

Giovanni Molo | Matteo Brunone

Kryptowährungen im Visier der staatlichen Kontrolle

Strafrechtliche und regulatorische Aspekte

In der zweiten Hälfte des Jahres 2021 haben Kryptowährungen weltweit die Zahl von 200'000'000 Benutzern erreicht. Das Fehlen einer Vermittlung durch ein echtes Bankinstitut ist oft ein zentraler Punkt für die Attraktivität von Kryptowährungen, wirkt sich aber gleichzeitig auf die Vulnerabilität aus, sowohl in finanzieller als auch in regulatorischer Hinsicht. Mit den neuen Richtlinien der FATF (Financial Action Task Force – Guidance 2021) wurden die Lücken in diesem Bereich teilweise ausgefüllt, insbesondere mit der sogenannten «Travel Rule». Die schweizerische Regulierung hat jedoch – mit der FINMA – diese «Rule» bereits vorweggenommen.

Au second semestre 2021, les cryptomonnaies ont dépassé la barre des 200 000 000 d'utilisateurs dans le monde. L'absence de véritable établissement bancaire comme intermédiaire constitue l'un des principaux facteurs dans l'attrait des cryptomonnaies, mais cet état de fait a également un impact sur la vulnérabilité, tant sur le plan financier que réglementaire. Les nouvelles directives du GAFI (Groupe d'action financière – Lignes directrices 2021) ont partiellement comblé les lacunes dans ce domaine, notamment grâce à la «Travel Rule». La réglementation suisse a toutefois déjà anticipé cette obligation – sous l'impulsion de la FINMA.

-
- I. Einführung
 - II. Ausgangssituation
 - III. Die Merkmale einer Kryptowährung unter einer «funktionalen» Definition
 - IV. Krypto-Ökosystem
 - V. Strafrechtliche Bekämpfung der Geldwäscherei im Umgang mit den Kryptowährungen
 - VI. Diebstahl oder Veruntreuung von Kryptowährungen
 - VII. Beweisfragen im Zusammenhang mit Kryptowährungen in Strafverfahren

GIOVANNI MOLO, Dr. iur., LL.M., Partner Anwaltskanzlei COLLEGAL (Lugano), Dozent SUPSI (The University of Applied Sciences and Arts of Southern Switzerland).

MATTEO BRUNONE, MLaw, Junior Associate Anwaltskanzlei COLLEGAL (Lugano).

Anlass zu diesem Beitrag war das von der SRO (Selbstregulierungsorganisation des Schweizerischen Anwaltsverbandes und des Schweizerischen Notarenverbandes) organisierte und (an fünf verschiedenen Terminen in Zürich, Genf, Olten und Lugano) zwischen August und November 2021 durchgeführte «GwG-Weiterbildungseminar» (vgl. <https://www.sro-sav-snv.ch/aus-und-weiterbildung/seminare>). Der vorliegende Text beruht zum Teil auf dem von Giovanni Molo in diesem Rahmen gehaltenen Referat «Krypto Assets als Vehikel zur Geldwäscherei und deren Bekämpfung».

- VIII. Unterwerfung von Kryptowährungen unter das GwG
- IX. Sind Kryptowährungen dem AIA unterworfen?
- X. Der Ansatz der FINMA zu Kryptotransaktionen
- XI. Financial Action Task Force (on Money Laundering) – Guidance 2021
- XII. Fazit

I. Einführung

Es besteht weder eine Registrierung der Kryptowährungen noch deren Benutzer. Bekannt sind nur die erheblichen Kurschwankungen der berühmtesten Kryptowährungen, wie Bitcoin oder Ethereum.¹ Trotz der Unsicherheit der Kryptowährungen, die sowohl deren genauen Bestand als auch deren Wert betrifft, ist eine Sache sicher: Die Anzahl der Benutzer von Kryptowährungen und das Volumen von Kryptotransaktionen steigen ständig. So wurde berechnet, dass in der zweiten Hälfte von 2020 weltweit die Benutzer von Kryptowährungen (*crypto users*) die Schwelle von 100 Millionen überstiegen haben, während es in 2018 noch ungefähr 35 Millionen waren.² Die sog. *global crypto population* ist im Verlauf von 2021 weiter gestiegen und es wurde berechnet, dass bereits im Juni 2021 die Schwelle von 200 Millionen Be-

¹ Für eine Prüfung der Volatilität dieser zwei Kryptowährungen siehe <https://www.bitcoinsuisse.com/de/research/decrypt/pruefung-der-krypto-volatilitat>, besucht am 31. Januar 2022.

² Cambridge Centre for Alternative Finance (CCAF), 3rd Global Cryptoasset Benchmarking Study, 2020, <https://www.jbs.cam.ac.uk/wp-content/uploads/2021/01/2021-ccaf-3rd-global-cryptoasset-benchmarking-study.pdf>, 44, besucht am 31. Januar 2021.

nutzer überschritten wurde.³ Bezüglich der Merkmale der *crypto users* können zwei *Trends* festgestellt werden.

Erstens bleibt der Kryptomarkt trotz des steigenden Interesses bezüglich Kryptowährungen seitens institutionellen Anlegern *primarily retail-driven*; m.a.W. ist die sog. Kryptobevölkerung (immer noch) vielmehr von Retailkunden als von professionellen Investoren zusammengesetzt.⁴ Zweitens ist der Trend zur Übernahme der Kryptowährungen in den Entwicklungsländern bzw. in Staaten mit einem schwachen Finanzsystem oder mit unstablen Währungen, wie etwa Nigeria, Vietnam oder Brasilien viel stärker als in Nordamerika oder Westeuropa, wo die Kryptowährungen teilweise als eine reine Mode betrachtet werden.⁵

Neue technologische Entwicklungen können zu grossen Veränderungen in Gesellschaft und Wirtschaft (die sog. *Disruption*) führen. Der Gebrauch von Kryptowährungen mittels «*Distributed Ledger*»- bzw. Blockchain-Technologien bringt wesentliches Disruptionspotenzial mit sich. Die wichtigsten Knackpunkte für die Finanzmarktregulierung sind dabei die Dezentralisierung, die eine private und öffentliche «Kontrolle» der Kryptoflüsse erschwert, sowie die Anonymität der dahinterstehenden Parteien, die mit dem Erfordernis der Kenntnis des wirtschaftlichen Begünstigten in Konflikt steht.⁶

Ausgehend von der unaufhaltsamen Verbreitung der Kryptowährungen sowie dem dabei involvierten Disruptionspotenzial sind die Reaktionen der Staaten unterschiedlich. Einige Staaten haben sich für ein absolutes Verbot der Transaktionen mit Kryptowährungen entschieden. So hat insbesondere die chinesische Zentralbank im September 2021 mitgeteilt, dass alle Transaktionen mit Kryptowährungen unrechtmässig sind und dementsprechend inskünftig strafrechtlich behandelt werden. Dieser Schritt war insbesondere von den mit den Kryptowährungen verbundenen Gefahren, so etwa die Entgeltung bzw. die Finanzierung von kriminellen Tätigkeiten oder die Geldwäscherei, motiviert. Gleichzeitig wurde die künftige Einführung eines *digitalen Renminbis* verkündet.⁷ Gemäss einem anderen Ansatz soll es kein absolutes Verbot der Kryptowährungen geben aber die Kryptotransaktionen sollen ähnlich wie die Transaktionen mit Fiat Geld effektiv unter die Kontrolle des Staates fallen. So hat insbesondere der Chairman der amerikanischen FED (*US Securities and Exchange Commission*) das Krypto Ökosystem mit dem «Wild West» verglichen, welches *de facto* von der Durchsetzung eines effektiven Rechtsrahmens weitgehend entbunden ist und demzufolge unter eine starke und wirksame staatliche Kontrolle gesetzt werden muss.⁸ Dieser zweite Ansatz prägt insbesondere auch die Trendlinien der regulatorischen Impulse, die von OECD und FATF entwickelt und von der Schweiz befolgt werden. Die OECD und FATF, die sich in den letzten 20 Jahren als wesentliche globale Standardsetter zu einer zunehmend uniformierten Finanzmarktregulierung durchgesetzt haben,⁹ könnten demzufolge eine ähnliche Rolle im Umgang mit Kryptowährungen übernehmen. Noch mehr als in Bezug auf die Regulierung der Finanztransaktionen sind in diesem Umfeld unentbehrlich regulatorische Vorgaben zu ent-

wickeln, die über die Grenzen der Nationalstaaten hinaus in ähnlicher Weise umgesetzt werden können. Ansonsten besteht die Gefahr, dass die Krypto-Benutzer die staatlichen Regeln mittels ausländischer digitaler Plattformen leicht umgehen und die Krypto-Dienstleister sich in regulatorisch freundlichen Ländern gemäss einem bekannten Pattern zur *Regulatory arbitrage* und *race to the bottom*¹⁰ etablieren. Die nachfolgende Aufzeichnung der regulatorischen Instrumente gegenüber den Kryptowährungen fokussiert sich auf deren elementarste Erscheinungen, d.h. die Kryptotransaktionen. Auf deren Gebrauch als Investitionsmittel oder auf andere *virtual assets* wie die NFT¹¹ wird in diesem Beitrag nicht eingegangen.

II. Ausgangssituation

Um die Besonderheiten der mit den Kryptowährungen involvierten Risiken zu verdeutlichen, kann ein fiktives Beispiel angeführt werden. Nehmen wir an, ein in der Schweiz ansässiger Arzt (A) verwendet einen Cloud-Speicher, um die Daten und Informationen seiner Patienten zu verwalten. Bei der Cloud-Speicherung handelt es sich um eine Technik, bei der eine Reihe von Computern (einschliesslich Smartphones), die sich an verschiedenen Orten befinden, zusammenarbeiten, um gemeinsame Aufgaben unterschiedlicher Art auszuführen.

Dieses System ist (sehr oft) für den Speicherplatz erforderlich, die von einem einzelnen Arbeitsplatz nicht bereitgestellt werden können. In diesem Zusammenhang sind Cloud-Speicherdienste sehr bekannt, d.h. «*services*», die im Internet Platz zum Speichern eigenen Dateien zur Verfügung stellen. Sobald diese gespeichert sind, können sie von einer Vielzahl von Geräten (z.B. PCs, Smartphones und Tablets, aber auch Smart-TVs und andere verbundene Ge-

3 <https://blog.crypto.com/global-crypto-users-over-200-million/>, besucht am 25. Januar 2022.

4 Vgl. Fn. 2, 46.

5 J. WHEATLE/A. KLASA, Cryptocurrencies: developing countries provide fertile ground, *Financial Times*, 09/2021, <https://www.ft.com/content/1ea829ed-5dde-4f6e-be11-99392bdc0788>, besucht am 31. Januar 2022.

6 R. H. WEBER, Führen die neuen Technologien zur Disruption der Finanzmarktregulierung?, *RSDA* 2018, 684 ff.

7 E. OLCOTT/E. SZALAY, China expands crackdown by declaring all crypto activities 'illegal', *Financial Times*, 09/2021, <https://www.ft.com/content/31f7edf7-8e05-46e1-8b13-061532f8db5f>, besucht am 31. Januar 2022.

8 REUTERS, Let us regulate 'wild west' of cryptocurrency, SEC chair urges, *The Guardian*, 3. August 2021, <https://www.theguardian.com/technology/2021/aug/03/cryptocurrency-sec-regulation#:~:text=The%20chair%20of%20the%20US,with%20fraud%20and%20investor%20risk>, besucht am 31. Januar 2022.

9 Zu ihrer Rolle und Merkmalen siehe m.w. H. G. MOLO, *Du secret bancaire à la transparence financière*, Genf 2017 (= DDE 32), 45–47.

10 Sie diesbezüglich m.w. H. MOLO (Fn. 9), 33 f.

11 Ein Non-Fungible Token (NFT) ist eine besondere Art von kryptografischem Token, der die Urkunde und das Echtheitszertifikat eines einzigartigen (digitalen oder physischen) Vermögenswerts auf der Blockchain darstellt; nicht-fungible Token sind daher nicht untereinander austauschbar. Dies steht im Gegensatz zu Kryptowährungen wie Bitcoin und vielen Netzwerk- oder Utility-Tokens, die von Natur aus fungibel sind.

räte) nach dem Durchsuchen eines Browsers oder der Installation einer speziellen Software angezeigt werden.

Plötzlich werden die Daten in der Cloud von A verschlüsselt. A erhält eine E-Mail von einem Hacker, der 10 000 USD in Bitcoin (BTC) von ihm verlangt, um den Entschlüsselungsschlüssel zu erhalten, damit A wieder auf seine sensiblen Daten zugreifen kann. A zahlt unverzüglich und ohne Rücksprache mit den Behörden 10 000 USD von seinem Schweizer Konto auf ein Konto (ebenfalls auf den Namen des Arztes) bei einer estnischen Bank ein. Sobald das Geld auf die estnische Bank eingezahlt wurde, führt er eine Überweisung von diesem Konto an einen VASP (*Virtual Asset Service Provider*) durch, der seine Kryptowährungen verwaltet. Schliesslich überweist der VASP 10 000 USD in BTC an die *wallet* des Hackers, der die Entschlüsselung erlaubt.

III. Die Merkmale einer Kryptowährung unter einer «funktionalen» Definition

Gemäss der Definition, die von Satoshi Nakamoto am 31. Oktober 2008 geprägt wurde, ist eine Kryptowährung eine virtuelle Währung, die ein Peer-to-Peer-Zahlungssystem ermöglicht.¹² Satoshi Nakamoto ist das Pseudonym der Person, die die Kryptowährung Bitcoin «erfunden» hat. Der Begriff «Bitcoin» bezieht sich auch auf die *Open-Source-Software*, mit der das Kommunikationsprotokoll und das daraus resultierende Peer-to-Peer-Netzwerk implementiert werden.

In einer Stellungnahme der EZB¹³ vom 12. Oktober 2016 wurde der Begriff «virtuelle Währungen» wie folgt definiert: «eine digitale Darstellung eines Werts, die von keiner Zentralbank oder öffentlichen Stelle emittiert wurde und nicht zwangsläufig an eine echte Währung angebunden ist, aber von natürlichen oder juristischen Personen als Zahlungsmittel akzeptiert wird und auf elektronischem Wege übertragen, gespeichert und gehandelt werden kann».¹⁴

Diese Haltung lässt den Schluss zu, dass es sich bei einer Kryptowährung noch nicht um eine offizielle Währung handelt.¹⁵ Insbesondere besteht im Zusammenhang mit einer Kryptowährung kein offizieller Kurs und sie kann im Zahlungsverkehr nicht zwingend als Zahlungsmittel anerkannt werden. Gerade weil in der Schweiz die Zuständigkeit zur Emittierung der Währung ausschliesslich bei der SNB¹⁶ liegt, ist ein BTC weder eine Währung im strengen juristischen Sinne noch ein Buchgeld oder eine elektronische Währung (wie eine Prepaid-Karte).¹⁷ Es handelt sich jedoch um eine Währung im wirtschaftlichen Sinne,¹⁸ eben weil sie (i) ein Tauschmittel mit (ii) einer Recheneinheit und (iii) einem Wert ist und daher eine «private Währung» im Sinne des ZGB und des OR sein kann.¹⁹

Im Gegensatz zur Schweiz war El Salvador der erste Staat, der Bitcoin als offizielle Währung zugelassen hat und ab September 2021 wird die digitale Währung zusammen mit dem US-Dollar landesweit offiziell anerkannt.²⁰ Die Neuigkeit ist jedoch, dass Kryptowährungen auf der *blockchain*, d.h. einem digitalen Register, dessen Einträge in «Blöcken» gruppiert und in chronologischer Reihenfolge

verkettet²¹ werden, ausgetauscht werden und somit sind die Rückverfolgbarkeit, die Anonymität, das Fehlen von Transaktionskosten und die Unmittelbarkeit der Ausführung immer garantiert, da sie dezentralisiert sind. Anzumerken ist, dass die Kryptowährungen nicht nur als Privatwährungen, da sie dem Monopol der Zentralbanken entzogen sind, sondern auch als dezentralisierte Währungen gelten, da sie der Intermediation von Banken und anderen Finanzdienstleistern herausgegriffen werden. Das staatliche Geldmonopol wurde bereits in den 70er Jahren von Friedrich von Hayek in seinem Werk «*The Denationalisation of Money*» sowie von Milton Friedman als Gründer des Monetarismus infrage gestellt. Um die Versuchung zu beseitigen, den staatlichen Haushalt durch eine politisch gesteuerte Abwertung der Währung zu sanieren, und dadurch Inflation zu verursachen, wurde ein System verschiedener, parallel existierender Währungen vorgeschlagen, die durch private Stellen ausgegeben und gesteuert werden.²² Ungefähr 40 Jahre nach dieser neoliberalen Vision zerbrechen die Kryptowährungen tatsächlich die ausschliessliche Souveränität der Staaten zur Geldemittierung. Sie gehen sogar einen Schritt weiter, indem sie von der Zugriffsmöglichkeit, der vom Staat beauftragten und beaufsichtigten Intermediäre, d.h. insbesondere der Banken, losgelöst werden. Da solche Intermediäre Kernbestandteile zur Wahrung von öffentlichen Interessen – insbesondere im Rahmen der Vermeidung von Geldwäscherei und der steuerlichen Transparenz – geworden sind, besteht der problematische Charakter der Kryptowährungen vor allem darin.

IV. Krypto-Ökosystem

Man könnte sich ein Ökosystem bezüglich Überweisung durch Kryptowährungen vorstellen. Grundsätzlich hat jede *wallet*, in der Kryptowährungen aufbewahrt werden können, einen öffentlichen Schlüssel (*public key*) und einen privaten Schlüssel (*private key*). Der öffentliche Schlüssel ist dem *Ex*

12 Vgl. <https://bitcoin.org/bitcoin.pdf>.

13 Europäische Zentralbank.

14 Stellungnahme der Europäischen Zentralbank vom 12. Oktober 2016 zu einem Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Änderung der Richtlinie (EU) 2015/849 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung und zur Änderung der Richtlinie 2009/101/EG (CON/2016/49); § 1.1.3.

15 L. MÜLLER/M. ONG, Aktuelles zum Recht der Kryptowährungen, in: AJP/PJA 2020, 198 ff.

16 Schweizerische Nationalbank.

17 MÜLLER/M. ONG (Fn. 15).

18 Vgl. auch Bundesgesetz über die Währung und die Zahlungsmittel (WZG).

19 L. MÜLLER/ONG (Fn. 15).

20 Vgl. <https://nzzas.nzz.ch/wirtschaft/bitcoin-offizielles-zahlungsmittel-in-el-salvador-ld.163011?reduced=true>.

21 m.a.W. eine dezentral geführte Kontobuchtechnologie, d.h. Distributed-Ledger-Technologie.

22 Siehe dazu H.M. PETRY, Universelle Kryptowährungen und Blockchain-Technologie aus der schweizerischen Rechnungslegungs-, Steuer- und Revisionsperspektive, 2021, 15 f.

*change*²³ bekannt, so dass im Falle von Transaktionen die beiden Parteien, die Kryptowährungen kaufen und/oder verkaufen, den öffentlichen Schlüssel der jeweils anderen Partei kennen. Und dies gilt sowohl für Transaktionen von USD mit BTC (d.h. der Umtausch von klassischer Währung in Kryptowährung) als auch für Transaktionen von BTC mit BTC (Kryptowährung mit Kryptowährung).

Im Gegensatz dazu ist der private Schlüssel, der die *wallet* identifiziert, nur dem rechtmässigen Eigentümer bekannt. Bei den *wallet provider* unterscheidet man zwischen Anbietern mit Verwahrung (*custodial*) und Anbietern ohne Verwahrung (*non-custodial*).²⁴

Custodial wallet provider definieren sich auch als «Unternehmen», die Dienstleistungen zur Sicherung von privaten Schlüsseln im Namen ihrer Kunden anbieten, um virtuelle Währungen zu halten, zu speichern und zu übertragen. Im Gegenteil ist ein *non-custodial wallet provider*, die eine *Crypto-Wallet* bietet, ein «Unternehmen» bei dem nur der Eigentümer Zugriff auf die privaten Schlüssel der *wallet* hat. Das bedeutet, dass nur der Nutzer z.B. auf BTC in der *wallet* zugreifen kann.²⁵ Durch den Eingriff eines VASPs, der eine *custodial wallet* führt, wird der Zahlungsverkehr mittels Kryptowährungen in einer gewissen Weise wieder zentralisiert. Die Bewahrung und der Austausch solcher Werteinheiten erfolgt denn durch Intermediäre, welche die Funktion der Finanzdienstleister im (traditionellen) Finanzsektor analoger Weise im Krypto-Ökosystem übernehmen.

V. Strafrechtliche Bekämpfung der Geldwäscherei im Umgang mit den Kryptowährungen

Der Begriff «Geldwäscherei» geht auf die metaphorische Verwendung der Worte «Wäsche» und «Geld» zurück und diese Begriffsverknüpfung ist offensichtlich die Übersetzung der englischen und amerikanischen Begriffe *money washing* bzw. *money laundering*.²⁶ Geldwäscherei im weitesten Sinne umfasst alle Handlungen, die darauf abzielen unrechtmässig erworbene Vermögenswerte (mit Hilfe rechtmässiger oder unrechtmässiger Finanzmarktmittel) zu verschleiern.²⁷ Der Zweck dahinter ist immer, Erträge aus Straftaten zu erhalten und zu vermehren sowie den Ermittlungsbehörden zu entgehen.²⁸ Mit anderen Worten, ist «Geldwäsche» ein Prozess, bei dem die Existenz, die unrechtmässige Herkunft oder die Verwendung von Gewinnen verheimlicht wird.²⁹ Im Prinzip kann jeder wegen Geldwäsche haftbar gemacht werden. Gegenstand der Geldwäscherei sind Vermögenswerte, die aus einem Verbrechen stammen (Art. 305^{bis} Abs. 1 StGB).³⁰ Bei der Definition von Verbrechen wird die technische Definition von Art. 10 Abs. 2 StGB verwendet.³¹ Danach muss es sich um echte (vorsätzliche)³² Vereitelungshandlungen handeln, die verhindern, dass die wahre (und kriminelle) Herkunft des fraglichen Vermögenswertes erkannt wird.³³ Da es nicht nur um Geld i.e.S. geht, fragt sich, ob Kryptowährungen überhaupt Gegenstand der Geldwäscherei sein können.

Bei den Kryptowährungen handelt es sich denn weder um gesetzliche Währungen noch um bewegliche oder un-

bewegliche Sachen im Sinne des ZGB oder um Wertpapiere wie Aktien, Obligationen oder Derivate.³⁴

Kryptowährungen sind jedoch Vermögenswerte im Sinne einer erweiterten Definition. Wie bereits erwähnt, handelt es sich um Währungen im wirtschaftlichen Sinne, die einen Austausch zwischen Privatpersonen ermöglichen. Kryptowährungen fallen daher unter die weit gefasste Definition von Vermögenswerten, die eine Geldwäschehandlung ermöglichen können: Die Umwandlung in Kryptowährungen und die Durchführung eines Transfers fallen potenziell unter Artikel 305^{bis} StGB. Dies bedeutet, dass wenn eine qualifizierte Vortat (d.h. ein Verbrechen) vorliegt (wie z.B. Veruntreuung gem. Art. 138 StGB, Betrug gem. Art. 146 StGB oder betrügerischer Konkurs gem. Art. 163 StGB), auch Kryptowährungen unter die potenziellen Vermögenswerte fallen, die geeignet sind, den Geldwäscherei-Tatbestand zu erfüllen.³⁵ Dies wäre nicht der Fall, wenn es sich um einen Fall von Steuerhinterziehung handeln würde, wohl aber wenn es um ein qualifiziertes Steuervergehen ginge. Aus Artikel 305^{bis} Abs. 1^{bis} StGB ergibt sich nämlich, dass das qualifizierte Steuervergehen ein Steuerbetrug im Sinne von Art. 186 DBG³⁶ oder 59 Abs. 1 StHG³⁷ ist.³⁸ Diese beiden letztgenannten Straftatbestände sind miteinander

23 Wörtlich übersetzt wäre das eine Kryptobörse, d.h. ein Unternehmen, das es Kunden ermöglicht, Kryptowährungen oder digitale Währungen gegen andere Vermögenswerte wie herkömmliches Fiatgeld oder andere digitale Währungen zu tauschen. *Exchanges* können Kreditkartenzahlungen, Überweisungen oder andere Formen der Zahlung im Austausch gegen digitale Währungen oder Kryptowährungen akzeptieren.

24 M. KUNZ, Regulierung von Verwahrungslösungen für Virtual Assets nach Schweizer Recht (online article), in: MME Magazine (verfügbar unter dem Link: <https://www.mme.ch/de-ch/magazin/artikel/regulierung-von-verwahrungslösungen-für-virtual-assets-nach-schweizer-recht>).

25 KUNZ (Fn. 24).

26 J.-B. ACKERMANN/S. ZEHNDER, in: J.-B. Ackermann (Hg.), Kommentar. Kriminelles Vermögen. Kriminelle Organisationen. Band II, Zürich 2018, StGB 305^{bis} N 1 ff.

27 K. SALA, Riciclaggio di denaro ex art. 305^{bis} CP, in: *Novità Fiscali* 2020 (6).

28 A. DONATSCH/M. THOMMEN/W. WOHLERS, Strafrecht IV. Delikte gegen die Allgemeinheit, 5. Aufl., Zürich 2017, 491.

29 ACKERMANN/ZEHNDER, (Fn. 26), StGB 305^{bis} N 1 ff.; M. PIETH, in: M. A. Niggli/H. Wiprächtiger (Hg.), Basler Kommentar zum Strafrecht. Band II, 4. Aufl., Basel 2018, Vor. StGB 305^{bis} N 1 ff.

30 D. OSWALD, Erlös aus Kryptowährungen, Ein unterschätztes Geldwäscherei-Risiko der Banken, NIWUZ – Veröffentlichungen aus dem LL.M.-Studiengang Internationales Wirtschaftsrecht der Universität Zürich und des Europa Instituts an der Universität Zürich Band/Nr. 111 (2021), 29 ff.

31 «Verbrechen sind Taten, die mit Freiheitsstrafe von mehr als drei Jahren bedroht sind».

32 Art. 305^{bis} StGB ist ein Vorsatzdelikt und für die Vollendung der Straftat ist entweder Vorsatz erforderlich oder *dolus eventualis* ausreichend.

33 PIETH, (Fn. 29); Vor StGB 305^{bis} N 1 ff; SALA (Fn. 27).

34 G. MOLO/J. DRZALIC, Können Kryptowährungen compliant sein?, in: *AJP/PJA* 2019, 40 ff.

35 MOLO/DRZALIC (Fn. 34).

36 Bundesgesetz über die direkte Bundessteuer.

37 Bundesgesetz über die Harmonisierung der direkten Steuern der Kantone und Gemeinden.

38 B. ISENING, in: A. Donatsch (Hg.), StGB/JStG Kommentar. Mit weiteren Erlassen und Kommentar zu den Strafbestimmungen des SVG, BetmG und AuG/AIG, 20. Aufl., Zürich 2018, StGB 305^{bis} N 22.

verbunden, so dass ein qualifiziertes Steuervergehen nur bei der Verwendung gefälschter, inhaltlich unwahrer oder verfälschter Dokumente zum Zwecke der Steuerhinterziehung vorliegt.³⁹ Das qualifizierte Steuervergehen gilt übrigens nur dann als begangen, «wenn die hinterzogenen Steuern pro Steuerperiode mehr als 300 000 Franken betragen».

Demgegenüber stellt eine Überweisung einer «Gegenleistung in Kryptowährung» für eine kriminelle Tat (wie Drogenhandel oder Erpressung gem. Art. 156 StGB) keine «Selbstgeldwäsche» dar, aber ihre anschliessende Übertragung ist Geldwäscherei, insbesondere wenn sie darauf abzielt, zu verhindern, dass die Herkunft der Erträge aus der Straftat festgestellt werden kann. In unserem Ausgangsbeispiel stellt die Zahlung von A (der erpresst wurde) also keine Geldwäscherei dar. Von dem Moment an, in dem der Hacker die in BTC erhaltenen Werte auf eine andere *Exchange* verschiebt, sie abhebt oder verwendet, begeht er eine Handlung, die geeignet ist, die Ermittlung der Herkunft, die Auffindung oder die Einziehung von Vermögenswerten zu vereiteln und erfüllt damit die rechtlichen Voraussetzungen der Geldwäscherei.

VI. Diebstahl oder Veruntreuung von Kryptowährungen

Ein Diebstahl von Kryptowährungen fällt nicht unter den Tatbestand von Art. 139 StGB, weil Kryptowährungen nicht als körperliche Gegenstände qualifiziert werden können. Sie können aber auf einem CPU (wie z.B. ein USB-Stick) und damit auf einer «beweglichen Sache» verarbeitet, gespeichert oder übertragen werden und dann kommt ein solcher Tatbestand in Frage.⁴⁰ Wenn ein Täter folglich versucht, die Auffindung der Vermögenswerte zu verhindern, liegt eine Geldwäschereihandlung vor.⁴¹ Da der Diebstahl von Kryptowährungen in sich kein Diebstahl i.S.v. Art. 139 StGB ist, erfolgt jedoch eine unrechtmässige Datenerhebung i.S.v. Art. 143 StGB.⁴² Im Rahmen der Anwendung von Art. 143 StGB könnte man sich hypothetisch vorstellen, dass ein Hacker nicht nur wie in unserem Ausgangsbeispiel einen Arzt erpresst, sondern auch in den Besitz des *private keys* einer *wallet* auf einer *Exchange* gelangt. An dieser Stelle ist die Veruntreuung von Vermögenswerten, d.h. Art. 138 Abs. 2 StGB, zu prüfen. Da es sich bei Kryptowährungen tatsächlich um Vermögenswerte handelt, erfüllen sie eine der objektiven Voraussetzungen der Veruntreuung. Es liegen aber zwei unterschiedliche Szenarien vor: eines geht davon aus, dass es einem Hacker gelingt, den privaten Schlüssel einer Person zu stehlen. Dies würde nicht unter den Begriff der Veruntreuung fallen, aber unter denjenigen der unrechtmässigen Datenerhebung, weil der Täter den Besitz der Kryptowährungen nicht rechtmässig erwirbt. Im Gegenteil, wenn eine Person vorsätzlich einem Dritten seine privaten Schlüssel für den Zugang zur *wallet* anvertraut und ihm erlaubt, Transaktionen mit seinen Kryptowährungen durchzuführen, könnte – im Fall eines Missbrauchs – eine Veruntreuung begangen werden.

VII. Beweisfragen im Zusammenhang mit Kryptowährungen in Strafverfahren

Im Hinblick auf die Beweisführung, ermöglicht die *blockchain* die Rückverfolgbarkeit und macht die Finanzströme unveränderbar, was die Rekonstruktion der Ermittlungen erleichtert. Wie bereits erwähnt, kann die *blockchain* als eine gemeinsam genutzte und unveränderliche Struktur definiert werden, die auch für den Austausch von Informationen verwendet wird.

Da es sich um ein Register handelt, das die Rückverfolgbarkeit des gesamten Austauschs zwischen verschiedenen Nutzern enthält, wird die «Chronologie» des Registers ständig gemeinsam genutzt, und jede Komponente besitzt eine aktualisierte Kopie. Die Sicherheit und der Datenschutz werden durch Kryptographie gewährleistet, da der Inhalt des Registers, sobald er einmal geschrieben wurde, nicht mehr gelöscht werden kann und unveränderbar bleibt.⁴³ Dadurch werden alle Austauschvorgänge und Transaktionen, die innerhalb des Registers stattgefunden haben, aufgezeichnet und können rückwirkend rekonstruiert werden, was auch einem eventuellen Strafverfahren zugutekommt.⁴⁴ Bemerkenswert ist, dass das FBI in den USA gezeigt hat, dass es die *blockchain* sogar ausnutzen kann, indem es BTC, die als Lösegeld an russische Hacker (von DarkSide) gezahlt wurden, nachverfolgt hat. Durch die Untersuchung der *blockchain* konnten die Strafverfolgungsbehörden mehrere BTC-Transfers zurückverfolgen und feststellen, dass es sich dabei um den Erlös aus der Zahlung eines Opfers handelte. Die BTCs wurden dann an eine bestimmte Adresse übertragen, für die das FBI den privaten Schlüssel ergriffen hat. Es ist unklar, wie genau das FBI in den Besitz des privaten Schlüssels der Hacker gekommen ist, möglicherweise durch die Beschlagnahme einiger Server von DarkSide, auf denen die privaten Schlüssel der *wallet* gehostet waren.⁴⁵

Dementsprechend kann man – wenn man herausfinden kann, wer hinter einer *wallet* «steckt» – tatsächlich auch herausfinden, wer der Täter bzw. Geldwäscher ist. Dies ist jedoch nur möglich, wenn der Eigentümer der virtuellen *wallet* «entschlüsselt» werden kann, d.h. sein Name einem VASP bekannt ist oder sonst wie herausgefunden werden kann.

Was die Einziehung von Erträgen aus Straftaten oder einer gleichwertigen Entschädigung (Art. 70 und 71 StGB) betrifft, so ist die Einziehung oder Beschlagnahme durch Zwangsmassnahmen gegen den Eigentümer der virtuellen

39 ISENRING (Fn. 38), StGB 305^{bis} N 22; SALA (Fn. 27).

40 Bericht des Bundesrates zu virtuellen Währungen in Beantwortung der Postulate Schwaab (13.3687) und Weibel (13.4070) vom 25 Juni 2014, 21 f.

41 MOLO/DRZALIC (Fn. 34).

42 Vgl. Fn. 33.

43 MÜLLER/ONG (Fn. 15).

44 MÜLLER/ONG (Fn. 15); vgl. auch <https://bitcoin.org/bitcoin.pdf>.

45 C. NUTTAL, *Feds use blockchain for busts*, in: Financial Time (online/ 8. Juni 2021).

wallet nur möglich, wenn ein «*custodial wallet Provider*»⁴⁶ vorhanden ist.⁴⁷

Wenn die Ermittlungsbehörden CPUs oder Smartphones beschlagnahmen, die wiederum eine durch einen privaten Schlüssel geschützte wallet enthalten, wird es schwierig, diese ohne die Mithilfe des Beschuldigten in einem Strafverfahren zu verwerten. Grundsätzlich gilt jedoch auch im IT-Strafrecht der *nemo-tenetur*-Grundsatz, der besagt, dass niemand gezwungen werden kann, sich selbst zu beschuldigen.⁴⁸ Die Selbstbeschuldigung schliesst die Übergabe des privaten Schlüssels, der den Zugang zur wallet ermöglicht, ein. Demzufolge kann der Beschuldigte nicht gezwungen werden, aktiv an der Aufklärung des Sachverhalts mitzuwirken und er ist daher nicht verpflichtet, seinen privaten Schlüssel zur Verfügung zu stellen.⁴⁹

Unter Umständen könnte allerdings bei Verweigerung eine Untersuchungshaft (UH) nach Art. 220 ff. StPO in Frage kommen. Weigert sich ein Beschuldigter, der Staatsanwaltschaft seinen privaten Schlüssel mitzuteilen, könnte diese, aufgrund der Fluchtgefahr (Art. 221 Abs. 1 lit. a StPO) oder Kollusionsgefahr (lit. b), die UH anordnen,⁵⁰ denn ohne die Freigabe des privaten Schlüssels durch den Beschuldigten (der möglicherweise Millionen von BTC in seiner wallet hat), besteht das Risiko, dass er in ein anderes Land flieht (lit. a) oder die Beweise unterschlägt (lit. b). Die UH darf jedoch in keinem Fall als Druckmittel angewendet werden.

VIII. Unterwerfung von Kryptowährungen unter das GwG

Neben den strafrechtlichen Regelungen (StGB/StPO) gibt es auch einen regulatorischen Ansatz, d.h. das Geldwäschereigesetz (GwG; RS 955.0). Folglich gibt es in der Schweiz nebst dem Strafrecht auch einen präventiven und regulatorischen Aspekt, der nur bestimmte Akteure, nämlich die Finanzintermediäre (FI), betrifft.

FI werden in Art. 2 Abs. 2 und 3 GwG definiert und sind in der Regel (unter anderem) Banken, Vermögensverwalter, Trustees, Investmentgesellschaften, Versicherungseinrichtungen, und so weiter. FI sind auch Personen, die Dienstleistungen für den Zahlungsverkehr erbringen, namentlich für Dritte elektronische Überweisungen vornehmen (Art. 2 Abs. 3 lit. b GwG). Dies impliziert, dass der gewerbmässige Umtausch von Wertpapieren in Kryptowährungen oder von Kryptowährungen in Wertpapiere oder andere Kryptowährungen (sog. «*virtual currency exchanges*») dem GwG (vgl. Art. 1 Abs. 1 GwG) unterliegen. Im Gegenteil unterliegen die Flüsse von Kryptowährungen als solche nicht dem GwG.

Nach der von der *Financial Action Task Force (on Money Laundering)* in seinen *Guidances* (sowohl im 2019 als auch im 2021) gegebenen Definition ist ein *Virtual Asset Service Provider* (VASP) jede natürliche oder juristische Person, die berufsmässig tätig ist und (unter anderem) eine der folgenden Tätigkeiten führt: Austausch (*exchange*) zwischen virtuellen Vermögenswerten und Fiat-Währungen⁵¹ oder Übertragung (*transfer*) von virtuellen Vermögenswerten.⁵²

Die Folge von gesetzlichen oder regulatorischen Pflichten für einen VASP, der als FI qualifiziert wird, ist die Unterwerfung unter alle Vorschriften welche die klassischen KYC- und CDD-Prinzipien (*know your customer* und *client due diligence*) entwickeln. Daneben wird verlangt, dass FI welche Tätigkeiten ausüben, die mit einem Geldwäschereirisiko verbunden sind, sich unabhängig einer Selbstregulierungsorganisationen (SRO) anschliessen müssen.⁵³

Dies bedeutet, dass VASPs auch unter die Definition des FIs im Sinne des GwG fallen, und dies impliziert dass auch für VASPs die Identifizierung der wirtschaftlichen Eigentümer einer wallet und die Überprüfung des Hintergrunds der Transaktionen immer notwendig sind.⁵⁴ Die VASPs, die eine breitere Kategorie als eine *Exchange* darstellen, sollen auch die wichtigsten Vorschriften für FI respektieren: Es ist immer notwendig die Identifizierung (durch die massgebenden Dokumente) der Vertragspartei nach Art. 3 GwG durchzuführen oder z.B. der Meldepflicht nach Art. 9 GwG nachzugehen. Die Technologie kann ebenfalls nützlich sein, da es die «*storing transaction data on blockchain*» möglich macht und demzufolge wird der virtuelle «*paper trail*» vereinfacht. Dies erleichtert unter Umständen auch eine Meldung an die MROS (gem. Art. 9 GwG).⁵⁵ Die Aufsicht über die Einhaltung dieser Pflichten liegt für FI bei der FINMA oder bei den anerkannten SRO.⁵⁶

Das schweizerische Aufsichtssystem ist sozusagen hybrid: die FINMA bewilligt einzelne FI, aber die Aufsicht bleibt manchmal auch privat und wird durch SRO ausgeführt, welche ihrerseits selbst der Bewilligung der FINMA unterliegen.⁵⁷ Im traditionellen Finanzsektor ist eine FINMA-Bewilligung ab dem Zeitpunkt erforderlich, an dem das Vermögen eines Kunden angenommen wird und für ihn

46 Bei der *custodial wallet* wird die *private key* dem Finanzintermediär «anvertraut».

47 MOLO/DRZALIC (Fn. 34).

48 R. HAUSER/E. SCHWERI/K. HARTMANN, Schweizerisches Strafprozessrecht, Basel, § 39 N 14.

49 HAUSER/SCHWERI/HARTMANN (Fn. 48), § 39 N 14; vgl. auch «Rechtliche Voraussetzungen und praktische Umsetzbarkeit der Einziehung von Kryptowährungen im Strafverfahren», 14. September 2021 (auf <<https://www.strafrecht-digital.com>>, besucht am 25. Januar 2022).

50 M. FORSTER, in: M. A. Niggli/M. Heer/H. Wiprächtiger (Hg.), Basler Kommentar zur Schweizerischen Strafprozessordnung (StPO)/Jugendstrafprozessordnung (JStPO), 2. Aufl., Basel 2014, StPO 220 N 3.

51 Fiatgeld bezeichnet ein Zahlungsmittel, das nicht durch Reserven anderer Materialien (z.B. Goldreserven) gedeckt ist und daher keinen inneren Wert (auch nicht indirekt) hat. Gesetzliches Zahlungsmittel (in der Regel in Form von Banknoten, aber auch in Form von Münzen aus Nichtedelmetall) hat daher einen Wert aufgrund der Tatsache, dass es eine Behörde (regelmässig den Staat) gibt, die so handelt, als hätte es diesen Wert.

52 Vgl. <<https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf>>, besucht am 25. Januar 2022.

53 Vgl. Art. 14 GwG.

54 MOLO/DRZALIC (Fn. 34).

55 Am 16. Februar 2018 hat die FINMA eine Wegleitung für Unterstellungen betreffend Initial Coin Offerings (ICOs) veröffentlicht, in der Token-Kategorien festgelegt und die Rechtsfolgen bei der Qualifikation als Effekten erläutert werden (Ziff. 3.3 ff.); vgl. auch MOLO/DRZALIC (Fn. 34).

56 Vgl. Art. 12 GwG.

57 MOLO/DRZALIC (Fn. 34).

Finanzleistungen ausgeübt werden. Entsprechend eines Ansatzes von Technologieneutralität, gilt dieses Erfordernis auch für FI, die Dienstleistungen mit virtuellen Währungen anbieten und dafür ein *Crypto-wallet* unterhalten. Gemäss der aktuellen Praxis der FINMA ist eine Bankbewilligung jedoch *nicht* notwendig, wenn virtuelle Vermögen ausschliesslich zur Verwahrung übertragen und pro Kunde separat auf der *blockchain* gehalten werden und dem einzelnen Kunden jederzeit zugeordnet werden können. Deshalb ist das schweizerische Aufsichtssystem hybrid, denn da eine Bewilligung der FINMA nicht erforderlich ist, fallen die Erbringung von Verwahrungs- und Zahlungsdienstleistungen mit virtuellen Währungen (sog. *custodial wallet provider*) sowie der Betrieb von *Exchanges*, die den Kauf und Verkauf von z.B. BTC anbieten, unter das Geldwäschereigesetz (GwG) und folglich auch unter die SROs.⁵⁸

IX. Sind Kryptowährungen dem AIA unterworfen?

Der AIA (Automatischer Informationsaustausch (IA) oder AEO) wurde durch den Bundesrat als ein «*in regelmässigen Abständen zwischen zwei Staaten stattfindender Austausch von Informationen über Konten, die eine in einem bestimmten Staat steuerpflichtige natürliche oder juristische Person bei einem Finanzinstitut in einem anderen Staat hält*», definiert.⁵⁹ Diese systematische und regelmässige Übermittlung einer im Voraus bestimmten Menge von Informationen, in bestimmten periodischen Intervallen, von einem Staat an einen anderen Staat, zum Zweck der Steigerung der steuerlichen Konformität der Steuerpflichtigen⁶⁰ ist, wie aus dem Abschnitt IA GMS (d.h. gemeinsamer Meldestandard; Melde- und Sorgfaltsstandard der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) für Informationen über Finanzkonten) hervorgeht, auf die durch meldende Finanzinstitute gehaltenen meldepflichtigen Konten eingegrenzt. Können *Crypto-wallets* als meldepflichtige Konten betrachtet werden?

An sich ist in der enumerativen Bezeichnung der Begriffsbestimmungen von Finanzinstitut, -vermögen und -konto, die in den Abschnitten VIIIA und VIIC GMS enthalten sind und die auf eine Auflistung von Fallgruppen aufgebaut wird, keine Rede von Kryptowährungen und -vermögensbestandteile. Demzufolge ist es *de lege lata* unklar ob gemäss dem internationalen Standard des OECDs⁶¹ und der schweizerischen Implementierung dieses Standards⁶² die Kryptowährungen durch den AIA gedeckt sind oder nicht. Indem in der Schweiz die Registrierung als meldendes Finanzinstitut unaufgefordert und auf eigene Initiative des Instituts erfolgt,⁶³ übt das Finanzinstitut einen gewissen Ermessensspielraum über seinen eigenen Status aus und hat mit Bezug auf die Qualifizierung der VASPs als meldende Finanzinstitute keine feste Praxis entwickelt. Es erscheint, dass diese, soweit sie der FINMA-Bewilligung und -Aufsicht unterstehen, sich als meldende Finanzinstitute registrieren. So informiert ein solches Institut auf seiner Website, dass sofern ein Kunde in einem Staat (Jurisdiktion) ansässig ist, mit dem die Schweiz ein AIA-Abkommen unterzeichnet

hat, es verpflichtet ist, Informationen zur Identität des Kunden sowie bestimmte Kontoinformationen an die Eidgenössische Steuerverwaltung zu melden.⁶⁴ Während die VASPs, die der Bankbewilligung und -Aufsicht durch die FINMA unterliegen, sich zugleich als meldende Finanzinstitute zu den AIA-Zwecken qualifizieren lassen, ist nicht ersichtlich, ob dies auch in Bezug auf VASPs, die lediglich dem GWG aber nicht dem BankG unterstellt sind, der Fall ist.

Um Klarheit zu schaffen und den objektiven Anwendungsbereich des AIA auf die Kryptowährungen zu erstrecken, hätte Ende 2021 in der OECD ein neues multilaterales Regelwerk betreffend den Austausch von Informationen über virtuelle Vermögenswerte («Krypto-Standard») verabschiedet werden sollen. Dieser Standard sollte unabhängig vom bestehenden AIA-Standard angewendet werden um auch diejenigen Staaten, die den geltenden AIA-Standard nicht umsetzen (darunter die USA), miteinzuziehen.⁶⁵ Dieses Regelwerk wurde zurzeit noch nicht geschaffen. Es bleibt abzuwarten, inwieweit alle VASPs tatsächlich miteingezogen werden können. Äusserst schwierig, wenn nicht sogar unmöglich, wird es jedenfalls sein, die horizontalen dezentralisierten *peer-to-peer* Kryptoflüsse sowie die *non custodial wallet* zu umfassen. Denn der AIA basiert auf einem meldenden Institut, das in einem dezentralisierten Austauschsystem definitionsgemäss fehlt.

X. Der Ansatz der FINMA zu Kryptotransaktionen

Die FINMA hat am 26. August 2019 die FINMA-Aufsichtsmitteilung 02/2019, «Zahlungsverkehr auf der Blockchain» erlassen. Diese Aufsichtsmitteilung erweitert die *Guidance* der FATF, d.h. *Financial Action Task Force (on Money Laundering)* von 2019 (*Guidance for a Risk-Based Approach, Virtual Assets and Virtual Asset Service Providers*, Juni 2019).

Derzeit gibt es im Bereich der Kryptotransaktionen, kein System, das wie das SWIFT für die Banken funktioniert. Eine solche Methode würde eine zuverlässige Übermittlung von Identifizierungsdaten im Zusammenhang mit Zahlungsvorgängen in die *blockchain* erlauben. Aus dem Fehlen der SWIFT-Methode in der *blockchain*, müssen sich in der

58 FINMA, Faktenblatt Stand 1. Januar 2020 Virtuelle Währungen, <<https://www.finma.ch/de/~media/finma/dokumente/dokumententcenter/myfinma/faktenblaetter/faktenblatt-virtuelle-waehrungen.pdf?la=de>>, besucht am 31. Januar 2022.

59 Botschaft zum AIA, BBl 2015 5437, 5447.

60 G. MOLO/L. SCHLICHTING/S. VORPE, Automatischer Informationsaustausch in Steuersachen. Kommentar, Basel 2018, AIAG 6 N 4 und 6.

61 Siehe dazu A. KNOBEL, Report commissioned by the Greens/EFA Group in the European Parliament, Reporting taxation: Analysing loopholes in the EU's automatic exchange of information and how to close them, 15. Oktober 2018, 18.

62 Siehe dazu T. FERNANDEZ-LEENKNECHT, Common Reporting Standard: The blockchain-based assets case, 15. November 2019, in <www.lawded.ch>, 17.

63 MOLO/SCHLICHTING/VORPE (Fn. 60), AIAG 13 N.

64 <<https://www.cryptofinance.ch/automatischer-informationsaustausch-in-steuersachen-aia/>>, besucht am 19. Januar 2022.

65 T. PFAMMATTER, Blickpunkt internationale Steuerpolitik 2021, RF 76/2021 618 – 620.

Schweiz solche Zahlungsvorgänge oder Vereinbarungen zwischen FI bewähren und einer angemessenen GwG-Aufsicht unterstehen.

Im Gegensatz zu den von der FATF herausgegebenen Standards, sieht Art. 10 GwV-FINMA keine Ausnahmen für Zahlungen mit nicht von beaufsichtigten VASPs betriebenen *wallets* vor. Aus diesem Grund hat die FINMA für die Welt der VASPs strengere Richtlinien als die FATF gesetzt. Es wurde mit anderen Worten ein «*swiss-finish*» geschaffen. Wenn es beispielsweise für einen FI «subjektiv» notwendig ist, seinen Kunden zu kennen, so ist es objektiv auch notwendig, die Herkunft eines bestimmten Vermögenswertes zu kennen.

Bei Transaktionen über das SWIFT-System werden sowohl der Kommittent als auch der Destinatär identifiziert (vgl. Art. 10 GwV-FINMA).⁶⁶ Aus diesen Prinzipien, verlangt die FINMA Technologieneutralität.⁶⁷ Es ist aber nicht möglich das SWIFT-System auf einer Kette (wie der *blockchain*) zu benutzen, da es dezentralisiert ist und die beiden Parteien nicht bekannt sind. Für die FINMA ist es notwendig, dass die Parteien immer identifiziert sind und die Aufsichtsbehörde erlaubt deshalb (mit einer strengeren Regelung als derjenigen unter den FATF-Standards), dass Zahlungen nur an bereits bekannte Kunden oder an externe *wallets* eines bekannten Kunden geleistet werden können. Dieser «*swiss-finish*»-Ansatz geht über die Anforderungen der FATF-Standards hinaus, weil der VASP und die FINMA als Aufsichtsbehörden die Details aller an der Kryptotransaktion Beteiligten kennen müssen. Im Gegensatz dazu legt die FATF weniger Wert auf die Abklärung der Gegenpartei bei einer Kryptotransaktion, und konzentriert sich ausschliesslich auf die Rolle der VASPs und auf die Kundenidentifizierung.

In unserem fiktiven Beispiel war die estnische Bank genau aus diesem Grund beteiligt, weil dies in der Schweiz aufgrund der von der FINMA auferlegten Regeln nicht möglich gewesen wäre.⁶⁸

XI. Financial Action Task Force (on Money Laundering) – Guidance 2021

Im Oktober 2021 aktualisierte die *Financial Action Task Force (on Money Laundering)* (FATF) ihre «alte» *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (VASPs)* von 2019.⁶⁹ Die FATF-Standards verlangen von den Ländern, ihre Risiken im Zusammenhang mit Finanzaktivitäten und Anbietern virtueller Vermögenswerte zu bewerten und zu mindern, Anbieter zu lizenzieren oder zu registrieren und sie der Aufsicht oder Überwachung durch die zuständigen nationalen Behörden zu unterwerfen.

VASPs unterliegen denselben einschlägigen FATF-Massnahmen, die auch für Finanzinstitute gelten. Dieser neue *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* (erschieden am 28. Oktober 2021)⁷⁰ soll Staaten und VASPs helfen, ihre Verpflichtungen zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung und die Anforderungen der FATF, die für die-

sen Sektor gelten, wirksam umzusetzen. Der neue *Guidance* enthält einschlägige Beispiele und mögliche Lösungen für Umsetzungshindernisse und schliesst auch Aktualisierungen ein, die sich auf die folgenden Schlüsselbereiche konzentrieren:

- **Klärung der Definitionen von virtuellen Vermögenswerten und VASPs**, d.h. die Leitlinien stellen klar, dass digitale Währungen von Zentralbanken nicht als *virtual assets* betrachtet werden, obwohl die FATF-Standards auf jede andere Form von Fiat-Währung anwendbar wären.⁷¹ Alle Arten von VASPs, unabhängig von ihrem Geschäftsmodell, sollten hingegen aus regulatorischer und aufsichtsrechtlicher Sicht gleichbehandelt werden.⁷²
- **Leitlinien für die Anwendung der FATF-Standards auf Stablecoins**. *Stablecoins* sind Kryptowährungen, deren Preis an eine Kryptowährung, an Fiatgeld oder an börsengehandelte Rohstoffe (wie Edelmetalle oder Industriemetalle) gekoppelt ist. Das berühmteste Beispiel ist *Tether*, ein Blockchain-basierter Vermögenswert der mit minimalen Schwankungen (d.h. möglichst 1:1) an den US-Dollar gekoppelt und gehandelt ist, also ein *Stablecoin* ist.⁷³
- **Zusätzliche Leitlinien zu den Risiken und den Instrumenten, die den Staaten zur Verfügung stehen, um die Risiken der Geldwäsche und der Terrorismusfinanzierung bei Peer-to-Peer-Transaktionen (auch P2P-Transaktionen genannt) anzugehen**. Dieser Grundsatz baut auf den Massnahmen auf, welche die Staaten in Betracht ziehen sollten, um die Risiken von P2P-Transaktionen zu verstehen und zu mindern. In den Leitlinien wird ferner dargelegt, wie die Definition von «*correspondent banking and other relationships*»⁷⁴ in den FATF-Standards auszulegen ist und im Zusammenhang mit der *Recommendation 16 (wire transfer and travel rule)* verbessert der *Guidance* den Text über die *travel rule*. Die *Travel Rule* ist die allgemeine Bezeichnung für die FATF-*Recommendation* Nr. 16 zur Bekämpfung der Geldwäscherei. Sie verlangt, dass sowohl Finanzinstitute als auch Kryptounternehmen – wie gesagt, auch bekannt als *Virtual Asset Service Providers (VASPs)* – personenbezogene Daten von Teilnehmern an Transaktionen über 1000 USD/EUR sammeln müssen. Für Finanzinstitute und Kryptounternehmen bedeutet dies, dass sie die Namen und Kontonummern von Absendern und Empfängern erfassen müssen. Für die Daten, die über die Absender gesammelt werden, gibt es einige be-

66 Verordnung der Eidgenössischen Finanzmarktaufsicht über die Bekämpfung von Geldwäscherei und Terrorismusfinanzierung im Finanzsektor vom 3 Juni 2015.

67 Vgl. FINMA-Aufsichtsmittteilung 02/2019, «Zahlungsverkehr auf der Blockchain», 26. August 2019.

68 Vgl. Fn. 36.

69 Vgl. <https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf> (1 ff.).

70 Vgl. <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf> (1 ff.).

71 Vgl. Fn. 70.

72 Vgl. Fn. 70.

73 MÜLLER/ONG (Fn. 15).

74 Korrespondenzbank- und anderen Beziehungen.

sondere Anforderungen. Dazu gehört die zusätzliche Erfassung der physischen Adresse, der eindeutigen ID-Nummer (nationale Identitätsnummer usw.), der Kundenidentifikationsnummer oder des Geburtsdatums und -orts. Die *travel rule* verlangt von Banken und Kryptoplattformen auch, dass sie bei Transaktionen Absender- und Empfängerdaten untereinander austauschen. Aus diesem Grund wird diese Verordnung als «*Travel Rule*» bezeichnet, da die personenbezogenen Daten der Transaktionsparteien mit ihren Überweisungen «mitreisen». Während die Übermittlung personenbezogener Daten zwischen Banken ein seit langem etablierter Prozess ist, handelt es sich um eine völlig neue Anforderung für die Krypto-Industrie.⁷⁵

Ob die *Travel Rule* auch (schon) in der Schweiz eingehalten wird, soll aufgrund der Grundlage der Geldwäschereiverordnung-FINMA (GwV-FINMA)⁷⁶ bzw. in der FINMA-Aufsichtsmitteilung 02/2019, «*Zahlungsverkehr auf der Blockchain*» vom 26. August 2019 bejaht werden. Die FINMA hat bei der Regulierung der allgemeinen Sorgfaltspflichten (in Art. 10 GwV-FINMA, in Kraft seit Januar 2020) die Norm zu den Informationen für Zahlungsaufträge anerkannt. Der wichtigste Grundsatz der Verordnung ist, dass der FI des Auftraggebers den Namen, die Kontonummer und die Adresse des Auftraggebers sowie den Namen und die Kontonummer des Begünstigten kennen «muss».⁷⁷ Dies bedeutet, dass auch wenn es sich beim *Guidance 2021* um eine (neue und stärkere) Konkretisierung und Weiterentwicklung der *Travel Rule* handelt, das bereits im Schweizer Recht verankerte Konzept (d.h. in Art. 10 GwV-FINMA) ausreicht, um zu bestätigen, dass die FINMA auch die Krypto-Industrie wirksam beaufsichtigt und verlangt, dass die Kunden- und Begünstigteninformationen klar und bekannt sind.⁷⁸ Beispielsweise ist es für einen FI «subjektiv» notwendig, seinen Kunden zu kennen, wie es die *Travel Rule* verlangt, aber es ist auch objektiv notwendig, die Herkunft eines bestimmten Vermögenswertes zu kennen. Dies, gerade aufgrund der FINMA-Aufsichtsmitteilung 02/2019, «*Zahlungsverkehr auf der Blockchain*» vom 26. August 2019, in der die FINMA Technologieneutralität fordert, lässt darauf schliessen, dass die FINMA bereits eine Anwendung der FATF-Grundsätze (inkl. *Travel Rule* die mit der ersten *Guidance 2019* entstanden ist und mit dem *Update 2021* konkretisiert wurde) vorverlegt hat.

- **Grundsätze für den Informationsaustausch und die Zusammenarbeit zwischen den Aufsichtsbehörden für VASPs.** Dies ist ein neuer Abschnitt in den *Guidance*, der die FATF-Grundsätze des Informationsaustauschs und der Zusammenarbeit zwischen den Aufsichtsbehörden der VASPs erörtert. Jeder Staat muss mindestens eine zuständige Behörde als Aufsichtsbehörde für VASPs für Zwecke der Geldwäschebekämpfung benennen. Heute sind schon eine Reihe von VASP-Aufsichtsbehörden benannt, darunter Finanzdienstleistungsaufsichtsbehörden, Zentralbanken, Wertpapieraufsichtsbehörden, Steuerbehörden, spezialisierte VASP-Aufsichtsbehörden, usw. Einige

Staaten behandeln VASPs als eine klar identifizierbare, spezifische Geschäftskategorie, während andere VASPs als eine Untergruppe bereits bestehender Geschäftskategorien betrachten (z.B. als Gelddienstleistungsunternehmen).⁷⁹ In der Schweiz wird die FINMA VASPs beaufsichtigen, die eine Genehmigung der FINMA benötigen. Danach folgen in einem fast skalaren Modell die SRO, die sich mit einer gezielteren Aufsicht über das GwG befassen und in Sachen AIA ist es die Eidgenössische Steuerverwaltung (ESTV), die sich damit befasst (und in Zukunft befasst wird). Welche Behörde in der Schweiz die spezifischen Aufgaben der internationalen Zusammenarbeit in Kryptosachen übernehmen wird, lässt sich noch nicht klarstellen. Wahrscheinlich wird es die FINMA sein.

Zusammenfassend machen diese neuen Leitlinien deutlich, dass der Sektor der virtuellen Vermögenswerte (*virtual asset*; VA) schnelllebig und technologisch dynamisch ist, was bedeutet, dass eine kontinuierliche Überwachung und ein (neues) Engagement zwischen dem öffentlichen und dem privaten Sektor erforderlich ist. Im Juni 2020 schloss die FATF ihre 12-monatige Überprüfung der überarbeiteten FATF-Standards zu virtuellen Vermögenswerten und VASPs⁸⁰ ab, bei der Bereichen ermittelt wurden, in denen die FATF mehr Leitlinien benötigt, um die Anwendung der überarbeiteten FATF-Standards zu klären.

Die *Updated Guidance* ist jetzt Teil der laufenden Überwachung des Sektors der virtuellen Vermögenswerte und der Anbieter virtueller Vermögensdienstleistungen (VASP) durch die FATF. Die FATF wird wachsam sein und den VA- und VASP-Sektor genau beobachten, um wesentliche Änderungen zu erkennen, die eine weitere Überarbeitung oder Klarstellung der FATF-Standards erforderlich machen.⁸¹

XII. Fazit

Die Dezentralisierung der Kryptoflüsse verhindert die Ausübung der staatlichen Kontrolle, die der Staat über die Finanzdienstleister ausübt. Damit werden die Geldwäschereibekämpfung und die internationale steuerliche Transparenz im Umgang mit Kryptowährungen lahmgelegt. Einerseits, um die Kontrolle auf die Kryptoflüsse zu erwerben, werden die VASPs ähnlichen Compliance- und Aufsichtspflichten wie der Finanzdienstleister unterstellt und der Begriff solcher Kryptodienstleister wird so breit wie möglich ausgelegt.

75 Vgl. <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Quick-guide-RBA-VA-VASPs.pdf>, vgl. auch «*Travel Rule Report*» von gwp/Incore (https://www.gwp.ch/en/news/519_2020-11-05_travel-rule-report).

76 Verordnung der Eidgenössischen Finanzmarktaufsicht über die Bekämpfung von Geldwäscherei und Terrorismusfinanzierung im Finanzsektor, RS. 955.033.0.

77 Vgl. Art. 10 Abs. 1 GwV-FINMA.

78 Vgl. auch: <https://notabene.id/world/switzerland>.

79 Vgl. Fn. 75.

80 12-Month Review of the Revised FATF Standards on VAs and VASPs; https://www.fatf-gafi.org/media/fatf/documents/recommendations/12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASP_S.pdf.

81 Vgl. Fn. 75.

Darüber hinaus wird ein Ansatz von technologischer Neutralität angestrebt. Danach sollen Krypto- und Fiat-Geldflüsse ähnlichen Compliance Standards unterstellt sein. Um eine solche Gleichstellung tatsächlich zu gewährleisten, soll die VASP-Definition so breit wie möglich sein. Andererseits werden Hindernisse gesetzt mit Bezug auf Kryptotransaktionen wobei keine VASPs involviert werden und die zwei Parteien der Transaktion nicht vollumfänglich identifiziert sind. Der FATF-Gremium hat diesbezüglich die *Travel Rule* übernommen, die von der Schweiz, und insbesondere von der FINMA, gemäss einem *Swiss Finish* bereits implementiert war. Ob solche Massnahmen eingeführt bzw. auf einen aterritorialen digitalen Raum tatsächlich durchgesetzt werden sollen, bleibt noch abzuwarten. Noch unsicher ist auch, ob die Anstrengungen des FATFs und der GAFI einen globalen *level playing field* zu erreichen sich lohnen werden. Falls dies der Fall sein wird, bleibt letztlich zu überprüfen, ob eine wirksame staatliche Kontrolle über die Kryptowährun-

gen deren Attraktivität nicht massiv herabsetzen würde. Denn das Paradox aus dem Gesichtspunkt der Kryptowährungen besteht gerade darin, dass sie aus einer Vision von Dezentralisierung und Befreiung von der Intermediation von Finanzinstituten entstanden sind und aus der Sorge zur Erfüllung der Compliance Standards in den Bereichen KYC, CDD und steuerlicher Transparenz die Notwendigkeit einer Intermediation mittels beaufsichtigter Dienstleister, nämlich den VASPs, wieder entsteht.⁸² Solche Regulierungen könnten die Nachfrage von Kryptowährungen in entwickelten Finanzplätzen wie der Schweiz bremsen. Der Zuwachs solcher Nachfragen erscheint hingegen in den Ländern mit einem schwachen bzw. unstabilen Finanzplatz unaufhaltsam. Die Auffassung der zukünftigen Entwicklung der Kryptowährungen wird demzufolge eine tiefe Interoperabilität (*interface capability*) zwischen dem technologischen Wissen, Wirtschaftsforschung und Wirtschaftsrecht benötigen.⁸³

Zusammenfassung

Kryptowährungen bleiben in der Schweiz eine Währung im wirtschaftlichen, aber nicht im rechtlichen Sinne. Bei der Bekämpfung der Geldwäscherei im Umgang mit den Kryptowährungen hat sich gezeigt, dass das Konzept der VASPs im Wesentlichen auf den allgemeineren Begriff des FI angeknüpft wird. Dies bedeutet, dass auch VASPs den klassischen KYC- und CDD-Grundsätzen (*know your customer* und *client due diligence*) unterliegen. Solche VASPs können u.U. auch AIA-pflichtig sein. Heikel bleiben jedoch die P2P-Beziehungen, die dem GwG und dem AIA entfliehen können. Aufgrund des Erfordernisses der «Technologie-neutralität», hat die FINMA in der Schweiz die neue und aktuelle «*Travel Rule*» – die von der FATF in ihrer «*Guidance 2021*» aufgenommen wurde – schon umgesetzt. Grundlegend, verlangt die «*Travel Rule*» (auch) von Kryptoplattformen, dass sie bei Transaktionen Absender- und Empfängerdaten untereinander austauschen. Dies bedeutet, dass der FI (inkl. VASP) des Auftraggebers den Namen, die Kontonummer und die Adresse des Auftraggebers sowie des Begünstigten kennen muss.

Résumé

En Suisse, les cryptomonnaies ont actuellement le statut de monnaie au sens économique, mais pas au sens juridique. Dans le contexte de la lutte contre le blanchiment d'argent au moyen de cryptomonnaies, il est apparu que le concept de VASP (Virtual Asset Service Provider) est essentiellement rattaché à la notion plus générale d'institution financière, ce qui signifie que les VASP sont également soumis aux principes classiques de KYC et CDD (*know your customer* et *client due diligence*). Ces VASP peuvent également être soumis à l'échange automatique de renseignements (EAR) dans certaines circonstances. Les relations P2P, qui ne sont pas assujetties à la LBA et à l'EAR, restent toutefois délicates. Pour répondre à l'exigence de «neutralité technologique», la FINMA applique déjà la dernière version de la «*Travel Rule*» en Suisse – une règle reprise par le GAFI dans ses «*Lignes directrices 2021*». Dans le principe, la «*Travel Rule*» exige (également) des plateformes de cryptomonnaies qu'elles échangent entre elles les données de l'expéditeur et du destinataire des transactions. Cela signifie que l'institution financière (y compris les VASP) du donneur d'ordre doit connaître le nom, le numéro de compte et l'adresse du donneur d'ordre et du bénéficiaire.

82 Siehe mit Bezug auf solchem Paradox bereits MOLO/DRZALIC (Fn. 34).

83 Zum Querbegriff des Wirtschaftsrechts siehe bereits P. V. KUNZ, Schweizer Wirtschaftsrecht im 21. Jahrhundert: Ausblick(e) zwischen Hoffen und Bangen, AJP 2015, 411–426; E. SCHANZE, What is law and economics today? An European View, in: P. Nobel (ed.), New frontiers of law and economics, First international scientific conference on law and economics at the University of St. Gallen, 2006, 89–113.