* als «Kontrollprotokoll» noch gegen das Netzwerk selbst.<sup>66</sup> Kryptowährungen enthalten folglich «weder einen Fundamentalwert noch ein Zahlungsverprechen».<sup>67</sup> Es handelt sich also um einen Vermögenswert *sui generis*, der aufgrund der Abwesenheit einer derartigen schuldrechtlichen Beziehung im dezentralen Netzwerk nicht ohne Weiteres mit herkömmlichen Forderungen gleichgesetzt werden kann.<sup>68</sup>

### 3. Kryptowährungen als Daten mit Vermögenswert *sui generis*

Kryptowährungen lassen sich dem Vorgegangenen folgend als *Daten mit Vermögenswert* eigener Art definieren. Es handelt sich dabei nicht um herkömmliche elektronische Daten, die bereits in sich selbst ihren Charakter bzw. unter Umständen ihren Wert erhalten, sondern um Daten, welchen als Schlüssel erst in Kombination mit der zugehörigen *Blockchain* ein Vermögenswert zukommt. Im Vergleich zu herkömmlichen Daten handelt es sich bei virtuellen Währungen also um solche, die nur innerhalb der zugrundeliegenden Infrastruktur des Netzwerkes Anwendung finden können.<sup>69</sup> Diese Art von Vermögenswert existiert demzufolge allein als Eintrag in der gemeinsamen Datenbank. Die Daten erhalten ihren Wert nicht durch ihre Speicherung auf der Festplatte, sondern dadurch, dass durch die *Blockchain* belegt werden kann, dass ein Inhaber einer Adresse berechtigt ist, einen Wert

zu transferieren.<sup>70</sup> Folglich basiert der Vermögenswert auf dem Netzwerk und hängt von der tatsächlichen Verfügungsgewalt über die Daten ab.<sup>71</sup> Der Besitz des *Private Keys* wiederum entscheidet über diese relevante Verfügungsgewalt hinsichtlich des Vermögenswerts, da dieser direkt von der Verfügbarkeit und der Nutzbarkeit des Codes abhängt.<sup>72</sup>

Aufgrund dieser spezifischen Natur ergibt sich – in Abgrenzung zu anderweitigen Vermögenswerten – die Problemlage, dass nur der private Schlüssel konfisziert werden kann. Damit ist der Vermögenswert aufgrund der Funktionsweise der *Blockchain* und der Reproduzierbarkeit des Schlüssels allerdings noch nicht ausreichend sichergestellt. Dezentralität und Pseudoanonymität erlauben es dabei, weder eine Beschränkung auf einen Inhaber der Verfügungsgewalt sicherzustellen noch den Vermögenswert eindeutig zuzuordnen. Deshalb können die Zugangsdaten zwar auf einem Datenträger gespeichert und damit fassbar sein, die Erlangung der Verfügungsgewalt ist mit dem Zugang zum privaten Schlüssel und der Sicherstellung des Datenträgers jedoch nicht vollendet. Erschwerend tritt hinzu, dass *Blockchain*-Transaktionen unwiderruflich bzw. unumkehrbar sind.<sup>73</sup> In diesem Sinne kann in der Folge von einer Qualifikation der Kryptowährungen als einer spezifischen Kombination aus Daten und Vermögenswerten gesprochen werden, die auf einem Gegenstand gespeichert oder notiert sein können, dies jedoch nicht sein müssen. Aufgrund der Abwesenheit eines klar definierten Schuldners, der allgemeinen Reproduzierbarkeit des Schlüssels und der beschränkten Wirkung einer einfachen Konfiskation in Bezug auf die Verfügungsgewalt ergeben sich relevante Differenzen zu herkömmlichen Kategorien, welche eine einfache Klassifikation nicht erlauben bzw. als wenig zielführend erscheinen lassen. Es verbleibt also die Frage, ob diese Charakteristiken für eine strafprozessrechtliche Subsumtion unter die relevanten Bestimmungen, die den Anforderungen des Bestimmtheitsgebots zu genügen hat, ausreicht oder ob sich – neben allfälligen praktischen Umsetzungsproblemen – auch Rechtslücken offenbaren.

<sup>63</sup> Bericht des Bundesrates (FN 27), 8; für das deutsche Recht z.B. BOEHM/PESCH (FN 23), 77. Deshalb wird z.B. auch nach herrschender Praxis der Handelsregisterämter den meisten Kryptowährungen Sacheinlagefähigkeit zugesprochen, da sie nach Art. 959 Abs. 2 OR als Vermögenswerte i.S.d. Rechnungslegungsrechts aktivierungspflichtig sind; dazu MÜLLER/STOLTZ/KALLENBACH (FN 4), AJP 2017, 1323 f.

<sup>64</sup> HELGO EBERWEIN, Bitcoins in der Gesellschaft, in: Helgo Eberwein/Anna-Zoe Steiner (Hrsg.), Bitcoins, Wien 2014, 13 ff., 14.

<sup>65</sup> RÜCKERT (FN 6), 296.

<sup>66</sup> So GLESS/KUGLER/STAGNO (FN 34), 87 mit Verweis auf KÜTÜK/SORGE (FN 62), 644.

<sup>67</sup> So EUGSTER (FN 5), 41.

<sup>68</sup> Vgl. RÜCKERT (FN 6), 296.

<sup>69</sup> JÖRG PLATZER, Bitcoin, Köln 2014, 17.

<sup>70</sup> PLATZER (FN 69), 23.

<sup>71</sup> RÜCKERT (FN 6), 296.

<sup>72</sup> Vgl. RÜCKERT (FN 6), 296.

<sup>73</sup> LITWACK (FN 29), 318.

### III. Beschlagnahme von Kryptowährungen nach Art. 263 ff. StPO

#### A. Grundlagen der Beschlagnahme

##### 1. Zweck und Wesen

Die Beschlagnahme als Zwangsmassnahme bezweckt, der betroffenen Person die Verfügungsmacht über ein «deliktsverstricktes Objekt» zu entziehen und es bis zum endgültigen Entscheid über sein Schicksal staatlich sicherzustellen.<sup>74</sup> Rechtsstaatlichen Prinzipien folgend können Zwangsmassnahmen durch die Strafbehörden nur dann ergriffen werden, wenn sie auf einer gesetzlichen Grundlage basieren, ein hinreichender Tatverdacht vorliegt, die damit angestrebten Ziele nicht durch mildere Massnahmen erreicht werden können und die Bedeutung der Straftat die Zwangsmassnahme rechtfertigt.<sup>75</sup> Diese Voraussetzungen und insbesondere die Verhältnismässigkeit muss jeweils im Einzelfall geprüft werden.<sup>76</sup> Es steht einer Beschlagnahme von Kryptowährungen diesbezüglich grundsätzlich nichts im Weg, da der Zweck dieser Bestimmung im Allgemeinen auch im Falle von virtuellen Währungen sachgemäss erscheinen kann.

##### 2. Beschlagnahmearten

Gemäss Art. 263 Abs. 1 StPO können Gegenstände und Vermögenswerte einer beschuldigten Person oder einer Drittperson beschlagnahmt werden, wenn die Gegenstände und Vermögenswerte voraussichtlich als Beweismittel gebraucht werden, zur Sicherstellung von Verfahrenskosten, Geldstrafen, Bussen oder Entschädigungen

dienen können, den Geschädigten zurückzugeben sind oder einzuziehen sind. Somit sieht Art. 263 Abs. 1 StPO folgende vier Arten der Beschlagnahme vor: Beweismittelbeschlagnahme (lit. a), Kostendeckungsbeschlagnahme (lit. b), Restitutionsbeschlagnahme (lit. c) und Einziehungsbeschlagnahme (lit. d). Systematisch lässt sich die Beschlagnahme in zwei Grundmuster einteilen: Die Beschlagnahme zu Beweis Zwecken und die Beschlagnahme zu Einziehungszwecken.<sup>77</sup>

Die Beschlagnahme zu Beweis Zwecken erfolgt, falls das Objekt geeignet erscheint, als Beweis für eine entscheidungswesentliche Tatsache zu dienen.<sup>78</sup> Vorausgesetzt für eine Beweismittelbeschlagnahme ist ein laufendes Strafverfahren, die Beweisbedeutung des zu beschlagnahmenden Gegenstandes sowie kein Vorliegen eines Beschlagnahmeverbotes. In Hinblick auf eine Anwendbarkeit auf Kryptowährungen wird noch zu klären sein, inwiefern diese ein taugliches Beweisobjekt darstellen können, da sich die Beweismittelbeschlagnahme nur auf Gegenstände bezieht. Es ist im Allgemeinen unwahrscheinlich, wenn auch nicht ausgeschlossen, dass Kryptowährungen für diese Beschlagnahmeart von grosser Bedeutung sein werden. Deshalb erlaubte eine allfällige Subsumtion unter den Begriff des Vermögenswerts und damit eine Eignung für die anderen Beschlagnahmearten zumindest eine weitgehende Abdeckung der relevanten Fälle. Es ist dennoch nicht ausgeschlossen, dass auch virtuelle Währungen bzw. gerade auch Einträge in der *Blockchain* oder Ausdrücke von *Private Keys* Beweismittelrelevanz erlangen können, sofern mit ihrer Existenz nachgewiesen werden soll, dass diese aus illegalen Aktivitäten herrühren. Folglich bliebe die Nichtanwendbarkeit der Beweismittelbeschlagnahme problematisch.

Die Beschlagnahme zu Einziehungszwecken richtet sich nach Art. 69 und 70 ff. StGB. Die Sicherungseinziehung zielt auf Gegenstände i.S.v. Art. 263 Abs. 1 StPO, «die zur Begehung einer Straftat gedient haben oder bestimmt waren oder die durch eine Straftat hervorgebracht worden sind, wenn diese Gegenstände die Sicherheit von Menschen, die Sittlichkeit oder die öffentliche Ordnung gefährden».<sup>79</sup> Es sind demnach einerseits ein Deliktikonnex und andererseits eine potentielle Bedrohlichkeit des Gegenstands gefragt.<sup>80</sup> Bezüglich Kryptowährungen ist –

<sup>74</sup> BSK StPO II-BOMMER/GOLDSCHMID, Vor Art. 263–268 N 1, in: Marcel Alexander Niggli/Marianne Heer/Hans Wiprächtiger (Hrsg.), Schweizerische Strafprozessordnung und Jugendstrafprozessordnung, Basler Kommentar, 2. A., Basel 2014 (zit. BSK StPO II-Verfasser); PC CPP-MOREILLON/PAREIN-REYMOND, Vor Art. 263–268 N 3, Code de procédure pénale, Petit Commentaire, 2. A., Basel 2016 (zit. PC CPP-Verfasser); CR CPP-LEMBO/JULEN BERTHOD, Art. 263 N 3, in: André Kuhn/Yvan Jeanneret (Hrsg.), Code de procédure pénale suisse, Commentaire Romand, Basel 2011 (zit. CR CPP-Verfasser).

<sup>75</sup> Art. 197 StPO i.V.m. Art. 36 BV; StPO Komm.-HUG/SCHIEDERGER, Art. 197 N 2 ff., in: Andreas Donatsch/Thomas Hansjakob/Viktor Lieber (Hrsg.), Kommentar zur Schweizerischen Strafprozessordnung (StPO), 2. A., Bern 2014 (zit. StPO Komm.-Verfasser); CR CPP-LEMBO/JULEN BERTHOD (FN 74), Art. 263 N 17.

<sup>76</sup> NIKLAUS SCHMID/DANIEL JOSITSCH, Handbuch des Schweizerischen Strafrechts, 3. A., Zürich/St. Gallen 2017, 485; PC CPP-MOREILLON/PAREIN-REYMOND (FN 74), Vor Art. 263–268 N 7; CR CPP-LEMBO/JULEN BERTHOD (FN 74), Art. 263 N 17; StPO Komm.-HEIMGARTNER (FN 75), Art. 263 N 4; BSK StPO II-BOMMER/GOLDSCHMID (FN 74), Vor Art. 263–268 N 15.

<sup>77</sup> SCHMID/JOSITSCH (FN 76), 485; StPO Komm.-HEIMGARTNER (FN 75), Art. 263 N 2; BSK StPO II-BOMMER/GOLDSCHMID (FN 74), Vor Art. 263 N 7; CR CPP-LEMBO/JULEN BERTHOD (FN 74), Art. 263 N 4 ff.

<sup>78</sup> BSK StPO II-BOMMER/GOLDSCHMID (FN 74), Vor Art. 263–268 N 5.

<sup>79</sup> Art. 69 Abs. 1 StGB.

<sup>80</sup> CR CPP-LEMBO/JULEN BERTHOD (FN 74), Art. 263 N 24; PC CPP-MOREILLON/PAREIN-REYMOND (FN 74), Vor Art. 263–268 N 8;

einmal abgesehen von der infrage stehenden Qualifikation als «Gegenstand» – zweifelhaft, ob von ihnen eine derartige Gefährdung ausgehen kann. Plausibler ist eine Beschlagnahme zur späteren Einziehung von Vermögenswerten. Diese unterliegen der Einziehungsbeschlagnahme, wenn sie durch eine Straftat erlangt worden sind oder dazu bestimmt waren, eine Straftat zu veranlassen oder zu belohnen.<sup>81</sup> Sinn und Zweck dieser Norm ist, dass der Täter nicht im Genuss eines durch eine strafbare Handlung erlangten Vermögensvorteils bleibt; strafbares Verhalten soll sich nicht lohnen.<sup>82</sup> Entsprechend wäre eine Anwendung auf Kryptowährungen, die aus kriminellen Aktivitäten herrühren, grundsätzlich mit dem Zweck dieser Bestimmung vereinbar. Auch wenn es unter Umständen schwierig ist, dem Beschuldigten eine *Wallet* zweifelsfrei zuzuordnen,<sup>83</sup> erlaubt die Öffentlichkeit der *Blockchain* und die Rückverfolgbarkeit von Transaktionen mittels deren Einträge, Geldflüsse und damit einen allfälligen Deliktsskonnex aufzudecken.

Deliktische Vermögenswerte werden nicht eingezogen, wenn sie zur Wiederherstellung des rechtmässigen Zustands dem Berechtigten auszuhändigen sind. Die Rückgabe an den Geschädigten ist nur möglich, wenn ihm der betreffende Vermögenswert durch die Straftat direkt entzogen wurde,<sup>84</sup> was bei virtuellen Währungen z.B. im Falle einer unrechtmässigen oder betrügerischen Entwendung denkbar ist. Die Kostendeckungsbeschlagnahme soll die Verfügbarkeit von Mitteln garantieren und zielt auf wertvolle Güter. Im Unterschied zu den anderen zwei Hauptarten der Beschlagnahme ist ein innerer Zusammenhang zwischen der Tat und den beschlagnahmten Vermögenswerten nicht notwendig.<sup>85</sup> Auch für diese Beschlagnahmeart ist eine Praxisrelevanz von Kryptowährungen nicht ausgeschlossen.

BSK StPO II-BOMMER/GOLDSCHMID (FN 74), Art. 263 N 36; StPO Komm.-HEIMGARTNER (FN 75), Art. 263 N 16.

<sup>81</sup> Art. 70 Abs. 1 StGB.

<sup>82</sup> BGE 129 IV 322 E. 2.4.4; GÜNTER STRATENWERTH/WOLFGANG WOHLERS, Schweizerisches Strafgesetzbuch, Handkommentar, 3. A., Bern 2013, Art. 70 StGB N 2 ff.

<sup>83</sup> GÖGER (FN 8), 434.

<sup>84</sup> Art. 70 Abs. 1 StGB i.V.m. Art. 267 Abs. 2 StPO und Art. 263 Abs. 1 lit. c StPO; SCHMID/JOSITSCH (FN 76), 483.

<sup>85</sup> Siehe Art. 268 StPO; BSK StPO II-BOMMER/GOLDSCHMID (FN 74), Art. 268 N 1; StPO Komm.-HEIMGARTNER (FN 75), Art. 268 N 6a; CR CPP-LEMBO/JULEN BERTHOD (FN 74), Art. 268 N 6.

## B. Eignung von Kryptowährungen als Beschlagnahmeobjekt

### 1. ... als «Gegenstand»?

Beschlagnahmen werden können, wie bereits summarisch ausgeführt, primär einmal «Gegenstände». Darunter fallen im Allgemeinen bewegliche körperliche Sachen.<sup>86</sup> Es ist deshalb zunächst danach zu fragen, ob es sich bei Kryptowährungen um einen «Gegenstand» im Sinne von StPO und StGB handelt.<sup>87</sup> Wie bereits eruiert, handelt es sich bei Kryptowährungen um Daten mit Vermögenswert. Daten gelten nicht als Sachen.<sup>88</sup> Während vom Sachbegriff nach h.L. und Rechtsprechung eindeutig nur körperliche Gegenstände umfasst sind, ist beim Gegenstands begriff nach Art. 263 Abs. 1 StPO allerdings umstritten, ob auch unkörperliche Objekte wie elektronische Daten unter diesen Begriff fallen können. Generell kommen als Gegenstände auch Objekte in Betracht, «die nicht aufgrund ihrer eigenen (ursprünglichen) Beschaffenheit beweistauglich sind, sondern in ihrer Funktion als Träger von Informationen».<sup>89</sup> Die h.L. ging bis anhin jedoch davon aus, dass demzufolge nur auf einem physischen Datenträger gespeicherte elektronische Daten und damit in irgendeiner Weise «fassbare Daten»<sup>90</sup> der Beschlagnahme unterliegen.<sup>91</sup> Die Beschlagnahme eines Datenträgers wie eines USB-Sticks oder einer Speicherplatte, auf dem sich Kryptowährungen befinden, fände entsprechend eine gesetzliche Grundlage. Unerheblich ist dabei, dass es den

<sup>86</sup> BSK StPO II-BOMMER/GOLDSCHMID (FN 74), Art. 263 N 26; HEIMGARTNER (FN 61), 13 f.

<sup>87</sup> Dazu für das deutsche Strafprozessrecht SCHROEDER (FN 52), Abs. 119; GÖGER (FN 8), 432 f.

<sup>88</sup> BSK StGB II-NIGGLI/RIEDO, Vor Art. 137 N 68, in: Marcel Alexander Niggli/Hans Wiprächtiger (Hrsg.), Strafrecht II, Basler Kommentar, 3. A., Basel 2013 (zit. BSK StGB II-Verfasser).

<sup>89</sup> BSK StPO II-BOMMER/GOLDSCHMID (FN 74), Art. 263 N 27.

<sup>90</sup> StPO Komm.-HEIMGARTNER (FN 75), Art. 263 N 1a; HEIMGARTNER (FN 61), 87.

<sup>91</sup> SIMON BANGERTER, Hausdurchsuchungen und Beschlagnahmen im Wettbewerbsrecht unter vergleichender Berücksichtigung der StPO, Zürich 2014, 282–285, 245 ff.; ANDREAS DONATSCH/NIKLAUS SCHMID, Der Zugriff auf E-Mails im Strafverfahren – Überwachung (BÜPF) oder Beschlagnahme?, in: Christian Schwarzenegger/Oliver Arter/Florian S. Jörg (Hrsg.), Internet-Recht und Strafrecht, 4. Tagungsband, Bern 2005, 151 ff., 162; HEIMGARTNER (FN 61), 89; NIKLAUS SCHMID, Strafprozessuale Fragen im Zusammenhang mit Computerdelikten und neuen Informationstechnologien im allgemeinen, ZStr 1993, 81 ff., 96; dazu auch ausführlich MICHAEL AEPLI, Die strafprozessuale Sicherstellung von elektronisch gespeicherten Daten, Diss. Zürich, Zürich 2004, 44 ff. m.w.N.; DOMINIC RYSER, «Computer Forensics», eine neue Herausforderung für das Strafprozessrecht, in: Christian Schwarzenegger/Oliver Arter/Florian S. Jörg (Hrsg.), Internet-Recht und Strafrecht, 4. Tagungsband, Bern 2005, 553 ff., 561 ff.

Behörden nicht auf die Gegenstände selbst ankommt, sondern auf die auf ihnen gespeicherten Daten.<sup>92</sup>

Da jedoch die alleinige Beschlagnahme eines solchen Speichermediums in vorliegendem Zusammenhang noch keineswegs als tatsächliche Sicherstellung gelten kann, sondern erst die Übertragung des virtuellen Geldes die Verfügungsgewalt des Beschuldigten endgültig aufhebt, reicht der Zugriff auf den Datenträger nicht aus, damit diese Zwangsmassnahme ihren Zweck erfüllt. Des Weiteren können Kryptowährungen, bei welchen *Cloud Computing* Anwendung findet und welche sich deshalb keiner *Hardware* oder IT-Infrastruktur des Nutzers bedienen – was regelmässig der Fall sein wird –, schwerlich als körperlicher Gegenstand oder als «fassbar» i.e.S. gelten. Als Zwischenfazit lässt sich folglich festhalten, dass einer Beschlagnahme von Datenträgern, auf denen sich Kryptowährungen bzw. die relevanten Zugangscodes befinden, grundsätzlich nichts im Weg steht, dass aber damit die Grundproblematik keineswegs gelöst ist. Bei Kryptowährungen selbst handelt es sich zweifellos nicht um «körperliche Gegenstände»,<sup>93</sup> auch wenn sich der private Schlüssel auf einem solchen Gegenstand befinden kann. Es stellt sich deshalb die für den vorliegenden Untersuchungsgegenstand massgebliche Frage, ob auch «nicht-fassbare» Daten unter den Gegenstandsbegriff subsumiert werden können. Denn eine zielführende Beschlagnahme von Kryptowährungen erfordert einen Zugriff nicht nur auf einen körperlichen Gegenstand, sondern auf die immaterielle Information selbst.

## 2. ... als «Daten»?

Nach dem gesetzlichen Wortlaut unterliegen nur «Gegenstände» und «Vermögenswerte» der Beschlagnahme.<sup>94</sup> In enger Auslegung bedeutete das, wie bereits angedeutet, dass Informationen nur mit dem gegenständlichen Datenträger, auf dem sie sich befinden, beschlagnahmt werden können.<sup>95</sup> In der Botschaft der StPO zur Beschlagnahmungsbestimmung ist von Daten oder Datenträgern nicht explizit die Rede.<sup>96</sup> Ob Daten – und damit auch Kryptowährungen – in weiter Auslegung des Gegenstandsbegriffs der Beschlagnahme unterliegen, ist umstritten. Gemäss HEIMGARTNER kann der Gegenstandsbegriff in Anwendung einer grammatikalischen Auslegung weiter

gefasst werden als der Sachbegriff. So könnte ein Gegenstand i.w.S. «als Synonym für ein abgeschlossenes, reales oder ideales Objekt, das dem Betrachter gegenübersteht», aufgefasst werden, was dem Sinn und Zweck der Beschlagnahme entsprechen würde.<sup>97</sup> Ähnlich auch BANGERTER, für den sich im Ergebnis einzig aus historischer Perspektive eine Beschränkung auf körperliche Objekte ergebe, es jedoch angezeigt sei, den Begriff des Gegenstands auch auf unkörperliche Objekte auszuweiten und sie damit der Beschlagnahme zugänglich zu machen.<sup>98</sup> Eine andere Meinung vertritt AEPLI. Er kommt zum Schluss, dass Daten keine Gegenstände sind und folglich zumindest nicht Objekt der Beweismittelbeschlagnahme sein können.<sup>99</sup> Ihm folgt RYSER, der eine Ausweitung des Gegenstandsbegriffs auf unkörperliche Objekte ebenso verneint und zum Schluss kommt, dass deshalb nur verkörperte Speichermedien der Beweismittelbeschlagnahme unterliegen.<sup>100</sup> Gemäss BOMMER lassen sich Daten als unkörperliche Objekte auch hinsichtlich der Einziehung nicht bei den Gegenständen einreihen. Ein ausnahmsweises Absehen vom Erfordernis der Körperlichkeit lasse sich nicht begründen.<sup>101</sup>

Es ist in der Tat fraglich, ob die gerade hinsichtlich der Zwangsmassnahmen geltenden hohen Anforderungen an das Bestimmtheitsgebot eine derart weite Auslegung des Gegenstandsbegriffs erlauben. Auch wenn SCHMID argumentiert, dass Zwangsmassnahmen nach dem Grundsatz *a maiore ad minus* auch auf immaterielle Informationen angewendet werden könnten, weshalb eine Ausweitung auf die Einziehung von unkörperlichen Daten gerechtfertigt sei,<sup>102</sup> bleibt diese Ausweitung problematisch. Denn Daten stellen insbesondere bei Kryptowährungen nicht einfach eine Unterkategorie von Gegenständen oder materialisierten Informationen dar. Vielmehr kommen ihnen grundsätzlich wesensverschiedene Eigenschaften zu. Gemäss bundesgerichtlicher Rechtsprechung handelt es sich bei Gegenständen um Objekte, die «gewissermassen aus der Schublade herausgenommen werden könnten».<sup>103</sup> Kryptowährungen können unbestreitbar nicht einfach gegenständlich «aufbewahrt» oder «vorgelegt» werden. Auch wenn die Beschlagnahme von Datenträgern also zu-

<sup>92</sup> BSK StPO II-BOMMER/GOLDSCHMID (FN 74), Art. 263 N 27.

<sup>93</sup> Zum gleichen Schluss kommt für das deutsche Recht RÜCKERT (FN 6), 299.

<sup>94</sup> Art. 263 Abs. 1 StPO.

<sup>95</sup> Vgl. HEIMGARTNER (FN 61), 89.

<sup>96</sup> Botschaft vom 21. Dezember 2005 zur Vereinheitlichung des Strafprozessrechts, BBl 2006 1085 ff.

<sup>97</sup> HEIMGARTNER (FN 61), 89.

<sup>98</sup> BANGERTER (FN 91), 248.

<sup>99</sup> AEPLI (FN 91), 59.

<sup>100</sup> RYSER (FN 91), 561.

<sup>101</sup> FELIX BOMMER, Löschung als Einziehung von Daten, in: Christian Schwarzenegger/Oliver Arter/Florian S. Jörg (Hrsg.), Internet-Recht und Strafrecht, 4. Tagungsband, Bern 2005, 171 ff., 178.

<sup>102</sup> SCHMID (FN 91), 96 und 106.

<sup>103</sup> So das Bundesgericht zustimmend hinsichtlich des Einwandes der Beschwerdeführerin in BGE 126 I 50 E. 4c S. 58 f.

lässig bleibt, misslingt eine Subsumtion der Kryptowährungen selbst oder nicht auf Datenträgern vorhandener Zugangscodes (z.B. im Rahmen von *Web-Wallets*) unter den Gegenstandsbegriff.

### 3. ... als «Vermögenswert»?

Da es sich, wie ausführlich dargelegt, bei Kryptowährungen um Daten mit *Vermögenswert* handelt, stellt sich des Weiteren die Frage, ob eine Subsumtion unter diesen Begriff eine Anwendung der entsprechenden Bestimmungen erlaubt und deshalb die Unklarheit um die Möglichkeiten zum Zugriff auf Daten im vorliegenden Fall ohne wesentliche Konsequenzen bleibt. Wie bereits erwähnt, scheint es zunächst nicht von grosser Tragweite, dass Kryptowährungen nicht der Beweismittelbeschlagnahme unterliegen, insbesondere weil diesem Umstand immerhin damit begegnet werden kann, dass Ausdrücke oder Nachweise von Transaktionen in eine gegenständliche Form gebracht werden können.

Kryptowährungen stellen hingegen, wie einführend festgestellt, einen Vermögenswert dar. Vermögenswert i.S.d. Vermögensstrafrechts meint «jeden konkreten spezifischen Vermögensbestandteil».<sup>104</sup> Diese relative Weite des Begriffs zeigt sich auch daran, dass unter den Begriff i.S.v. Art. 70 StGB jegliche wirtschaftlichen Vorteile fallen, welche sich «rechnerisch ermitteln lassen».<sup>105</sup> Als Vermögenswerte kommen entsprechend auch unkörperliche Objekte wie Forderungen oder andere Rechte infrage, d.h. auch Daten.<sup>106</sup> Letztere stellen dann einen Vermögenswert dar, wenn sie gegen Entgelt veräussert werden können,<sup>107</sup> was bei Kryptowährungen der Fall ist. Damit werden sie grundsätzlich selbständig beschlagnahm- und einziehbar.

Aufgrund des spezifischen Charakters von virtuellen Währungen und ihres Vermögenswerts stellt sich die Frage, inwiefern Parallelen zur Beschlagnahme von Buchgeld oder von Forderungen zu ziehen sind und ob sich hier eine analoge Anwendung rechtfertigt. Buchgelder, die weder als Bargeld noch in verbriefter Form vorhanden sind, sondern sich als Vermögenswert auf einem Bankkonto befinden, gelten unbestrittenermassen zu den Vermögenswerten und können deshalb ein taugliches Beschlagnahmeobjekt bilden.<sup>108</sup> Die im Normalfall ange-

zeigte Verfügung von Kontosperrern ist jedoch aufgrund der Abwesenheit einer zentralen Instanz im Falle von Kryptowährungen eine nicht gangbare Lösung. Auch in Bezug auf Forderungen ergeben sich Analogien. Soweit diese derart verbrieft sind, dass die Übergabe des Wertpapiers kausal für die Übertragung ist, kann die Beschlagnahme mittels Sicherstellung der Urkunde erfolgen.<sup>109</sup> Bei Kryptowährungen ist allerdings die Übergabe, auch wenn der private Schlüssel auf einem physischen Dokument notiert ist, allein für eine Sicherstellung nicht ausreichend, kann doch der Code grundsätzlich vervielfältigt worden und damit eine Weiterverwendung nicht ausgeschlossen sein. Sind Forderungen nicht auf diese Weise verbrieft, können sie nicht durch physischen Zugriff sichergestellt werden.<sup>110</sup> Folglich geschieht eine Beschlagnahme durch eine Benachrichtigung des Schuldners nach Art. 266 Abs. 4 StPO. Auch dies ist jedoch bei Kryptowährungen kein taugliches Instrument, da kein Schuldner vorhanden ist. Die Übertragung von Immaterialgüterrechten kann ferner durch Verfügungsbeschränkungen gesichert werden, wobei dadurch auch hier die Übertragung solcher Rechte an Dritte nicht gänzlich verhindert werden kann, sodass gemäss HEIMGARTNER ergänzende Sicherstellungsmassnahmen in Betracht zu ziehen sind, z.B. mittels eines Registereintrags beim Institut für geistiges Eigentum.<sup>111</sup>

Es lässt sich demzufolge festhalten, dass Kryptowährungen als Vermögenswerte grundsätzlich der Vermögensbeschlagnahme gemäss Art. 263 Abs. 1 StPO unterliegen und damit zumindest hinsichtlich der Einziehungs-, Restitutions- und Kostendeckungsbeschlagnahme eine gesetzliche Grundlage besteht. Dabei ergeben sich gewisse Parallelen zu Forderungen und anderen Rechten, wobei aufgrund der erwähnten Differenzen unklar bleibt, wie eine solche Beschlagnahme zu bewerkstelligen ist. Das Gesetz *de lege lata* äussert sich nicht dazu, ob und wie Vermögenswerte, bei denen kein Schuldner vorhanden ist und die nicht verbrieft sind, beschlagnahmt werden können. Die Möglichkeit, Speichermedien oder Vermögenswerte zu beschlagnehmen, löst das Problem also nicht abschliessend. Die Frage nach dem Schicksal des Beschlagnahmenen oder Eingezogenen bleibt insofern zunächst offen.<sup>112</sup>

<sup>104</sup> BSK StGB II-NIGGLI/RIEDO (FN 88), Vor Art. 137 N 62.

<sup>105</sup> BGE 100 IV 105 f.; 104 IV 229; 120 IV 367; STRATENWERTH/WOHLERS (FN 82), Art. 70 StGB N 2.

<sup>106</sup> RYSER (FN 91), 560; AEPLI (FN 91), 46.

<sup>107</sup> BOMMER (FN 101), 174.

<sup>108</sup> So HEIMGARTNER (FN 61), 94.

<sup>109</sup> HEIMGARTNER (FN 61), 98.

<sup>110</sup> HEIMGARTNER (FN 61), 98.

<sup>111</sup> HEIMGARTNER (FN 61), 99.

<sup>112</sup> Vgl. BOMMER (FN 101), 179 f.

#### 4. Zwischenfazit

Die bisherigen Ausführungen zeigen, dass sich bei der Beschlagnahme von Kryptowährungen Eigenheiten ergeben, welche im geltenden Recht nicht spezifisch gelöst sind, und daher Unklarheiten verbleiben. Einerseits fallen webbasierte *Wallets* und deren Inhalte, welche nicht auf einem Datenträger gespeichert sind, nicht unter den Gegenstandsbegriff. Damit sind sie der Beweismittelbeschlagnahme nicht zugänglich. Andererseits verbleibt für auf Datenträgern vorhandene virtuelle Währungen das Problem, dass nicht klar ist, ob die gesetzliche Grundlage das sofortige Transferieren der auf diesem Gegenstand enthaltenen Vermögenswerte und damit eine ausreichende Sicherstellung bzw. eigentliche Löschung der Daten erlaubt. Auch wenn es als zulässig erachtet wird, von Datenbeständen auf Datenträgern Ausdrucke bzw. Kopien der elektronischen Daten zu erheben und dafür z.B. die Datenverarbeitungsanlage oder entsprechende Programme zu verwenden,<sup>113</sup> ist es doch fraglich, inwiefern – und das wäre bei Kryptowährungen nötig – daraus auch ein Recht abgeleitet werden kann, Daten zu übertragen und damit das «Zurückbleibende» auf dem Datenträger zu löschen bzw. zu «entwerten». Diese Frage gilt es, im Folgenden weiter zu klären. Dennoch kann als Zwischenfazit festgehalten werden, dass Kryptowährungen als Daten mit Vermögenswert im Allgemeinen ein taugliches Beschlagnahmeobjekt darstellen.

### C. Beschlagnahme durch Übertragung auf staatliche Wallets

#### 1. Rechtliche Grundlage

Mit der Beschlagnahme sollen Gegenstände oder Vermögenswerte der Verfügungsgewalt einer Person entzogen und der Verfügungsgewalt der Behörden unterstellt werden.<sup>114</sup> Die Art und Weise, wie eine Beschlagnahme durchgeführt wird, ist von ihrem Gegenstand abhängig. Handelt es sich um bewegliche Sachen, so wird die Beschlagnahme durch deren physische Ergreifung vollzogen.<sup>115</sup> Bei Grundstücken erfolgt die Beschlagnahme durch Ein-

tragung einer Verfügungssperre im Grundbuch.<sup>116</sup> Forderungen werden beschlagnahmt, indem der Schuldner angewiesen wird, dass die Schuld durch Zahlung an den Gläubiger nicht getilgt wird.<sup>117</sup> Es stellt sich nun die Frage, wie Kryptowährungen als Vermögenswerte eigener Art beschlagnahmt werden können, da es an einer mit Art. 266 Abs. 3 und Abs. 4 StPO vergleichbaren expliziten Regelung mangelt.

Bei der Beschlagnahme erfahren die «vorbestehenden Eigentums- oder Inhaberverhältnisse» keine Änderung.<sup>118</sup> Gemäss neuerer Rechtsprechung des Bundesgerichts liegt keine sichernde und lediglich vorsorgliche Massnahme i.S.d. Beschlagnahme vor, wenn die Beschlagnahme aufgrund ihrer Dauer und der Art der Vornahme die Verwendung des beschlagnahmten Objekts zum vorgesehenen Zweck endgültig verunmöglicht und damit einen irreversiblen Eingriff in die Eigentums- und Vermögensrechte des Betroffenen darstellt. In einem solchen Fall müsste die Staatsanwaltschaft direkt einen Einziehungsbefehl erlassen,<sup>119</sup> der an das erstinstanzliche Gericht weitergezogen werden kann.<sup>120</sup> Da die Beschlagnahme von Kryptowährungen, wie bereits mehrfach betont, aufgrund der mühelosen Reproduzierbarkeit nicht nur eine Konfiskation des kryptographischen Schlüssels, sondern darüber hinaus auch eine Übertragung der virtuellen Vermögenswerte erfordert, stellt sich die Frage, inwiefern diesen Ansprüchen Genüge getan ist. Einerseits scheint eine Übertragung dem Zweck der Beschlagnahmebestimmung zu entsprechen, da nur so die Verfügungsmacht des Beschuldigten über das Objekt gebrochen und dieses tatsächlich in die Verfügungsgewalt des Staates überführt werden kann. Andererseits lässt sich nicht leugnen, dass mit einer Übertragung zum Staat die Eigentumsverhältnisse eine Änderung erfahren.

Dennoch legt eine teleologische Auslegung die Zulässigkeit einer solchen Übertragung von Kryptowährungen zum Staat nahe. Einerseits ist nur so dem Zwecke der Beschlagnahme, also dem tatsächlichen Gewahrsams- und Verfügungsbruch, zu genügen. Der Akt der Beschlagnahme soll insbesondere gegen aussen deutlich machen, dass eine Veräusserung bösgläubig wäre. Dies kann allerdings durch eine Konfiskation des *Private Keys* bzw. eines Speichermediums nicht zielführend erreicht werden, da es

<sup>113</sup> Dazu DONATSCH/SCHMID (FN 91), 164 mit Verweis auf AEPLI (FN 91), 74 ff.; SCHMID (FN 91), 96.

<sup>114</sup> CHRISTOPH RIEDO/GERHARD FIOKA/MARCEL ALEXANDER NIGGLI, Schweizerisches Strafprozessrecht sowie Rechtshilfe in Strafsachen, Freiburg 2011, N 1933.

<sup>115</sup> BSK StPO II-BOMMER/GOLDSCHMID (FN 74), Vor Art. 263–268 N 8.

<sup>116</sup> Art. 266 Abs. 3 StPO i.V.m. Art. 56 lit. a der Grundbuchverordnung vom 23. September 2011 (GBV; SR 211.432.1).

<sup>117</sup> Art. 266 Abs. 4 StPO.

<sup>118</sup> BSK StPO II-BOMMER/GOLDSCHMID (FN 74), Vor Art. 263–268 N 1.

<sup>119</sup> Im Rahmen eines selbständigen Einziehungsverfahrens gemäss Art. 376 ff. StPO.

<sup>120</sup> BGE 130 I 360 E. 14.4; vgl. SCHMID/JOSITSCH (FN 76), 481.

technisch unmöglich ist, sicherzustellen, dass nebst dem Beschuldigten nicht auch noch Dritte Kenntnis des privaten Schlüssels haben, welche jederzeit über die Vermögenswerte verfügen könnten, oder dass der Beschuldigte seinen Code auf mehreren Daten- oder Schriftträgern gespeichert hat.<sup>121</sup> Andererseits ist auch mit Blick auf die in Art. 266 Abs. 2 StPO normierte Anweisung an die Behörden, die beschlagnahmten Gegenstände «sachgemäss» aufzubewahren, anzunehmen, dass die Behörden aufgefordert sind, in der Verfolgung des Sicherstellungszwecks geeignete Methoden zu eruieren. Dazu kommt, dass eine Veräusserung nach Art. 266 Abs. 2 StPO oder die bundesgesetzliche Regelung zur Anlage beschlagnahmter Vermögenswerte<sup>122</sup> eine Transaktion der Vermögenswerte erfordert. Konsequenterweise kann davon ausgegangen werden, dass auch die Übertragung von virtuellen Währungen zum Staat eine rechtliche Grundlage findet.

## 2. Durchführung der Beschlagnahme in der Praxis

Neben der Frage der rechtlichen Grundlage einer Beschlagnahme von virtuellen Währungen sind die Ermittlungsbehörden auch mit nicht zu unterschätzenden praktischen Problemen konfrontiert. Kryptowährungen können nicht einfach «in ein Couvert verpackt und in einem Tresor verstaut werden».<sup>123</sup> Für den Zugriff auf Kryptowährungen ist zunächst einmal der Zugang zum kryptographischen Schlüssel des Beschuldigten erforderlich. Während aus Benutzersicht die angemessene Aufbewahrung des *Private Keys* relevantes Sicherheitskriterium ist, ist es aus Ermittlungsperspektive also zentral, dass dieser Aufbewahrungsort bekannt ist.<sup>124</sup> Es tritt erschwerend hinzu, dass es dafür darüber hinaus nötig sein wird, sich den Zugang zur i.d.R. passwortgeschützten *Wallet* zu verschaffen, dass also der Fund einer *Wallet* allein noch keine Verfügungsgewalt garantiert. In der Praxis dürfte – im Falle mangelnder Kooperation des Beschuldigten – bereits dies die Behörden vor Schwierigkeiten stellen, gerade auch weil die meisten Nutzer von Kryptowährungen zur Verhinderung von unbefugten Zugriffen regelmässig mehrere *Hot* und *Cold Storages* benutzen, auf denen des Weiteren verschiedenste virtuelle Währungen vorhanden sind. Die Durchführung der Beschlagnahme bedingt das Auffinden dieser Zugangsdaten in schriftlicher oder elektronischer

Form bei Hausdurchsuchungen oder bei der Auswertung von Beweismaterial.<sup>125</sup> Sofern sich der private Schlüssel unverschlüsselt auf einem physischen Datenträger befindet, kann dieser durch die Behörden sichergestellt und so der Zugang zum virtuellen Wert generiert werden.<sup>126</sup>

Einen Spezialfall stellt es dar, wenn der Betroffene die Kryptowährungen nicht selbst aufbewahrt, sondern sie in einer speziellen *Web-Wallet* durch einen gewerblichen Dienstleistungsanbieter fremd verwalten lässt. Die technische Besonderheit liegt hierbei darin, dass die privaten Schlüssel, die die Verfügungsgewalt über die Vermögenswerte ermöglichen, nicht beim Beschuldigten, sondern beim Anbieter gespeichert sind. Der Beschuldigte hat in diesem Fall eine schuldrechtliche Forderung gegenüber dem Anbieter, die einen Anspruch auf Herausgabe der Werte beinhaltet.<sup>127</sup> In diesem Fall wäre in sinngemässer Anwendung von Art. 266 Abs. 4 StPO eine Benachrichtigung des Anbieters geboten. Weitergehend kann in diesem Fall auch eine, noch zu diskutierende Herausgabepflicht gemäss Art. 265 StPO bestehen.

Ist es den Behörden gelungen, Kenntnis des *Private Keys* zu erlangen, ist es in einem nächsten Schritt angezeigt, diese Daten auf dem Datenträger des Betroffenen zu löschen. Wie bereits ausgeführt, erfordert eine zielführende Sicherstellung im Falle von Kryptowährungen, dass die Möglichkeit des Beschuldigten, über das Beschlagnahmeobjekt zu verfügen, aufgehoben wird. Diese Sicherungsmassnahme erfordert in diesem Fall eine weitergehende Massnahme als die blosser Konfiskation eines Datenträgers oder der Daten selbst. Folglich ist es notwendig, möglichst unverzüglich die virtuellen Währungen auf eine staatliche *Wallet* zu transferieren. Damit wird sichergestellt, dass der Beschuldigte die Werte nicht unwiderruflich weitertransferieren kann, falls er noch über weitere Kopien der privaten Schlüssel verfügt, was i.d.R. der Fall sein wird.<sup>128</sup>

## 3. Herausgabepflicht

Die Durchsuchung von Schrift- und Datenträgern nach Zugangsdaten zu *Wallets* ist in der Praxis sicherlich keine leichte Aufgabe. Umso grösser wird das Interesse an einer Mitwirkung des Beschuldigten oder anderer Akteure bei der Sicherstellung von virtuellen Währungen.

<sup>121</sup> Vgl. GÖGER (FN 8), 433.

<sup>122</sup> Verordnung vom 3. Dezember 2010 über die Anlage beschlagnahmter Vermögenswerte (SR 312.057).

<sup>123</sup> So EUGSTER (FN 5), 44.

<sup>124</sup> Vgl. EUGSTER (FN 5), 43.

<sup>125</sup> GÖGER (FN 8), 431.

<sup>126</sup> RÜCKERT (FN 6), 298.

<sup>127</sup> RÜCKERT (FN 6), 299, der als Beispiel die Bitcoin Deutschland AG nennt und auf § 12 Nr. 5 AGB Bitcoin-Deutschland verweist.

<sup>128</sup> RÜCKERT (FN 6), 298.

Im Idealfall gibt der Beschuldigte die Vermögenswerte eigenständig heraus. Dem Verhältnismässigkeitsprinzip entsprechend erfolgt eine Beschlagnahme gegen den Willen des Betroffenen nur, falls dieser die virtuellen Währungen nicht freiwillig zur Verfügung stellt.<sup>129</sup> Gemäss Art. 265 Abs. 1 StPO besteht im Allgemeinen eine Herausgabepflicht für die Inhaber von zu beschlagnehmenden Gegenständen und Vermögenswerten. Den Beschuldigten selbst trifft jedoch gemäss Abs. 2 lit. a derselben Bestimmung keine Herausgabepflicht. Dies wiegt im Falle der Kryptowährungen besonders schwer, da bei Nichtvorhandensein von Passwörtern und privaten Schlüsseln eine Mitwirkung des Beschuldigten zwingend erforderlich ist.<sup>130</sup> Auch wenn es denkbar wäre, den Inhaber zu verpflichten, den Zugang zur Verfügung zu stellen, besteht ohne gesetzliche Grundlage keine derartige Mitwirkungspflicht des Beschuldigten.<sup>131</sup> Eine solche würde ferner grundlegenden strafprozessualen Prinzipien zuwiderlaufen. Der Beschuldigte muss Durchsuchungen und eine Beschlagnahme zwar dulden, er kann allerdings nicht zur Herausgabe von Passwörtern oder zur Mitwirkung an einer Entschlüsselung verpflichtet werden.<sup>132</sup>

Bei Dritten ist eine Beschlagnahme allerdings möglich und sie trifft – abgesehen von den in Abs. 2 lit. b und lit. c normierten Ausnahmefällen – auch eine Herausgabepflicht. So können z.B. gewerbliche *Wallet-Provider* oder Handelsplattformen verpflichtet werden, Vermögenswerte herauszugeben.<sup>133</sup> Mittels einer Editionsverfügung können diese Akteure unter Strafandrohung von Art. 292 StGB zur Herausgabe der Vermögenswerte verpflichtet werden.<sup>134</sup>

#### 4. Einrichtung einer staatlichen Wallet

Möchten Strafverfolgungsbehörden für eine sachgemässe Beschlagnahme von Kryptowährungen i.S.v. Art. 263 Abs. 1 i.V.m. Art. 266 Abs. 2 StPO gerüstet sein, muss notwendig eine eigenständige Infrastruktur zur sicheren Aufbewahrung von Kryptowährungen, d.h. eine *staat-*

*liche Wallet*, zur Verfügung stehen.<sup>135</sup> Aufgrund der zunehmenden Relevanz von virtuellen Währungen im Zusammenhang mit Straftaten obliegt den Strafverfolgungsbehörden demzufolge die Aufgabe, zeitnah um diese technische Infrastruktur bemüht zu sein. Bei der Einrichtung einer staats- bzw. polizeieigenen *Wallet* gilt es allerdings, einiges zu beachten.

Mehrere Staatsanwaltschaften und Polizeibehörden zeigen sich bereits um die Beschaffung von *Hardware-Wallets* bemüht. Um die beschlagnahmten Beträge schliesslich verwerten bzw. veräussern zu können, sei es vorzeitig oder nach rechtskräftigem Abschluss des Verfahrens, benötigt der Staat allerdings darüber hinaus Zugang zu Kryptowährungsbörsen. In diesem Zusammenhang kommen dafür bevorzugt Börsen mit Sitz in der Schweiz infrage, welche auch der schweizerischen Finanzmarktaufsicht unterstehen. Sowohl bei der Beschaffung von *Hardware-Wallets* als auch bei der Wahl geeigneter Börsen gilt es zu beachten, dass verschiedene Kryptowährungen Beschlagnahmeobjekt bilden können, also keineswegs nur *Bitcoin*. Folglich ist es wichtig, mindestens auch für die verbreitetsten *Altcoins* entsprechende Applikationen bereitzustellen und bei der Wahl der Börsen auf ein breites Angebot zu achten.

Des Weiteren stellt die sichere Aufbewahrung der virtuellen Währungen auch beim Staat eine Herausforderung dar, gerade weil die *Blockchain* es nicht erlaubt, Transaktionen rückgängig zu machen, bzw. verlorene Zugangsdaten von keiner zentralen Instanz kompensiert werden können. EUGSTER schlägt deshalb vor, dass der Zugriff auf diese Vermögenswerte nicht allein beim polizeilichen Sachbearbeiter liegt, sondern doppelt gesichert werden soll. Es könne dabei von der sog. *Pay-to-Script-Hash*-Methode Gebrauch gemacht werden, welche die Auszahlungsbedingung an verschiedenste Skripte knüpft, womit für die Auszahlung mindestens zwei Signaturen vorausgesetzt wären, z.B. eine weitere der Verfahrensleitung.<sup>136</sup>

Ein alternativer, ebenfalls in der Literatur diskutierter Ansatz zur Eindämmung der Weiterveräusserung oder des Umtauschs von illegal erworbenen Kryptowährungen wäre die Einführung sog. Transaktions-Sperrlisten.<sup>137</sup> Durch eine Straftat hervorgebrachte Einheiten könnten in eine solche *Blacklist* eingetragen werden und Dienstleistern würde es gesetzlich verboten, diese als Zahlungsmittel zu akzeptieren, womit sich der Handel mit derartigen Werten deutlich unattraktiver gestaltete. Allerdings fehlt

<sup>129</sup> SCHMID/JOSITSCH (FN 76), 489.

<sup>130</sup> SONJA HEINE, Bitcoins und Botnetze – Strafbarkeit und Vermögensabschöpfung bei illegalem Bitcoin-Mining, NStZ 2016, 441 ff., 445.

<sup>131</sup> Ähnlich für den Fall des Zugriffs auf E-Mails DONATSCH/SCHMID (FN 91), 163.

<sup>132</sup> Vgl. bereits SCHMID (FN 91), 97.

<sup>133</sup> Vgl. SABINE GLESS, Strafverfolgung im Internet, ZStrR 2012, 3 ff., 7.

<sup>134</sup> BSK StPO II-BOMMER/GOLDSCHMID (FN 74), Art. 265 N 17; SCHMID/JOSITSCH (FN 76), 491.

<sup>135</sup> So auch GÖGER (FN 8), 433; EUGSTER (FN 5), 44; JÄNKE (FN 13), 66.

<sup>136</sup> Dazu EUGSTER (FN 5), 44.

<sup>137</sup> Dazu z.B. GRZYWOTZ/KÖHLER/RÜCKERT (FN 26), 759.

es diesem Ansatz aktuell an einer gesetzlichen Grundlage und er würde eine internationale Kooperation erfordern, weshalb sich für den Moment die Einrichtung einer eigenen staatlichen *Wallet*-Infrastruktur erübrigt.

## D. Veräusserung beschlagnahmter Vermögenswerte

### 1. Volatilität und vorzeitige Verwertung von Kryptowährungen

Kryptowährungen gelten derzeit als äusserst volatil.<sup>138</sup> Betrachtet man das Beispiel *Bitcoin*, zeigt sich dies deutlich. Eine Einheit hatte am 1. Januar 2017 noch den Wert von ca. CHF 1'000, kurz vor Weihnachten 2017 stieg der Kurs auf ein Rekordhoch von knapp CHF 20'000, bevor Anfang Februar 2018 ein Einbruch auf unter CHF 6'000 zu verzeichnen war.<sup>139</sup> Diese Volatilität stellt für die Strafverfolgungsbehörden hinsichtlich der Beschlagnahme und einer allfälligen späteren Einziehung ein Risiko dar. Es stellt sich deshalb die Frage, inwiefern eine vorzeitige Veräusserung angezeigt sein kann.

Vermögenswerte bleiben grundsätzlich bis zum Abschluss des Verfahrens beschlagnahmt. Nach Art. 266 Abs. 5 StPO können Gegenstände, die einer schnellen Wertverminderung unterliegen oder einen kostspieligen Unterhalt erfordern, sowie Wertpapiere oder andere Werte mit einem Börsen- oder Marktpreis nach den Bestimmungen des SchKG allerdings auch sofort verwertet werden. Bei einer derartigen vorzeitigen Verwertung handelt es sich jedoch um eine Ausnahme, da im Regelfall über eine allfällige Verwertung erst im Endentscheid befunden wird.<sup>140</sup> Da zwischen Beschlagnahme und rechtskräftigem Verfahrensabschluss Monate oder Jahre vergehen können, scheint die Möglichkeit der vorzeitigen Verwertung nach Art. 266 Abs. 5 StPO in Anbetracht der beschriebenen, doch extremen Kursschwankungen bei Kryptowährungen grundsätzlich ein geeignetes Mittel darzustellen, um das Haftungsrisiko der Strafverfolgungsbehörden zu minimieren bzw. Vermögensnachteile für den Beschuldigten zu verhindern.<sup>141</sup> Es ist allerdings natürlich auch möglich, dass der Kurs der beschlagnahmten *Coins* in derselben

Zeitspanne ansteigen könnte und die Behörden Vermögensvorteile daraus ziehen.

### 2. Voraussetzungen und Umsetzung einer Veräusserung

Da Kryptowährungen einen Vermögenswert darstellen, können sie als «andere Werte mit einem Börsen- oder Marktpreis» unter die Bestimmung von Art. 266 Abs. 5 StPO subsumiert werden, weshalb eine vorzeitige Verwertung im Allgemeinen eine Grundlage findet. Dem Wortlaut nach dürften solche Werte folglich ohne weitere Voraussetzungen vorzeitig verwertet werden, da sich das Kriterium der «schnellen Wertverminderung» nur auf Gegenstände bezieht.<sup>142</sup> In der Lehre wird jedoch mehrheitlich die Meinung vertreten, dass auch bei Vermögenswerten mit Börsen- oder Marktpreis nur ein konkretes Risiko eines Wertverlustes eine vorzeitige Verwertung zu legitimieren vermöge.<sup>143</sup> Eine andere Meinung vertreten BOMMER und GOLDSCHMID, die von einem nur scheinbaren behördlichen Ermessen ausgehen.<sup>144</sup> Dieses schrumpfte und verdichtete sich zu einer Pflicht zur vorzeitigen Verwertung. Die Strafverfolgungsbehörde erwerbe mit der hoheitlichen Gewalt über die Vermögenswerte die Pflicht zu deren sorgfältiger Verwaltung.<sup>145</sup> Eine Ausnahme von dieser Pflicht sei nur bei einem Einspruch gegen die vorzeitige Verwertung anzunehmen. Liege ein solcher vor, gehe dies jedoch mit der gleichzeitigen Verpflichtung des Betroffenen einher, allfällige Verluste selbst zu tragen und andere Sicherheiten zu leisten.<sup>146</sup> Gemäss Bundesstrafgericht muss davon ausgegangen werden, dass sich das Interesse des Inhabers auf den Wert beziehe und nicht auf das Wertpapier selbst.<sup>147</sup> Hinsichtlich Kryptowährungen trifft

<sup>138</sup> So z.B. LUKA MÜLLER, Wie funktioniert eine Bitcoin-Transaktion?, *Asset Manager* 2016, 8 ff., 8; ECB, *Analysis* (FN 10), 23.

<sup>139</sup> Siehe z.B. <https://www.finanzen.ch/devisen/historisch/bitcoin-franken-kurs> (Abruf 9.7.2018).

<sup>140</sup> Art. 267 Abs. 3 StPO; PC CPP-MOREILLON/PAREIN-REYMOND (FN 74), Art. 266 N 19; CR CPP-LEMBO/JULEN BERTHOD (FN 74), Art. 266 N 12.

<sup>141</sup> Vgl. BGE 130 I 360 E. 14.2.

<sup>142</sup> BSK StPO II-BOMMER/GOLDSCHMID (FN 74), Art. 266 N 32.

<sup>143</sup> YVAN JEANNERET/ANDRÉ KUHN, *Précis de procédure pénale*, N 14085; StPO Komm.-HEIMGARTNER (FN 75), Art. 266 N 10; HEIMGARTNER (FN 61), 307; NIKLAUS SCHMID/DANIEL JOSITSCH, *Schweizerische Strafprozessordnung, Praxiskommentar*, 3. A., Zürich/St. Gallen 2017, Art. 266 StGB N 8.

<sup>144</sup> BSK StPO II-BOMMER/GOLDSCHMID (FN 74), Art. 266 N 32.

<sup>145</sup> So auch das Bundesstrafgericht in BStGer, BB.2012.146, 30.1.2013, E. 2.5; CÉDRIC REMUND/DOMINIC WYSS, *Urteilsbesprechung* BB.2013.190, BB.2013.189, *forumpoenale* 2014, 333 ff., 336.

<sup>146</sup> BSK StPO II-BOMMER/GOLDSCHMID (FN 74), Art. 266 N 32. Gemäss einem Entscheid der Anklagekammer des Kantons St. Gallen aus dem Jahr 2011 soll die vorzeitige Verwertung bei der Kostendeckungsbeschlagnahme nur ausnahmsweise erlaubt sein, aber nie gegen den Willen des Beschuldigten (AK.2011.220, *Entscheid* vom 27.9.2011, Internet: [https://www.gerichte.sg.ch/home/dienstleistungen/rechtsprechung/kantonsgericht/entscheid\\_2011/ak\\_2011\\_220.html](https://www.gerichte.sg.ch/home/dienstleistungen/rechtsprechung/kantonsgericht/entscheid_2011/ak_2011_220.html) [Abruf 9.7.2018]).

<sup>147</sup> BStGer, BB.2012.146, 30.1.2013, E. 2.5.

dies allerdings wohl nur dann zu, wenn der Wert der virtuellen Einheiten im Zeitpunkt einer allfälligen vorzeitigen Verwertung höher ist, als dies zum Zeitpunkt des Erwerbs der Fall war.

Aus dieser unklaren Lehrmeinung hinsichtlich der Legitimität einer sofortigen Veräusserung von Wertpapieren in Verbindung mit der jedoch in Art. 266 Abs. 5 StPO klar statuierten Rechtsgrundlage einer Verwertung von Vermögenswerten ergibt sich hinsichtlich der Kryptowährungen, dass eine Verwertung grundsätzlich zulässig ist.<sup>148</sup> Eine solche sollte jedoch jedenfalls sachgemäss und verhältnismässig sein. Ein Blick auf die Kursentwicklung und die Volatilität der infrage stehenden virtuellen Währung ist folglich angebracht. Bei der Beschlagnahme zur Sicherstellung von Verfahrenskosten scheint das Einholen der Zustimmung der beschuldigten Person angemessen. Dabei kann zugleich eine Bestätigung eingeholt werden, dass bei einem Verzicht auf Veräusserung allfällige Kursverluste durch den Beschuldigten selbst zu tragen sind (Haftungsausschluss). Bei der Restitutions- und Einziehungsbeseitigung ist gerade aufgrund der aktuell persistenten Kursschwankungen und des damit einhergehenden hohen Risikos eines Wertverlustes allerdings eine vorzeitige Verwertung nahezu legen – auch gegen den Willen der beschuldigten Person.<sup>149</sup>

#### IV. Fazit

Wie der vorliegende Beitrag offenbarte, handelt es sich bei der Beschlagnahme von virtuellen Währungen um eine neuartige Herausforderung für Strafverfolgungsbehörden, welche sowohl rechtliche Unklarheiten als auch praktische Schwierigkeiten mit sich bringt. Dennoch konnte aufgezeigt werden, dass sich für die Beschlagnahme von Kryptowährungen als *Daten mit Vermögenswert sui generis* in Art. 263 Abs. 1 StPO eine zunächst ausreichende Rechtsgrundlage findet und auch die Bestimmungen zur Herausgabepflicht und zur Veräusserung sinngemäss Anwendung finden. Dennoch hinterlässt die Subsumtion unter den Begriff des Vermögenswerts bei gleichzeitiger Nichtanwendbarkeit der Beschlagnahme auf nichtfassba-

re Daten den unbefriedigenden Nachgeschmack, dass die Beweismittelbeschlagnahme unzulässig bleibt.

Einer Sicherstellung von Daten mit Vermögenswert zu Einziehungszwecken steht jedoch nichts im Wege und die Strafverfolgungsbehörden sind angewiesen, eine solche gegebenenfalls anzuordnen. Eine Beschlagnahme von Kryptowährungen erfordert jedoch, wie ausführlich dargetan werden konnte, die Übertragung der Vermögenswerte zum Staat. Die Durchführbarkeit der Beschlagnahme hängt dabei von diversen Faktoren ab, u.a. von der Zugänglichkeit der *Wallet* und des *Private Keys*, andererseits von der staatlich zur Verfügung stehenden Infrastruktur. Wenn auch festgestellt wurde, dass für diese Zwangsmassnahme im Hinblick auf Kryptowährungen eine gesetzliche Grundlage besteht, würde eine explizite Regelung die Unklarheiten der Berechtigungen und des Verbleibs der virtuellen Währungen beseitigen. Zudem könnte damit den Strafbehörden eine konkrete Handlungsanweisung zur Verfügung gestellt werden. Einerseits wäre eine Ergänzung von Art. 266 StPO um den Spezialfall der Kryptowährungen denkbar. Andererseits könnte eine explizite Normierung auch Eingang in die Verordnung über die Anlage beschlagnahmter Vermögenswerte<sup>150</sup> finden. Zudem wäre eine grundlegende gesetzgeberische Klärung, wie mit nichtfassbaren Daten umzugehen ist, in Anbetracht der zunehmenden Bedeutung verschiedenartiger nichtverkörperter Daten des Weiteren allgemein zu begrüssen. Dieser Problemlage liesse sich mit einer zeitgemässen Ausweitung des Art. 263 StPO auf Daten einfach begegnen.

Aufgrund der zunehmenden Relevanz, die Kryptowährungen im Zusammenhang mit Straftaten zukommt, ist anzunehmen, dass die Beschlagnahme derartiger virtueller Währungen rasch an Bedeutung gewinnen wird. Umso wichtiger ist es, dass die Behörden sich auf diesen Umstand einstellen und die Infrastruktur und Abläufe optimieren. Aufgrund der Komplexität der Funktionsweise dieser Währungen, der Abwesenheit zentraler Ansprechpartner und der Globalität des Kryptowährungsmarktes kommen die Verantwortlichen ferner nicht umhin, bei den Ermittlern darüber hinaus ein konzeptionelles Verständnis für die entsprechenden Mechanismen zu fördern, was u.a. mittels gezielter Ausbildung erreicht werden kann.<sup>151</sup>

<sup>148</sup> Auch der deutsche BGH kam in einem Fall vergleichbar zum Schluss, dass Bitcoin tauglicher Gegenstand einer Verfallsanordnung sei; siehe BGH, 1 StR 412/16, 27.7.2017, N 67.

<sup>149</sup> Vgl. SCHMID/JOSITSCH (FN 143), Art. 266 StGB N 8 mit Verweis auf FP 2012 288 (AK-Entscheid); in Analogie zu Aktien: BSK StPO II-BOMMER/GOLDSCHMID (FN 74), Art. 266 N 10; HEIMGARTNER (FN 61), 307; REMUND/WYSS (FN 145), 333.

<sup>150</sup> Verordnung vom 3. Dezember 2010 über die Anlage beschlagnahmter Vermögenswerte (SR 312.057).

<sup>151</sup> Vgl. auch EUGSTER (FN 5), 50.