Universität St.Gallen

Hochschule für Wirtschafts-, Rechts- und Sozialwissenschaften sowie
Internationale Beziehungen (HSG)

Masterarbeit im Master in Rechtswissenschaft

Wie lassen sich Crypto-Assets (insbesondere Bitcoin) strafprozessual beschlagnahmen?

Vorgelegt von

Vivian Lersch
Tobelhofstrasse 15
8044 Zürich
vivian.lersch@student.unisg.ch
Matrikel-Nr.: 14-609-028

Referent:

Prof. Dr. Marc Forster

Korreferentin:

Ass.-Prof. Dr. Monika Simmler

Eingereicht am 21. November 2022

Inhaltsverzeichnis

Literaturverzeichnis

ACKERMANN JÜRG-BEAT (Hrsg.), Kommentar Kriminelles Vermögen – Kriminelle Organisation: Einziehung, Kriminelle Organisation, Finanzierung des Terrorismus, Geldwäscherei, Bd. II, Zürich/Basel/Genf 2018 (zit. KV-KO VERFASSER, Art. 1 StGB N 1.).

AEPLI MICHAEL, Die strafprozessuale Sicherstellung von elektronisch gespeicherten Daten, Diss., Zürich/Basel/Genf 2004.

ANTONOPOULOS ANDREAS M., Mastering Bitcoin, 2. Aufl., Beijing/Boston/Farnham/ Sebastopol/Tokyo 2017.

BANGERTER SIMON, Hausdurchsuchungen und Beschlagnahmen im Wettbewerbsrecht – unter vergleichender Berücksichtigung der StPO, Diss., Zürich 2014.

BÄRTSCHI HARALD/MEISSER CHRISTIAN, Virtuelle Währungen aus finanzmarkt- und zivilrechtlicher Sicht, in: WEBER ROLF H./THOUVENIN FLORENT (Hrsg.), Rechtliche Herausforderungen durch webbasierte und mobile Zahlungssysteme, Zürich 2015, S. 113 ff.

BOMMER FELIX, Löschung als Einziehung von Daten, in: SCHWARZENEGGER CHRISTIAN/ARTER OLIVER/JÖRG FLORIAN S. (Hrsg.), InternetRecht und Strafrecht, 4. Tagungsband, Bern 2005, S. 171 ff.

BREITENFELDT FRIEDO, BGer 1B_59/2021: Die vorzeitige Verwertung beschlagnahmter Kryptoguthaben, AJP 2022, S. 393 ff.

BURCKHARDT PETER/RYSER ROLAND M., Die erweiterten Beschlagnahmeverbote zum Schutz des Anwaltsgeheimnisses insbesondere im neuen Strafverfahren, AJP 2013, S. 159 ff.

DONATSCH ANDREAS/LIEBER VIKTOR/SUMMERS SARAH/WOHLERS WOLFGANG (Hrsg.), Kommentar zur Schweizerischen Strafprozessordnung StPO, Art. 196-457, 3. Aufl., Zürich/Basel/Genf 2020 (zit. VERFASSER, StPO-Kommentar, Art. 1 N 1).

ECKERT MARTIN, Digitale Daten als Wirtschaftsgut: digitale Daten als Sache, SJZ 112/2016, S. 245 ff.

GEISER THOMAS/FOUNTOULAKIS CHRISTINA (Hrsg.), Basler Kommentar Zivilgesetzbuch II, 7. Aufl., Basel 2022 (zit. BSK ZGB II-VERFASSER, Art. 1 N 1).

GLESS SABINE, Internationales Strafrecht, Grundriss für Studium und Praxis, 2. Aufl., Basel 2015 (zit. GLESS Internationales Strafrecht).

GLESS SABINE, Strafrechtsschutz für virtuelles Geld, in: Jositsch, Daniel/Schwarzenegger, Christian/Wohlers, Wolfgang (Hrsg.), Festschrift für Andreas Donatsch, Zürich 2017 (zit. GLESS Strafrechtsschutz für virtuelles Geld).

GLESS SABINE/KUGLER PETER/STAGNO DARIO, Was ist Geld? Und warum schützt man es?, recht 2015, S. 85 ff.

GOGER THOMAS, Bitcoins im Strafverfahren: Virtuelle Währung und reale Strafverfolgung, MMR 2016, S. 431 ff.

HAUSER-SPÜHLER GABRIELA/MEISSER LUZIUS, Eigenschaften der Kryptowährung Bitcoin, in: Digma, Zeitschrift für Datenrecht und Informationssicherheit, 2018.1, S. 6 ff.

HEIMGARTNER STEFAN, Strafprozessuale Beschlagnahme, Wesen, Arten und Wirkungen, Habilitationsschrift Universität Zürich, Zürich/Basel/Genf 2011.

HESS MARTIN/LIENHARD STEPHANIE, Übertragung von Vermögenswerten auf der Blockchain, Darstellung der technischen Grundlagen und der Übertragungsformen de lege lata et ferenda, Jus-letter vom 4. Dezember 2017.

HOSTETTLER OTTO, Darknet, Die Schattenwelt des Internets, Zürich 2017 (zit. HOSTETTLER, Darknet).

HOSTETTLER OTTO, Hilflose Ermittler, Warum Kriminelle im Darknet wenig zu befürchten haben, APuZ 46–47/2017, S. 10 ff. (zit. HOSTETTLER, Hilflose Ermittler).

JOSITSCH DANIEL/POULIKAKOS GEORGE, Beschlagnahme als Zwangsmassnahme, Wie lange ist zu Lange?, ContraLegem 2/2019, S. 151 ff.

MEISSER LUZIUS, Kryptowährungen: Geschichte, Funktionsweise, Potential, in: Weber Rolf H./Thouvenin Florent (Hrsg.), Rechtliche Herausforderungen durch webbasierte und mobile Zahlungssysteme, Zürich 2015.

MOLO GIOVANNI/BRUNONE MATTEO, Kryptowährungen im Visier der staatlichen Kontrolle, sic! 7-8/2022, S. 299 ff.

MOLO GIOVANNI/DRZALIC JANA, Können Kryptowährungen compliant sein?, AJP 2019, S. 40 ff.

NIGGLI MARCEL ALEXANDER/HEER MARIANNE/WIPRÄCHTIGER HANS (Hrsg.), Basler Kommentar, Schweizerische Strafprozessordnung/Jugendstrafprozessordnung (StPO/JStPO), 2. Aufl., Basel 2014 (zit. BSK StPO- VERFASSER, Art. 1 N 1).

NIGGLI MARCEL ALEXANDER/WIPRÄCHTIGER HANS (Hrsg.), Basler Kommentar, Strafrecht, Strafgesetzbuch und Jugendstrafgesetz (StGB/JStG), 4. Aufl., Basel 2018 (zit. BSK StGB-VERFASSER, Art. 1 N 1).

RÜCKERT CHRISTIAN, Vermögensabschöpfung und Sicherstellung bei Bitcoins - Neue juristische Herausforderungen durch die ungeklärte Rechtsnatur von virtuellen Währungseinheiten, MMR 2016, S. 295 ff.

RYSER DOMINIC, «Computer Forensics», eine neue Herausforderung für das Strafprozessrecht, in: SCHWARZENEGGER CHRISTIAN/ARTER OLIVER/JÖRG FLORIAN S. (Hrsg.), Internet-Recht und Strafrecht, 4. Tagungsband, Bern 2005, S. 553 ff.

SCHÄR NOËMIE/SIMMLER MONIKA, Die Erfassung von Kryptowährungen im Schweizer Vermögensstrafrecht, ZSR 2019 I (4), S. 401 ff.

SCHMID NIKLAUS, Strafprozessuale Fragen im Zusammenhang mit Computerdelikten und neuen Informationstechnologien im allgemeinen, ZStrR 1993, S. 81 ff.

SCHMID NIKLAUS/JOSITSCH DANIEL, Handbuch des schweizerischen Strafprozessrechts, 3. Aufl., Zürich/St. Gallen 2017 (zit. SCHMID/JOSITSCH, Handbuch StPO).

SCHMID NIKLAUS/JOSITSCH DANIEL, Schweizerische Strafprozessordnung, Praxiskommentar, 3. Aufl., Zürich/St. Gallen 2018. (zit. SCHMID/JOSITSCH, Praxiskommentar StPO).

SEILER BENEDIKT/SEILER DANIEL, Sind Kryptowährungen wie Bitcoin (BTC), Ethereum (ETH), Ripple (XRP) und Co. als Sachen im Sinne des ZGB zu behandeln?, sui-generis 2018, S. 149 ff.

SIMMLER MONIKA/SELMAN SINE/BURGERMEISTER DANIEL, Beschlagnahme von Kryptowährungen im Strafverfahren, AJP 2018, 963 ff.

STENGEL CORNELIA/AUS DER AU ROMAN, Blockchain: Eine Technologie für effektiven Datenschutz, sic! 2018, S. 439 ff.

STRATENWERTH GÜNTER/BOMMER FELIX, Schweizerisches Strafrecht, Allgemeiner Teil II: Strafen und Massnahmen, 3. Aufl., Bern 2020. (zit. STRATENWERTH/BOMMER, AT II, § 1 N 1).

TRECHSEL STEFAN/PIETH MARK (Hrsg.), Praxiskommentar Schweizerisches Strafgesetzbuch, 4. Aufl., Zürich 2021 (zit. PK StGB- VERFASSER, Art. 1 N 1).

TSCHUDI DOMINIK, Die Einziehung von Kryptowährungen im Strafverfahren, Diss., Basel 2020.

TUOR PETER/SCHNYDER BERNHARD/SCHMID JÖRG/JUNGO ALEXANDRA, Das Schweizerische Zivilgesetzbuch, 14. Aufl., Zürich/Basel/Genf 2015.

TZANETAKIS MEROPI, Drogenhandel im Darknet: Gesellschaftliche Auswirkungen von Kryptomärkten, APuZ 46–47/2017, S. 41 ff.

VOCK DOMINIK, Vorzeitige Verwertung von kryptobasierten Vermögenswerten im Strafverfahren, ZZZ 2022, S. 227 ff.

VOCK DOMINIK/HOFMANN DOMINIK, DLT-basierte Token: Pfändung und Konkursbeschlag, SJZ 2019, S. 307 ff.

VON DER CRONE HANS CASPAR/KESSLER FRANZ J./ANGSTMANN LUCA, Token in der Blockchain – privatrechtliche Aspekte der Distributed Ledger Technologie, SJZ 2018, S. 337 ff.

WEBER ROLF H./THOUVENIN FLORENT, Dateneigentum und Datenzugangsrechte – Bausteine der Informationsgesellschaft?, ZSR 2018, S. 43 ff.

ZOGG SAMUEL, Zwangsvollstreckungsrechtliche Behandlung von Kryptowährungen, recht 2020, S. 1 ff.

Rechtsprechungsverzeichnis

Amtlich publizierte Urteile des Bundesgerichts:

BGE 148 IV 74	Urteil vom 18. Oktober 2021
BGE 141 IV 108	Urteil vom 14. Januar 2015
BGE 126 I 97	Urteil vom 23. Juni 2000
BGE 126 I 50	Urteil vom 5. April 2000

Nicht amtlich publizierte Urteile des Bundesgerichts:

BGer 1B_59/2021	Urteil vom 18. Oktober 2021
BGer 1B_357/2019	Urteil vom 06. November 2019
BGer 1B_125/2019	Urteil vom 26. April 2019

BGer 6B_99/2019, 6B_148/2019	Urteil vom 18. April 2019
BGer 1B_461/2017	Urteil vom 08. Januar 2018
BGer 1B_114/2015	Urteil vom 01. Juli 2015
BGer 1B_95/2011	Urteil vom 9. Juni 2011
BGer 6B_659/2010	Urteil vom 20. Dezember 2010
BGer 1B_157/2007	Urteil vom 25. Oktober 2007
BGer 1S.16/2005	Urteil vom 07. Juni 2005
BGer 1P.456/2003	Urteil vom 04. März 2004
Weitere Urteile:	
OGer ZH UH220009	Beschluss des Obergerichts des Kantons Zürich vom 26. April 2022
BStGer BB.2012.146	Beschluss des Bundesstrafgerichts vom 30. Januar 2013

Materialienverzeichnis

Interdepartementalen Koordinationsgruppe zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (KGGT), Bericht zu Geldwäscherei- und Terrorismus-finanzierungsrisiken von Krypto-Assets und Crowdfunding, Oktober 2018, Internet: https://www.newsd.admin.ch/newsd/message/attachments/56167.pdf (Abruf 20.07. 2022; zit. KGGT-Bericht 2018).

Interdepartementalen Koordinationsgruppe zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (KGGT), Bericht über die nationale Beurteilung der Geldwäscherei- und Terrorismusfinanzierungsrisiken in der Schweiz, Oktober 2021, Internet: https://www.sif.admin.ch/sif/de/home/dokumentation/fachinformationen/bericht_kggt.html (Abruf 24.10.2022; zit. KGGT-Bericht 2021).

Schweizerischer Bundesrat, Bericht zu virtuellen Währungen in Beantwortung der Postulate Schwaab (13.3687) und Weibel (13.4070), 25. Juni 2014, Internet: https://www.news.admin.ch/NSBSubscriber/message/attachments/35361.pdf (Abruf 11.10.2022; zit. BR-Bericht virtuelle Währungen).

Schweizerischer Bundesrat, Rechtliche Grundlagen für Distributed Ledger-Technologie und Blockchain in der Schweiz, 14. Dezember 2018, Internet:

https://www.newsd.admin.ch/newsd/message/attachments/55150.pdf (Abruf 11.10.2022; zit. BR-Bericht DLT/Blockchain).

Schweizerischer Bundesrat, Stellungnahme zur Interpellation Schmid (17.4024), Risiken und Chancen rund um Bitcoins und Cyberwährungen, 31. Januar 2018, Internet: https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId =20174024 (Abruf: 24.10.2022; zit. BR-Stellungnahme Risiken und Chancen).

Schweizerischer Bundesrat, Stellungnahme zum Postulat der SiK-N (22.3017), Stärkung der Strafverfolgungsbehörden im Bereich der Kryptowährungen, 27.04.2022, Internet: https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20223017 (Abruf: 24.10.2022; zit. BR-Stellungnahme Stärkung der Strafverfolgungsbehörden).

Internetquellenverzeichnis

Appinventiv, Custodial vs. Non-Custodial Wallets: Understanding the Difference Points, Internet: https://appinventiv.com/blog/custodial-vs-non-custodial-wallets/ (Abruf 18.11.2022).

Bitcoin, Häufig gestellte Fragen, 2022, Internet: https://bitcoin.org/de/faq#wie-funktioniert-bitcoin (Abruf 20.07.2022; zit. Bitcoin, FAQ).

Bitcoin, Wie funktioniert Bitcoin, Internet: https://bitcoin.org/de/wie-es-funktioniert (Abruf 18.11.2022; zit. Bitcoin, Blockchain).

Bitpanda, Was sind Altcoins?, Internet: https://www.bitpanda.com/academy/de/lektionen/was-sind-altcoins/ (Abruf 18.11.2022).

Bundesgericht, Medienmitteilung vom 18.11.2021, Urteil vom 18. Oktober 2021 (1B_59/2021), Verwertung von Kryptobeständen erfordert Fachwissen, Internet: https://www.bger.ch/files/live/sites/bger/files/pdf/de/1b_0059_2021_2021_11_18_T_d_09_57_52.pdf (Abruf: 23.09.2022) (zit. Bundesgericht, Medienmitteilung, Abschn. 1).

Bundesrat, Umsetzungsplan der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018–2022, Mai 2019, Internet: https://www.newsd.admin.ch/newsd/message/attachments/56943.pdf (Abruf 24.10.2022; zit. Bundesrat, Umsetzungsplan NCS).

BURGERMEISTER DANIEL/BROGER DAMIAN, Cybercrime – neue Herausforderungen für die Strafverfolgungsbehörden, Vortragsabend St.Galler Juristenverein, 01.09.2022, Internet:

https://st-galler-juristenverein.ch/index_htm_files/Referat%20Cybercrime%20Juristenverein.pdf (Abruf 20.11.2022).

CoinMarketCap, Internet: https://coinmarketcap.com/ (Abruf 22.07.2022).

Cryptopedia, Hot Wallets vs. Cold Wallets, 10.04.2022, Internet: https://www.gemini.com/cryptopedia/crypto-wallets-hot-cold (Abruf 18.11.2022).

Cryptopedia, What Are Crypto Brain Wallets?, 27.01.2021, Internet: https://www.gemini.com/cryptopedia/crypto-cold-storage-brain-wallets (Abruf 18.11.2022; zit. Cryptopedia, Brain).

Ethereum, What is Ethereum?, Internet: https://ethereum.org/en/what-is-ethereum/ (Abruf 18.11.2022).

Europarat, Who are the Parties to the Budapest Convention?, Internet: https://www.coe.int/en/web/cybercrime/the-budapest-convention (Abruf 16.11.2022).

European Central Bank, Virtual currency schemes – a further analysis, Februar 2015, Internet: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf (Abruf 27.08.2022; zit. European Central Bank, Analysis, S.).

Europol, Internet Organised Crime Threat Assessment (IOCTA) 2021, Publications Office of the European Union, Luxembourg, 2021, Internet: https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf (Abruf 27.08.2022; zit. Europol, IOCTA, S.).

Eurospider, Was sind Kryptowährungs-Mixer?, Internet: https://www.eurospider.com/de/know-how/compliance/210-was-sind-kryptow%C3%A4hrungs-mixer#:~:text=Ein%20Mixer%20oder%20auch%20Tumbler,%C3%BCberweist%20Bitcoins%20an%20den%20Mixerdienst (Abruf 05.11.2022).

FINMA, Entwicklungen im Bereich Fintech, Internet: https://www.finma.ch/de/dokumentation/dossier/dossier-fintech/entwicklungen-im-bereich-fintech/ (Abruf 18.11.2022; zit. FINMA, Fintech Entwicklung).

FINMA, Warnung vor möglicherweise unerlaubt tätigen Anbietern, Internet: https://www.finma.ch/de/finma-public/warnliste/ (Abruf 16.07.2022; zit. FINMA, Warnliste).

International Counter Ransomware Initiative, 2022 Joint Statement, 01.11.2022, Internet: https://www.whitehouse.gov/briefing-room/statements-releases/2022/11/01/international-counter-ransomware-initiative-2022-joint-statement/ (Abruf 14.11.2022; zit. CRI 2022).

Interpol, Darknet and Cryptocurrencies, Internet: https://www.interpol.int/How-we-work/Innovation/Darknet-and-Cryptocurrencies (Abruf 23.05.2021).

Kantonspolizei Bern, Kanton Bern: Kryptowährungen beschlagnahmt – Mann angehalten, Internet: https://www.police.be.ch/de/start.html?newsID=6b273a19-35c6-4985-8ee6-059e113e627c (Abruf 27.09.2022; zit. Polizeimeldung Bern).

MORDRELLE EFLAMM/HONEGGER LORENZ, Wie kam es zum FTX-Debakel – und wie geht es jetzt weiter mit dem Krypto-Markt? Die wichtigsten Fragen und Antworten, Internet: https://www.nzz.ch/finanzen/ftx-was-bedeutet-das-aus-der-bitcoin-boerse-fuer-den-krypto-markt-ld.1712941 (Abruf 20.11.2022, zit. NZZ FTX).

MUKHOPADHYAY UJAN/SKJELLUM ANTHONY/HAMBOLU OLUWAKEMI/OAKLEY JON/YU LU/BROOKS RICHARD, A brief survey of Cryptocurrency systems, in: 2016 14th Annual Conference on Privacy, Security and Trust (PST), IEEE, Auckland 2017, Internet: DOI: 10.1109/PST.2016.7906988 (Abruf 19.11.2022).

ROTH SIMON, Das Bundesgericht bestätigt das Territorialitätsprinzip bei grenzüberschreitenden Strafuntersuchungen, 2020, Internet: https://www.lexfutura.ch/en/whats-keeping-us-busy/article/das-bundesgericht-bestaetigt-das-territorialitaetsprinzip-bei-grenzueberschreitenden-strafuntersuchungen/ (Abruf 06.11.2022).

SATOSHI NAKAMOTO, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, Internet: https://bitcoin.org/bitcoin.pdf (Abruf 20.07.2022).

SCHWARZ DENNIS/VOLKERY CARSTEN/KRÖNER ANDREAS, «Ende des Wilden Westens»: Das sind die wichtigsten Fakten über die EU-Regeln für die Krypto-Branche, 01.07.2022, Internet: https://www.handelsblatt.com/finanzen/maerkte/devisen-rohstoffe/mica-richtlinie-ende-des-wilden-westens-das-sind-die-wichtigsten-fakten-ueber-die-eu-regeln-fuer-die-krypto-branche/28472342.html (Abruf 18.11.2022, zit. Handelsblatt, MiCA-Richtlinie).

SCHWEINGRUBER SANDRA, Cybercrime – eine Herausforderung für die Strafverfolgung, Herbstveranstaltung des Aargauischen Juristenvereins, Aarau, 12.11.2018, Internet:

https://www.jv-aargau.ch/jwa/vfs/web/2015.jv-aargau.ch/media/publikationen/PDF/Cybercrime.pdf (Abruf 27.09.2022).

SETH SHOBHIT, The 6 Most Private Cryptocurrencies, 27.05.2022, Internet : https://www.investopedia.com/tech/five-most-private-cryptocurrencies/ (Abruf 18.11.2022; zit. SETH, Kryptowährung).

United Nations Office on Drugs and Crime (UNODC), Darknet Cybercrime Threats to Southeast Asia, 2020, Internet: https://www.unodc.org/roseap/uploads/documents/Publications/2021/Darknet_Cybercrime_Threats_to_Southeast_Asia_report.pdf (Abruf 20. 07.2022; zit. UNODC Report, S.).

U.S. Department of The Treasury, Cyber-related Designation, Specially designated nationals list update, 08.08.2022, Internet: https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20220808 (Abruf 18.11.2022; U.S. Cyber-related Designation).

Zug, Wie kann ich meine Steuern mit Kryptowährungen bezahlen?, 04.02.2021, Internet: https://www.zg.ch/behoerden/finanzdirektion/steuerverwaltung/zahlen-mit-kryptowaehrungen/allgemeine-fragen-3/wie-kann-ich-meine-steuern-mit-kryptowaehrungen-bezahlen (Abruf 11.11.2022).

Rechtsquellenverzeichnis

BÜPF	Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs vom 18. März 2016 (SR 780.1).
BV	Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999 (SR 101).
CCC	Übereinkommen über die Cyberkriminalität vom 23. November 2001 (SR 0.311.43).
DSG	Bundesgesetz über den Datenschutz vom 19. Juni 1992 (SR 235.1)
IRSG	Bundesgesetz über internationale Rechtshilfe in Strafsachen vom 20. März 1981 (SR 351.1).
StGB	Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (311.0).
StPO	Schweizerische Strafprozessordnung vom 5. Oktober 2007 (SR 312.0).

Verordnung vom 3. Dezember 2010 über die Anlage beschlagnahmter Vermögenswerte (SR 312.057).

Abkürzungsverzeichnis

A.M.	Anderer Meinung
Abs.	Absatz
Abschn.	Abschnitt
AJP / PJA	Aktuelle Juristische Praxis /Pratique Juridique Actuelle
Anh.	Anhang
Art.	Artikel
Aufl.	Auflage
BAKOM	Bundesamt für Kommunikation
BBI	Bundesblatt
BGE	Leitentscheide des Bundesgerichts
BGer	Bundesgericht
BSK	Basler Kommentar
bspw.	beispielsweise
BStGer	Bundesstrafgericht
BTC	Bitcoin
bzw.	beziehungsweise
ca.	circa
CHF	Schweizer Franken
d.h.	das heisst
Diss.	Dissertation
E.	Erwägung
édit	éditeur (frz.)
eds.	editor (engl.)
EDV	Elektronische Datenverarbeitung

engl.	englisch
et al.	et alii = und weitere
etc.	et cetera (lat.)
EU	Europäische Union
Europol	The European Union’s law enforcement agency
evtl.	eventuell
f. / ff.	folgend(e) / fortfolgende
FBI	United States Federal Bureau of Investigation
Fedpol	Bundesamt für Polizei
FN	Fussnote
frz.	französisch
gem.	gemäss
Gl.M.	Gleicher Meinung
GovWare	GovernmentWare
h.L.	heutige Lehre
Hrsg.	Herausgeber
HTML	Hypertext Markup Language
http	Hypertext Transfer Protocol
i.d.R.	in der Regel
i.e.S.	im engeren Sinn(e)
i.S.v.	im Sinne von
i.S.d.	im Sinne des
i.V.m.	in Verbindung mit
i.w.S.	im weiteren Sinne
Inc.	incorporated (engl.)

insb.	insbesondere
Interpol	International Criminal Police Organisation
IP-Adresse	Internet Protocol
IT	Informationstechnik
jur.	juristisch
Kap.	Kapitel
Kt.	Kanton
lat.	lateinisch
lit.	litera
m.a.W.	mit anderen Worten
m.E.	meines Erachtens
m.w.H.	mit weiteren Hinweisen
Mio.	Million(en)
MMR	Multimedia und Recht
N	Note
nat.	natürlich
NCSC	Nationales Zentrum für Cybersicherheit
NEDIK	Netzwerk digitale Ermittlungsunterstützung Internetkriminalität
No.	Number (engl.)
Nr.	Nummer
NZZ	Neue Zürcher Zeitung
resp.	respektive
sic!	Zeitschrift für Immaterialgüter-, Informations- und Wettbewerbsrecht
sog.	sogenannt(e)
SRF	Schweizer Radio und Fernsehen

StA	Staatsanwalt; Staatsanwaltschaft
SZK	Schweizerische Zeitschrift für Kriminologie
u.a.	unter anderem
U.S.	United States
u.U.	unter Umständen
v.a.	vor allem
vgl.	vergleiche
vs.	versus
WWW	World Wide Web
z.B.	zum Beispiel
ZIS	Zeitschrift für Internationale Strafrechtsdogmatik
zit.	zitiert
ZSR	Zeitschrift für Schweizerisches Recht
ZStrR	Schweizerische Zeitschrift für Strafrecht
ZStW	Zeitschrift für die gesamte Strafrechtswissenschaft

I. Einleitung[1]

A. Einführung

Der Autor mit dem Pseudonym Satoshi Nakamoto beschreibt in seinem White Paper während der Finanzkrise zum ersten Mal die Kryptowährung Bitcoin. Er erklärt, wie eine «peer-to-peer» Version von elektronischem Geld als online Zahlungsmittel ohne den Einbezug von Finanzinstitutionen funktioniert.[2] Bitcoin Transaktionen basieren auf der Blockchain Technologie, welche ein «öffentliches Buchungssystem» darstellt, in dem jede Überweisung gespeichert wird.[3] Die Bedeutung der Crypto-Assets auf dem Finanzmarkt ist nicht zu unterschätzen; allein alle sich aktuell im Umlauf befindenden Bitcoins weisen eine Marktkapitalisierung von rund USD 318 Mrd. auf.[4] Nach der Entstehung von Bitcoin wurde diese virtuelle Währung rasch als Zahlungsmittel im Darknet eingesetzt. Heute werden Zahlungen im Darknet primär mit Kryptowährungen getätigt. Als Folge davon sind Dienstleistungen erhältlich, die es Kriminellen ermöglichen, die digitalen Spuren ihrer illegalen Transaktion zu verwischen und letztendlich Geld zu waschen. Daher müssen Strafbehörden entsprechend geschult und über geeignete strafprozessuale Massnahmen verfügen, um kriminelle Aktivitäten in der digitalen Welt aufzudecken und einzudämmen.[5] So ergeben sich potentielle Schwierigkeiten bei der Beschlagnahme nach Art. 263 ff. StPO von Bitcoin im Strafverfahren, da dafür die Strafverfolgungsbehörden bspw. Zugriff auf die kryptobasierten Vermögenswerte benötigen und dieser aufgrund der dezentralen Verwaltung von Kryptowährungen erschwert wird.[6] Daher soll in dieser Arbeit untersucht werden, unter welchen Voraussetzungen Crypto-Assets (insbesondere Bitcoins) strafprozessual beschlagnahmt werden können und wie dies in der Praxis ausgestaltet wird.

[1] Herzlicher Dank gilt dem Referenten Prof. Dr. Marc Forster für den Vorschlag, sich mit dieser aktuellen Thematik im Rahmen meiner Masterarbeit zu befassen. Zudem möchte ich Frau Ass.-Prof. Dr. Monika Simmler für die Annahme des Korreferats danken. Ebenso bedanke ich mich herzlich bei meinen Interviewpartnern: Herr Daniel Burgermeister, Herr Marcel Meier, Herr Philippe Meier, Herr Lorenz Kilchenmann, Herr Reto Steiger, Herr Stephan Walder für die hilfreichen Einblicke in die Strafverfolgung in der Praxis.
Anmerkung zur Geschlechter-Formulierung: Alle personenbezogenen Formulierungen meinen beide Geschlechter mit, selbst wenn aus Lesbarkeitsgründen die männliche Form gebraucht wird.
[2] SATOSHI, S. 1 ff.
[3] Bitcoin, FAQ.
[4] CoinMarketCap, Stand 18.11..2022.
[5] Europol, IOCTA, S. 9, 18; KGGT-Bericht 2021, S. 51 ff.; UNODC Report, S. 20 ff.
[6] BR-Stellungnahme Risiken und Chancen, 2018; SIMMLER ET AL., S. 964.

B. Vorgehen und Aufbau

Anhand der Arbeit soll folgende Forschungsfrage beantwortet werden:

Wie lassen sich Crypto-Assets (insbesondere Bitcoin) strafprozessual beschlagnahmen?

Die Arbeit wird in sieben Teile gegliedert. Im ersten Teil werden die Funktionsweise der Crypto-Assets mit einem Hauptaugenmerk auf den technischen Grundlagen von Bitcoins sowie deren strafrechtliche Bedeutung erklärt. Zusätzlich wird die Rechtsnatur von Bitcoin diskutiert. Anhand dieser Einführung wird die (strafprozessrechtliche) Relevanz von Crypto-Assets allgemein und die Bedeutung ihrer Beschlagnahme dargelegt.

Nachdem die Grundlagen zu Crypto-Assets sowie deren Wichtigkeit erläutert wurden, folgt der Hauptteil (Kap. III-V), in welchem die Forschungsfrage nach den Beschlagnahmemöglichkeiten von Bitcoin beantwortet wird sowie ausgewählte Problemfelder der Strafverfolgungsbehörden im Zusammenhang mit der Beschlagnahme von Crypto-Assets betrachtet werden.

Die Forschungsfrage wird im erwähnten Hauptteil mit Hilfe einer Literaturanalyse sowie Experteninterviews beantwortet. Die Methoden kommen wie folgt zum Einsatz:

1. Literaturanalyse

Anhand der Literaturanalyse wird der Status Quo des Forschungsstandes zum rechtlichen Rahmen der Kryptowährungen dargelegt. Ebenfalls werden bestehende rechtliche Probleme bei der Beschlagnahme von Kryptowährungen identifiziert.

2. Experteninterviews

Im Rahmen von vier Experteninterviews (Leitfadeninterviews) sollen diejenigen strafprozessualen Schwierigkeiten analysiert werden, welche im Zuge der Literaturanalyse identifiziert wurden. Hierzu wurden deutschsprachige kantonale Strafverfolgungsbehörden angefragt, die über ein Kompetenzzentrum für Cybercrime verfügen. Der detaillierte Leitfaden findet sich gemeinsam mit den transkribierten Interviews im Anhang. Die Experteninterviews dienen dazu, die aktuelle Rechtslage in der Hinsicht zu validieren, ob in der Praxis anhand von derzeit gültigen Bestimmungen die Beschlagnahme von Crypto-Assets funktioniert und falls nicht, festzustellen, wo Verbesserungspotential besteht. Zudem werden mögliche Massnahmen in der Praxis diskutiert sowie Möglichkeiten aufgezeigt, wie der Gesetzgeber die dargelegten Problematiken der Kryptowährungen hinsichtlich der Beschlagnahme mindern könnte.

Die Analyse bzw. Interpretation der Literatur sowie der Experteninterviews dient als Basis für die Entwicklung der Handlungsempfehlungen für Strafverfolgungsbehörden und Gesetzgeber, welche den aufgezeigten Schwierigkeiten bei der Beschlagnahme von Crypto-Assets entgegenwirken sollen.

Diese Handlungsempfehlungen für Strafverfolgungsbehörden und Gesetzgeber sollen entsprechend in Kap. VI ausgearbeitet werden. Zuletzt wird im Rahmen eines Fazits die Beantwortung der Forschungsfrage reflektiert und ein Ausblick zu zukünftigen Forschungsfeldern gegeben (Kap. VII).

II. Crypto-Assets: Technische Einführung und rechtliche Ausgangslage

Um die strafprozessuale Beschlagnahmefähigkeit von Crypto-Assets in der vorliegenden Arbeit beurteilen zu können, müssen zunächst die technische Funktionsweise von Kryptowährungen erläutert sowie deren Rechtsnatur geklärt werden. Zudem soll die kriminalpolitische Relevanz der Crypto-Assets dargelegt werden.

A. Funktionsweise von Crypto-Assets

Zunächst wird die Funktionsweise von Crypto-Assets betrachtet, da diese die potenzielle Beschlagnahme nach Art. 263 ff. StPO massgeblich beeinflusst und dementsprechend das technische Know-How ebenfalls zentral für die Strafverfolgungsbehörden ist.[7] Zunächst wird auf die Kryptowährung Bitcoin und anschliessend kurz auf andere Crypto-Assets eingegangen. Anschliessend soll zudem die Aufbewahrungsmöglichkeit des Private Key erklärt werden, dem, wie im Verlauf der vorliegenden Arbeit noch erläutert, eine essenzielle Rolle in der Verfügungsmacht über Crypto-Assets zukommt.

1. Bitcoin

Bitcoin (BTC) ist eine Sammlung von Konzepten und Technologien, welche die Grundlage eines digitalen Geld-Ökosystems bilden. Währungseinheiten namens Bitcoins werden zum Speichern und Übertragen von Werten zwischen Teilnehmer am Bitcoin-Netzwerk verwendet. Bitcoin-Benutzer kommunizieren miteinander über das Bitcoin-Protokoll, was hauptsächlich über das Internet geschieht. Benutzer können Bitcoin über das Netzwerk übertragen, um so die gleichen Transaktionen tätigen zu können, die auch mit herkömmlichen Währungen möglich sind – z.B. Waren kaufen oder verkaufen, Geld an Personen senden. Die Bitcoin-Technologie umfasst Funktionen, die auf Verschlüsselung und digitale Signaturen basiert, um die Sicherheit

[7] Anh. 2: Interview MEIER/MEYER, Frage 7; SIMMLER ET AL., S. 978.

des Bitcoin-Netzwerks zu gewährleisten. Bitcoins können gekauft, verkauft und gegen andere Währungen an spezialisierten Währungsbörsen getauscht werden.[8]

Im Gegensatz zu herkömmlichen Währungen sind Bitcoins vollständig virtuell. Es gibt keine physischen Coins oder sogar digitale Münzen an sich. Die Münzen sind in Transaktionen impliziert, die Werte werden vom Absender zum Empfänger übertragen. Benutzer von Bitcoin besitzen Schlüssel (Keys), die es ihnen ermöglichen, den Besitzer von Transaktionen im Bitcoin-Netzwerk nachzuweisen. Diese Schlüssel werden zumeist in einer Art digitalem Schlüsselanhänger (Wallet) auf dem Computer jedes Benutzers gespeichert. Der Besitz des Schlüssels, der eine Transaktion freischaltet, ist die einzige Voraussetzung, um Geld ausgeben zu können, wodurch die Kontrolle vollständig in die Hände jedes Benutzers gelegt wird.[9]

Bitcoin hat aktuell eine Marktkapitalisierung von rund USD 318 Mrd. und ist damit die derzeit am weitesten verbreitete und bedeutendste Kryptowährung.[10] BTC setzt sich aus Satoshi (benannt nach dem mutmasslichen Erfinder Satoshi Nakamoto) zusammen, welche die kleinste Bitcoineinheit darstellen.[11]

a) Peer-to-Peer Netzwerk

Bitcoin ist ein weit-verteiltes Peer-to-Peer-System. Daher gibt es keinen „zentralen" Server oder Kontrollpunkt. Bitcoins werden durch einen Prozess namens „Mining" erstellt. Jeder Teilnehmer des Bitcoin-Netzwerks (also jedes Gerät, auf dem das vollständige Bitcoin-Protokoll ausgeführt wird) kann als Miner arbeiten und die Rechenleistung seines Computers nutzen, um das darunterliegende Problem zu lösen, was zur Erstellung (Mining) von Bitcoins notwendig ist. Durchschnittlich wird alle 10 Minuten eine neue Lösung von jemandem gefunden und diese Person ist damit in der Lage, die Transaktionen der letzten 10 Minuten zu validieren und somit auch Zugang zu neuen Bitcoins erhält. Im Wesentlichen dezentralisiert Bitcoin-Mining die Währungsausgabe und Clearing-Funktionen einer Zentralbank und ersetzt deren Notwendigkeit durch diesen globalen Wettbewerb.[12]

Bitcoin ist als Peer-to-Peer-Netzwerkarchitektur auf dem Internet aufgebaut. Der Begriff Peer-to-Peer oder P2P bedeutet, dass die Computer, die am Netzwerk teilnehmen, untereinander alle gleich sind und es keine „speziellen" Knoten gibt. Knoten teilen sich die Last der Bereitstellung von Netzwerkdiensten. Die Netzwerkknoten sind miteinander in einem Mesh-Netzwerk mit

[8] ANTONOPOULOS, S. 1 ff.
[9] ANTONOPOULOS, S. 2 ff.
[10] Coin Market Cap, Stand 18.11.2022.
[11] TSCHUDI, S. 9.
[12] MUKHOPADHYAY ET AL., S. 1 ff.

einer „flachen“ Topologie verbunden. Es gibt keinen „Server“, keinen zentralisierten Dienst, und keine Hierarchie innerhalb des Netzwerks. Knoten in einem Peer-to-Peer-Netzwerk stellen gleichzeitig Dienstleistungen bereit und konsumieren sie auch. Peer-to-Peer-Netzwerke sind von Natur aus belastbar, dezentralisiert und offen. Das herausragendste Beispiel einer P2P-Netzwerkarchitektur war das frühe Internet selbst, wo Knoten im IP-Netzwerk gleich waren. Die heutige Internetarchitektur ist hierarchischer, aber das Internet Protocol behält immer noch seine Essenz der flachen Topologie.[13]

b) Das Bitcoin-Protokoll

Das Bitcoin-Protokoll enthält eingebaute Algorithmen, die die Mining-Funktion über das Netzwerk regulieren. Die Schwierigkeit des Problems, das Miner lösen müssen, wird dynamisch angepasst, sodass im Durchschnitt alle 10 Minuten jemand eine richtige Antwort findet unabhängig davon, wie viele Miner (und CPUs) gerade an dem Problem arbeiten Das Protokoll halbiert auch die Rate, mit der alle 4 Jahre neue Bitcoins erstellt werden und begrenzt die Gesamtzahl der Bitcoins, die erstellt werden, auf eine feste Gesamtzahl von 21 Millionen Coins. Daraus ergibt sich, dass die Anzahl der sich im Umlauf befindlichen Bitcoins einer leicht vorhersehbaren Kurve folgt, die bis zum Jahr 2140 21 Millionen erreicht. Aufgrund der sich immer weiter verlangsamenden Ausgaberate von Bitcoins ist die Bitcoin-Währung langfristig deflationär. Außerdem kann Bitcoin nicht inflationär werden, indem neues Geld über das Erwartete hinaus „gedruckt“ wird.[14]

c) Mining und Blockchain

Die Blockchain ist das gemeinsame öffentliche Hauptbuch (Ledger), auf das sich das gesamte Bitcoin-Netzwerk stützt. Alle bestätigten Transaktionen werden in die Blockchain aufgenommen. Es ermöglicht Bitcoin-Geldbörsen, ihr auszugebendes Guthaben zu berechnen, sodass neue Transaktionen verifiziert werden können. Dadurch wird sichergestellt, dass sie tatsächlich dem Ausgebenden gehören. Die Integrität und die chronologische Reihenfolge der Blockchain wird mit Kryptografie abgesichert.[15]

Das Bitcoin-Vertrauenssystem basiert auf Computerberechnungen. Transaktionen werden in Blöcke gebündelt, deren Nachweis einen enormen Rechenaufwand erfordert, aber nur einen geringen Berechnungsaufwand zur Verifizierung. Dieser Prozess wird *Mining* genannt und dient zwei Zwecken für Bitcoin:

---

[13] ANTONOPOULOS, S. 139 ff.
[14] MUKHOPADHYAY ET AL., S. 2 ff.
[15] Bitcoin, Blockchain und Mining.

- Beim Mining werden in jedem Block neue Bitcoins erzeugt, was etwa dem Vorgang des Gelddruckens durch eine Zentralbank gleicht. Die Menge an Bitcoins, die pro Block erstellt wird, ist festgelegt und nimmt mit der Zeit ab.
- Mining schafft Vertrauen, indem sichergestellt wird, dass Transaktionen nur bestätigt werden, wenn genug Rechenleistung dem Block gewidmet wurde, der sie enthält. Mehr Blöcke bedeuten mehr Berechnungen, was wiederum mehr Vertrauen bedeutet.[16]

Eine gute Art Mining zu beschreiben, ist wie ein riesiges kompetitives Sudoku-Spiel, das jedes Mal zurückgesetzt wird, wenn jemand eine Lösung findet und folglich die Schwierigkeit automatisch angepasst wird.[17]

d) Transaktionen

Einfach ausgedrückt teilt eine Transaktion dem Netzwerk mit, dass der Besitzer einer Anzahl von Bitcoins die Übertragung einiger dieser Bitcoins an einen anderen Eigentümer genehmigt hat. Der neue Besitzer kann diese Bitcoins jetzt ausgeben, indem er eine weitere Transaktion erstellt, welche die Übertragung an einen anderen Eigentümer autorisiert und dieser in einer Art Eigentumskette wiederum die gleichen Möglichkeiten zum Transfer hat. Transaktionen lassen sich wie Zeilen in einem Hauptbuch (Ledger) der doppelten Buchführung darstellen. Jede Transaktion enthält eine oder mehrere „Inputs“, bei denen es sich um Belastungen eines Bitcoin-Kontos handelt. Auf der anderen Seite der Transaktion gibt es einen oder mehrere „Outputs“, bei denen es sich um Gutschriften handelt, die einem Bitcoin-Konto hinzugefügt werden. Die Ein- und Ausgänge (Be- und Entlastungen) müssen sich nicht auf den gleichen Betrag summieren. Stattdessen summieren sich die Outputs zu etwas weniger als die Inputs und die Differenz stellt eine implizite Transaktionsgebühr dar, die von dem Miner erhoben wird der die Transaktion in das Ledger aufnimmt. Die Transaktion enthält auch einen Eigentumsnachweis für jede Bitcoin-Menge (Inputs), dessen Wert in Form einer digitalen Unterschrift des Eigentümers übertragen wird und von jedem mit Zugang zum Ledger unabhängig validiert werden kann. In der Bitcoin-Sprache bedeutet „Ausgeben“ das Signieren einer Transaktion, die mit Hilfe einer Bitcoin-Adresse den Wert einer früheren Transaktion auf einen neuen identifizierten Eigentümer überträgt.[18]

[16] ANTONOPOULOS, S. 26 f.
[17] ANTONOPOULOS, S. 26 f.
[18] ANTONOPOULOS, S. 18 ff.

2. Weitere bedeutende Crypto-Assets

Neben Bitcoin gibt es noch eine Reihe von weiteren Crypto-Assets, welche auf globaler Ebene Anklang gefunden haben. Im Folgenden sollen nun einzelne dieser Crypto-Assets vorgestellt werden, wobei sich die vorliegende Arbeit auf Bitcoin als repräsentative Kryptowährung bezieht.

a) Altcoins

Als Altcoins werden die Nachfolger der ersten und ältesten Kryptowährung Bitcoin bezeichnet. Alle Crypto-Assets, welche als Alternative zu Bitcoin auf den Markt gebracht wurden, fallen unter diese Nomenklatur.[19]

b) Ether

Ether ist das Transaktionstoken, das Operationen im Ethereum-Netzwerk ermöglicht. Alle Programme und Dienste, die mit dem Ethereum-Netzwerk verbunden sind, erfordern Rechenleistung, Ausrüstung, Internetverbindungen und Wartung. Ether ist die Zahlung, die Benutzer den Netzwerkteilnehmern für die Ausführung ihrer angeforderten Operationen im Netzwerk geben. Der wesentliche Unterschied zu Bitcoin besteht in der Tatsache, dass das Ethereum Netzwerk programmierbar ist und somit auch dezentrale Anwendungen in seinem Netzwerk erstellt und bereitgestellt werden können.[20]

c) Anonyme Kryptowährungen: Monero, Zcash und Dash

Die Popularität von Monero (XMR) hat zugenommen, hauptsächlich aufgrund seiner Fähigkeit, Benutzer zu anonymisieren. Monero-Transaktionen sind schwieriger nachzuverfolgen, da sie Ringsignaturen und Stealth-Adressen verwenden. Diese Methoden helfen, die Identitäten des Absenders und des Empfängers zu verbergen. Darüber hinaus hilft Ring Confidential Transactions oder RingCT, den Transaktionsbetrag zu verbergen und sorgt für mehr Privatsphäre.[21]

Zcash (ZEC) definiert sich selbst als „Wenn Bitcoin wie http für Geld ist, ist Zcash https“, was seine verbesserten Sicherheits- und Datenschutzfunktionen unterstreicht. Zcash hat ein kryptografisches Tool namens Zero-Knowledge Proof implementiert und gewährt den Teilnehmern die Option, Transaktionen abzuschirmen. Es ermöglicht Nutzern, Transaktionen

[19] Bitpanda.
[20] Ethereum.
[21] SETH, Monero.

durchzuführen, ohne dass einer von ihnen seine Adressen an die anderen weitergibt. Zero-Knowledge-Proof verschleiert auch den Transaktionsbetrag.[22]

DASH wurde 2014 entwickelt und ist eine Kryptowährung, die es dem Benutzer ermöglicht, mit CoinJoin zu wählen, ob seine Transaktionen anonym und privat sind oder nicht. Die Eigenschaft funktioniert, indem sie die Herkunft ihrer Gelder verschleiert. Wenn sich Nutzer für die Verwendung der Funktion entscheiden, wird die Gebühr für die Transaktion leicht erhöht. DASH erreicht dies durch ein Mischprotokoll, das ein innovatives dezentrales Netzwerk von Servern verwendet, die als Master-Knoten bezeichnet werden. Eine weitere Funktion, die DASH bietet, ist Instant Send, das Transaktionen so schnell wie eine Kreditkarte verarbeiten kann.[23]

3. Aufbewahrungsmöglichkeiten des privaten Schlüssels (Private Key)

Das Eigentum an Bitcoin wird durch digitale Schlüssel, Bitcoin-Adressen und digitale Signaturen festgelegt. Die digitalen Schlüssel werden im Netzwerk nicht gespeichert, sondern erstellt und von Endbenutzern in einer Datei oder einer einfachen Datenbank gespeichert, die als Wallet bezeichnet wird. Die digitalen Schlüssel innerhalb des Wallets eines Benutzers sind völlig unabhängig vom Bitcoin-Protokoll und können von der Wallet-Software des Benutzers ohne Bezugnahme auf die Blockchain oder Internetzugang generiert und verwaltet werden. Schlüssel ermöglichen viele der inhärenten Eigenschaften von Bitcoin, darunter dezentralisiertes Vertrauen und Kontrolle, Eigentumsbescheinigung und das kryptografische Sicherungsmodell.[24]

Crypto-Assets bleiben permanent auf der Blockchain gespeichert und werden mittels Schlüsselpaaren ihren jeweiligen Nutzern zugeteilt. Ein Public Key ist öffentlich bekannt und funktioniert als Kontonummer. Der nicht öffentlich zugängliche Private Key dient der gültigen Signatur von Transaktionen. Daher ist eine sichere Aufbewahrung des privaten Schlüssels zentral, da dessen Kenntnis letztendlich die Verfügungsgewalt über die Crypto-Assets ermöglicht.[25]

Für die Speicherung des Private Keys stehen dem Nutzer verschiedene Möglichkeiten zur Verfügung. Der Speicherort eines privaten Schlüssels wird Wallet genannt. Die Wallet speichert, wie der oftmals fälschliche Vergleich mit einer physischen Geldbörse vermuten lässt,

[22] SETH, Zcash.
[23] SETH, DASH.
[24] ANTONOPOULOS, S. 63.
[25] ANTONOPOULOS, S. 63 f.

nicht die Crypto-Assets selbst, sondern den Private Key. Wallets lassen sich im Prinzip wie Schlüsselanhänger verstehen, die Paare von Private oder Public Keys enthalten. Nutzer signieren Transaktionen mit ihren Keys, wodurch sie nachweisen, dass sie die rechtmässigen Besitzer des Transaktionsresultats (der Bitcoins) sind. Es besteht auch die Option Multisignatur-Wallets einzurichten. Dies bedeutet, dass für eine autorisierte Transaktion mehr als eine Signatur bzw. mehr als ein privater Schlüssel benötigt wird.[26]

Grundsätzlich werden Wallets angeboten, die entweder von Dritten (sog. Custodial Wallets) oder vom Nutzer selbst (sog. Non-Custodial Wallets) verwahrt werden. Eine weitere Unterscheidung der Walletart erfolgt anhand dessen, ob sie eine Internetverbindung benötigt.[27] Nachfolgend wird näher auf die unterschiedlichen Aufbewahrungsmöglichkeiten von Private Keys eingegangen.

a) Hot Storage

Webbasierte Wallets, mobile Wallets und Desktop-Wallets können alle als typische Software-basierte Hot Wallets bezeichnet werden. Unter ihnen sind Web-Wallets am wenigsten sicher, obwohl alle Krypto-Hot-Wallets anfällig für Online-Angriffe sind, da sie eine ständige Internetverbindung haben. Ein Vorteil von Hot Wallets besteht in der Benutzerfreundlichkeit. Da sie immer online sind, müssen Nutzer nicht zwischen offline und online wechseln, um eine Krypto-Transaktion durchzuführen. Beispielsweise verwenden viele Menschen mobile Hot Wallets, um mit Kryptowährung zu handeln oder Einkäufe zu tätigen. Dies mit einer Cold Wallet umzusetzen, wäre unpraktisch. Der Nutzer müsste ein Gerät (z.B. einen Computer) finden, welches er mit der Cold Wallet verbinden kann, um dann die erforderliche Menge an Kryptowährung in eine Hot Wallet zu verschieben und letztendlich den Kauf zu tätigen. Benutzer, die große Mengen an Kryptowährung besitzen, bewahren normalerweise keine nennenswerten Mengen an Krypto in Hot Wallets auf. Die meisten angesehenen Börsen speichern den Großteil der Gelder ihrer Kunden offline in einer Matrix von Cold Wallets und bewahren dann einen bestimmten Betrag, der für Abhebungen benötigt wird, in Hot Wallets auf.[28]

b) Cold Storage

Im Allgemeinen sind Cold Storage Wallets ziemlich sicher. Das Stehlen aus einer Cold Wallet würde normalerweise den physischen Besitz oder Zugriff auf die Cold Wallet sowie alle zugehörigen PINs oder Passwörter erfordern, die für den Zugriff auf die Gelder verwendet

[26] ANTONOPOULOS, S. 84 ff.
[27] Appinventiv.
[28] Cryptopedia.

werden müssen. Die meisten Hardware Wallets sind Cold Wallets und leben auf Geräten, die wie ein kleiner bis mittelgroßer USB-Stick aussehen.[29] Es ist auch möglich, anstelle des gesamten hochsensiblen privaten Schlüssels einen sog. Seed-Key auszudrucken, der die Berechnung des privaten Schlüssels ermöglicht.[30] Paper-Wallets, physische Bitcoins oder ein sekundärer Offline-Computer, der zum Speichern von Kryptowährung verwendet wird, sind ebenfalls Cold-Storage-Wallet-Optionen.[31]

Hardware-Wallets sind so konzipiert, dass sie gegen Hackerangriffe immun sind. Selbst wenn eine Hardware-Wallet an Ihren Computer angeschlossen oder über Bluetooth verbunden ist, sind die auf dem Laufwerk gespeicherten Gelder je nach Speichermethode nur schwer oder gar nicht zu stehlen. Während Benutzer technisch mit dem Internet verbunden sind, erfolgt die Unterzeichnung von Transaktionen im Gerät und wird erst anschließend über die Internetverbindung des Computers an das Netzwerk gesendet. Mit dieser Signatur können Benutzer dem Empfänger einer Kryptowährungstransaktion das Eigentum zuweisen. Da die Private Keys das Gerät jedoch nie verlassen, wäre es selbst dann, wenn Malware auf dem Computer versucht, Geld zu stehlen, indem sie eine in der Hardware-Wallet initiierte Transaktion böswillig „signiert", nicht die richtige Signatur wäre, sodass die Transaktion nicht durchgeführt werden könnte.[32]

Eine weitere Art von Cold Storage ist die Mind/Brain Wallet. Wie der Name suggeriert, handelt es sich hierbei um einen im eigenen Gedächtnis «gespeicherten» Private Key oder einen Seed-Phrase, der entsprechend auch nur auf Basis der Erinnerung abgerufen werden kann. Ursprünglich war eine Brain Wallet eine hexadezimale Zeichenfolge. Mittlerweile können Brain Wallets als eine Folge von 12-24 Wörtern (oft als Mnemonik bezeichnet) gespeichert werden.[33]

c) Verwahrung durch einen Dritten

Ein Custodial Wallet ist definiert als ein Wallet, in dem die privaten Schlüssel von einem Dritten aufbewahrt werden. Das bedeutet, dass der Drittanbieter die volle Kontrolle über die Gelder hat, während der eigentliche Besitzer der Crypto Assets nur die Erlaubnis erteilen muss, Zahlungen zu senden oder zu empfangen. Die Anbieter von Custodial Wallets (Custodial

[29] Cryptopedia.
[30] SIMMLER ET AL., S. 967.
[31] Cryptopedia.
[32] Cryptopedia.
[33] Cryptopedia, Brain.

Wallet Provider) haben somit die Verfügungsgewalt über die Crypto-Assets.[34] Bekannte Anbieter von Custodial Wallets sind bspw. Free Wallet, Binance, BitMex oder Bitgo.[35]

B. Rechtliche Einordnung der Crypto-Assets

Eine Eingrenzung der Rechtsnatur von Kryptowährungen ist für viele Rechtsordnungen eine Herausforderung. Bisher hat keine ausdrückliche rechtliche Reglementierung von Crypto-Assets im Schweizer Recht stattgefunden. Allerdings ist gemäss dem Bundesrat nicht von einem «rechtsfreien Raum» auszugehen.[36]

Um die strafprozessuale Beschlagnahme von Kryptowährungen beurteilen zu können, ist die rechtliche Einordnung der Crypto-Assets unabdingbar. Denn nur nach einer Klärung, ob bspw. Bitcoin unter die vorhandenen Rechtsbegriffe subsumiert werden kann, ist die Anwendbarkeit von strafprozessualen Rechtsnormen überprüfbar.[37]

Für die strafprozessuale Beschlagnahme kommen nach dem Wortlaut von Art. 263 StPO Gegenstände und Vermögenswerte in Frage.

Aus diesem Grund wird nachfolgend die Rechtsnatur von Crypto-Assets (insb. Bitcoin) erforscht. Zuerst wird geprüft, ob Kryptowährungen unter die bestehenden Rechtsbegriffe Gegenstand und Sachen, Daten oder Vermögenswerte gefasst werden können. Anschliessend wird die Inhaberschaft der Crypto-Assets untersucht.

1. Einordnung von Crypto-Assets als Sachen, Daten oder Vermögenswerte

Crypto-Assets werden von der Europäischen Zentralbank als eine «digitale Repräsentation eines Wertes» beschrieben.[38] Der Bundesrat umschreibt Kryptowährungen als jeweils eine «virtuelle Währung» sowie eine «digitale Darstellung eines Wertes, welche im Internet handelbar» ist und über eine Geldersatzfunktion verfügt.[39]

a) Sachen

Als Erstes wird untersucht, ob Crypto-Assets unter den zivilrechtlichen Sachbegriff des Schweizer Rechts gefasst werden können. Im Strafrecht wird neben der des Sachbegriffs ebenfalls die Bezeichnung «Gegenstand» verwendet, welcher mit Sachen eng verknüpft ist.[40]

---

[34] FINMA, Fintech Entwicklung.
[35] Appinventiv.
[36] KGGT-Bericht 2018, S. 8; SIMMLER ET AL., S. 968; TSCHUDI, S. 46.
[37] SIMMLER ET AL., S. 968.
[38] European Central Bank, Analysis, S. 4; SIMMLER ET AL., S. 968.
[39] Bericht des Bundesrates, S. 7 f.; SIMMLER ET AL., S. 968.
[40] TSCHUDI, S. 46, 49.

Auch wenn sich im ZGB keine Legaldefinition des Sachbegriffs finden lässt, werden Sachen von der herrschenden Lehre als unpersönliche, körperliche, für sich bestehende Gegenstände, welche der menschlichen Herrschaft unterworfen werden können, aufgefasst. Aus diesem geltenden sachenrechtlichen Verständnis lässt sich ableiten, dass Crypto-Assets auf die Charakteristika der Unpersönlichkeit, Abgegrenztheit, Körperlichkeit sowie Beherrschbarkeit zu überprüfen sind – wobei der Sachbegriff als Funktionsbegriff zu verstehen ist. Entsprechend wird nach teleologischen Aspekten beurteilt, ob ein Objekt als Sache zu qualifizieren ist.[41]

- Unpersönlichkeit von Crypto-Assets

  Kryptowährungen lassen sich mühelos als vom «menschlichen Körper verschieden» definieren und dementsprechend bereitet die Prämisse der Unpersönlichkeit von Sachen i.S.d. ZGB keine Schwierigkeiten.[42]

- Abgegrenztheit

  Die Abgegrenztheit der Sache manifestiert sich darin, dass sie räumlich von anderen Sachen abgegrenzt werden kann und für sich selbst besteht.[43] Insbesondere bei Mengensachen kommt die Bedeutung der Funktionalität zum Ausdruck. So ist ein einzelnes Objekt, wie bspw. ein Getreidekorn, nicht automatisch als Sache i.S.d. ZGB zu definieren. Nur der verkehrsüblichen Menge (bspw. der Getreidesack), die eine wirtschaftliche Einheit bildet und als solche Gegenstand des Rechtsverkehrs ist, kommt die Sachqualität zu.[44]

  Die Einheiten von Crypto-Assets lassen sich klar voneinander abgrenzen und sind ebenfalls individuell definierbar. Zusätzlich ist eine wirtschaftliche Einheit gegeben, da sich z.B. bei einer Transaktion von Bitcoins diese immer auf andere Bitcoin-Einheiten auf der Blockchain beziehen.[45] Zusätzlich zur wirtschaftlichen Einheit ist aber ein gewisses Mass an Körperlichkeit unabdingbar.[46] Eine körperliche Abgegrenztheit hängt mit der Voraussetzung der Körperlichkeit eines Objekts zusammen. Daher wird die körperliche Abgegrenztheit von Crypto-Assets im nachfolgenden Abschnitt im Rahmen der vorausgesetzten Körperlichkeit bestimmt.[47]

- Körperlichkeit

[41] SEILER/SEILER, Rz. 19, S. 156; TUOR ET AL., § 88 N 2; BSK ZGB II-WOLF/WIEGAND, Vor Art. 641 ff. N 6.
[42] SEILER/SEILER, Rz. 21, S. 156.
[43] BSK ZGB II-WOLF/WIEGAND, Vor Art. 641 ff. N 7, 8; SEILER/SEILER, Rz. 22, S. 157.
[44] BSK ZGB II-WOLF/WIEGAND, Vor Art. 641 ff. N 9; SEILER/SEILER, Rz. 22, S. 157.
[45] SEILER/SEILER, Rz. 23, S. 157.
[46] BSK ZGB II-WOLF/WIEGAND, Vor Art. 641 ff. N 8, 9.
[47] SEILER/SEILER, Rz. 23, S. 157.

Die Körperlichkeit ist die wichtigste Voraussetzung für die Sachqualität. Diese ist in dem Fall zu bejahen, wenn es sich um einen greifbaren Gegenstand handelt.[48] Crypto-Assets verfügen nicht über dieses Charakteristikum. Deshalb besteht die stark überwiegende Auffassung, dass Kryptowährungen keine Sachqualität zukommt.[49] Konträr zum Kriterium der Körperlichkeit werden teilweise bestimmte unkörperliche Objekte vom Gesetzgeber explizit als Sachen definiert.[50] Zugleich wird Gegenständen, welchen formell eine Sachqualität zukommen könnte, diese nicht zugesprochen.[51] Dementsprechend darf die Körperlichkeit unter bestimmten Umständen nicht als ein zwingendes Kriterium für die Bestimmung eines Objekts als Sache i.S.d. ZGB erachtet werden. Der Voraussetzung der Beherrschbarkeit sollte in einem solchen Fall eine grössere Bedeutung zukommen.[52]

- Beherrschbarkeit

  Das Kriterium der Beherrschbarkeit ist erfüllt, wenn das fragliche Objekt mittels Erwerb oder Nutzung tatsächlich und rechtlich zulässig beherrscht werden kann.[53] So können unmöglich bspw. der Mond, Luft oder offenes Meer dem menschlichen Willen unterworfen werden.[54] Ebenfalls rechtlich nicht beherrschbar sind, vor allem aus ethischen Gründen, z.B. menschliche Körper(-teile).[55]

  Crypto-Assets erfüllen die Voraussetzung der Beherrschbarkeit, denn eine Transaktion ist nur durch das aktive Zutun des Inhabers der Kryptowährungseinheit möglich. Zudem ist eine gleichzeitige Nutzungsmöglichkeit verschiedener Personen, das sog. double-spending, unmöglich. Somit ist bei Crypto-Assets eine ausschliessliche Herrschaft des Inhabers über seine Währungseinheit gegeben.[56]

Dennoch plädiert ECKERT dafür, den Sachbegriff auf digitale Daten auszuweiten. Er führt den Begriff «res digitalis» ein und argumentiert, dass die Körperlichkeit keine gesetzliche Voraussetzung sei, wenn ausnahmsweise auch Unkörperliches wie Naturkräfte gemäss Art. 713 ZGB vom Sachenrecht erfasst werden.[57] Gegen eine solche Subsumtion von digitalen Daten

[48] SEILER/SEILER, Rz. 25, S. 158.
[49] SEILER/SEILER, Rz. 25, S. 158; SIMMLER ET AL., S. 968; TSCHUDI, S. 47.
[50] BSK ZGB II-WOLF/WIEGAND, Vor Art. 641 ff. N 6, 13a; SEILER/SEILER, Rz. 26, S. 158; TSCHUDI, S. 47.
[51] BSK ZGB II-WOLF/WIEGAND, Vor Art. 641 ff. N 6, 16.
[52] SEILER/SEILER, Rz. 27, Fn. 73, S. 159.
[53] BSK ZGB II-WOLF/WIEGAND, Vor Art. 641 ff. N 11-13; SEILER/SEILER, Rz. 28, S. 159.
[54] BSK ZGB II-WOLF/WIEGAND, Vor Art. 641 ff. N 12.
[55] BSK ZGB II-WOLF/WIEGAND, Vor Art. 641 ff. N 13.
[56] SEILER/SEILER, Rz. 29, S. 159-160.
[57] ECKERT, S. 248 f.

unter den Sachbegriff spricht sich die h.L. aufgrund der fehlenden Körperlichkeit aus, da die Ausnahmen gesetzlich geregelt sind.[58]

Folglich können virtuelle Währungen nicht unter den Sachbegriff subsumiert werden, da ihnen die zentrale Körperlichkeit fehlt, wie sie für Sachen vorausgesetzt wird, und keine ausdrückliche gesetzliche Bestimmung vorhanden ist, die ihnen eine Sachqualität zusprechen würde.[59]

b) Daten

Aus der technischen Perspektive betrachtet stellen Crypto-Assets digitale Informationen dar, die auf der Blockchain gespeichert sind; daher ist ebenfalls zu untersuchen, ob sie vom Datenbegriff erfasst werden können und welche rechtlichen Konsequenzen sich daraus ergeben würden.[60] Zunächst ist zu überprüfen, wie Daten in der schweizerischen Rechtsordnung einzuordnen sind, da diese im Beschlagnahmeartikel der Strafprozessordnung nicht ausdrücklich erwähnt werden.[61]

Grundsätzlich wird der Datenbegriff sehr weit gefasst. Charakteristisch ist, dass es sich um digitale oder analoge Informationen handelt, was technisch betrachtet auf Crypto-Assets zutrifft.[62] Jedoch behandelt das Gesetz nicht alle Daten gleich und schützt die unterschiedlichen Daten auf jeweils andere Art, wobei nicht jede digitale Information geschützt sein muss. STENGEL/AUS DER AU schlussfolgern in ihrer Untersuchung, dass Public als auch Private Keys als Personendaten i.S.d. Datenschutzgesetzes definiert werden können, da sie Rückschlüsse auf die Nutzer ermöglichen können.[63]

ECKERT definiert Daten wie folgt: «Digitale Daten sind in einem Binärcode codierte und gespeicherte, maschinenlesbare Informationen.»[64] Er ergänzt, dass je nach Dateninhalt andere Rechte von diesen verkörpert werden.[65] Diese Definition lässt eine Klassifizierung der Crypto-Assets als digitale Daten zu, jedoch hilft diese nicht bzgl. der Definition ihrer Rechtsnatur.[66]

---

[58] BÄRTSCHI/MEISSER, S. 141; BSK ZGB II-WOLF/WIEGAND, Vor Art. 641 ff. N 6, 19 a-d; GLESS ET AL., S. 90; TSCHUDI, S. 47 f.; VON DER CRONE/KESSLER/ANGSTMANN, S. 339 f.; WEBER/THOUVENIN, S. 49.
[59] GLESS, Strafrechtsschutz für virtuelles Geld, S. 49; HAUSER-SPÜHLER/MEISSER, S. 9; SIMMLER ET AL., S. 968; TSCHUDI, S. 48.
[60] TSCHUDI, S. 52.
[61] Art. 263 Abs. 1 StPO; SIMMLER ET AL., S. 972.
[62] TSCHUDI, S. 52.
[63] STENGEL/AUS DER AU, S. 444-446; TSCHUDI, S. 53.
[64] ECKERT, S. 247.
[65] ECKERT, S. 247; TSCHUDI, S. 53.
[66] TSCHUDI, S. 53.

In der Lehre wird diskutiert, ob der Gegenstandsbegriff weiter ausgelegt werden könnte, um Daten beschlagnahmen zu können. Dies ist für diese Arbeit von Interesse, da die strafprozessuale Beschlagnahme wortwörtlich Gegenstände und Vermögenswerte beinhaltet, jedoch Daten nicht erwähnt. Im Kap. III. A. 3. erfolgt eine Auseinandersetzung mit dieser Diskussion.

c) Vermögenswerte

Zuletzt ist zu prüfen, ob Crypto-Assets wie Bitcoin unter den Begriff der Vermögenswerte in der Schweizer Rechtsordnung subsumiert werden können.

Nach der zivil- sowie öffentlich-rechtlicher Definition lassen sich alle einer Person zustehenden Sachen und Rechte unter den Vermögensbegriff fassen.[67] Im Strafrecht bestimmt der juristische Vermögensbegriff ausschliesslich die Gesamtheit der Vermögensrechte und -pflichten einer Person als Vermögen, die von den zivil- und öffentlich-rechtlichen Zuteilungsordnungen zugerechnet werden kann. Diese Vermögensdefinition würde Kryptowährungen nicht beinhalten, da Bitcoins weder eine eigentumsfähige Sache noch ein gesetzlich zugewiesenes Recht darstellen.[68] Eine rein wirtschaftliche Definition wäre hingegen zu unspezifisch und würde eine rechtliche Güterzuordnung nicht ermöglichen.[69]

Heute wird nach stark überwiegender Auffassung und Rechtsprechung der Vermögensbegriff juristisch-wirtschaftlich im Strafrecht definiert. Dies bedeutet, dass das Vermögen die Summe der rechtlich geschützten wirtschaftlichen Werte umfasst, die einer Person von Rechts wegen zustehen.[70] NIGGLI konkretisiert, dass im Strafrecht unter Vermögenswerte jeder konkrete spezifische Vermögensbestandteil gefasst werden muss.[71] Das Ideal zu dem, was als geldwertes Gut angesehen werden kann, lässt sich demnach vor allem durch den jeweiligen Marktwert des Guts oder Rechts bestimmen; wobei allerdings auch ein etwaiger Tauschwert massgebend sein kann – dieser ist bilateral-subjektiv zwischen den Parteien zu bestimmen.[72]

Einzig bleibt zu klären, ob Crypto-Assets auch rechtlich geschützte und keine missbilligten Vermögenswerte darstellen. In der Schweizer Rechtsordnung lassen sich derzeit keine expliziten Gesetze zu Kryptowährungen finden. Allerdings werden Crypto-Assets alles andere als verboten. Die fehlenden Rechtsnormen hängen viel eher mit der Neuartigkeit der

[67] TSCHUDI, S. 54.
[68] GLESS ET AL., S. 91.
[69] BSK StGB-NIGGLI/RIEDO, Vor Art. 137 N 20; GLESS ET AL., S. 91; TSCHUDI, S. 56.
[70] BSK StGB-NIGGLI/RIEDO, Vor Art. 137 N 20; GLESS ET AL., S. 91.
[71] BSK StGB-NIGGLI/RIEDO, Vor Art. 137 N 62.
[72] BSK StGB-NIGGLI/RIEDO, Vor Art. 137 N 21; GLESS ET AL., S. 91.

kryptobasierten Vermögenswerte zusammen, denn bereits heute ist eine zukünftige Gesetzgebung zu Crypto-Assets geplant. Von einer Missbilligung kann keinesfalls ausgegangen werden, wenn selbst Schweizer Behörden Bitcoins als Zahlungsmittel für bestimmte Gebühren akzeptieren.[73]

Zusammenfassend stellen Kryptowährungen zwar keinen herkömmlichen, jedoch aber einen durchaus tolerierten Vermögenswert in der Schweiz dar und können unter den juristisch-wirtschaftlichen Vermögensbegriff des Strafrechts gefasst werden.[74]

2. Inhaberschaft

Wenn Crypto-Assets als Vermögenswerte definiert werden, ist zu klären, wie diese vermögensrechtlich einer Person zugeordnet werden können. Das Besondere an Kryptowährungen ist, dass sie zum Vermögen einer Person gehören, obwohl kein Recht an den Crypto-Assets besteht.[75]

Wie im Rahmen der Funktionsweise von Kryptowährungen erläutert, kann nur die Person über die Crypto-Assets verfügen, die Kenntnis des Private Keys hat. Denn der Besitz des privaten Schlüssels stellt die technische Voraussetzung für Transaktionen dar. Somit ermöglicht die Kenntnis des Private Keys, schuldrechtliche Beziehungen einzugehen, indem Güter oder Dienstleistungen mit Crypto-Assets erworben werden. Dies lässt die Schlussfolgerung zu, dass derjenigen Person die Kryptowährungen vermögensrechtlich zuzuordnen sind, die Kenntnis des Private Keys hat. Diese Person ist der entsprechende Inhaber der kryptographischen Vermögenswerte.[76]

Der Inhaber der Crypto-Assets ist aber nicht immer gleichzeitig die wirtschaftlich berechtigte Person. Beispielsweise werden kryptobasierte Vermögenswerte bzw. die entsprechenden Private Keys häufig nicht durch die jeweiligen Nutzer verwahrt, sondern verbleiben in der Obhut eines Custodial Wallet Providers. Bei einer solchen Drittverwahrung hat die wirtschaftlich berechtigte Person einen obligatorischen Anspruch gegen die Drittperson.[77]

[73] BR-Bericht DLT/Blockchain, S. 12; TSCHUDI, S. 58.
[74] BR-Bericht DLT/Blockchain, S. 139; BR-Bericht virtuelle Währungen, S. 26; GLESS ET AL., S. 91 f.; KGGT-Bericht 2018, S. 31; SCHÄR/SIMMLER, S. 410 f.; TSCHUDI, S. 58.
[75] TSCHUDI, S. 59; ZOGG, S. 5.
[76] GLESS ET AL., S. 92; RÜCKERT, S. 296; TSCHUDI, S. 59.
[77] TSCHUDI, S. 30 f.; ZOGG, S. 3.

C. Kriminalpolitische Relevanz der Crypto-Assets

Crypto-Assets geniessen bereits seit Längerem den zweifelhaften Ruf, als Zahlungsvehikel für Kriminelle zu dienen. In der Vergangenheit wurden immer wieder Fälle bekannt, in welchen die spezielle Funktionsweise und pseudoanonyme Natur solcher Währungen ausgenutzt wurde, um illegale, strafrechtlich relevante Handlungen auszuführen. Als prominentestes Beispiel lässt sich dazu sicher die mittlerweile geschlossene Schwarzmarktplattform «Silk Road» nennen. Diese diente mehrheitlich als globaler Umschlagplatz für illegale Güter (z.B. Drogen oder Kinderpornographie), welche zur Verschleierung der Geschäfte ausschliesslich mit Kryptowährungen bezahlt werden konnten.[78] Obwohl bzw. gerade weil dieser Fall mittlerweile nur als einer von vielen angesehen werden kann, lässt sich festhalten, dass Währungen wie Bitcoin inzwischen zum favorisierten Zahlungsmittel im sogenannten Darknet aufgestiegen sind. In solchen Schattenwirtschaften haben sich diese Zahlungsmittel besonders aufgrund der mit ihnen verbundenen Pseudoanonymität sowie der sich daraus ergebenen, erschwerten strafrechtlichen Verfolgbarkeit etablieren können. Crypto-Assets eröffnen Kriminellen neue Möglichkeiten jenseits des Rechts zu agieren.[79]

Neben der Verwendung von Crypto-Assets als Zahlungsmittel für illegale Aktivitäten, hat sich in den letzten Jahren jedoch auch noch ein zusätzlicher Straftatbestand ergeben, welcher vor allem auf die Popularität und den folglich rasanten Wertzuwachs unterschiedlicher Kryptowährungen (besonders Bitcoin) zurückzuführen ist. Dabei handelt es sich zumeist um Hacking und den versuchten Diebstahl von Crypto-Assets, bei dem zumeist Handelsplätze oder Wallet-Betreiber attackiert werden – quasi eine moderne (virtuelle) Version des Bankraubs.[80]

Darüber hinaus hat sich besonders in jüngerer Vergangenheit ein weiterer Bereich herauskristallisiert, welcher die strafrechtliche Relevanz von Crypto-Assets in einem weiteren Straftatbestand hervorhebt. Das hochaktuelle Beispiel der Online Crypto-Handelsplattform «FTX» zeigt in erschreckender Weise, wie leicht betrügerische Handlungen über solche Plattformen abgewickelt werden können. Aufgrund der komplexen Materie und Funktionsweise von Crypto-Assets war es dem Gründer Sam Bankman-Fried gelungen, seinen Wissensvorsprung gegenüber sowohl seinen Kunden als auch den Aufsichtsbehörden auszunutzen, um unrechtmässig Bitcoin umzuleiten und sich selbst anzueignen.[81] Dieser Fall

[78] TZANETAKIS, S. 41 f.
[79] HOSTETTLER, S. 10 f.
[80] SIMMLER ET AL., S. 966.
[81] NZZ, FTX.

zeigt zudem auf anschauliche Weise, dass selbst grossen und professionellen Plattformen kein Blankoscheck für Vertrauen ausgestellt werden kann.

Die o.g. Beispiele zeigen deutlich, dass Straftaten in Verbindung mit Crypto-Assets in unserer Gesellschaft angekommen sind. Trotzdem stehen Strafverfolgungsbehörden weltweit vor neuen Problemen, welche die Ahndung etwaiger Delikte mit Beteiligung von Crypto-Assets erschweren. Vor allem das Fehlen einer zentralen, staatlichen Kontrollinstanz ermöglicht Kriminellen, Kryptowährungen für Straftaten zu verwenden, während die Chancen einer strafrechtlichen Verfolgung vergleichsweise gering sind. Dies ist grösstenteils auf die schon vorher angedeutete «Pseudoanonymität» von Crypto-Assets zurückzuführen. Zwar ist das Blockchain Protokoll, welches die Basis aller Kryptowährungen bildet, öffentlich einsehbar, jedoch kann jeder Nutzer eine unendlich grosse Anzahl an unabhängigen Schlüsseln generieren, wobei diese sogenannten Public Keys auch nicht direkt mit der Identität des eigentlichen Besitzers in Verbindung gebracht werden können.[82] Strafverfolgungsbehörden stehen entsprechend vor einer nie dagewesenen Herausforderung, in welcher sie neue Wege einschlagen müssen und teilweise sogar auf die Kooperation von Beschuldigten angewiesen sind (z.B. in Bezug auf die Entschlüsselung einer Crypto-Wallet wie in Kap. V. B. 1) beschrieben, um Straftaten aufzuklären. Zusätzlich ergeben sich jedoch aus der öffentlichen Einsehbarkeit der Blockchain neue Möglichkeiten für Strafverfolgungsbehörden. Besonders der Aspekt der Nachvollziehbarkeit und Herkunft illegaler Vermögenswerte lässt sich im Rahmer neuer Technologien leichter umsetzen. Durch bspw. Data Mining können unterschiedliche Datenbanken miteinander verknüpft und Daten in der Blockchain potenziell de-anonymisiert werden; wobei die Abwesenheit einer zentralen/staatlichen Kontrollinstanz auch in solchen Fällen die Verfolgung kompliziert gestaltet.[83]

III. Grundlagen der Beschlagnahme als Zwangsmassnahme (Art. 263 ff. StPO)

A. Allgemein

1. Zweck und Wesen

Die Beschlagnahme stellt eine Zwangsmassnahme dar und bezweckt die Sicherstellung von Gegenständen und Vermögenswerten einer beschuldigten Person oder Dritten im Rahmen eines

[82] SIMMLER ET AL., S. 965 f.
[83] SIMMLER ET AL., S. 965 f.

Strafprozesses.[84] Die rechtlichen Besitz- sowie Eigentumsverhältnisse bleiben durch eine Beschlagnahme unberührt, lediglich die freie Verfügungsgewalt bzw. -befugnis über die beschlagnahmten Objekte wird der betroffenen Person entzogen und an den Staat überführt.[85]

2. Betroffene Personen

Beschlagnahmt werden können Gegenstände und Vermögenswerte von der beschuldigten Person als auch einer Drittperson. Jedoch ist bei Dritten ein höheres Mass an Zurückhaltung geboten, da diese Massnahme in die Grundrechte einer nicht beschuldigten Person eingreift, wie im Art. 197 Abs. 2 geregelt. Zu den Betroffenen einer Beschlagnahme gehören indes keine Behörden.[86]

3. Objekte

Das Gesetz erfasst in Art. 263 Abs. 1 StPO Gegenstände und Vermögenswerte als zwei mögliche Beschlagnahmeobjekte.

Ob Daten allenfalls bei einer grosszügigen Auslegung des Gegenstandsbegriffs vom Beschlagnahmerecht erfasst werden, wird kontrovers diskutiert.

Im schweizerischen Strafrecht wird abgesehen vom Sachbegriff der Begriff des Gegenstandes erwähnt. So auch im Zusammenhang mit der Beschlagnahme in Art. 263 Abs. 1 StPO. Grundsätzlich können als Gegenstände Objekte aufgefasst werden, «die nicht aufgrund ihrer ursprünglichen Beschaffenheit beweistauglich sind, sondern in ihrer Funktion als Träger von Informationen».[87] Nach der gängigen Rechtsprechung als auch stark überwiegender Auffassung qualifizieren sich ausschliesslich körperliche Sachen als Gegenstände i.S.d. Strafrechts.[88] Die herrschende Ansicht ist, dass Daten nur insoweit in Frage kommen, solange sie greifbar sind. Das bedeutet, dass bspw. Computerspeicherplatten oder USB-Sticks mit ihren gespeicherten Daten als Beschlagnahmeobjekte in Frage kommen.[89]

Die Autoren BANGERTER, HEIMGARTNER und SCHMID hingegen befürworten eine Ausweitung des Gegenstandbegriffs auch auf immaterielle Objekte.[90] Insbesondere ist die Argumentation von BANGERTER überzeugend, dass die Norm nur aus historischer Interpretation auf

[84] HEIMGARTNER, StPO-Kommentar, Art. 263 N 1, 1a.
[85] BSK StPO-BOMMER/GOLDSCHMID, Vor Art. 263-268 N 1.
[86] BSK StPO-BOMMER/GOLDSCHMID, Vor Art. 263-268 N 3.
[87] BSK StPO-BOMMER/GOLDSCHMID, Art. 263 N 26 f.; SIMMLER ET AL., S. 971.
[88] AEPPLI, S. 59; BGE 126 I 50 E. 4.c; BOMMER, S. 178 f.PK StGB-TRECHSEL/CRAMERI, Vor Art. 137 N 1; STRATENWERTH/BOMMER, AT II, § 12 N 85; TSCHUDI, S. 49.
[89] HEIMGARTNER, StPO-Kommentar, Art. 263 N 1a; HEIMGARTNER, S. 87; SIMMLER ET AL., S. 971.
[90] BANGERTER, S. 246 ff.; HEIMGARTNER, Beschlagnahme, S. 89; SCHMID, S. 96, 106.

körperliche Objekte anwendbar ist und entsprechend einer modernen Auffassung die Ausweitung auf unkörperliche Objekte notwendig ist. Zudem würde bei einer Beschränkung des Gegenstandbegriffs auf körperliche Objekte aus systematischen Überlegungen im Widerspruch zu Art. 246 StPO stehen.[91] Diese Norm hält fest: «Schriftstücke, Ton-, Bild- und andere Aufzeichnungen, Datenträger sowie Anlagen zur Verarbeitung und Speicherung von Informationen dürfen durchsucht werden, wenn zu vermuten ist, dass sich darin Informationen befinden, die der Beschlagnahme unterliegen.»[92] Konsequenterweise müssen die gespeicherten Informationen bzw. digitalen Daten als Gegenstände beschlagnahmefähig sein.[93] Gegen eine solche weite Interpretation des Gegenstandsbegriffs argumentieren AEPPLI, BOMMER, RYSER als auch das Bundesgericht in einem älteren Leitentscheid.[94]

Der Begriff «Gegenstände» wird im Zusammenhang mit der Beschlagnahme zu Einziehungszwecken in Art. 69 Abs. 1 StGB über die Sicherungseinziehung ausgeführt. Zusammengefasst bezieht sich der Begriff auf gefährliche Gegenstände. Welche Beschlagnahmeobjekte unter den Begriff der «Vermögenswerte» fallen, wird wiederum durch die Regelung zur Einziehung von Vermögenswerten in Art. 70 Abs. 1 StGB konkretisiert.[95] Im Kapitel III. B. 2. a) zu den Beschlagnahmearten wird eine detailliertere Bestimmung der jeweiligen Objekte vorgenommen.

B. Voraussetzungen der Beschlagnahme

1. Allgemein aus Art. 197 StPO

Die Beschlagnahme stellt eine Zwangsmassnahme i.S.v. Art. 196 lit. a und b StPO dar und muss die in Art. 197 StPO festgelegten Grundsätze für Zwangsmassnahmen erfüllen. Dies bedeutet, dass eine gesetzliche Grundlage (Art. 197 lit. a StPO), ein hinreichender Tatverdacht (Art. 197 lit. b StPO) und Verhältnismässigkeit (Art. 197 lit. c und d StPO) im Allgemeinen für eine gerechtfertigte Beschlagnahme erforderlich sind.[96]

Als gesetzliche Grundlage dient ein formelles Gesetz, wobei bspw. eine Verordnung bei leichterem Grundrechtseingriff genügt. Damit besteht ein numerus clausus der

[91] BANGERTER, S. 246 ff.
[92] Art. 246 StPO.
[93] BANGERTER, S. 246 ff.
[94] AEPPLI, S. 59; BGE 126 I 50 E. 4c, S. 58 f; BOMMER, S. 178 f.
[95] BSK StPO-BOMMER/GOLDSCHMID, Vor Art. 263-268 N 7.
[96] BSK StPO-BOMMER/GOLDSCHMID, Vor Art. 263-268 N 9-11; SCHMID/JOSITSCH, Praxiskommentar StPO, Art. 197 N 1.

Zwangsmassnahmen. Die Beschlagnahme findet ihre gesetzliche Grundlage in den Art. 263 ff. StPO.[97]

Ein hinreichender Tatverdacht bedeutet, dass grundsätzlich von der Begehung einer Straftat ausgegangen werden muss. Der benötigte Verdachtsgrad hängt von der Eingriffsart sowie Dauer der Zwangsmassnahme ab, somit ist nicht zwingend vorausgesetzt, dass noch kein konkreter Tatverdächtiger vorhanden sein.[98]

Zudem greift die Behörde mit der Anordnung einer Zwangsmassnahme in die Grundrechte der betroffenen Person ein. Die resultierende Grundrechtseinschränkung muss den Verhältnismässigkeitsanforderungen von Art. 36 BV entsprechen.[99]

2. Materiell

Zusätzlich zu den allgemeinen Voraussetzungen der Zwangsmassnahmen müssen beschlagnahmte Gegenstände und Vermögenswerte im Verlauf des Strafprozesses wahrscheinlich zu einem in Art. 263 Abs. 1 lit. a-d StPO aufgelisteten Zweck eingesetzt werden. Die Anforderungen an die Wahrscheinlichkeit der Verwendung der Objekte nehmen im Verlauf des Strafverfahrens zu.[100]

Die Beschlagnahme kann aus prozessualen oder materiellen Gründen unzulässig sein. Dies kann bspw. bei der Vermögenseinziehungsbeschlagnahme der Fall sein, wenn die Einziehung verjährt ist (Art. 70 Abs. 3 StGB). Zudem kann ein Beschlagnahmeverbot aufgrund der Herkunft oder des Inhalts der Gegenstände bestehen, wenn die in Art. 264 StPO normierten Ausnahmen zutreffen.[101]

a) Beschlagnahmearten

Der Gesetzgeber unterscheidet in Art. 263 Abs. 1 StPO zwischen den folgenden Beschlagnahmearten: Beweismittelbeschlagnahme (lit. a), Kostendeckungsbeschlagnahme (lit. b), Restitutionsbeschlagnahme (lit. c) und Einziehungsbeschlagnahme (lit. d). Die Arten der Beschlagnahme lassen sich systematisch zwei Grundmustern zuordnen: Die Beschlagnahme zu Beweiszwecken und die Beschlagnahme zu Einziehungszwecken. Die Kostendeckungsbeschlagnahme wird von BOMMER/GOLDSCHMID als systematischer Fremdkörper bezeichnet und separat betrachtet.[102] In Anlehnung an diese Einteilung wird

[97] BSK StPO-BOMMER/GOLDSCHMID, Vor Art. 263-268 N 14; BSK StPO-WEBER, Art. 197 N 4.
[98] BSK StPO-WEBER, Art. 197 N 6, 8.
[99] BSK StPO-BOMMER/GOLDSCHMID, Vor Art. 263-268 N 11.
[100] BGer 1B_157/2007 E. 2.2.; HEIMGARTNER, StPO-Kommentar, Art. 263 N 12 f.
[101] BSK StPO-BOMMER/GOLDSCHMID, Art. 264 N 1; HEIMGARTNER, StPO-Kommentar, Art. 263 N 14.
[102] BSK StPO-BOMMER/GOLDSCHMID, Vor Art. 263-268 N 4.

vorliegend zunächst die Beschlagnahmeform der Beweismittelbeschlagnahme, anschliessend die Beschlagnahme zu Einziehungszwecken (inkl. Restitutionsbeschlagnahme) und zuletzt die Kostendeckungsbeschlagnahme definiert.

(1) Beschlagnahme zu Beweiszwecken (Art. 263 Abs. 1 lit. a)

Die Beweismittelbeschlagnahme (auch sog. Individualbeschlagnahme) dient dazu, entscheidwesentliche Objekte als Beweismittel zu beschaffen. Die Voraussetzungen hierfür sind, dass die Beschlagnahme während eines laufenden Strafverfahrens erfolgt, kein Beschlagnahmeverbot vorliegt sowie die Relevanz des zu beschlagnahmenden Objekts für den Entscheid.[103] Das BGer entschied, dass sich hierfür körperliche Gegenstände als Beschlagnahmeobjekt eignen.[104] Die Körperlichkeit von digitalen Information kann jedoch bspw. mittels Kopien oder Ausdrucken erreicht werden und somit eignen sie sich ebenfalls als Beweismittelbeschlagnahmeobjekte.[105] Eine verschriftlichte Form wird aber bei Cloud Computing basierten Walletlösungen kaum möglich sein, da sie nicht Teil einer Hardware oder IT-Infrastruktur des Nutzers sind.[106]

(2) Beschlagnahme zu Einziehungszwecken (Art. 263 Abs. 1 lit. c und d StPO)

Die Beschlagnahme zu Einziehungszwecken richtet sich materiell grundsätzlich nach den Vorgaben in Art. 69 und 70 ff. StGB.[107]

Für zu beschlagnahmende Gegenstände, die später potenziell einer Einziehung unterliegen, sind die materiellen Grundlagen in den Bestimmungen zur Sicherungseinziehung in Art. 69 StGB zu finden. Die Beschlagnahme von Vermögenswerten knüpft an die Vorgaben zur Vermögenseinziehung nach Art. 70 ff. StGB an.[108] Die Beschlagnahme von Gegenständen oder Vermögenswerten, die der geschädigten Person zurückgegeben werden sollen, folgt materiell den Vorgaben in Art. 70 Abs. 1 und Art. 73 Abs. 1 lit. b StGB.

(a) Sicherungseinziehungsbeschlagnahme

Vorgaben zum Umfang der Beschlagnahme im Rahmen einer Sicherungseinziehung lassen sich in Art. 69 StGB finden und werden im Folgenden betrachtet.[109]

---

[103] BSK StPO-BOMMER/GOLDSCHMID, Vor Art. 263-268 N 5; SIMMLER ET AL., S. 970.
[104] BGE 126 I 50 E. 4c; gl.M.: AEPLI, S. 44 ff., 59; KELLER, StPO-Kommentar, Art. 246 N 6; RYSER, S. 561.
[105] SIMMLER ET AL., S. 970-973; Vgl. BGE 143 IV 270.
[106] Anh. 3: Interview KILCHENMANN/STEIGER, Frage 5.2; Anh. 4: Interview WALDER, Frage 7.1, 7.2; Vgl. BGE 143 IV 270.
[107] BSK StPO-BOMMER/GOLDSCHMID, Vor Art. 263-268 N 6; TSCHUDI, S. 85.
[108] BSK StPO-BOMMER/GOLDSCHMID, Art. 263 N 32.
[109] BSK StPO-BOMMER/GOLDSCHMID, Art. 263 N 36.

Art. 69 Abs. 1 StGB über die Sicherungseinziehung legt fest, dass Gegenstände der Einziehung unterliegen, wenn diese zur Begehung einer Straftat gedient haben oder bestimmt waren oder sie durch eine Straftat hervorgebracht worden sind, sofern diese Gegenstände die Sicherheit von Menschen, die Sittlichkeit oder die öffentliche Ordnung gefährden. Das Gericht verfügt die Einziehung ohne Rücksicht auf die Strafbarkeit einer bestimmten Person.

Die Sicherungseinziehung ist auf gefährliche Gegenstände beschränkt, die über einen Zusammenhang zu einer Straftat verfügen. Folglich bezweckt diese Einziehungsart den Schutz der Polizeigüter und verhindert die Gefährdung der Allgemeinheit.[110]

Diese Einziehungsart stellt nach der gängigen Lehre und Rechtsprechung eine sachliche Massnahme ohne repressiven Charakter dar. Dies bedeutet, dass sich die Sicherungseinziehung nicht gegen eine Person, sondern gegen die einzuziehende Sache allein richtet.[111]

(b) Vermögenseinziehungsbeschlagnahme

Die Sicherheitseinziehungsbeschlagnahme kann klar von der Vermögenseinziehungsbeschlagnahme abgegrenzt werden. Während die Beschlagnahme zum Zweck der Sicherheitseinziehung dazu dient, eine potenzielle zukünftige Rechtsgutgefährdung zu verhindern, verfolgt die Vermögenseinziehungsbeschlagnahme das Ziel, dass sich Straftaten nicht finanziell rentieren.[112]

Im Hinblick auf eine Vermögenseinziehung gemäss Art. 70 Abs. 1 StGB sind Löhne als auch Erlöse aus Delikten geeignete Objekte. Ebenfalls geeignete Beschlagnahmeobjekte zu Einziehungszwecken stellen nicht nur die direkt aus Straftaten stammenden Erlöse in Form von Vermögenswerten und Gegenständen, sondern auch deren Surrogate dar.[113] Zur Problematik der Vermögenseinziehungsbeschlagnahme von Surrogaten siehe Kap. V. E. 1. Somit kann unter den Vermögensbegriff alles gefasst werden, was im Rahmen eines Rechtsgeschäfts «Tausch gegen Geld» verwendet wird.[114]

(c) Restitutionsbeschlagnahme

Die Restitutionsbeschlagnahme folgt denselben Vorgaben wie die Vermögenseinziehungsbeschlagnahme. Der Unterschied besteht ausschliesslich darin, dass die

---

[110] PK StGB-TRECHSEL/JEAN-RICHARD, Art. 69 N 5; BSK StGB-BAUMANN, Art. 69 N 2.
[111] BGer 6B_659/2010 E. 5.1; BSK StGB-BAUMANN, Art. 69 N 3; a.M. KV-KO THOMMEN, Art. 69 StGB N 68 ff.
[112] KV-KO SCHOLL, Art. 70 StGB N 99.
[113] BSK StGB-BAUMANN, Art. 70/71 N 47.
[114] BSK StGB-BAUMANN, Art. 70/71 N 43; BSK StGB-MAEDER/NIGGLI, Art. 146 N 24 ff; BSK StGB-NIGGLI/RIEDO, Vor Art. 137 N 21 f.; TSCHUDI, S. 79 f.

beschlagnahmten Werte nicht dem Staat zukommen, sondern einer geschädigten Person.[115] Zudem hat die Restitution wie in Art. 70 Abs. 1 StGB gegenüber einer Einziehung zu Gunsten des Staats Vorrang.[116]

Eine Restitution wird bisher nur im Rahmen der Vermögenseinziehung in Art. 70 Abs. 1 festgeschrieben und in den Normen zur Sicherungseinziehung nicht erwähnt. Dennoch ist eine Beschlagnahme zum Zweck der Restitution bei Gegenständen, die einer Sicherungseinziehung unterliegen, nicht auszuschliessen. Es ist vorstellbar, dass der zu beschlagnehmende Gegenstand nur in der Verfügungsmacht des Täters aber nicht des Eigentümers gefährlich ist.[117]

Bei der Einziehungsbeschlagnahme ist somit stets zu prüfen, ob ein Verletzter ein Anrecht auf die Wiederherstellung des rechtmässigen Zustands hat und dementsprechend die beschlagnahmten Gegenstände oder Vermögenswerte am Ende des Verfahrens an den Geschädigten auszuhändigen sind. Doch zum Anordnungszeitpunkt der Beschlagnahme muss noch nicht bekannt sein, ob es sich um ein opferloses Delikt handelt. Entscheidend ist, dass im Beschlagnahmebefehl eindeutig ist, ob mutmassliche, unrechtmässige deliktische Vermögensvorteile abgeschöpft werden sollen und somit die Absicht der Beschlagnahme im Rahmen der Vermögenseinziehung als auch Restitution gleich sind.[118]

(3) Beschlagnahme zu Kostendeckungszwecken (Art. 263 Abs. 1 lit. b)

Die Kostendeckungsbeschlagnahme fällt systematisch betrachtet aus der Reihe der Beschlagnahmearten von Art. 263 ff. StPO, da die beschlagnahmefähigen Objekte keinen Deliktskonnex aufweisen müssen. Insofern dient diese Massnahme lediglich dazu, voraussichtliche Verfahrenskosten (Art. 268 Abs. 1 lit. a) und Entschädigungen sowie Geldstrafen und Bussen (Art. 268 Abs. 1 lit. b) zu sichern.[119] Dementsprechend kommen nur verwertbare Objekte für die Beschlagnahme in Frage.[120]

Aufgrund des nicht vorausgesetzten Deliktskonnex kann diese als Sicherungsmittel auch neben anderen Arten der Beschlagnahme angeordnet werden, wenn die andere Beschlagnahmeart zur Kostendeckung nicht ausreicht. Ebenfalls kann die Kostendeckungsbeschlagnahme eingesetzt werden, wenn andere Beschlagnahmeformen nicht ergriffen werden können.[121]

---

[115] BSK StPO-BOMMER/GOLDSCHMID, Art. 263 N 49.
[116] BSK StPO-BOMMER/GOLDSCHMID, Vor Art. 263-268 N 6; TSCHUDI, S. 85.
[117] BSK StGB-BAUMANN, Art. 70/71 N 15; BSK StPO-BOMMER/GOLDSCHMID, Art. 263 N 52.
[118] BSK StPO-BOMMER/GOLDSCHMID, Art. 263 N 50, 52.
[119] BSK StPO-BOMMER/GOLDSCHMID, Art. 268 N 1.
[120] BSK StPO-BOMMER/GOLDSCHMID, Vor Art. 263-268 N 7.
[121] BSK StPO-BOMMER/GOLDSCHMID, Art. 268 N 1.

3. Formell

In Art. 263 Abs. 2 StPO werden die Formalien der Beschlagnahme festgelegt. Im Normalfall bedarf es einer zeitnahen Eröffnung eines Strafverfahrens oder eines selbständigen Einziehungsverfahrens (Art. 377 Abs. 1 StPO) sowie eines Beschlagnahmebefehls.[122]

Für die Anordnung des Beschlagnahmebefehls sind laut Art. 198 Abs. 1 lit. a und b die Staatsanwaltschaft und das Gericht funktional zuständig. Der Beschlagnahmebefehl sollte folgende Punkte beinhalten: Ausführungen zur Anschuldigung und der Beweislage bzw. dem Tatverdacht; Deliktskonnex des zu beschlagnahmenden Objekts (ausser bei Ersatzforderungs- und Kostendeckungsbeschlagnahme); Beschlagnahmeart; entsprechende Gesetzesartikel.[123]

Sollte in dringenden Fällen ein schriftlicher Befehl nicht möglich sein und stattdessen mündlich bspw. telefonisch mitgeteilt werden, so muss unverzüglich eine nachträgliche schriftliche Bestätigung des Beschlagnahmebefehls vorgenommen werden.[124]

IV. Eignung der Crypto-Assets als Beschlagnahmeobjekt

Nach den vorliegenden Ausführungen sind aus der technischen Perspektive Crypto-Assets digitale Informationen, die einen Vermögenswert beinhalten. Rechtlich betrachtet lassen sie sich unter den juristisch-wirtschaftlichen Vermögensbegriff fassen.

Damit Kryptowährungen grundsätzlich als Objekte der Beweismittelbeschlagnahme sein können, müssen sie als relevantes Beweismittel dienen können. Die Funktionsweise der blockchainbasierten Crypto-Assets wie Bitcoin lässt die Annahme zu, dass Kryptowährungen durchaus beweisrelevant aufgrund der Tatsache sein können, dass jede Transaktion in der Blockchain gespeichert und somit rückverfolgbar bleibt. Dementsprechend können Blockchaineinträge für Strafverfolgungsbehörden von grossem Interesse sein, um bspw. die deliktische Herkunft von Crypto-Assets zu belegen.[125] Da die Beweismittelbeschlagnahme wie im Kap. III. B. 2. a) (1) beschrieben bei Cloud Computing beschränkt ist, wäre eine weite Auslegung der Norm auch auf nicht fassbare Daten sinnvoll, damit die Beschlagnahme von höchstwahrscheinlich beweisrelevanten Crypto-Assets von den Strafverfolgungsbehörden getroffen werden darf. SIMMLER ET AL. zweifeln jedoch an der Vereinbarkeit einer grosszügigeren Interpretation des Gegenstandbegriffs mit der hohen Anforderung an das

[122] HEIMGARTNER, StPO-Kommentar, Art. 263 N 22; a.M. BSK StPO-BOMMER/GOLDSCHMID, Art. 263 N 11, sie setzen ein laufendes Strafverfahren voraus.
[123] HEIMGARTNER, StPO-Kommentar, Art. 263 N 23 f.
[124] HEIMGARTNER, StPO-Kommentar, Art. 263 N 25.
[125] SIMMLER ET AL., S. 966, 972; Vgl. Kap. II. C.

Bestimmtheitsgebot von Zwangsmassnahmen.[126] Dies würde dazu führen, dass ausschliesslich Crypto-Assets als Beweismittelbeschlagnahmeobjekte in Frage kämen, deren zugehörige Private Keys auf einer körperlichen Wallet gespeichert wären.[127]Aufgrund der unklaren Rechtslage und dem nicht zufriedenstellenden Untersuchungsergebnis wäre eine Konkretisierung der Beschlagnahmenorm vom Gesetzgeber angezeigt, damit nicht greifbare Daten eindeutig unter den Gegenstandsbegriff gefasst werden könnten und entsprechend Crypto-Assets unabhängig der Wallet-Art zu Beweiszwecken beschlagnahmefähig wären.[128]

Die Anwendung der Sicherheitseinziehungsbeschlagnahme auf Crypto-Assets ist fraglich, da eine Rechtsgutgefährdung sowie eine zukünftige Gefahr für die öffentliche Sicherheit, Sittlichkeit und Ordnung ausgehend von Kryptowährungen zweifelhaft erscheint. Zudem richtet sich die Beschlagnahme bei einer Sicherheitseinziehung gegen gefährliche Gegenstände. Wie bereits bei der rechtlichen Einordnung der Crypto-Assets festgestellt, sind diese als unkörperliche Vermögenswerte zu qualifizieren. Dadurch ist höchstens eine indirekte Gefahr durch Kryptowährungen für die erwähnten Rechtsgüter denkbar, indem sie der Veranlassung einer Gefährdung dienen (bspw. Anstiftung eines Täters durch Zahlung einer Summe in Kryptowährungen). Folglich stellen Crypto-Assets kein geeignetes Beschlagnahmeobjekt im Rahmen einer Sicherheitseinziehung dar.[129]

Nachdem feststeht, dass sich Crypto-Assets für eine Beschlagnahme zum Zweck der Sicherheitseinziehung nicht eignen, ist noch zu prüfen, ob sie ein taugliches Objekt der Vermögenseinziehungsbeschlagnahme darstellen.

In dieser Arbeit wurde dargelegt, dass Crypto-Assets als Vermögenswerte in der Schweizer Rechtsordnung aufgefasst werden können. Wie im Kapitel zur Vermögenseinziehungsbeschlagnahme erläutert, wird der Vermögenswertbegriff weit gefasst. Wie einleitend beschrieben, werden Crypto-Assets für Internetkäufe verwendet oder im Kanton Zug zur Gebührentilgung akzeptiert.[130] Da Kryptowährungen immer breiter akzeptierte Zahlungsmittel darstellen, können sie unter den neo-juristischen Vermögensbegriff von NIGGLI gefasst werden. Dementsprechend stellen sie ein taugliches Beschlagnahmeobjekt zum Zweck der Vermögenseinziehung dar.[131]

[126] SIMMLER ET AL., S. 972.
[127] SIMMLER ET AL., 972.
[128] SIMMLER, S. 966, 978.
[129] SIMMLER ET AL., S. 970 f ; TSCHUDI, S. 68, 75.
[130] Zug.
[131] SIMMLER ET AL., S. 973; TSCHUDI, S. 79 f.

Entsprechend müssen Crypto-Assets ebenfalls ein Objekt der Restitutionsbeschlagnahme sein können, wenn ein Geschädigter vorhanden ist, was bspw. bei Krypto-Betrugsfällen erfüllt ist.[132]

Ebenfalls ist die Beschlagnahme von Kryptowährungen zum Zweck der Kostendeckung zu bejahen. Da kein Deliktskonnex notwendig ist, erscheint eine solche Beschlagnahme nur dann sinnvoll, wenn keine anderen geeigneten Kostendeckungsbeschlagnahmeobjekte vorliegen, da Crypto-Assets hohen Kursschwankungen unterliegen.[133]

Schlussfolgernd kann die Beschlagnahmefähigkeit von Crypto-Assets eindeutig zum Zweck der Vermögenseinziehung, Restitution sowie grundsätzlich der Kostendeckung bejaht werden.

V. Durchführung der Beschlagnahme und Probleme der Strafverfolgung in der Praxis

A. Gesetzliche Bestimmungen zur Durchführung der Beschlagnahme

In der schweizerischen Strafprozessordnung regelt der Art. 266 StPO die Durchführung der Beschlagnahme. Wenn die Beschlagnahme der Gegenstände resp. Vermögenswerte durchgeführt wird, so wird dem bisherigen Inhaber die Verfügungsgewalt über diese Objekte bis zum Endentscheid über deren strafprozessuales Schicksal entzogen.[134] In der Regel werden bei der Durchführung die beschlagnahmten Gegenstände oder Vermögenswerte amtlich verwahrt. Zunächst muss hierfür der Aufbewahrungsort der infrage stehenden Objekte ermittelt und diese müssen anschliessend sichergestellt werden. Die tatsächliche Sicherstellung erfolgt mittels einer Edition bzw. einer Durchsuchungsmassnahme. Die Anordnung dieser strafprozessualen Zwangsmassnahmen kann bereits zusammen mit dem Beschlagnahmebefehl verfügt werden, sofern die zu beschlagnahmenden Objekte individualisiert sind.[135]

Nach Art. 266 Abs. 1 StPO wird mit der Übergabe des Beschlagnahmebefehls oder einer separaten Quittung der betroffenen Person bestätigt, dass die Verfügungsmacht über die beschlagnahmten Objekte an den Staat übertragen wurde. Zusätzlich hat die anordnende Strafbehörde ein Vollzugsprotokoll bzw. ein Verzeichnis der beschlagnahmten Gegenstände resp. Vermögenswerte gemäss Art. 266 Abs. 2 StPO zu erstellen. Dieses dient dazu, die Überprüfbarkeit der Vollständigkeit der beschlagnahmten Objekte zu gewährleisten. Laut Abs.

[132] SIMMLER ET AL., S. 973 ; TSCHUDI, S. 86.
[133] Anh. 1: Interview BURGERMEISTER, Frage 2.1; SIMMLER ET AL., S. 971, 973.
[134] BSK StPO-BOMMER/GOLDSCHMID, Art. 266 N 1.
[135] HEIMGARTNER, StPO-Kommentar, Art. 266 N 1; TSCHUDI, S. 118.

2 obliegt der Strafverfolgungsbehörde weiter eine sachgemässe Aufbewahrung der betroffenen Gegenstände und Vermögenswerte.[136]

Die Art und Weise der Durchführung hängt jeweils vom Beschlagnahmeobjekt ab. Die Überführung in die staatliche Hoheit erfolgt bei beweglichen Sachen durch eine physische Entziehung.[137] Mittels einer Grundbuchsperre werden Liegenschaften nach Art. 266 Abs. 3 StPO i.V.m. Art. 56 lit. a GBV beschlagnahmt. Bei Forderungen erfolgt die Beschlagnahme, indem sie gegenüber dem Gläubiger verfügt wird und dem Schuldner ein Beschlagnahmebefehl mit der Erklärung zugestellt wird, dass die Zahlung an den Gläubiger die Schuld nicht tilgt.[138] Im Fall von zu beschlagnahmenden Bankguthaben wird eine Kontosperre verfügt und die Bank angewiesen, keine Bezüge oder Überweisungen durch den Inhaber oder Drittpersonen zuzulassen oder selbst solche vorzunehmen.[139]

Nachfolgend soll beleuchtet werden, auf welche Art und Weise Crypto-Assets erfolgreich beschlagnahmt werden können.

B. Relevanz des Private Key für die Beschlagnahme

Ziel der Beschlagnahme von Crypto-Assets ist, diese der staatlichen Verfügungsgewalt zu unterwerfen. Wie im Kapitel zur Funktionsweise der Kryptowährungen erläutert, ist die Kenntnis des privaten Schlüssels notwendig, um die Verfügungsmacht über Kryptowährungen zu erlangen. Dies liegt an der kryptographischen Komponente, dass ein entsprechender Private Key für die Autorisation einer Übertragung von Kryptowährungen notwendig ist, indem die Transaktionsnachricht passend signiert wird.[140] Folglich muss die Strafbehörde Kenntnis des privaten Schlüssels erhalten, damit die Beschlagnahme der Crypto-Assets überhaupt durchführbar wird.[141]

1. Zugang zur Wallet

Die erforderliche Kenntnis des Private Keys für die Beschlagnahme von Kryptowährungen bedeutet, dass die Strafverfolgungsbehörde sich Zugang zum Speicher- bzw. Aufbewahrungsort des privaten Schlüssels verschaffen muss. Für die Speicherung dienen Wallets, wie in Kap. II. A. 3. erklärt. Um sich den Zugang zur entsprechenden Wallet zu

[136] BSK StPO-BOMMER/GOLDSCHMID, Art. 266 N 5, 7 f.; HEIMGARTNER, StPO-Kommentar, Art. 266 N 3.
[137] BSK StPO-BOMMER/GOLDSCHMID, Vor Art. 263-268 N 8; BSK StPO-BOMMER/GOLDSCHMID, Art. 266 N 1; SIMMLER ET AL., S. 974.
[138] Art. 266 Abs. 4 StPO; BSK StPO-BOMMER/GOLDSCHMID, Art. 266 N 8; HEIMGARTNER, StPO-Kommentar, Art. 266 N 6; SIMMLER ET AL., S. 974.
[139] BSK StPO-BOMMER/GOLDSCHMID, Art. 266 N 15; TSCHUDI, S. 119.
[140] TSCHUDI, S. 120.
[141] MOLO/DRZALIC, S. 47 f.; SIMMLER ET AL, S. 974; TSCHUDI, S. 120.

verschaffen, muss die Strafverfolgungsbehörde in einem ersten Schritt diese beschlagnahmen.[142]

Für eine erfolgreiche Beschlagnahme der Wallet bedarf es in der Regel vorgängig zusätzlicher strafprozessualer Zwangsmassnahmen. Nachfolgend werden die Probleme in der Praxis bzgl. des Zugangs zur Wallet für die Strafverfolgungsbehörden ersichtlich.[143]

a) Zugang zur Paper Wallet

Wie anfangs dieser Arbeit erläutert, gehört die Paper Wallet zu den Cold Storages und stellt eine Speichermöglichkeit des Private Keys ohne Internetanbindung dar. In diesem Fall muss der Strafverfolgungsbehörde die Beschlagnahme des analogen Speichermediums im Rahmen einer Hausdurchsuchung und nachfolgend mittels einer Durchsuchung von Aufzeichnungen gelingen. Falls der Beschuldigte die Aufzeichnungen hat siegeln lassen, muss vor deren Durchsuchung ein Entsiegelungsgesuch gestellt werden. Die Chancen die Paper Wallet mit dem Private Key zu finden und letztendlich den Zugang zu den zu beschlagnahmenden Crypto-Assets zu erhalten, stehen vergleichsweise gut.[144] Geheime Zwangsmassnahmen können bei Hardware, Software und Paper Wallet bei unbekanntem Aufbewahrungsort von den Strafverfolgungsbehörden in Erwägung gezogen werden.[145]

b) Zugang zur Hardware Wallet

Eine weitere Speicherung des privaten Schlüssels ohne eine Verbindung zum Internet kann in Form einer Hardware Wallet erfolgen. Um an die Hardware selbst zu gelangen, kann die Strafverfolgungsbehörde ähnlich wie bei der Paper Wallet eine Hausdurchsuchung sowie anschliessend die Durchsuchung von Aufzeichnungen anordnen. Letztere ist essenziell, denn häufig ist der Zugang zu den Hardware-Informationen nur mittels eines Passworts oder eines PIN-Codes möglich.[146]

c) Zugang zur Mind Wallet

Eine grössere Herausforderung stellt für die Strafverfolgungsbehörden eine dritte Cold Storage Variante dar: die Mind Wallet. Sollte sich der Beschuldigte seinen privaten Schlüssel lediglich gemerkt haben, ohne diesen anderweitig aufzubewahren, ist die Strafverfolgungsbehörde auf die Kooperation der betroffenen Person angewiesen. In der Praxis ist die Bedeutung der

---

[142] SIMMLER/SELMAN/BURGERMEISTER, S. 975.
[143] TSCHUDI, S. 120.
[144] Anh. 1: Interview BURGERMEISTER, Frage 2.3; Anh. 2: Interview MEIER/MEYER, Frage 1.2 ; TSCHUDI, S. 120 f.
[145] TSCHUDI, S. 123 f.
[146] TSCHUDI, S. 121.

Kooperationswilligkeit von Tatverdächtigen allerdings nicht zu unterschätzen. Wichtig anzumerken ist, dass jegliche erzwungene Kooperation der beschuldigten Person widerrechtlich ist. Die Strafverfolgungsbehörden müssen den strafprozessualen Grundsatz nemo tenetur achten.[147]

d) Zugang zur Software Wallet

Die häufigste Anwendung der online Speicherung des Private Keys und damit mit einer Internetverbindung ist die Software Wallet. Wie bereits erläutert, handelt es sich bei der Wallet um eine Software, welche den privaten Schlüssel speichert und der Nutzer bspw. über sein Mobiltelefon oder Computerdesktop darauf zugreifen kann. Die Strafverfolgungsbehörden stehen wie bei der Paper und Hardware Wallet vor der Herausforderung, das Gerät ausfindig zu machen, auf welchem sich das Computerprogramm befindet. Nach einer erfolgten Beschlagnahme des entsprechenden Geräts kann der Zugang zur Software Wallet wiederum mittels eines PIN-Codes oder Passworts erschwert werden. Der Hauptunterschied zur Hardware Wallet besteht aber darin, dass sich dank der Verbindung zum Internet den staatlichen Behörden mehr Optionen in der Zugangsbeschaffung präsentieren. Mit Hilfe von EDV-Spezialisten wäre ein hacken der Software Wallet seitens der Strafverfolgungsbehörden denkbar. Dieser Vorgang wäre theoretisch mit der GovWare möglich, jedoch ist der Einsatz dieser Software im Gesetz ausschliesslich auf die Überwachung des Fernmeldeverkehrs beschränkt. Vereinzelt wird in der Literatur eine Erweiterung der zulässigen Anwendung der GovWare diskutiert. Dies ist aus zwei Gründen abzulehnen: einerseits aufgrund von rechtsstaatlichen Bedenken und andererseits würden mittels der Verwendung der GovWare die Durchsuchungs- sowie Hausdurchsuchungsvorschriften umgegangen, was widerrechtlich ist.[148] Damit stellt die Verwendung einer Software Wallet die Strafverfolgungsbehörden vor grosse Schwierigkeiten bei mangelnder Kooperation der betroffenen Person.[149]

e) Zugang bei Verwahrung des Private Key durch einen Dritten

Eine weitere mögliche Speicherungskonstellation ist, dass wie in Kap. II A. 3. c) erläutert, ein Dritter die Kryptowährung verwahrt und der Beschuldigte seine privaten Schlüssel nicht kontrolliert. Die beschuldigte Person steht lediglich über einen obligatorischen Auszahlungsanspruch seiner Crypto-Assets gegen den Dritten. Dementsprechend kann die Strafverfolgungsbehörde die kryptobasierten Vermögenswerte nicht direkt beschlagnahmen,

[147] Anh. 1: Interview BURGERMEISTER, Frage 2.3; Anh. 4: Interview WALDER, Frage 7.9; TSCHUDI, S. 124; Vgl. Art. 6 Ziff. 1 EMRK.
[148] TSCHUDI, S. 122 f.
[149] Anh. 1: Interview BURGERMEISTER, Frage 6.1; Anh. 4: Interview WALDER, Frage 1.3.

sondern muss die Forderung gegenüber der Tauschbörse oder dem Wallet-Anbieter mit Beschlag belegen.[150] Wenn Dritte den Private Key verwahren bleibt die Strafverfolgungsbehörde von den Schwierigkeiten verschont, die mit der Lokalisation der Wallet und dem Wallet-Zugang verbunden sind. Allerdings wird in dieser Konstellation die Beschlagnahme auf andere Arten erschwert. Zum einen kann die Schweizer Strafverfolgungsbehörde dem Dritten die Beschlagnahme der Forderung nur direkt mitteilen, wenn sich diese Person im Inland befindet.[151] Die wenigsten Wallet-Provider und Exchanger befinden sich in der Schweiz und zwingen die Schweizer Strafverfolgungsbehörden auf den Weg der internationalen Rechtshilfe auszuweichen.[152]

2. Herausgabepflicht des Private Key

Grundsätzlich ist gemäss Art. 265 Abs. 1 StPO der Inhaber verpflichtet, Gegenstände und Vermögenswerte, die beschlagnahmt werden sollen, herauszugeben. Ausgenommen von der Herausgabepflicht sind Personen, denen aus bestimmten Gründen keine aktiven Mitwirkungspflichten zukommen.[153] Bei der Beschlagnahme von Crypto-Assets könnte eine Herausgabepflicht des Private Keys die Arbeit der Strafverfolgungsbehörden aufgrund der obigen Schilderungen erleichtern. Nachfolgend soll jeweils die Herausgabepflicht der tatverdächtigen Person sowie einer Drittperson wie bspw. eines Wallet-Anbieters betrachtet werden.

a) Pflicht zur Herausgabe des Beschuldigten

Der Beschuldigte gehört zu den privilegierten Personen, die nach Art. 265 Abs. 2 lit. a von der Herausgabepflicht explizit ausgenommen sind. Diese Ausnahme lässt sich auf den Grundsatz «nemo tenetur» zurückführen, welcher besagt, dass sich niemand selbst belasten muss und dadurch den Beschuldigten keine Pflicht trifft, Objekte herauszugeben, die als etwaige Beweismittel dienen können.[154]

Dies bedeutet für die Beschlagnahme von Crypto-Assets, dass der Täter nicht zur Herausgabe seiner Kryptowährungen verpflichtet ist, sofern diese seiner Straftat entstammen. Da die

[150] TSCHUDI, S. 124 f.
[151] TSCHUDI, S.125.
[152] Anh. 1: Interview BURGERMEISTER, Frage 2.3; Anh. 3: Interview KILCHENMANN/STEIGER, Frage 1.3; Anh. 4: Interview WALDER, Frage 1.1, 1.2; TSCHUDI, S. 125.
[153] HEIMGARTNER, StPO-Kommentar, Art. 265 N 5.
[154] HEIMGARTNER, StPO-Kommentar, Art. 265 N 6; Vgl. Art. 6 Ziff. 1 EMRK.

erfolgreiche Beschlagnahme in diesem Fall die Kenntnis des Private Keys bedingt, darf dementsprechend der Beschuldigte nicht gezwungen werden, diesen preiszugeben.[155]

Eventuell könnte, wie von MOLO/BRUNONE ausgeführt, eine Untersuchungshaft gemäss Art. 220 ff. StPO der beschuldigten Person bei mangelnder Kooperation Anwendung finden. Als Gründe für eine Anordnung der Untersuchungshaft führen sie eine mögliche Fluchtgefahr oder Kollusionsgefahr nach Art. 221 Abs. 1 lit. a und b StPO auf, da ohne die Kenntnis des Private Keys die tatverdächtige Person ihre Crypto-Assets unterschlagen oder ins Ausland fliehen kann. Richtigerweise fügen die Autoren an, dass die Untersuchungshaft unter keinen Umständen als Druckmittel verwendet werden darf.[156]

Aus den Interviews mit den Strafverfolgungsbehörden wurde bisher keine Untersuchungshaft in diesem Zusammenhang erwähnt und der «nemo tenetur» Grundsatz betont.[157]

b) Pflicht zur Herausgabe Dritter

Schliesslich ist zu prüfen, ob eine Herausgabepflicht besteht, wenn eine Drittperson Inhaberin der zu beschlagnahmenden Crypto-Assets ist. Nach dem Gesetz sind Dritte von der Herausgabepflicht nur ausnahmsweise in den Fällen befreit, wenn sie vom Aussage- oder Zeugnisverweigerungsrecht Gebrauch machen können.[158]

Bei Crypto-Assets sind zwei Szenarien denkbar, in welchen ein Dritter Inhaber der betroffenen Vermögenswerte ist. Ein möglicher Fall sieht vor, dass der Straftäter die zu beschlagnahmenden Kryptowährungen in der Zwischenzeit an einen Dritten transferiert hat. Des Weiteren ist denkbar, dass der Beschuldigte seine Crypto-Assets durch eine Drittperson wie z.B. einen Wallet-Provider oder Exchanger verwahren lässt.[159]

In der ersten Konstellation ist zu prüfen, ob der Dritte das Guthaben in Unkenntnis des Beschlagnahmegrundes gekauft und eine gleichwertige Gegenleistung erbracht hat. Zusätzlich ist abzuwägen, ob die Beschlagnahme für diese Drittperson eine unverhältnismässige Härte darstellen würde. Zudem muss die Drittperson ein dingliches Recht oder eine ähnliche Rechtsposition erworben haben. Sollten diese Tatsachen zutreffen, so liegt ein Drittenprivileg vor, welches eine Beschlagnahme der Crypto-Assets ausschliessen würde. Sollte hingegen kein

[155] MOLO/BRUNONE, S. 304; SIMMLER ET AL., S. 976; TSCHUDI, S. 126.
[156] MOLO/BRUNONE, S. 304; Vgl. Art. 113 StPO, Art. 6 Ziff. 1 EMRK.
[157] Anh. 1: Interview BURGERMEISTER, Frage 2.3; Anh. 4: Interview WALDER, Frage 7.9; Vgl. Art. 113 StPO, Art. 6 Ziff. 1 EMRK.
[158] HEIMGARTNER, StPO-Kommentar, Art. 265 N 7; BSK StPO-BOMMER/GOLDSCHMID, Art. 265 N 4.
[159] TSCHUDI, S. 127.

Drittenprivileg nachweisbar sein, unterliegen die Crypto-Assets dementsprechend der Beschlagnahme und die Drittperson ist nicht von der Herausgabepflicht befreit.[160]

Im zweiten Fall sind der Zeitpunkt der Drittverwahrung als auch die (Un-)Kenntnis des deliktischen Ursprungs der Crypto-Assets entscheidend. Einerseits konnte die beschuldigte Person ihre Kryptowährungen nach der Straftat an einen Dritten (bspw. ein Wallet-Anbieter, eine Tauschbörse) zur Verwahrung übertragen, dann verhält sich der Fall wie im ersten, obigen Szenario: Der Beschuldigte hat eine Forderung gegenüber der unwissenden Drittperson als Gegenleistung für den Transfer der Crypto-Assets erhalten, somit stellt dies eine Gegenleistung im Sinne des Drittenprivilegs dar. Folglich ist eine Beschlagnahmemöglichkeit des kryptographischen Guthabens beim Dritten zu verneinen.[161]

Andererseits konnte der Beschuldigte seine Crypto-Assets von Anfang an drittverwahren lassen. In einem solchen Fall verfügt die beschuldigte Person ebenso über eine Forderung gegenüber der Drittperson, jedoch wurde der Beschuldigte nie eigentlicher Inhaber der Kryptowährungen, sondern nur die wirtschaftlich berechtigte Person an den zu beschlagnahmenden Crypto-Assets. Dementsprechend stellt die Forderung gegenüber der Drittperson den zu beschlagnahmenden Wert dar.[162]

3. Strafrechtliche Folgen einer Zuwiderhandlung gegen die Beschlagnahme

Die Zuwiderhandlung gegen die strafprozessuale Beschlagnahme ist gemäss Art. 289 StGB und Art. 292 StGB durchaus strafbar. Die erstgenannte Norm findet Anwendung auf Fälle, in welchen die betroffene Person gegen eine Beschlagnahmeanordnung agiert.[163] Diese Straftat ist bei Crypto-Assets denkbar, wenn der Beschuldigte über die mit Beschlag belegten Vermögenswerte weiterhin verfügen würde.[164] Die zweite Gesetzesbestimmung findet auf Drittpersonen Anwendung. Dritte können sich ebenfalls strafbar machen, wenn sie sich ihrer Herausgabepflicht der zu beschlagnahmenden Objekte widersetzen.[165]

4. Rechtshilfe zur Erlangung des Private Key

Grundsätzlich bestimmt sich die Zuständigkeit Schweizer Strafverfolgungsbehörden nach dem Territorialitäts- sowie Ubiquitätsprinzip. Die Handlungsbefugnis von Schweizer

[160] TSCHUDI, S. 127.
[161] TSCHUDI, S. 127.
[162] TSCHUDI, S. 127.
[163] BSK StPO-BOMMER/GOLDSCHMID, Art. 265 N 28; BSK StGB-HAGENSTEIN, Art. 289 N 3 ff.; TSCHUDI, S. 128 f.
[164] TSCHUDI, S. 128.
[165] BSK StPO-BOMMER/GOLDSCHMID, Art. 265 N 28; TSCHUDI, S. 129.

Strafverfolgungsbehörden ist basierend auf dem ersten Prinzip auf das Hoheitsgebiet der Schweiz beschränkt. Das zweite Prinzip besagt jedoch, dass die Schweizer Behörde auch zuständig sein kann, wenn entweder der Handlungs- oder Erfolgsort die Schweiz ist.[166]

Bisher muss die Behörde, wenn keine besonderen Verträge mit anderen Staaten bestehen, über die Internationale Rechtshilfe in Strafsachen nach den Bestimmungen des IRSG eine Beschlagnahme ersuchen, wenn nicht fassbare Informationen im Ausland gespeichert sind.[167]

Die Schweiz ist Vertragsstaat des Übereinkommens über die Cyberkriminalität.[168] Die Art. 29 ff. dieser Konvention sehen vor, dass auf das Rechtshilfeersuchen einer Vertragspartei hin gespeicherte Computerdaten sichergestellt werden können. Dementsprechend kann die Schweizer Strafverfolgungsbehörde gestützt auf dieses Übereinkommen ein entsprechendes Rechtshilfeersuchen formulieren, wenn sie einen Private Key nicht selbst sicherstellen kann, weil sich dieser auf einer Hardware oder Software Wallet im Ausland befindet.[169] Dank dieses Übereinkommens haben Strafverfolgungsbehörden in der Schweiz die Möglichkeit Wallet Provider in Vertragsstaaten direkt anzufragen, ob sie auf die entsprechenden Daten zugreifen dürfen.[170]

Wie WALDER und STEIGER/KILCHENMANN beschreiben entwickelt sich allmählich das Zugriffsprinzip zum Standardvorgehen für die Behörde, um an digitale Informationen zu gelangen.[171] Dies ist vor allem deshalb von Bedeutung, da viele Wallet Provider ihre Daten auf Rechnern in Ländern gespeichert haben, die keine Vertragsparteien des CCC sind und zudem kaum Rechtshilfe leisten.[172]

C. Übertragung auf eine staatliche Wallet

Wie bereits im Kapitel zum Zweck und Wesen der Beschlagnahme erläutert, muss sichergestellt werden, dass der Beschuldigte über keine Verfügungsmacht über den zu beschlagnehmenden Gegenstand oder Vermögenswert verfügt. Die Herrschaft über die beschlagnahmten Werte soll entsprechend bei der Strafverfolgungsbehörde liegen. Dabei soll die Beschlagnahme die vorbestehenden Eigentums- sowie Inhaberverhältnisse unberührt lassen. Zudem ist die

[166] Art. 3-8 StGB; TSCHUDI, S. 93 f.
[167] TSCHUDI, S. 100 f.; Vgl. BGE 143 IV 270.
[168] Europarat, Who are the Parties to the Budapest Convention?.
[169] SIMMLER ET AL., S. 967.
[170] BURGERMEISTER/BROGER, S. 19; Art. 32 CCC; Vgl. BGE 141 IV 108.
[171] Anh. 3: Interview KILCHENMANN/STEIGER, Frage 5.2; Anh. 4: Interview WALDER, Frage 7.1, 7.2; Vgl. BGE 143 IV 270.
[172] Anh. 1: Interview BURGERMEISTER, Frage 7.1; Anh. 3: Interview KILCHENMANN/STEIGER, Frage 1.1, 1.2, 1.3; Anh. 4: Interview WALDER, Frage 7.1.

Strafbehörde gemäss Art. 266 Abs. 2 dazu verpflichtet, eine sachgemässe Aufbewahrung der beschlagnahmten Gegenstände und Vermögenswerte sicherzustellen. Dies bedeutet, dass die betroffenen Gegenstände in ihrem Wert aufgrund der Lagerung nicht vermindert werden, Beschädigung und Verlust ebenfalls zu vermeiden sind.[173] Die Anlage beschlagnahmter Vermögenswerte wird vom Bundesrat in einer Verordnung gestützt auf Art. 266 Abs. 6 StPO konkretisiert und zwar sollen beschlagnahmte Vermögenswerte möglichst sicher, werterhaltend und Ertrag-bringend angelegt werden.[174]

Bei Crypto-Assets besteht die Problematik, dass die beschuldigte Person oftmals über mehrere Kopien des privaten Schlüssels verfügt, die sich auf den Strafverfolgungsbehörden unbekannten Speicherorten befinden. Daher reichen die Beschlagnahme einer Wallet und die Kenntnis des Private Keys alleine nicht aus, um gewährleisten zu können, dass dem Staat die alleinige Verfügungsmacht über die Kryptowährungen zukommt. Deshalb erweist sich die Einrichtung einer staatlichen Wallet als essenziell, um die beschlagnahmten Crypto-Assets auf diese zu übertragen, damit die beschuldigte Person oder eine Drittperson die beschlagnahmten Kryptowährungen nicht mit Hilfe den Strafverfolgungsbehörden unbekannten Kopien des privaten Schlüssels weitertransferieren kann. Auf diese Weise kann sichergestellt werden, dass die Verfügungsgewalt über die beschlagnahmten Kryptowährungen tatsächlich dem Tatverdächtigen entzogen wurde und dem Staat zukommt.[175]

Natürlich wird so dem Grundsatz der unveränderten Eigentums- oder Inhaberverhältnisse nicht nachgekommen. Jedoch lässt sich das Vorgehen bei Crypto-Assets mittels einer teleologischen Interpretation der Beschlagnahmeregelungen rechtfertigen. Denn für eine sachgemässe Aufbewahrung müssen die Strafverfolgungsbehörden selbst geeignete Möglichkeiten ausfindig machen und die Regelung des Bundesrats zur Anlage von beschlagnahmten Vermögenswerten setzt in bestimmten Fällen eine Übertragung von Vermögenswerten voraus. Zusätzlich ist die faktische Verfügung nur mittels eines Transfers der Crypto-Assets auf eine staatliche Wallet zu brechen und somit der Zweck der Beschlagnahme erreichbar.[176]

In der Praxis hat sich bereits in einigen Schweizer Kantonen die Methode der Übertragung von Crypto-Assets auf eine staatseigene Wallet etabliert. Die Wallets werden entweder selbst von

[173] BSK StPO-BOMMER/GOLDSCHMID, Art. 266 N 7a.
[174] SIMMLER ET AL., S. 974; Verordnung vom 3. Dezember 2010 über die Anlage beschlagnahmter Vermögenswerte (SR 312.057).
[175] SIMMLER ET AL., S. 974-976.
[176] SIMMLER ET AL., S. 974-975; Verordnung vom 3. Dezember 2010 über die Anlage beschlagnahmter Vermögenswerte (SR 312.057).

den Behörden oder von Dritten verwaltet.[177] Bei der Selbstverwaltung werden Hardware Wallets bevorzugt.[178] Dies bedeutet einen Mehraufwand für die Polizei oder Staatsanwaltschaft. So muss gewährleistet werden, dass einerseits die zugehörige Software auf dem neusten Stand ist und andererseits, dass das erforderliche Wissen vorhanden ist, um bspw. bei einem Systemzusammenbruch die Wallet wiederherstellen zu können.[179] Die verwendeten Hardware Wallets ermöglichen es den Strafverfolgungsbehörden auf verschiedene Kryptowährungen vorbereitet zu sein bzw. mehrere Adressen zu besitzen. Somit sind sie bei der Beschlagnahme nicht nur auf Bitcoin beschränkt.[180] Bei der Drittverwahrung ziehen die Behörden Anbieter vor, die ihren Firmensitz in der Schweiz haben und der Schweizer Finanzmarktaufsichtregulierung unterstehen.[181] Dies gewährt zusätzliche Sicherheit. Zudem bietet diese Aufbewahrungsmöglichkeit den Vorteil, dass die Verantwortung für die sorgfältige Aufbewahrung der beschlagnahmten Crypto-Assets wie bspw. die Wahl einer sicheren Wallet vertraglich auf den Dienstleister abgewälzt werden kann.[182] Zusätzlich ist der Mehraufwand für die Behörde geringer als bei der Aufbewahrung des Private Keys auf einer Hardware Wallet, da sie nur den Zugang zu ihrem entsprechenden Konto benötigen. Letztlich besitzen bei beiden Verwaltungsarten die Strafverfolgungsbehörden Public Keys, die eine Übertragung der kryptobasierten Vermögenswerte weg vom Beschuldigten und somit eine erfolgreiche Beschlagnahme ermöglichen.

D. Vorzeitige Verwertung beschlagnahmter Crypto-Assets

1. Vorzeitige Verwertung von Vermögenswerten

Wie sich die weitere Vorgehensweise mit beschlagnahmten Gegenständen und Vermögenswerten gestaltet, wird in Art. 267 StPO bestimmt. Im Normalfall verbleiben die beschlagnahmten Werte bis zum Verfahrensabschluss in Gewahrsam der Strafbehörde. Der Gesetzgeber lässt ausnahmsweise aber auch eine Verwertung der Beschlagnahmeobjekte nach den Bestimmungen des SchKG zu, bevor nach Art. 267 entschieden werden konnte. Diese Ausnahmesituation ergibt sich gemäss Art. 266 Abs. 5 StPO einerseits bei Gegenständen, die einer raschen Wertminderung unterliegen oder eines kostspieligen Unterhalts bedürfen; und andererseits bei Vermögenswerten mit einem Börsen- oder Marktpreis.[183]

---

[177] Anh. 1: Interview BURGERMEISTER, Frage 3; Anh. 2: Interview MEIER/MEYER, Frage 1.2, 2.1; Anh. 3: Interview KILCHENMANN/STEIGER, Frage 3.1; Anh. 4: Interview WALDER, Frage 2.1.
[178] Anh. 1: Interview BURGERMEISTER, Frage 3; Anh. 2: Interview MEIER/MEYER, Frage 1.2.
[179] Anh. 2: Interview MEIER/MEYER, Frage 1.2.
[180] Anh. 1: Interview BURGERMEISTER, Frage 3; Anh. 2: Interview MEIER/MEYER, Frage 1.2.
[181] Anh. 3: Interview KILCHENMANN/STEIGER, Frage 3.1; Anh. 4: Interview WALDER, Frage 2.1.
[182] Anh. 4: Interview WALDER, Frage 2.2.
[183] BSK StPO-BOMMER/GOLDSCHMID, Art. 266 N 29; SIMMLER ET AL, S. 977.

Art. 266 Abs. 5 StPO findet allerdings nur auf die Beschlagnahme zur Einziehung von Gegenständen oder Vermögenswerten Anwendung.[184] Dies hängt mit der Voraussetzung von Art. 267 Abs. 2 StPO zusammen, dass die vorzeitige Verwertung nur erfolgen kann, wenn eine potenzielle Einziehung des beschlagnahmten Vermögenswerts möglich ist. Im Fall der Restitutionsbeschlagnahme ist das Beschlagnahmeobjekt der berechtigten Person zurückzugeben und nicht zu verwerten.[185] In Ausnahmefällen erscheint eine vorzeitige Veräusserung auch bei der Restitutionsbeschlagnahme als zulässig. Eine Ausnahme liegt gemäss BOMMER/GOLDSCHMID vor, wenn keine Alternative zur vorzeitigen Verwertung besteht, um die Interessen des «Aushändigungsberechtigten» zu wahren.[186] Bei einer Kostendeckungsbeschlagnahme hingegen sehen sie keine Anwendungsmöglichkeit der vorzeitigen Veräusserung, da der Deliktskonnex fehlt und lediglich monetäres Interesse am Beschlagnahmeobjekt besteht. Deshalb wäre es sogar missbräuchlich ein Objekt zu beschlagnahmen, bei welchem den Strafverfolgungsbehörden bereits im Voraus klar ist, dass dieses vorzeitig verwertet werden muss, da ein Wertzerfall droht.[187]

Gemäss dem Wortlaut von Art. 266 Abs. 5 StPO *kann* die Behörde die Beschlagnahmeobjekte sofort verwerten. BOMMER/GOLDSCHMID vertreten die Ansicht, dass es höchstwahrscheinlich ein scheinbares behördliches Ermessen darstellt, denn sollten alle Voraussetzungen der vorzeitigen Verwertung erfüllt sein, wird es vielmehr zu einer behördlichen Pflicht. Diese Verwertungspflicht resultiert aus der Pflicht zur sorgfältigen Verwaltung der beschlagnahmten Vermögenswerte, welche der Strafverfolgungsbehörde aufgrund der hoheitlichen Gewalt über die Beschlagnahmeobjekte obliegt.[188] Diese Argumentation unterstützt ebenfalls das Bundesstrafgericht. In seiner Erwägung führt dieses aus, dass anzunehmen ist, dass dem Inhaber der Vermögenswerte, die einem Marktwert unterliegen, wohl eher der monetäre Wert dieser wichtiger sei als die Vermögenstitel selbst.[189] Die tieferen Hürden für die vorzeitige Verwertung von Wertpapieren und anderen Werten im Vergleich zu Gegenständen dürften am fehlenden Affektionsinteresse des Eigentümers oder Inhabers von Vermögenswerten mit einem Markt- oder Börsenpreis liegen.[190]

[184] BSK StPO-BOMMER/GOLDSCHMID, Art. 266 N 30.
[185] BGE 128 I 129, 132 E. 3.1.1; BSK StPO-BOMMER/GOLDSCHMID, Art. 267 StPO N 31.
[186] BSK StPO-BOMMER/GOLDSCHMID, Art. 266 N 30.
[187] BSK StPO-BOMMER/GOLDSCHMID, Art. 266 N 30 Fn. 77.
[188] BSK StPO-BOMMER/GOLDSCHMID, Art. 266 N 32; BStrGer BB.2012.146 E 2.5.
[189] BStrGer BB.2012.146 E 2.5.
[190] HEIMGARTNER, StPO-Kommentar, Art. 266 N 9; TSCHUDI, S. 137.

Wenn eine vorzeitige Verwertung angezeigt ist, soll nach der Rechtsprechung des Bundesgerichts dieser Verkauf einen möglichst hohen Erlös erzielen und damit den Interessen des Staates als auch denjenigen der betroffenen Person dienen. Das Bundesgericht mahnt zum zurückhaltenden Gebrauch der vorzeitigen Verwertung, da mit dieser ein schwerer Eingriff in das Eigentum des Beschuldigten vorgenommen wird.[191] HEIMGARTNER vertritt ebenfalls die Ansicht, dass die vorzeitige Verwertung eine Ausnahme darstellen sollte. Seiner Meinung nach ist eine vorzeitige Veräusserung gegen den Willen des Inhabers nur dann unter dem Gesichtspunkt der Eigentumsgarantie (BV Art. 26) verhältnismässig, wenn aufgrund der Art der Anlagen und der Wirtschaftslage die Gefahr eines Wertverlustes offensichtlich ist.[192]

2. Vorzeitige Verwertung von Crypto-Assets

Wie zu Beginn dieser Arbeit festgestellt handelt es sich bei Crypto-Assets um Vermögenswerte, die i.d.R. einem Marktpreis unterliegen. Somit stellen Kryptowährungen durchaus i.S.v. Art. 266 Abs. 5 StPO andere Werte dar, die über einen Börsen- oder Marktpreis verfügen. Folglich *können* Crypto-Assets vorzeitig verwertet werden.[193] In welchen Fällen beschlagnahmte Crypto-Assets tatsächlich vorzeitig veräussert und in Fiatgeld umgewandelt werden sollen, wird in der Lehre als auch in der Praxis kontrovers diskutiert.

In Anbetracht der mehrmonatigen oder sogar mehrjährigen Verfahrensdauer sowie der starken Volatilität der Kryptowährungen stimmen SIMMLER ET AL. einer vorzeitigen Verwertung beschlagnahmter Crypto-Assets grundsätzlich zu. Sie argumentieren, dass sich die vorzeitige Veräusserung von Kryptowährungen dazu eignet, das Haftungsrisiko der Behörden und einen allfälligen Vermögensverlust des Tatverdächtigen zu minimieren.[194] Allerdings muss die sofortige Verwertung von den infrage stehenden Kryptowährungen sachgemäss und verhältnismässig sein. Konkret setzen SIMMLER ET AL. voraus, dass die Kursentwicklung sowie die Volatilität der Crypto-Assets beachtet werden. Zudem bedarf es der Zustimmung der betroffenen Person, wenn die Beschlagnahme der Sicherstellung von Verfahrenskosten dient. Des Weiteren wird vorgeschlagen, dass der Beschuldigte einem Haftungsausschluss seitens des Staats zustimmt und bestätigt, eventuelle Kursverluste selbst zu tragen, sollte er auf eine Verwertung verzichten. Einzig bei der Einziehungs- sowie Restitutionsbeschlagnahme wird in

[191] BGer 1B_357/2019 E. 4.1; 1B_125/2019 E 5.2; 1B_461/2017 E. 2.1.; TSCHUDI, S. 135.
[192] HEIMGARTNER, StPO-Kommentar, Art. 266 N 10.
[193] SIMMLER ET AL., S. 977 f.; TSCHUDI, S. 136.
[194] SIMMLER ET AL, S. 977.

Anbetracht der anhaltenden Volatilität eine vorzeitige Veräusserung der Crypto-Assets auch gegen den Willen des Beschuldigten empfohlen.[195]

Die Staatsanwaltschaft des Kantons St.Gallen beachtet bei der vorzeitigen Verwertung von Crypto-Assets im Prinzip dieselben Kriterien wie von SIMMLER ET AL. aufgeführt.[196] BURGERMEISTER führt aus, dass massgeblich für den Entscheid einer Veräusserung der Beschlagnahmegrund ist. Wenn das beschlagnahmte Deliktsgut letztendlich vom Staat eingezogen wird oder einer geschädigten Person zurückgegeben werden soll, so kann es der beschuldigten Person grundsätzlich gleichgültig sein, wie hoch der Erlös aus den Crypto-Assets sein wird. Anders verhält es sich bei einer Beschlagnahme zur Kostensicherung. In diesem Fall hat der Beschuldigte ein grösseres Interesse daran, bei der vorzeitigen Verwertung einen möglichst hohen Erlös zu erzielen. Daher würde Burgermeister eher zurückhaltend eine Veräusserung bei der Sicherungsbeschlagnahme anordnen. Grundsätzlich betont er, dass ein Austausch von den betroffenen Parteien hinsichtlich einer vorzeitigen Verwertung essenziell ist, um einen bestmöglichen Beschluss fassen zu können.[197]

Eine ähnliche Ansicht teilt die Staatsanwaltschaft für Besondere Aufgaben des Kantons Bern. Sie betont insbesondere die Einzelfallbetrachtung sowie die Gewährung des rechtlichen Gehörs im Rahmen der vorzeitigen Veräusserung von beschlagnahmten Crypto-Assets. Die Anordnung einer vorzeitigen Verwertung hängt für sie im Wesentlichen von der Art der Kryptowährung sowie der Untersuchungsdauer ab. Ebenfalls entscheidend wirkt die Wahrscheinlichkeit einer Freigabe der beschlagnahmten Crypto-Assets nach Verfahrensabschluss. Falls eine Restitution erfolgen soll, präferiert die Staatsanwaltschaft Bern die Crypto-Assets als solche an den Geschädigten zu übertragen. Allerdings spricht sie sich in den übrigen Beschlagnahmefällen für eine vorzeitige Veräusserung aus, sofern keine konkrete Anweisung seitens der betroffenen Person vorliegt, da die Kursprognose für Kryptowährungen praktisch unmöglich sei.[198]

Zurückhaltender bzgl. der Veräusserung verhalten sich die Staatsanwälte des Kompetenzzentrums Cybercrime des Kantons Aargau. Gerade aufgrund der Kursschwankungen wird das Risiko eines Wertzuwachses als zu hoch eingeschätzt. Denn bei einer vorzeitigen Veräusserung droht stets die Gefahr, dass im Endentscheid eine Freigabe der beschlagnahmten Werte beschlossen wird. In einem solchen Fall könnte ein Wertersatz zum

[195] SIMMLER ET AL, S. 978.
[196] Die gleiche Ansicht liegt vermutlich daran, dass der Staatsanwalt BURGERMEISTER Co-Autor des Beitrags von SIMMLER ET AL. ist.
[197] Anh. 1: Interview BURGERMEISTER, Frage 4.1.
[198] Anh. 2: Interview MEIER/MEYER, Frage 3.1, 3.2.

aktuellen Marktwert an die betroffene Person geleistet werden müssen. Deshalb lassen KILCHENMANN/STEIGER in der Regel die Crypto-Assets als solche bei einem Dritten verwahren und geben die Crypto-Assets bei Bedarf an das Gericht weiter, welches die allfällige Umwandlung in Fiatgeld anordnen und dieses anschliessend einziehen würde.[199]

Ebenso gegen eine grundsätzliche vorzeitige Verwertungspflicht von Crypto-Assets argumentiert BREITENFELDT. In Anbetracht der Tatsache, dass Bitcoins eine Geldersatzfunktion einnehmen können, ist seiner Ansicht nach der Sicherungszweck der Beschlagnahme ohne eine kategorische Veräusserung und dem mit ihr einhergehenden Grundrechtseingriff erreichbar. Nur wenn die betroffenen Personen wie der Beschuldigte oder Geschädigte einer vorzeitigen Verwertung Gelegenheit hatten zuzustimmen und dies dem staatlichen Werterhaltungsinteresse entspricht, sei diese vertretbar.[200]

A.M. ist TSCHUDI. Insbesondere kritisiert er die von SIMMLER ET AL. aufgeführten Kriterien für eine Veräusserung von Kryptowährungen, da diese keine Rechtssicherheit sowie Klarheit bieten würden. Er argumentiert, dass in Übereinstimmung mit BOMMER/GOLDSCHMID[201] die Strafverfolgungsbehörden verpflichtet sind, eine vorzeitige Verwertung von Kryptowährungen auch gegen den Willen der betroffenen Person vorzunehmen. Seiner Ansicht nach spricht die hohe Volatilität der Kryptowährungen und gerade die Werteinbussen von bspw. Bitcoin in jüngerer Vergangenheit für eine sofortige Veräusserung der beschlagnahmten kryptobasierten Vermögenswerte. Eine Verwertung und Umwandlung in Fiatgeld wirken zusätzlich dem Risiko entgegen, dass die Strafverfolgungsbehörden einen Private Key bei unsachgemässer Aufbewahrung verlieren könnten und dadurch die Crypto-Assets verlieren würden.[202]

Die Staatsanwaltschaft II Zürich schätzt das Wertzerfallsrisiko bei Kryptowährungen ebenfalls höher als eine Gewinnerwartung ein. Deshalb praktiziert sie eine möglichst rasche vorzeitige Verwertung bzw. Umwandlung in Fiatwährung der beschlagnahmten Crypto-Assets. Aufgrund der unmöglichen Prognostizierbarkeit der Kursentwicklung von Kryptowährungen hält es WALDER für nicht vertretbar, die kryptobasierten Vermögenswerte als solche aufzubewahren. Er ist skeptisch, dass eine sorgfältige Aufbewahrung von den beschlagnahmten volatilen Kryptowährungen ohne eine vorzeitige Veräusserung gewährleistet werden kann.[203]

[199] Anh. 3: Interview KILCHENMANN/STEIGER, Frage 3.1, 3.2, 3.4.
[200] BREITENFELDT, S. 399.
[201] BSK StPO-BOMMER/GOLDSCHMID, Art. 266 N 32.
[202] TSCHUDI, S. 136 f.
[203] Anh. 4 Interview WALDER, Frage 2.2, 3.1.

Mit der vorzeitigen Verwertung von beschlagnahmten Crypto-Assets hat sich das Bundesgericht im Herbst 2021 befasst.[204] Die Staatsanwaltschaft II des Kantons Zürich beschlagnahmte im Rahmen einer Geldwäschereiuntersuchung verschiedene Crypto-Assets des Beschuldigten, die dieser bei einer Firma verwahrt hatte. Die Staatsanwaltschaft ordnete diese an, die betreffenden kryptobasierten Vermögenswerte an das staatseigene Konto bei einem spezialisierten Unternehmen für Crypto-Assets zu transferieren. Zusätzlich verfügte die Staatsanwaltschaft, dass die Kryptobestände nach erfolgter Übertragung auf ihr Konto von diesem Unternehmen in Schweizer Franken umzuwandeln und der Staatsanwaltschaft zu überweisen seien. Die beschuldigte Person erhob erfolglos Beschwerde gegen die Verfügung der Staatsanwaltschaft beim Obergericht des Kantons Zürich. Nach der Abweisung der Beschwerde gelangte der Beschuldigte mit Beschwerde in Strafsachen ans Bundesgericht. Das Bundesgericht hiess die Beschwerde gut und wies die Sache an die Staatsanwaltschaft zu neuem Entscheid zurück.[205] Es ist anzumerken, dass speziell in dem zu beurteilenden Fall der Beschuldigte äusserst hohe Kryptobestände hatte und eine sofortige gesamthafte Verwertung in der Lage gewesen wäre, den Marktpreis der Crypto-Assets massgeblich negativ zu beeinflussen, was ein schlechtes Verwertungsergebnis zur Folge gehabt hätte.[206]

In seinen Erwägungen bestätigte das Bundesgericht, dass Art. 266 Abs. 5 StPO unbestrittenermassen auf Crypto-Assets Anwendung findet und diese grundsätzlich vorzeitig verwertet werden *können*. Im Vordergrund des Entscheids stand deshalb vielmehr die Frage, wie die Behörden bei einer vorzeitigen Veräusserung der beschlagnahmten Kryptobestände vorzugehen haben.[207]

Vor diesem Hintergrund hat das Bundesgericht die Verfügung der Staatsanwaltschaft zur vorzeitigen Verwertung als zu unspezifisch bzgl. des Vorgehens angesehen. Das Bundesgericht erläutert in seinen Erwägungen, dass sowohl die bestmögliche Interessenwahrung des Staates und des Beschuldigten als auch ein möglichst hoher Erlös für eine zufriedenstellende vorzeitige Verwertung zentral sind. Dabei müssen die genauen Umstände des Einzelfalls beachtet werden.[208]

Das Bundesgericht spricht der Staatsanwaltschaft in diesem konkreten Fall kein genügendes Fachwissen zu. In seinem Entscheid empfiehlt es den Beizug von Fachpersonen, wenn die

[204] BGE 148 IV 74.
[205] BGer 1B_59/2021 Sachverhalt lit. A., B., E. 5; Bundesgericht, Medienmitteilung, Abschn. 2.
[206] BGE 148 IV 74 E. 4.4.2.
[207] BGE 148 IV 74 E. 4.4.
[208] BGE 148 IV 74 E. 4.3, 4.4.2.

Behörde nicht über «das nötige Fachwissen» verfügt. Die Verfügung der Staatsanwaltschaft liess keine Rückschlüsse auf besondere Abklärungen oder den Beizug von Experten zu.[209] VOCK ist in seiner Entscheidbesprechung der Ansicht, dass grundsätzlich von fehlender Expertise bei den Strafbehörden aufgrund der technischen Neuartigkeit der Crypto-Assets ausgegangen werden kann und empfiehlt den Behörden entsprechende Experten beizuziehen.[210]

Auf die Empfehlung, Fachpersonen beizuziehen, angesprochen, besteht Unsicherheit unter den interviewten Personen, zumal nicht eindeutig ist, wie die nötige Expertise zu bestimmen ist, da ein bundesweiter Standard fehlt. Die Interviewpartner sprechen sich selbst oder ihren Arbeitskollegen ein ausreichendes Fachwissen im Bereich Crypto-Assets zu, welches sie sich aus Eigeninitiative angeeignet haben. Bisher hatte keiner der Befragten eine Fachperson im Rahmen einer Beschlagnahme von Crypto-Assets beigezogen.[211] In komplexeren Fällen würden sich die Strafverfolgungsbehörden an eine Kryptobank oder spezialisierte Firma ihres Vertrauens wenden und von diesen (ihrer Ansicht nach) ausreichende fachliche Unterstützung erhalten.[212] WALDER weist darauf hin, dass nur eine fälschlich grosszügige Interpretation des Leitentscheids implizieren würde, dass in jedem Fall eine Fachperson beizuziehen sei. Zudem hätte das Obergericht des Kantons Zürich die Expertise bzgl. Crypto-Assets der Staatsanwaltschaft bestätigt, als eine Verfügung zur vorzeitigen Veräusserung aufgrund des fehlenden Beizugs einer Fachperson gestützt auf den Bundesgerichtsentscheid angefochten wurde.[213]

Aus dem Bundesgerichtsentscheid ist ersichtlich, dass eine klare Formulierung der Verfügung über die detaillierten Modalitäten der vorzeitigen Veräusserung der Crypto-Assets zentral ist. Die Staatsanwaltschaft sollte – um Transparenz zu schaffen – ihre Fachkompetenz nachweisen oder entsprechenden (geplanten) Beizug von Experten darlegen. Letztendlich soll dies dem Verlustausschluss bzw. der Interessenwahrung der betroffenen Personen dienen.[214]

Tendenziell stellt in der aktuellen, höchst volatilen Lage der Kryptomärkte[215] die vorzeitige Veräusserung aber den grundsätzlich sichereren Weg für die Strafverfolgungsbehörden dar, um allfälligem Wertverlust vorzubeugen. Insbesondere scheint eine vorzeitige Veräusserung von

[209] BGE 148 IV 74 E. 3.4, 4.4.2.
[210] VOCK, S. 230.
[211] Anh. 1: Interview BURGERMEISTER, Frage 4.2; Anh. 2: Interview MEIER/MEYER, Frage 3.4, 3.5; Anh. 3: Interview KILCHENMANN/STEIGER, Frage 3.4; Anh. 4: Interview WALDER, Frage 3.3.
[212] Anh. 1: Interview BURGERMEISTER, Frage 4.2; Anh. 2: Interview MEIER/MEYER, Frage 3.4, 3.5; Anh. 3: Interview KILCHENMANN/STEIGER, Frage 3.4; Anh. 4: Interview WALDER, Frage 3.3.
[213] Anh. 4: Interview WALDER, Frage 3.2; OGer ZH UH220009 E. 4.3, S. 10.
[214] BGer 1B_59/2021 E. 3.4, 4.4.2.
[215] Coin Market Cap, Stand 18.11.2022.

Bitcoins im Normalfall unproblematisch, da es aufgrund des grossen Gesamtmarktvolumen kaum möglich sein wird, den Bitcoin-Kurs zu beeinflussen.[216]

Schlussfolgernd kann festgestellt werden, dass Crypto-Assets vorzeitig verwertet werden *dürfen*. M.E. sollte nicht automatisch von einer vorzeitigen Verwertungspflicht ausgegangen werden, da die Fallkonstellationen sehr unterschiedlich sein können. Wie auch der Berner Staatsanwalt MEIER betont, ist die Einzelfallbetrachtung zentral und allfällige Richtlinien sind auf den konkreten Fall anzupassen.[217] Grundsätzlich sind für einen zufriedenstellenden Entscheid bzgl. der vorzeitigen Verwertung von beschlagnahmten Crypto-Assets der Austausch zwischen der Strafverfolgungsbehörde und dem Beschuldigten sowie allfälligen Geschädigten essenziell und die Berücksichtigung der Kursvolatilität der betroffenen Kryptowährung von Bedeutung. Ebenfalls sollte der Beschlagnahmegrund im Zusammenhang mit der voraussichtlichen Verfahrensdauer im Verwertungsentscheid beachtet werden. Letztlich soll die Verfügung der Staatsanwaltschaft so präzise wie nötig bzgl. der Verwertungsmodalitäten ausfallen.[218]

3. Umsetzung einer vorzeitigen Verwertung

Die vorzeitige Verwertung von Gegenständen und Vermögenswerten richtet sich nach den Bestimmungen des SchKG. Der Erlös wird mit Beschlag belegt und dieser ersetzt das verwertete Beschlagnahmeobjekt. Das SchKG sieht für die Verwertung der beschlagnahmten Vermögenswerte u.a. den Freihandverkauf in Art. 130 SchKG vor.[219] Nach der Rechtsprechung des Bundesgerichts stellt grundsätzlich ein Freihandverkauf die bestmögliche Variante dar, um einen möglichst hohen Verwertungserlös zu erzielen.[220]

Die vorzeitige Veräusserung von beschlagnahmten Crypto-Assets wird somit idealerweise von den Behörden auf einer gängigen Kryptobörse vorgenommen. Der daraus erzielte Erlös in Fiatgeld tritt anstelle der beschlagnahmten Crypto-Assets und wird auf ein Konto der Behörde überwiesen.[221]

Bei der Verwertung von Crypto-Assets darf nicht missachtet werden, dass die Tauschbörsen Gebühren für die Umwandlung der Kryptowährungen in Fiatgeld verlangen, welche derzeit

---

[216] Anh. 1: Interview BURGERMEISTER, Frage 4.1; Anh. 3: Interview KILCHENMANN/STEIGER, Frage 3.3; Anh. 4: Interview WALDER, Frage 3.2.
[217] Anh. 2: Interview MEIER/MEYER, Frage 3.1.
[218] Anh. 2: Interview MEIER/MEYER, Frage 3.1.
[219] BSK StPO-BOMMER/GOLDSCHMID, Art. 266 N 33 f.
[220] BGer 1B_59/2021 E. 3.3; BGer 1B_461/2017 E. 2.1; BGer 1B_95/2011 E. 3.1.
[221] Anh. 1: Interview BURGERMEISTER, Frage 3; Anh. 4: Interview WALDER, Frage 2.2; SIMMLER ET AL., S. 977; TSCHUDI, S. 137.

hoch ausfallen können. Diese Dienstleistungskosten werden jeweils aus dem Veräusserungserlös gedeckt (Art. 144 Abs. 3 SchKG, Art. 262 SchKG).[222]

4. Ausnahmen einer vorzeitigen Verwertung

Von einer vorzeitigen Verwertung der beschlagnahmten Vermögenswerte wird in Fällen abgesehen, in denen die betroffene Person gegen die behördliche Verfügung Einspruch erhebt und sie sich bereit erklärt, eventuelle Verluste selbst zu tragen sowie zusätzlich Sicherheiten leistet.[223]

In der Praxis spricht sich BURGERMEISTER klar für eine zurückhaltende vorzeitige Veräusserung im Fall der Kostensicherungsbeschlagnahme aus.[224] Eine vorzeitige Umwandlung der Crypto-Assets scheint angemessen, wenn der Beschuldigte dieser zugestimmt hat. Wenn der Betroffene keine vorzeitige Verwertung akzeptieren möchte, sollte die Strafverfolgungsbehörde allerdings sicherstellen, dass für sie ein Haftungsausschluss vereinbart wird.[225]

E. Ausgewählte Problemfelder bei der strafprozessualen Beschlagnahme von Crypto-Assets

Dieses Kapitel betrachtet Problemfelder, die sich im Zusammenhang mit der Beschlagnahme von Kryptowährungen ergeben und in den vorangehenden Kapiteln noch nicht erläutert wurden.

1. Voraussetzung des «Paper Trail» für die Einziehung bei Dritten oder der Surrogate von nicht mehr vorhandenem Deliktsgut

Die Einziehungsbeschlagnahme ist nur möglich, falls während des hängigen Strafverfahrens eine strafrechtliche Einziehung als spätere Sanktion nicht bereits ausgeschlossen erscheint. Folglich muss eine Einziehung grundsätzlich möglich sein, bevor eine Beschlagnahme von Vermögenswerten erfolgen darf. [226]

In diesem Zusammenhang stellt sich die Frage, ob ein Ersatzwert (Surrogat) genauso einzuziehen bzw. zu beschlagnahmen ist oder lediglich der ursprüngliche deliktische Originalwert.[227] Im letzten Jahrhundert wurde diese Frage kontrovers diskutiert, bis sich im Jahr 2000 das Bundesgericht für die Einziehungsbeschlagnahme von Ersatzwerten ausgesprochen hatte. Gemäss dieses Leitentscheids bedingt die Einziehung bzw.

---

[222] VOCK/HOFMANN, S. 313.
[223] BSK StPO-BOMMER/GOLDSCHMID, Art. 266 N 32; SIMMLER ET AL., S. 977.
[224] Anh. 1: Interview BURGERMEISTER, Frage 2.1, 4.1.
[225] SIMMLER ET AL., S. 978.
[226] BSK StGB-BAUMANN, Art. 72 N 20; Vgl. BGer 1S.16/2005, E. 5.2; BGer 1P.456/2003, E. 2.
[227] BSK StGB-BAUMANN, Art. 70/71 N 47.

Beschlagnahme, wenn das Deliktsgut nicht mehr vorhanden ist, die Bestimmbarkeit des Surrogats sowie eine lückenlose Rückverfolgbarkeit des zu beschlagnahmenden Vermögenswerts zum ursprünglichen deliktischen Originalwert.[228] SCHOLL betont, dass mit allen strafprozessual gültigen Beweismitteln aufgezeigt werden kann, dass ein bestimmter Wert das ursprüngliche Deliktsgut ersetzt hat. Zusätzlich führt der Autor aus, dass dieser Nachweis nicht auf Bankunterlagen o.ä. Dokumente eingeschränkt ist, worauf der Begriff der Papierspur fälschlicherweise hindeuten könnte.[229]

Die Anforderung einer solchen Papierspur (Paper Trail) muss entsprechend bei der Einziehungsbeschlagnahme von Crypto-Assets erfüllt werden. Im Fall von Kryptowährungen ist es beispielsweise denkbar, dass deliktische Bitcoins in Fiatgeld umgetauscht werden oder umgekehrt, gestohlenes Bargeld in Bitcoin getauscht wird. In beiden Fällen wird der zu beschlagnahmende Originalwert mit einem Surrogat ersetzt. In dieser Surrogatskonstellation stellt sich jeweils die Frage, inwiefern ein beweisbarer Paper Trail vorliegt.

Zur Verschleierung der Herkunft von Crypto-Assets können sich die Täter verschiedener Mittel bedienen. In der Schweiz sind die Exchanger dazu verpflichtet, ihre Vertragspartei zu identifizieren, da sie als Finanzintermediäre gelten.[230] Deshalb könnten diejenigen ausländischen Tauschbörsen besonders attraktiv erscheinen, die keine Identifikation der Inhaber der Bitcoin-Adresse verlangen. Dies führt dazu, dass die Strafverfolgungsbehörden auf die Kooperation der Exchanger oder deren Heimatstaaten angewiesen sind, um Informationen für die Nachverfolgung der Vermögenswerte zu erhalten.[231]

Weitere Methoden, die der Spurenverwischung dienen können, sind Tumbler oder Mixer. Diese Dienstleister erhalten von Nutzern Crypto-Assets, welche diese mittels automatisierter Prozesse untereinander vermischen und anschliessend an neue Adressen der Nutzer transferieren. Somit erhält der Beschuldigte, der seine deliktischen Kryptowährungen an einen Mixerdienst transferiert hat, Kryptowährungen, die teilweise oder ganz von anderen Nutzern stammen. Dies führt zu einer erschwerten Nachvollziehbarkeit der Überweisungen.[232] Dem Nachweis eines Paper Trail dürften solche Dienste aber nicht gänzlich im Wege stehen. Wenn nachverfolgt werden kann, dass die beschuldigte Person von einem solchen Tumbler Gebrauch gemacht hat,

[228] BGE 126 I 97 E. 3.c.bb; BSK StGB-BAUMANN, Art. 70/71 N 47; TSCHUDI, S. 90.
[229] KV-KO SCHOLL, Art. 70 StGB, N 234 f.
[230] TSCHUDI, S. 90.
[231] Anh. 1: Interview BURGERMEISTER, Frage 7.1; Anh. 3: Interview KILCHENMANN/STEIGER, Frage 1.1, 1.2, 1.3; Anh. 4: Interview WALDER, Frage 7.1.
[232] Eurospider; UNODC Report, S. 22 ff.

sollte dies für die Bestimmbarkeit des Surrogats im Sinne der Rechtsprechung ausreichend sein.[233]

Der Einsatz von Mixerdiensten bringt zusätzlich die Frage der Kontamination auf. TSCHUDI führt aus, dass die legale Nutzung solcher Dienstleistungen nicht dazu führen kann, dass ein Dritter kontaminierte Crypto-Assets erhält. Genauso wie nicht alle Gelder einer Bank kontaminiert werden, wenn sei deliktisches Vermögen erhält und Vermischungssachverhalten vorliegt.[234]

Der Vorteil der Nutzung von Crypto-Assets der tatverdächtigen Person besteht für die Strafverfolgungsbehörden darin, dass aufgrund der kryptographischen Komponenten jede Bitcoin-Transaktion auf der Blockchain rückverfolgbar bleibt. In der Schweiz scheint ein unzureichender Paper Trail den Strafverfolgungsbehörden kaum Schwierigkeiten zu bereiten.[235] Die Gründe hierfür sind vielfältig. Beispielsweise wurde das Kompetenzzentrum für Cybercrime in St.Gallen bisher nicht mit der Beschlagnahme von Ersatzwerten im Zusammenhang mit Crypto-Assets konfrontiert. Doch BURGERMEISTER ist sich sicher, dass dies nur eine Frage der Zeit ist.[236] Der Aargauer Staatsanwalt STEIGER betont, dass die Täter in der Regel kaum von den vorhandenen technischen Vertuschungsmethoden Gebrauch machen. Nichtsdestotrotz sind ihm spezialisierte Dienste bekannt, die bewusst keine klare Dokumentation der Aufträge vornehmen oder auch eine Nachverfolgung von deliktischen Crypto-Assets mittels Tradingrobotern verunmöglichen. Diese Anbieter zeigen sich dementsprechend auch nicht kooperativ mit Strafverfolgungsbehörden, da dies ihrem Geschäftsmodell zuwiderlaufen würde.[237]

In der Praxis endet der Paper Trail oftmals, wenn eine ausländische Tauschbörse involviert ist, da die Behörde ohne die Daten der Exchanger kaum mit der Strafverfolgung vorankommen kann. Einige Unternehmen erweisen sich zwar als äusserst kooperativ und geben die entsprechenden Informationen an die Schweizer Strafverfolgungsbehörden weiter, jedoch verweigern auch andere Exchanger vehement die direkte Zusammenarbeit und beharren darauf, dass die Schweizer Behörde über ein Rechtshilfeersuchen an die benötigten Daten gelangt. Dabei sind primär zwei Aspekte problematisch. Einerseits dauert die Bearbeitung der Rechtshilfeersuchen mehrere Monate und andererseits befinden sich viele Tauschbörsen in

[233] TSCHUDI, S. 91.
[234] BSK StGB-PIETH, Art. 305bis N 35; KV-KO SCHOLL, Art. 70 StGB, N 23; TSCHUDI, S. 91.
[235] Anh. 2, Interview MEIER/MEYER, Frage 4.1, 4.2; Anh. 3, Interview KILCHENMANN/STEIGER, Frage 2.
[236] Anh. 1, Interview BURGERMEISTER, Frage 5.
[237] Anh. 3, Interview KILCHENMANN/STEIGER, Frage 2.

Ländern, die kein Rechtshilfeübereinkommen mit der Schweiz ratifiziert haben (wie bspw. das CCC).[238]

Die interviewten Experten kamen zum Schluss, dass sich die Nachvollziehbarkeit der Papierspur im Fall von zu beschlagnahmenden Kryptowährungen leichter gestaltet als mit herkömmlichen Währungen. Schliesslich gestaltet sich die Nachverfolgbarkeit von Bargeld, welches z.B. eine zentrale Rolle in Geldwäschereifällen einnimmt, als komplizierter.[239]

Zusammenfassend lässt sich die Paper Trail Problematik im Fall von zu beschlagnahmenden Crypto-Assets in der Praxis als relativ klein bezeichnen, zumal alle Transaktionen auf der Blockchain ersichtlich bleiben. Die Schweizer Behörden begegnen bei ihrer Ermittlungstätigkeit viel eher anderen Herausforderungen, die in den folgenden Kapiteln genauer analysiert werden.

Ganz am Anfang der Strafverfolgung begegnen sie der Problematik der Identifikation der zu beschlagnahmenden Kryptowährungen und im Verlauf der Ermittlungen stossen sie zudem häufig an ihre Grenzen, wenn grenzübergreifende Massnahmen notwendig sind. Zusätzlich ist die hohe Anzahl sowie Geschwindigkeit der Transaktionen der Täter und die daraus resultierende Datenmenge herausfordernd, da der Strafverfolgungsbehörde in der Schweiz oftmals die Ressourcen fehlen, um die aufwändige Datenverfolgung sowie -entschlüsselung vorzunehmen. Zum Teil müssen Fälle sistiert werden, wenn Aufwand und Ertrag nicht in einem zu rechtfertigenden Verhältnis stehen.[240]

2. Identifikation der zu beschlagnahmenden Crypto-Assets sowie der Täterschaft

In den geführten Interviews wurde die Identifikation der zu beschlagnahmenden Crypto-Assets als erste Hürde der Strafverfolgung genannt.[241] Die Behörden müssen die betroffenen Bitcoins im Blockchainregister ausfindig machen, einem Public Key zuordnen oder die zugehörige Bitcoin-Adresse kennen und zusätzlich mit einer natürlichen Person verbinden. Die Pseudoanonymität der Crypto-Assets muss überwunden werden, um eine erfolgreiche Beschlagnahme vollziehen zu können, wenn der Private Key vom Täter selbst verwahrt wird.[242] Die Bearbeitung der Daten erfordert von den Strafverfolgungsbehörden einen hohen

[238] Anh. 1, Interview BURGERMEISTER, Frage 5; Anh. 2, Interview MEIER/MEYER, Frage 4.1, 4.2; Anh. 3, Interview KILCHENMANN/STEIGER, Frage 1.1, 2; Anh. 4, Interview WALDER, Frage 5.1; TSCHUDI, S. 130.
[239] Anh. 1, Interview BURGERMEISTER, Frage 5; Anh. 2, Interview MEIER/MEYER, Frage 4.1, 4.2; Anh. 3, Interview KILCHENMANN/STEIGER, Frage 1.1, 2 Anh. 4, Interview WALDER, Frage 5.1.
[240] Anh. 1, Interview BURGERMEISTER, Frage 5; Anh. 2, Interview MEIER/MEYER, Frage 4.1, 4.2; Anh. 3, Interview KILCHENMANN/STEIGER, Frage 1.1, 2 Anh. 4, Interview WALDER, Frage 5.1..
[241] Anh. 1: Interview BURGERMEISTER, Frage 2.1; Anh. 2: Interview MEIER/MEYER, Frage 1.2.
[242] Anh. 4: Interview WALDER, Frage 5.1; MOLO/DRZALIC, S. 47 ; TSCHUDI, S. 111 f.

Ressourceneinsatz. Deshalb müssen Behörden regelmässig erwägen, ob der Aufwand für die Strafverfolgung mit dem erhofften Ertrag in einem adäquaten Verhältnis zu einander stehen.[243]

3. Staatliche Ersatzforderung bei nicht mehr vorhandenem Deliktsgut

Wenn weder der zu beschlagnahmende Originalwert vorhanden noch dessen Surrogat bestimmbar ist, ist eine Einziehung bzw. die Beschlagnahme der entsprechenden deliktischen Vermögenswerte gescheitert und die Strafverfolgungsbehörde muss andere Massnahmen ergreifen.[244] In diesen Fällen kann die Behörde subsidiär zur Naturaleinziehung eine Ersatzforderung nach den Bestimmungen in Art. 71 StGB auferlegen. Diese Regelung soll dem Grundsatz, dass sich Straftaten nicht rentieren dürfen, Nachdruck verleihen.[245]

Die Strafbehörden können eine Ersatzforderung ebenfalls anordnen, wenn die Beschlagnahme der Vermögenswerte aus dem Ausland sich als unmöglich oder zu aufwändig erweisen sollte. Zusätzlich vertritt BAUMANN die Ansicht, dass ein Ausweichen auf die Ersatzforderungsbeschlagnahme geboten ist, wenn diese im Interesse der Gläubiger des Beschuldigten ist.[246]

Die Beschlagnahme im Rahmen von der staatlichen Ersatzforderung ist klar von der ordentlichen Vermögensbeschlagnahme nach Art. 263 Abs. 1 lit. d sowie derjenigen im Hinblick auf eine Rückgabe an den Geschädigten nach Art. 263 Abs. 1 lit. c StPO i.V.m. Art. 70 Abs. 1 bzw. Art. 73 Abs. 1 lit. b StGB abzugrenzen. Die Ersatzforderungsbeschlagnahme bezweckt nicht die Konfiskation von deliktischen Vermögenswerten des Beschuldigten oder ausnahmsweise der betroffenen Drittperson, sondern richtet sich gegen deren allgemeines Vermögen. Ähnlich wie bei einer Kostendeckungsbeschlagnahme nach Art. 263 Abs. 1 lit. b setzt die Beschlagnahme zu Ersatzforderungszwecken keinen Deliktskonnex der betroffenen Vermögenswerte voraus. Ein weiteres Unterscheidungsmerkmal ist, dass die staatliche Ersatzforderung nach Art. 71 Abs. 3 Satz 2 StGB gemäss den Vorschriften des SchKG-Verfahrens durchzusetzen ist und dem Staat kein Vorzugsrecht zukommt.[247]

Können die Strafverfolgungsbehörden Crypto-Assets nicht auf eine staatseigene Wallet übertragen und somit beschlagnahmen, weil bspw. der Private Key nicht vorhanden ist, sollte eine staatliche Ersatzforderung geltend gemacht werden können. Gerade im Zusammenhang

[243] Anh. 2: Interview MEIER/MEYER, Frage 4.3; Anh. 3: Interview KILCHENMANN/STEIGER, Frage 5.1, 5.4.
[244] BSK StPO-BOMMER/GOLDSCHMID, Art. 263 N 45.
[245] BSK StGB-BAUMANN, Art. 70-71 N 14 f., N 65; KV-KO SCHOLL, Art. 71 StGB N 18; TSCHUDI, S. 140 f.
[246] BSK StGB-BAUMANN, Art. 70-71 N 67.
[247] BGer 1B_114/2015, E. 4.4.1.; BSK StGB-BAUMANN, Art. 70-71 N 15 f.; BSK StPO-BOMMER/GOLDSCHMID, Art. 263 N 45.

mit Kryptowährungen scheitern Beschlagnahmen an der Unkenntnis des Private Key oder der Wallet, wenn der Beschuldigte oder Dritte nicht kooperieren. Zusätzlich erweist sich die Ermittlungsarbeit oft als derart ressourcenintensiv, dass sie nicht fortgeführt werden kann. Aufgrund der äusserst herausfordernden Strafverfolgung wäre eine staatliche Ersatzforderung als zulässig zu erachten, damit die Täterschaft nicht unbestraft davonkommen kann, in dem sie z.B. ihre Paper Wallet versteckt.[248]

VI. Handlungsempfehlungen für die Strafverfolgungsbehörden und Gesetzgeber

Nachfolgend werden zunächst mögliche Handlungsempfehlungen für die Strafverfolgungsbehörden und den Gesetzgeber auf nationaler Ebene und anschliessend auch für die internationale Ebene aufgezeigt.

A. Verbesserungsvorschläge für die Strafverfolgungsbehörden in Anbetracht der aktuellen Gesetzeslage

Bei unveränderter Rechtslage lassen sich für die Schweizer Strafverfolgungsbehörden vor allem im Zusammenhang mit dem Wissen rundum Crypto-Assets und deren Beschlagnahme zwei Bereiche mit Verbesserungspotential identifizieren. Namentlich sind die Ausbildungsmöglichkeiten sowie der interkantonale Ermittlungserfahrungsaustausch zu verbessern.

1. Wissensvermittlung und zertifizierte Ausbildungsmöglichkeit

Crypto-Assets basieren auf einer neuartigen Technologie und die damit verbundenen Delikte erfordern von den Behörden eine hohe Anpassungsfähigkeit. Der Bundesrat hat in diesem Zusammenhang Entscheide für die Umsetzung der «Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS)» gefällt. Unter den Bereich Cyber-Strafverfolgung der Bundesverwaltung fallen alle Massnahmen der Strafverfolgungsbehörden, die im Zusammenhang mit Cyber-Kriminalität ergriffen werden.[249] Eine gesamtschweizerische Koordination der Strafverfolgungsbehörden ist Teil dieses Umsetzungsplans. Umgesetzt wird dies mittels vierer Bausteine: Erstellung einer nationalen Fallübersicht, Netzwerk Ermittlungsunterstützung, digitale Kriminalitätsbekämpfung und Ausbildung.[250] Für den Austausch, die Strategieentwicklung und operative Abstimmung der Behörden wurde

[248] TSCHUDI, S. 142 ff; Anh. 1: Interview BURGERMEISTER, Frage 6.1; Anh. 2: Interview MEIER/MEYER, Frage 4.3; Anh. 3: Interview KILCHENMANN/STEIGER, Frage 5.1, 5.4.
[249] Bundesrat, Umsetzungsplan NCS, S. 4 f.
[250] Bundesrat, Umsetzungsplan NCS, S. 49 ff.

Cyberboard als Zusammenarbeitsform ins Leben gerufen. Auf der operativen Ebene befindet sich das Gremium Cyber-CASE, welchem NEDIK untergeordnet ist.[251]

Im Umsetzungsplan ist ersichtlich, dass mittlerweile Ausbildungsangebote an Hochschulen bestehen, die sich an die Polizei richten.[252] Aus den geführten Interviews bzw. Interviewanfragen geht hervor, dass das Wissen bzgl. des Umgangs mit Crypto-Assets nicht bei allen kantonalen Strafverfolgungsbehörden im selben Mass vorhanden ist.[253] Zwar dient die Plattform NEDIK der Polizei und Staatsanwaltschaft als Informationsquelle, jedoch scheint diese allein nicht ausreichend zu sein. Das nationale Gremium Cyber-Case, welches Staatsanwälten einen Austausch u.a. im Bereich Kryptowährungen ermöglicht, wird von den Interviewpersonen in seinem Nutzen gemischt bewertet. Als Gelegenheit für einen Informationsaustausch sowie Networking wird das Gremium als sinnvoll erachtet, jedoch reicht es scheinbar für eine zufriedenstellende Wissensvermittlung bzgl. Crypto-Assets nicht aus. Die Interviewpersonen haben sich ihr Wissen aus Eigeninitiative primär im Selbststudium angeeignet.[254]

Die Ausführungen der befragten Strafverfolgungsbehörden sowie die Komplexität der Crypto-Assets lassen den Schluss zu, dass das Ausbildungsangebot von Seiten des Cyberboards weiter ausgebaut und auch für Staatsanwälte angeboten werden sollte. Der Fokus auf den Zugang der Ausbildung lediglich für Mitarbeiter der Polizei erscheint weder besonders nachhaltig noch zielführend, da die Staatsanwaltschaft ebenfalls über ein grundsätzliches Verständnis der Funktionsweise bzw. Besonderheiten der Beschlagnahme von Kryptowährungen verfügen sollte. Gerade wenn sich bspw. die Frage der Verwertung der beschlagnahmten Crypto-Assets vor Verfahrensabschluss stellt, sollte die Behörde im Idealfall über ausreichende Kenntnisse verfügen, um das Schicksal der Kryptowährungen selbst einschätzen, eine etwaige Expertenmeinung nachvollziehen und diese vor Gericht entsprechend erläutern zu können. Zudem wäre die Kommunikation mit bzw. die Ermittlungstätigkeit der Polizei behindert, wenn Grundkenntnisse seitens der Staatsanwaltschaft fehlen, da die rechtliche Seite der Ermittlung mit der technischen Funktionsweise der Crypto-Assets zusammenhängt.[255]

[251] Bundesrat, Umsetzungsplan NCS, S. 49; SCHWEINGRUBER, S. 25.
[252] Bundesrat, Umsetzungsplan NCS, S. 51 f.
[253] Anh. 2: Interview MEIER/MEYER, Frage 1.2; 7; Anh. 3: Interview KILCHENMANN/STEIGER, Frage 4; Anh. 4: Interview WALDER, Frage 7.3; SIMMLER ET AL., S. 978.
[254] Anh. 3: Interview KILCHENMANN/STEIGER, Frage 4; Anh. 4: Interview WALDER, Frage 7.3; SIMMLER ET AL., S. 978.
[255] Anh. 2: Interview MEIER/MEYER, Frage 7.

2. Interkantonaler Erfahrungsaustausch

Aus den Expertenanfragen wird klar, dass selbst Strafverfolgungsbehörden, die sich mit Straftaten im Cyberbereich befassen, noch nicht genügend auf die Beschlagnahme von Crypto-Assets vorbereitet sind oder die Expertise (noch) nicht vorhanden ist.[256]

Zusätzlich hat sich aus den Interviews ergeben, dass die Herangehensweise an Tauschbörsen oder Wallet-Anbieter unterschiedlich ist und dementsprechend auch der damit verbundene Erfolg. Insb. liegen Unterschiede vor, wenn Informationen von der Tauschbörse Binance benötigt werden.[257] Positive Erfahrungen im Umgang mit ausländischen Dienstleistern im Zusammenhang mit der Erlangung der Kenntnis des Private Key sind für die Strafverfolgungsbehörden äusserst wertvoll.

Daher sollte vom Cyberboard die Optimierung der Ermittlungsabläufe vermehrt aktiv gefördert werden, als auch die Erfahrungen im Bereich der Crypto-Asset-Beschlagnahme zentral gesammelt und geteilt werden. Damit kann verhindert werden, dass sich jede kantonale Strafverfolgungsbehörde gesondert überlegen muss, wie sie sich im Hinblick auf die Delikte im Zusammenhang mit Kryptowährungen am besten organisiert. Dies beinhaltet sich wiederholende Entscheide zu: Walletart; Wallet Provider; Inhaber der Wallet (welche Behörde); Anforderungen, Abläufe sowie Zuständigkeit für Beschlagnahme und potenzielle Verwertung.[258]

B. Gesetzesänderungen auf nationaler Ebene

Wie in der vorliegenden Arbeit in Kap. IV und V zur Eignung bzw. Durchführung der strafprozessualen Beschlagnahme von Crypto-Assets ausführlich dargelegt, ist eine erfolgreiche Konfiskation der kryptobasierten Vermögenswerte grundsätzlich möglich und lässt sich unter der bestehenden Gesetzgebung durchführen. Jedoch würde eine unmissverständliche Erfassung von Crypto-Assets in den Beschlagnahmenormen Unsicherheiten der Strafverfolgungsbehörden im Umgang mit den beschlagnahmten Werten beseitigen und ebenfalls die Gelegenheit für eine Harmonisierung bieten.[259] Um eine Beschlagnahme zu Beweiszwecken von Crypto-Assets zu ermöglichen, müsste in Art. 263 StPO möglicherweise eine Präzisierung des Gegenstandbegriffs oder eine Ergänzung um

[256] Diese Schlussfolgerung lässt die Korrespondenz im Rahmen der Interviewanfrage mit dem Kompetenzzentrum für Cybercrime der Kantone Zug und Schwyz zu.
[257] Anh. 1: Interview BURGERMEISTER, Frage 2.3, 7.2, 7.3, 7.4; Anh. 3: Interview KILCHENMANN/STEIGER, Frage 1.3.

[258] Vgl. Anh. 1: Interview BURGERMEISTER, Frage 8.3; Anh. 2: Interview MEIER/MEYER, Frage 6.2; SIMMLER ET AL., S. 978.
[259] BREITENFELDT, S. 399; SIMMLER ET AL., S. 978; TSCHUDI, S. 159 f.

digitale Informationen erfolgen.[260] Die folgende Erweiterung der Beschlagnahmenorm würde ein hohes Bestimmtheitsmass des Gesetzesartikels erfüllen und dem unzufriedenstellenden Ausschluss von beweisrelevanten Crypto-Assets in der Beschlagnahme entgegenwirken.

> *Art. 263 Abs. 1bis StPO*
>
> *Digitale Daten einer beschuldigten Person oder einer Drittperson können zu den aufgeführten Zwecken in Art. 263 Abs. 1 StPO beschlagnahmt werden.*

Eine zielführende Ergänzung von Art. 266 StPO zur Durchführung der Beschlagnahme als auch der Verordnung des Bundesrats zur Anlage beschlagnahmter Vermögenswerte bietet sich an.[261] Neue Regelungen zu kryptbasierten Vermögenswerten im Zusammenhang mit der Beschlagnahme könnten wie folgt lauten:

> *Art. 266 Abs. 4bis StPO*
>
> *Die Beschlagnahme kryptobasierter Vermögenswerte erfolgt durch deren Übertragung auf eine staatliche Adresse.*[262]
>
> *Art. 1bis SR 312.057*
>
> *[1]Die Anlage kryptobasierter Vermögenswerte ist differenziert gestützt auf die Empfehlung des Crypto-Asset-Gremiums vorzunehmen.*

Die obige Ergänzung zu Art. 266 StPO ermöglicht es, die Veränderung der Besitzverhältnisse für die Übertragung der Crypto-Assets auf eine staatseigene Wallet auf einer rechtlichen Grundlage zu basieren. Mit einer angepassten Verordnung zur Anlage beschlagnahmter Vermögenswerte wird eine harmonische Handhabung beschlagnahmter Crypto-Assets ermöglicht, indem allgemeine Empfehlungen eines nationalen Gremiums beachtet werden. Dadurch können schweizweit die Anforderungen an die Kryptowährungsexpertise allgemein festgesetzt werden.[263] Hierfür wäre die Schaffung eines Expertengremium zum Umgang mit beschlagnahmten Crypto-Assets zu begrüssen. Ein solches «Crypto-Asset-Gremium» könnte dem Cyberboard angehören. MEIER betont, dass letztlich der jeweilige Verfahrensleiter die Verantwortung auf kantonaler Ebene trägt, ob die Handhabung der beschlagnahmten Crypto-Assets rechtens resp. erfolgreich ist.[264] Mit der Abstützung auf generelle Empfehlungen eines

[260] SIMMLER ET AL., S. 978.
[261] BREITENFELDT, S. 399; SIMMLER ET AL., S. 978; TSCHUDI, S. 159 f.
[262] TSCHUDI, S. 159.
[263] Anh. 2: Interview MEIER/MEYER, Frage 3.4; BREITENFELDT, S. 399; SIMMLER ET AL., S. 978.
[264] Anh. 2: Interview MEIER/MEYER, Frage 3.3.

Expertengremiums kann ein angemessener Umgang mit beschlagnahmten Kryptowährungen der Strafbehörden am wahrscheinlichsten garantiert werden.[265]

Die interviewten Strafverfolgungsbehörden fordern z.T. ebenfalls eine gesetzliche Grundlage für einen automatisierten interkantonalen Datenaustausch.[266] Eine entsprechende Norm sollte mit der Anpassung und Verabschiedung des Zentralstellengesetz im 4. Quartal 2022 in absehbarer Zeit vorhanden sein.[267] Dank eines Programms wie PICSEL können polizeiliche Daten interkantonal eingesehen werden und in Kombination mit einer justiziellen Fallübersicht gelingt die Erkennung von Deliktszusammenhängen bzw. -serien.[268] Die Wirksamkeit im Zusammenhang mit dem Aufspüren von deliktischen Kryptowährungen resp. der Beschlagnahme von Crypto-Assets bewerten die Strafverfolgungsbehörden allerdings bis auf eine Effizienzsteigerung begrenzt.[269]

C. Verbesserungsvorschläge auf internationaler Ebene

1. Internationaler Datenaustausch

WALDER und STEIGER/KILCHENMANN beschreiben wie allmählich das Zugriffsprinzip sich zum Standardvorgehen für die Behörde in der Zukunft entwickeln wird, um an Daten zu gelangen.[270] Einen vereinfachten internationalen Datenaustausch erachtet neben den interviewten Strafverfolgungsbehörden auch Europol als zentral in der Beschlagnahme bzw. Einziehung von Crypto-Assets.[271] Ein weitgreifender Informationsaustausch würde idealerweise mit einem internationalen Gremium kombiniert werden, welches ein koordiniertes Vorgehen gegen die hochprofessionelle Täterschaft ermöglichen würde. Auf diese Weise wäre eine Effizienz- und gleichzeitige Erfolgssteigerung in der Beschlagnahme von Kryptowährungen möglich. Gerade kleinere Länder wie die Schweiz verfügen nicht über genügend Ressourcen, um eine beachtliche Summe an Crypto-Assets zu beschlagnahmen, die den unbekannten Tätergruppierungen das deliktische Handeln unprofitabel machen würde.[272] Die Schaffung eines internationalen Gremiums mit entsprechenden Kompetenzen wird aber vermutlich kaum

[265] BREITENFELDT, S. 399; SIMMLER ET AL., S. 978
[266] Anh. 1: Interview BURGERMEISTER, Frage 8.3; Anh. 2: Interview MEIER/MEYER, Frage 6.2.
[267] Bundesrat, Umsetzungsplan NCS, S. 52.
[268] Anh. 2: Interview MEIER/MEYER, Frage 6.2.; Bundesrat, Umsetzungsplan NCS, S. 49 f.
[269] Anh. 1: Interview BURGERMEISTER, Frage 8.3; Anh. 2: Interview MEIER/MEYER, Frage 6.2.
[270] Anh. 3: Interview KILCHENMANN/STEIGER, Frage 5.2; Anh. 4: Interview WALDER, Frage 7.1, 7.2; Vgl. BGE 143 IV 270.
[271] Europol, IOCTA, S. 39
[272] Anh. 3: Interview KILCHENMANN/STEIGER, Frage 1.3.

realistisch sein.[273] Deshalb sind Staatsverträge wie das CCC umso wichtiger, die eine grenzübergreifende Beschlagnahme vereinfachen.[274]

2. Blacklisting beschlagnahmter bzw. eingezogener Crypto-Assets

Es bietet sich die Einführung von internationalen schwarzen Listen (Blacklist) für Crypto-Assets an, die der Einziehung unterliegen, aber nicht effektiv beschlagnahmt resp. eingezogen werden können, weil z.B. der Private Key unbekannt ist und sie deshalb nicht auf eine staatseigene Adresse transferiert werden können. Theoretisch müssten die Nutzer bei jeder Transaktionsüberprüfung sicherstellen, dass keine Crypto-Assets überwiesen werden, die auf einer solchen Liste stehen. Damit würde das Ziel der Einziehung erreicht werden, dass die digitalen Guthaben für deren Inhaber wertlos würden und sich dementsprechend die Straftat nicht gelohnt hätte.[275] So führen bspw. die Vereinigten Staaten eine solche schwarze Liste mit den entsprechenden Kryptowährungsadressen.[276]

Die Interviewpersonen äussern sich skeptisch zur Wirkung internationaler schwarzer Listen für Crypto-Assets. Sie gehen davon aus, dass diese von den Tätern umgangen werden können – schliesslich bestimmen die Nutzer, ob eine Transaktion gültig ist. Um eine Blacklist zielführend umzusetzen, müsste das Bitcoin Protokoll angepasst werden, damit Übertragungen zu bestimmten Adressen technisch nicht mehr möglich wären. Zudem müsste eine Beschwerdestelle für die Auflistung der Kryptowährungsadressen vorhanden sein.[277]

Ein anderer Ansatz besteht darin, Kryptowährungsanleger mit Hilfe von Warnlisten vor Betrugsfällen zu schützen. In der Schweiz führt die FINMA eine Liste mit Unternehmen, die möglicherweise ohne Erlaubnis Dienstleistungen für Crypto-Assets anbieten.[278] Die EU hat auch Regelungen zu Crypto-Asset-Dienstleistern herausgearbeitet und führt ebenfalls eine Liste von Anbietern, welche die «Markets in Crypto Assets»-Richtlinien nicht erfüllen.[279]

Es lässt sich festhalten, dass die Einführung schwarzer Listen von Staatsbehörden für beschlagnahmte Crypto-Assets keinerlei Einfluss auf ihre faktische Transaktionsmöglichkeit hat.

---

[273] Anh. 2: Interview MEIER/MEYER, Frage 6.1.
[274] Anh. 1: Interview BURGERMEISTER, Frage 7.1
[275] TSCHUDI, S. 150.
[276] U.S. Cyber-related Designation.
[277] Anh. 3: Interview KILCHENMANN/STEIGER, Frage 5.4; Anh. 4: Interview WALDER, Frage 7.7, 7.8.
[278] FINMA, Warnliste.
[279] Handelsblatt, MiCA-Richtlinie.

VII. Fazit und Ausblick

Crypto-Assets basieren auf der Blockchain Technologie und verfügen über ein digitales Geld-Ökosystems. Aufgrund ihrer besonderen Funktionsweise, die pseudoanonyme Transaktionen ermöglicht, sind kryptobasierte Vermögenswerte in der Schattenwirtschaft beliebt und folglich kriminalpolitisch relevant. Entsprechend stellen Crypto-Assets die Strafverfolgungsbehörden vor neue Herausforderungen. Dies liegt u.a. daran, dass sich in der Schweizer Rechtsordnung aktuell keine Normen zur Rechtsnatur oder Beschlagnahmefähigkeit kryptobasierter Vermögenswerte finden lassen. Die vorliegende Arbeit konnte aufzeigen, dass sich Crypto-Assets unter das bestehende Verständnis von Vermögenswerten i.S.d. Strafrechts subsumieren lassen. Entsprechend können Kryptowährungen grundsätzlich beschlagnahmt werden, jedoch stellen deren technischen Eigenschaften bzgl. der Verwahrung des Private Keys die Behörden vor Herausforderungen. Die Kenntnis des privaten Schlüssels der zu beschlagnehmenden Crypto-Assets ist für die Übertragung auf eine staatseigene Wallet zentral, um dem Beschuldigten die Verfügungsmacht entziehen und so eine effektive Beschlagnahme vornehmen zu können. Sobald Kryptowährungen in der Verfügungsgewalt der Behörde sind, muss sich diese sorgfältig überlegen, ob sie die beschlagnahmten Crypto-Assets vorzeitig verwerten muss. Die vorzeitige Verwertung ist für Crypto-Assets (insb. BTC) aufgrund der volatilen Marktpreise tendenziell anzuraten, jedoch ist eine grundsätzliche Regelung nicht möglich, da die Konstellation im Einzelfall entscheidend ist. Um den Veräusserungsentscheid fällen zu können bedarf es vor allem notwendiges Fachwissen zu Crypto-Assets.

Den Strafverfolgungsbehörden bereiten vor allem das Auffinden des Private Key, die Identifikation der Täterschaft sowie die Internationalität der Crypto-Assets Probleme im Rahmen der Beschlagnahme. Um die Ermittlungstätigkeit der Behörden in Zukunft zu verbessern, lassen sich auf nationaler Ebene folgende Handlungsempfehlungen festhalten:

- Ausbildungsmöglichkeiten für Staatsanwälte ausbauen sowie interkantonalen Ermittlungserfahrungsaustausch national koordinieren
- Explizite Erfassung der Crypto-Assets als taugliche Beschlagnahmeobjekte in den einschlägigen Rechtsnormen
- Regelung der Anlage von beschlagnahmten Crypto-Assets in der Verordnung des Bundesrats mit Hinweisen zur vorzeitigen Verwertung

Auf internationaler Ebene sollten folgende Anpassungen gefördert bzw. gestärkt werden:

- Internationalen Datenaustausch vereinfachen

- Blacklisting beschlagnahmter bzw. eingezogener Crypto-Asset-Adressen sowie von Diensten, die mit Delikten in Verbindung gebracht werden, die Crypto-Assets beinhalten

Die zu beobachtenden Entwicklungen auf nationaler als auch internationaler Ebene sind zu begrüssen. Im Rahmen des Cyberboards wird schliesslich bereits an Voraussetzungen für eine nationale Fallübersicht gearbeitet. Zudem hat der Gesetzgeber bereits erste Normen angepasst, um Anbieter, die «im Rahmen einer dauernden Geschäftsbeziehung» Transaktionen von Crypto-Assets ermöglichen, dem GwG zu unterstellen. Auf diese Weise wird versucht den KYC Standard auf das Ökosystem der Crypto-Assets nach dem Vorbild der EU auszuweiten.[280] Die Identitätserfassung der Nutzer von selbstverwahrten Wallets bleibt aber weiterhin unmöglich. Die OECD arbeiten ebenfalls an einem Regelwerk, welches die Erfassung der Inhaber von Crypto-Assets.[281] Damit wird eine Annäherung an die Idealvorstellung der Identifikation der Inhaber bzw. wirtschaftlich Berechtigten jeder einzelnen Wallet bzw. Kryptowährungsadresse vorgenommen.[282]

Basierend auf den Limitationen der vorliegenden Arbeit bietet sich darüber hinaus vor allem ein zukünftiges Forschungsfelder an. Ein Vergleich der internationalen Rechtslegung in Bezug auf die Beschlagnahme von Crypto-Assets kann nicht nur der Legislative weitere Erkenntnisse zur Gestaltung von massgeschneiderten Gesetzen geben; darüber hinaus bietet ein solcher Vergleich auch grosses Potenzial, die exekutiven Organe mit zusätzlichen Anhaltspunkten bei der erfolgreichen Umsetzung gesetzlicher Vorgaben zu unterstützen.

[280] Europol, IOCTA, S. 9; KGGT-Bericht 2021, S. 52 f; Vgl. Verordnung vom 18. Juni 2021 zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register (AS 2021 400).
[281] MOLO/BRUNONE, S. 305.
[282] Vgl. Anh. 2: Interview MEIER/MEYER, Frage 6.1.

Anhang

Interviewleitfaden

1. **Herausforderungen**
    a. Was sind Ihrer Meinung nach die grössten Hürden bei der Beschlagnahme von Crypto-Assets?
    b. Herausgabepflicht des Private Key
        i. Wie wird bei mangelnder Kooperation seitens der beschuldigten Person vorgegangen?
        ii. Wie hat sich bisher die Kooperation von Wallet-Providern und Strafverfolgungsbehörden bzgl. der Herausgabe des Private Keys gestaltet?
        iii. Gibt es Tauschbörsen oder Wallet Provider in der Schweiz, welche sich besonders kooperativ zeigen?

2. **Übertragung auf staatliche/polizeiliche Wallet**
    a. Wie wurde bisher mit den beschlagnahmten Crypto-Assets umgegangen?

3. **Vorzeitige Veräusserung**
    a. Welche Kriterien spielen für Sie eine Rolle beim Entscheid, ob die Kryptowährungen vorzeitig verwertet werden?
    b. Teilen Sie die Ansicht des Bundesgerichts im BGE 148 IV 74?

4. **Know-How**
    a. Wie haben Sie Ihr Wissen über Crypto-Assets erlangt?

5. **Genügender Paper Trail bei nicht mehr vorhandenem Deliktsgut**
    a. Sind Sie der Paper Trail Problematik bei Surrogaten bereits begegnet? Falls Ja, wie konnten Sie die Herausforderung meistern?

6. **Alternativen zur Beschlagnahme der Crypto-Assets**
    a. Welche zielführenden Alternativen sehen Sie zur Beschlagnahme von Crypto-Assets, wenn diese fehlschlägt?

7. Ausblick

a. Was müsste sich Ihrer Ansicht nach ändern, damit die Beschlagnahme von Crypto-Assets in Zukunft leichter bzw. erfolgreicher wird?
b. Welche Fortschritte bzw. Verbesserungsmöglichkeiten sehen Sie auf nationaler Ebene?
c. Wie erfolgt derzeit der interkantonale Datenaustausch und wie werden interkantonale Fälle bemerkt?
d. Inwiefern könnte ein internationales Übereinkommen zum Datenaustausch hinsichtlich der Beschlagnahme von Crypto-Assets hilfreich sein?
e. Inwiefern könnte die Einführung von Schwarzen Listen für deliktische Crypto-Guthaben sinnvoll sein?