

Oktober 2018

National Risk Assessment (NRA): Risiko der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets und Crowdfunding

Bericht der interdepartementalen Koordinationsgruppe zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (KGGT)

Inhalt

Executive summary	4
Liste der verwendeten Abkürzungen	6
Index	7
Einleitung	9
1. Virtuelle Währungen	12
1.1. Definition	12
1.2. Entwicklungen seit 2014.....	12
1.3. Typologien virtueller Währungen	12
1.3.1. Umtauschbare vs. nicht-umtauschbare virtuelle Währungen	12
1.3.2. Zentrale vs. dezentrale virtuelle Währungen	13
1.3.3. Funktionsweise der Technologie	13
2. Kryptowährungen in der Praxis.....	14
2.1 Kryptowährungen als Finanzierungsinstrument	14
2.2 Wallet-Anbieter.....	17
2.3 Wechselstuben und zentralisierte/dezentralisierte Handelsplattformen	18
2.4 Dezentralisierte Handelsplattformen.....	19
2.5 Off-chain Zahlungssysteme.....	20
2.6 Kryptofonds.....	20
3. Risikoanalyse	20
3.1. Gefährdungen in Verbindung mit Krypto-Assets.....	21
3.1.1. Untrennbar mit der Krypto-Asset-Technologie verbundene Gefährdung	21
3.1.2. Gefahren einer betrügerischen Nutzung von Kryptowährungen	27
3.2. Die Verwundbarkeiten der Schweiz angesichts der Gefahr der Geldwäscherei und Terrorismusfinanzierung durch Kryptowährungen.....	31
3.2.1. Verwundbarkeiten von Finanzintermediären, die Kryptotransaktionen durchführen.....	31
3.2.2. Die schwierige Repression von Geldwäscherei und Terrorismusfinanzierung durch Kryptowährungen	34
3.3. Bilanz der Risikoanalyse	35
4. Risikomindernde Faktoren.....	36
4.1. Aufsichtsrechtliche Einordnung der Krypto-Anwendungsfälle	36
4.1.1. Initial Coin Offerings	36
4.1.2. Wallet-Anbieter.....	37
4.1.3. Wechselstuben und zentralisierte Handelsplattformen	38
4.1.4. Dezentralisierte Handelsplattformen.....	38
4.1.5. Mining	39
4.1.6. Übersichtstabelle über die verschiedenen Arten von Krypto-Asset-Dienstleistungen und ihre Unterstellung unter das GwG.....	39

4.2. Die internationale Zusammenarbeit.....	40
4.3. Technologische Fortschritte zugunsten der Strafverfolgungsbehörden	41
4.4. Diverses.....	41
5. Crowdfundingplattformen	43
5.1. Erscheinungsformen	43
5.2. Risikoanalyse	43
5.3. Risikomindernde Faktoren.....	45
6. Schlussfolgerungen / Empfehlungen	47
6.1. Schlussfolgerungen aus der Analyse der Risiken im Zusammenhang mit Krypto-Assets.....	47
6.2. Schlussfolgerungen und Empfehlungen zur Analyse der Risiken von Crowdfunding-Plattformen	48
7. Bibliographie	49

Executive summary

Die Schweizer Behörden haben bis anhin noch keinen einzigen Fall von Terrorismusfinanzierung mittels Krypto-Assets oder Online-Crowdfunding identifiziert und erst wenige Fälle von Geldwäscherei durch die Nutzung dieser neuen Technologien erfasst. Das damit verbundene reelle Risiko der Geldwäscherei und Terrorismusfinanzierung lässt sich daher nicht präzise beurteilen. Der vorliegende Bericht kommt jedoch zum Schluss, dass die Gefährdungen durch diese Technologien und die Verwundbarkeiten der Schweiz in diesem Bereich erheblich sind, wobei nicht nur die Schweiz, sondern alle Länder davon betroffen sind.

Die Gefährdung im Zusammenhang mit Krypto-Assets ergibt sich aus der Anonymität der Token-Transaktionen, insbesondere betreffend die an den Vermögenswerten wirtschaftlich berechtigten Person, und daraus, dass ein Grossteil dieser Transaktionen direkt und ohne Finanzintermediär durchgeführt wird und sich somit jeglicher Kontrolle entzieht. Die Gefährdung äussert sich sowohl in der kriminellen Ausnutzung von Design-Fehlern bei den Kryptowährungen als auch im Investorenbetrug vor allem bei ICOs und der Nutzung von Kryptowährungen für Ransomware-Zahlungen. Die Verwendung von Kryptowährungen stellt aber auch in sonstigen kriminellen Mustern eine Gefahr dar: Terrorismusfinanzierung, Waschen von Geldern aus dem Verkauf von illegalen Dienstleistungen und Produkten, Phishing-Betrügereien oder auch Drogenhandel, insbesondere durch kriminelle Organisationen. Aufgrund ihrer Anonymität eignen sich Kryptowährungen besonders gut für die Geldwäscherei.

Wie andere Länder ist auch die Schweiz anfällig für diese Gefahr, weil sowohl für die Finanzintermediäre als auch die Strafverfolgungsbehörden die Feststellung der Identität der wirtschaftlich Berechtigten Person von bestimmten Vermögenswerten kompliziert ist. In den meisten Fällen ist die den Krypto-Assets zugrundeliegende Technologie dafür verantwortlich, dass sich diese Identität nicht ermitteln lässt. Einzig beim Kauf oder Verkauf von Kryptowährungen gegen Fiatgeld kann die Identität der wirtschaftlich Berechtigten der involvierten Vermögenswerte festgestellt werden. Aber auch dies schützt die Online-Wechselstuben, die solche Transaktionen durchführen, nicht umfassend gegen Betrug. Ihnen steht nämlich kein Mittel zur Verfügung, um die Identität der wirtschaftlich Berechtigten der Wallets zu überprüfen, denen sie im Auftrag ihrer Kunden Werte gutschreiben. Ausserdem lässt sich eine kriminelle Herkunft der an einer Kryptotransaktion beteiligten Vermögenswerte nur äusserst schwer nachweisen.

Diese neue Technologie stellt ebenfalls eine grosse Herausforderung für die Strafverfolgungsbehörden dar. Es ist nicht nur schwierig, die wirtschaftlich Berechtigten von Krypto-Assets zu identifizieren und den kriminellen Hintergrund einer Transaktion von solchen Vermögenswerten zu erkennen. Es ist zudem technisch nicht möglich, die auf einer Wallet deponierten Vermögenswerte zu beschlagnahmen, ohne über den entsprechenden *Private Key* zu verfügen. Weil Kryptotransaktionen überdies in der Regel grenzüberschreitend sind, sind internationale Rechtshilfesuche oder eine internationale polizeiliche Zusammenarbeit notwendig, um die damit verbundene Wirtschaftskriminalität zu ahnden. Die Strafverfolgungsbehörden werden daher oft von der Schnelligkeit und der Mobilität der Kryptotransaktionen überholt und es stellen sich häufig Probleme bezüglich der zuständigen Gerichtsbarkeit.

Die internationale polizeiliche Amtshilfe und justizielle Rechtshilfe stellt heute aber das effizienteste Instrument zur Bekämpfung der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets dar. Ihr sind die grössten Erfolge bei der Repression von Wirtschaftskriminalität in Verbindung mit Kryptowährungen zu verdanken. Dies zeigt auch, dass eine Antwort auf diese Art von transnationaler Gefährdung auf internationaler Ebene erarbeitet werden muss.

In dieser Hinsicht ist das Engagement der Schweiz innerhalb der GAFI für eine stärkere Harmonisierung der nationalen Regelungen zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung durch Krypto-Assets eine angemessene Antwort. Sie wird ergänzt durch Bemühungen zur Schulung der Straf-

verfolgungsbehörden im Bereich der Cyberkriminalität und durch die Schaffung einer nationalen Plattform zur justiziellen und polizeilichen Zusammenarbeit – dem Cyberboard – im Sommer 2018, die auf diese Art von Wirtschaftskriminalität spezialisiert ist.

Im Übrigen gilt das GwG in der Schweiz bereits für eine besonders breite Palette von Dienstleistungen, die sich mit dem Handel und mit Transaktionen von Krypto-Assets beschäftigen, wobei gewisse Präzisierungen zum Anwendungsbereich dieses Gesetzes gegenwärtig geprüft werden.¹

Der Bericht kommt zum Schluss, dass die Schweiz dank diesen verschiedenen Massnahmen das bestmögliche regulatorische Dispositiv zur Bekämpfung der erheblichen Gefährdung durch Krypto-Assets entwickelt hat, auch wenn dadurch nicht alle Verwundbarkeiten ausgemerzt werden können, die ebenfalls erheblich sind und die sich nur durch eine internationale Lösung deutlich vermindern lassen.

Beim Crowdfunding betrifft die grösste Gefahr die Terrorismusfinanzierung, wobei noch kein einziger solcher Fall in der Schweiz erfasst worden ist. Dabei ergibt sich die Gefahr bei dieser neuen Technologie zur Kapitalbeschaffung aus der Anonymität der Spender, aber auch daraus, dass gewisse Online-Crowdfunding-Plattformen nicht dem GwG unterstellt sind. Zur Verminderung dieses Risikos empfiehlt der Bericht zu prüfen, ob eine Nennung solcher Plattformen in der Verordnung des Bundesrats vom 11. November 2015 über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (GwV, SR 955.01) zweckmässig wäre.

¹ Siehe Empfehlungen im Bericht des Bundesrates „Rechtliche Grundlagen für Distributed Ledger-Technologie und Blockchain in der Schweiz“, 7. Dezember 2018.

Liste der verwendeten Abkürzungen

BA: Bundesanwaltschaft

BJ: Bundesamt für Justiz

DLT: Distributed Ledger Technology

ESBK: Eidgenössische Spielbankenkommission

FINMA: Eidgenössische Finanzmarktaufsicht

GAFI/FATF: Groupe d'Action financière/Financial Action Task Force

KGGT: Interdepartementale Koordinationsgruppe zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung

GwG: Bundesgesetz vom 10. Oktober 1997 über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung

ICO: Initial Coin Offering

ISB: Informatiksteuerungsorgan des Bundes

KKJPD: Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren

KKPKS: Konferenz der kantonalen Polizeikommandanten

MELANI: Melde- und Analysestelle Informationssicherung

MROS: Meldestelle für Geldwäscherei

NDB: Nachrichtendienst des Bundes

NRA: National Risk Assessment

SIF: Staatssekretariat für internationale Finanzfragen

SKP: Schweizerische Kriminalprävention

SSK: Schweizerische Staatsanwälte-Konferenz

SVS: Sicherheitsverbund Schweiz

Index

Asymmetrische Verschlüsselung: Die asymmetrische Verschlüsselung ist eine Verschlüsselungstechnik, die zwischen öffentlichen und privaten Schlüsseln unterscheidet, wobei letztere eigentlich die Entschlüsselung der übermittelten Daten ermöglichen. Diese Technik wird im Kryptobereich zur Durchführung von gesicherten Transaktionen zwischen zwei Wallets verwendet. Jede Wallet verfügt somit sowohl über einen öffentlichen (*Public Key*) als auch einen privaten Schlüssel (*Private Key*). Um eine Transaktion für eine Wallet durchführen zu können, muss die Person, die sie in Auftrag gibt, über den öffentlichen Schlüssel verfügen, damit die Krypto-Assets an eine bestimmte Wallet und nicht an eine andere überwiesen werden. Der private Schlüssel, über den nur der Inhaber dieser Wallet verfügt, ist der eigentliche Zugriffscode, dank dem er auf die gutgeschriebenen Vermögenswerte zugreifen kann. Gewisse Kryptowährungen nutzen jedoch auch andere Verschlüsselungstechniken, um Transaktionen zwischen zwei Wallets zu sichern.

Bitcoin: Der Bitcoin ist die älteste und populärste Kryptowährung, die 2009 als Reaktion auf die Finanzkrise geschaffen wurde.

Blockchain: Blockchain ist eine Computertechnologie zur Speicherung und Übertragung von Daten ohne zentrale Kontrollstelle. Im weiteren Sinne bezeichnet dieser Begriff auch die Datenbank, in der die Historie aller mit dieser Technologie durchgeführten Transaktionen enthalten ist. Die Blockchain wird vor allem im Bereich der Krypto-Assets verwendet. Sie ist die technische Grundlage zahlreicher Kryptowährungen, so auch von Bitcoin und Ether, bei denen sie die Lesbarkeit aller Transaktionen ermöglicht. Zur Aufzeichnung auf der Blockchain werden mehrere Transaktionen chronologisch in einem Block zusammengefasst, der dann an den vorangehenden Block angehängt wird, nachdem die Transaktionen von Minern validiert worden sind. Diese überprüfen, ob das Individuum, das die Transaktion in Auftrag gegeben hat, tatsächlich über die Vermögenswerte oder Daten verfügt, die es übermitteln will. Eine solche Validierung wird durch das Lösen einer mathematischen Aufgabe durchgeführt. Nachdem die Transaktionen auf der Blockchain aufgezeichnet sind, können sie nur noch von einer Person oder einer Gruppe von Personen gelöscht werden, die über mehr als 51 Prozent der Rechenleistung verfügt, die zur Validierung von Transaktionen in der gesamten Blockchain erforderlich ist.

Darknet: Der Begriff Darknet bezeichnet Netzwerke im Internet, die Zugriffsprotokolle verwenden, dank denen ihre Nutzer anonym bleiben können, dies vor allem, indem die IP-Adressen der Verbindungen verschleiert werden. Darknets befinden sich auf dem Deep Web, das heisst den Teilen des Internets, auf die herkömmliche Browser keinen Zugriff haben, und von denen es mehrere gibt. Das berühmteste dieser Netzwerke ist TOR (*The onion router*), für das es spezielle Browser gibt. Anonyme Netzwerke hosten legale Webseiten, die insbesondere für den Austausch vertraulicher Daten verwendet werden, aber auch zahlreiche Webseiten zum Verkauf von illegalen Produkten und Dienstleistungen. Auf diesen sogenannten *Dark Markets* werden vor allem Drogen, kinderpornografisches Material, Waffen oder auch gestohlene Kreditkarten angeboten. Der Inhalt der Darknets wird als Darkweb bezeichnet.

DLT (Distributed Ledger Technology): Unter DLT versteht man gemeinhin Technologien, die es individuellen Teilnehmern (Nodes) innerhalb eines Systems erlauben, auf sichere Art und Weise Operationen vorzuschlagen, zu validieren und in einem synchronisierten Datensatz (*Ledger*) zu speichern, der auf allen Nodes im System verteilt ist.

Ether: Der 2015 eingeführte Ether oder Ethereum ist nach dem Bitcoin die zweitwichtigste Kryptowährung.

Fiatgeld: Fiatgeld wird von einem Staat herausgegeben, deren Zentralbank den legalen Kurs festlegt und kontrolliert.

ICO: ICOs stehen für eine Form der Kapitalbeschaffung. Bei einem ICO überweisen die Anleger finanzielle Mittel (üblicherweise in Form von Kryptowährungen) an den Organisator eines ICOs. Im Gegenzug erhalten sie *Blockchain*-basierter «*Coins*» bzw. «*Token*», welche entweder auf einer in diesem Rahmen neu entwickelten Blockchain oder mittels eines sog. *Smart Contract* auf einer bereits bestehenden Blockchain geschaffen und dezentral gespeichert werden.

Krypto-Asset: Unter einem Krypto-Asset wird gemeinhin eine digitale Repräsentation eines Wertes verstanden, der auf einer Blockchain digital gehandelt werden kann und zum Zweck der Zahlung (Zahlungsfunktion), Nutzung (Nutzungsfunktion) oder Investition (Investitionsfunktion) verwendet werden kann.

Kryptowährung: Synonym für «virtuelle Währung». Vgl. unten.

Miner: Miner sind für die Validierung der Transaktionen zuständig. Die Miner (also validierenden *Nodes*) überprüfen, ob das Individuum, das eine Transaktion in Auftrag gibt, auch tatsächlich über die Vermögenswerte oder Daten verfügt, die es übermitteln will. Eine solche Validierung wird durch das Lösen von mathematischen Aufgaben durchgeführt. Sie fassen die Transaktionen zu einem Block zusammen und senden diesen zur Verifizierung an das Netzwerk. Die *Nodes* akzeptieren einen Block nur dann, wenn die darin enthaltenen Transaktionen gültig sind. *Miner* werden mit neu geschaffenen Bitcoin («Mining») sowie mit Transaktionsgebühren entschädigt.

Public Key/Private Key: *Public Keys* (oder Adressen) entsprechen Identitäten von Nutzern von Kryptowährungen. Ein Nutzer von Kryptowährungen kann von seiner Adresse eine Nachricht (resp. Transaktion) senden, indem er diese mit seinem *Private Key* signiert. Der *private key* ist somit der Signierschlüssel und der *public key* der Verifikationsschlüssel. Der *private key* muss geheim gehalten werden, der Verifikationsschlüssel wird typischerweise öffentlich bekannt gegeben.

Smart Contract: *Smart Contracts* oder «intelligente Verträge» sind Computerprotokolle, die Bestimmungen eines Vertrags automatisch ausführen und sich dabei auf Algorithmen stützen, die festlegen, wann welcher Entscheid getroffen werden muss. *Smart Contracts* wurden ursprünglich von der Stiftung Ethereum entwickelt, deren Kryptowährung Ether die erste war, die eine Anwendung solcher Protokolle möglich machte. Sie erlauben die Ausführung von Verträgen und die Überwachung von Transaktionen auf der Blockchain, die sie erzeugen, während gleichzeitig die mit dem menschlichen Handeln verbundenen Risiken der Willkür unterdrückt werden – weil der Grundsatz gilt, dass man nicht vom *Smart Contract*-Protokoll abweichen darf, das absolut rational und gerecht ist gegenüber allen und das somit zum Gesetz derjenigen wird, die diese Technologie nutzen («The code is the law»).

Token: Bei einem Token handelt es sich im Kontext einer Blockchain um eine Einheit, die entweder einen intrinsischen Wert enthält oder einen anderweitigen Vermögenswert oder eine Nutzungsfunktion repräsentiert. Blockchain-basierte Tokens sind in der Regel fungibel und können zwischen den Teilnehmern des Netzwerks ausgetauscht werden.

Virtuelle Währung: Eine virtuelle Währung ist eine elektronische Darstellung eines Wertes, im Internet handelbar und kann als Zahlungsmittel für reale Güter und Dienstleistungen verwendet werden. Sie hat eine eigene Denomination, ist jedoch meist nicht als gesetzliches Zahlungsmittel akzeptiert. Eine virtuelle Währung stellt lediglich einen digitalen Code dar und hat kein physisches Gegenstück zum Beispiel in Form von Münzen oder Noten.

Wallet: Ein Wallet ist eine Software, die es mittels eines Interface erlaubt, kryptographische Token zu verwalten.

Einleitung

Im Juni 2015 hat der Bundesrat den ersten Bericht über die nationale Beurteilung der Geldwäscherei- und Terrorismusfinanzierungsrisiken in der Schweiz zur Kenntnis genommen. Der Bericht der nationalen Risikoanalyse, das sogenannte National Risk Assessment (NRA), stellt die erste sektorübergreifende Gesamtbeurteilung der Geldwäscherei- und Terrorismusfinanzierungsrisiken in der Schweiz dar. Darin wird aufgezeigt, dass die Schweiz nicht von Finanzkriminalität verschont bleibt und dass auch hierzulande Erträge aus mehrheitlich im Ausland begangenen Straftaten gewaschen werden. Mit der Veröffentlichung der NRA setzt der Bundesrat die revidierten Empfehlungen 1 und 2 der *Groupe d'Action Financière* (GAFI) um. Die Empfehlungen der zwischenstaatlichen Organisation halten die Länder dazu an, ein Dispositiv zur effizienten Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung einzuführen. Der NRA-Bericht ist Bestandteil dieses Dispositivs, insofern er darauf abzielt, Geldwäscherei- und Terrorismusfinanzierungsrisiken in der Schweiz zu identifizieren, gezielte Gegenmassnahmen einzuleiten und deren Effizienz in regelmässigen Abständen zu überprüfen (*identify and assess their money laundering and terrorism financing risk on an ongoing basis*).² Mit der Publikation des NRA-Berichts ist der Prozess der nationalen Risikoanalyse nicht abgeschlossen. Die NRA stellt einen kontinuierlichen Prozess dar. Um längerfristig den Empfehlungen der GAFI zu entsprechen und um die Wirksamkeit des schweizerischen Geldwäscherei- und Terrorismusfinanzierungsdispositivs den neuen Gefährdungen anzupassen, werden weitere Risikoanalysen erarbeitet.

Der vorliegende Bericht über das Geldwäscherei- und Terrorismusfinanzierungsrisiko in Verbindung mit zwei der wichtigsten Anwendungsformen der FinTech – Krypto-Assets und Crowdfunding – ist als eine dieser weiteren Risikoanalysen mit sektorialem Charakter zu verstehen. Er behandelt zunächst das Risiko in Verbindung mit Krypto-Assets und dann in etwas kürzerer Form jenes im Zusammenhang mit dem Online-Crowdfunding.

Unter Krypto-Assets versteht man jede Form von virtuellen Vermögenswerten, die auf einem elektronische Medium gespeichert sind und mit denen eine Gemeinschaft von Nutzerinnen und Nutzern, die sie als Zahlungsmittel akzeptieren, auf solche Vermögenswerte lautende Transaktionen durchführen können, ohne auf eine gesetzliche Währung zurückzugreifen. Der Begriff «Krypto-Asset» umfasst zwar einen breiteren Bereich als jener der «virtuellen Währung» oder der «Kryptowährung» (vgl. oben). Im vorliegenden Bericht werden sie jedoch synonym verwendet.

Ende 2017 lenkte der spektakuläre Höhenflug des Bitcoin-Kurses die Aufmerksamkeit der Öffentlichkeit und der Medien auf die Krypto-Assets. Die Kryptowährung Bitcoin, die als Reaktion auf die weltweite Finanzkrise von 2008 entwickelt wurde, ist die älteste dieser Krypto-Assets, mit denen das traditionelle Bankensystem umgangen werden kann, indem eine anonyme, völlig dezentralisierte und damit keiner Regulierungsbehörde unterstellte Transaktionsform gewählt wird, die über das Internet abgewickelt wird. Schon sehr früh brachten die fehlende Kontrolle und die Anonymität der Bitcoins die Behörden dazu, sich mit den möglichen damit verbundenen Betrugs- und Geldwäscherei- oder gar Terrorismusfinanzierungsrisiken zu beschäftigen. So wies die GAFI ihre Mitglieder bereits 2014 und 2015 auf diese Gefahren hin und verfasste einen ersten Leitfaden zur Erarbeitung eines risikobasierten Ansatzes zur Beurteilung der mit Kryptowährungen verbundenen Gefahren der Geldwäscherei oder der Terrorismusfinanzierung.³ In der Schweiz wurden seit 2013 mehrere parlamentarische Vorstösse und Postulate zu

² FATF, *National Money Laundering and Terrorist Financing Risk Assessment*, 2013, S. 6, http://www.fatf-gafi.org/media/fatf/content/images/National_ML_TF_Risk_Assessment.pdf

³ FATF, *Virtual currencies. Key definitions and potential AML/CFT risks*, Juni 2014, <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>; id, *Virtual currencies. Guidance for a risk-based approach*, 2015, <http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf>

diesem Thema eingereicht, was den Bundesrat dazu veranlasste, 2014 einen Bericht zu virtuellen Währungen⁴ zu publizieren. Darin kam er zum Schluss, das Risiko sei noch gering und erfordere in unmittelbarer Zukunft keine besonderen Massnahmen. Seit damals sind aber neue wirtschaftliche Verwendungen von Krypto-Assets hinzugekommen, die Zahl solcher Währungen hat sich erhöht – gegenwärtig sind es über 2000 – und die diesen Währungen zu Grunde liegenden Technologien haben sich weiterentwickelt. Diese Faktoren ebenso wie die jüngste Begeisterung der Öffentlichkeit für virtuelle Währungen, die ausgelöst wurde durch den Höhenflug des Bitcoin-Kurses, veranlassten die nationalen und internationalen Instanzen zu prüfen, ob eine Neubeurteilung der damit verbundenen Geldwäscherei- oder gar Terrorismusfinanzierungsrisiken notwendig ist. Die GAFI plant die Erarbeitung einer vertieften Strategie zu diesem Thema⁵, mehrere Länder und namentlich die Europäische Union sind dabei, ihre Gesetzgebung im Hinblick auf die mit Kryptowährungen verbundenen Risiken⁶ zu ändern, und die Zahl der von verschiedenen Behörden und Organisationen verfassten Berichte zu diesem Thema nimmt kontinuierlich zu.⁷

Eine solche Neubeurteilung ist besonders wichtig für die Schweiz, die sich als Krypto-freundlicher Staat positioniert. So zieht der Kanton Zug zahlreiche Unternehmen dieses Sektors an und wird oft als Schweizer «Crypto Valley» bezeichnet, während der Kanton Genf, der es ihm gleich tun will, die Niederlassung solcher Unternehmen auf seinem Gebiet und die Entwicklung des Krypto-Sektors in seinen Banken ebenfalls fördert. Das Innovationspotenzial der Krypto-Assets und ihre zivil- und finanzmarktrechtlichen Auswirkungen sind Gegenstand eines separaten Berichts des Bundesrates⁸, den der vorliegende Bericht durch eine Untersuchung der Geldwäscherei- und Terrorismusfinanzierungsrisiken im Zusammenhang mit Krypto-Assets ergänzen will.

Im Gegensatz zu anderen Geldwäscherei- und Terrorismusfinanzierungsrisiken sind jene in Verbindung mit Kryptowährungen neuartig und es gibt noch nicht viele Quellen, die eine Beurteilung erlauben. Insbesondere sind bei der Meldestelle für Geldwäscherei (MROS) erst wenige Verdachtsmeldungen eingegangen und es können noch keine zuverlässigen statistischen Aussagen daraus abgeleitet werden. Die bei der MROS eingegangenen Verdachtsmeldungen wurden zwar im Rahmen des Möglichen zur Analyse genutzt, aber es war dennoch notwendig, auch andere Quellen hinzuzuziehen und einen eher qualitativen als quantitativen Ansatz zu wählen. Die Fachliteratur zum Thema ebenso wie Presseartikel und Berichte von ausländischen Behörden bilden somit die Grundlage dieses Berichts, die ergänzt wurde durch Konsultationen mehrerer Schweizer Polizei- und Justizbehörden und des Privatsektors, denen wir an dieser Stelle für ihre Verfügbarkeit danken.

Der erste Teil dieses Berichts ist der Definition der Begriffe und Konzepte im Bereich der Krypto-Assets und ihrer Technologie gewidmet und bewusst knappgehalten. Wer mehr darüber erfahren möchte, sei auf den Bericht des Bundesrates verwiesen, der bis Ende 2018 veröffentlicht wird und der diesen Aspekt ausführlicher behandeln wird.⁹ Das zweite Kapitel beschäftigt sich mit der Beschreibung der wichtigsten Dienste, die bei Token-Transaktionen in Anspruch genommen werden, sowie ihrer rechtlichen Qualifikation. Insbesondere werden Initial Coin Offerings (ICOs) vorgestellt und definiert. Deren Zahl hat sich in der Schweiz seit etwas mehr als einem Jahr vervielfacht und sie sind damit für den Gesetzgeber und

⁴ Bericht des Bundesrates zu virtuellen Währungen in Beantwortung der Postulate Schwab (13.3687) und Weibel (13.4070) vom 25. Juni 2014, <https://www.news.admin.ch/NSBSubscriber/message/attachments/35361.pdf>

⁵ FATF, FATF Fintech & RegTech Initiative, [http://www.fatf-gafi.org/fintech-reg-tech/?hf=10&b=0&s=desc\(fatf_releasedate\)](http://www.fatf-gafi.org/fintech-reg-tech/?hf=10&b=0&s=desc(fatf_releasedate))

⁶ <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2018-0178+0+DOC+PDF+V0//DE>

⁷ EUROPOL, 2017 *Virtual Currencies Money Laundering Typologies*, 2017; FANUSIE Yaya et ROBINSON, Tom, *Bitcoin laundering: an analysis of illicit flows into digital currency services*, Center on Sanctions & Illicit Finance und ELLIPTIC, 12. Januar 2018; European Parliament, *Virtual currencies and terrorist financing : assessing the risks and evaluating responses*, Mai 2018, [http://www.europarl.europa.eu/Reg-Data/etudes/STUD/2018/604970/IPOL_STU\(2018\)604970_EN.pdf](http://www.europarl.europa.eu/Reg-Data/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf);

⁸ Bericht des Bundesrates „Rechtliche Grundlagen für Distributed Ledger-Technologie und Blockchain in der Schweiz“, 7. Dezember 2018.

⁹ *Ibid.*

den Wirtschaftssektor zu einer besonderen Problematik geworden. Danach folgt im dritten Kapitel die eigentliche Risikoanalyse. Sie stützt sich auf die Erfahrungen der zuständigen Schweizer Behörden und Trends aus dem Ausland und ist aufgeteilt in eine Überprüfung der Gefährdungen und eine Darstellung der Verwundbarkeiten. Dabei wird aber unterstrichen, dass weder die einen noch die anderen spezifisch sind für die Schweiz, sondern als global betrachtet werden müssen. Am Schluss dieses Kapitels wird eine Risikoeinschätzung vorgenommen. Im vierten Kapitel werden schliesslich die Faktoren aufgezählt, die eine Verminderung der Geldwäscherei- und Terrorismusfinanzierungsrisiken im Zusammenhang mit Kryptowährungen ermöglichen. Der wichtigste dieser Faktoren ist eine umfassende Unterstellung der verschiedenen Gesellschaften, die im Token-Geschäft tätig sind, unter das Geldwäschereigesetz (GwG; SR 955.0). Andere regulatorische und operative Instrumente werden aber ebenfalls berücksichtigt.

Abschliessend geht der Bericht im fünften Kapitel auf das Online-Crowdfunding und die damit verbundenen Geldwäscherei- und Terrorismusfinanzierungsrisiken ein. Dieser Bereich, der wie die Krypto-Assets mit der Entwicklung der FinTech zusammenhängt, steht ebenfalls im Zentrum der nationalen und internationalen politischen Agenda, da im Ausland mehrere Fälle von Terrorismusfinanzierung mithilfe solcher Verfahren zur Mittelbeschaffung aufgedeckt wurden.¹⁰ Es erscheint sinnvoll zu analysieren, ob die Schweiz für den Umgang mit dieser Gefahr, auf die die GAFI bereits 2015 hingewiesen hat¹¹, gerüstet ist.

¹⁰ Siehe beispielsweise: TRACFIN, *Tendances et analyse de risques de blanchiment de capitaux et de financement du terrorisme en 2015*, 2015, S. 64 ff, <https://www.economie.gouv.fr/tracfin/tendances-et-analyse-des-risques-en-2015>.

¹¹ FATF, *Emerging Terrorist Financing Risks*, Oktober 2015, S. 6 und 31 ff, <http://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf>.

1. Virtuelle Währungen

1.1. Definition

Eine virtuelle Währung ist eine elektronische Darstellung eines Wertes, im Internet handelbar und kann als Zahlungsmittel für reale Güter und Dienstleistungen verwendet werden. Sie hat eine eigene Denomination, ist jedoch meist nicht als gesetzliches Zahlungsmittel akzeptiert. Eine virtuelle Währung stellt lediglich einen digitalen Code dar und hat kein physisches Gegenstück zum Beispiel in Form von Münzen oder Noten.¹² Virtuelle Währungen werden im Folgenden synonym verwendet für Kryptowährungen.

Für die vorliegende Risikoanalyse wird das Geldwäscherei- und Terrorismusfinanzierungsrisiko der dezentralen virtuellen Währungen und somit der Kryptowährungen analysiert und im Folgenden auch dieser Begriff verwendet.

1.2. Entwicklungen seit 2014

Im Jahr 2014 publizierte der Bundesrat den Bericht zu virtuellen Währungen in Beantwortung der Postulate Schwaab (13.3687) und Weibel (13.4070).¹³ Der Bitcoin war schon damals die grösste virtuelle Währung und besass am 5. Januar 2014 einen Wert von unter 1000 USD pro Bitcoin¹⁴ bei einer Marktkapitalisierung von gerundet 10.5 Mrd. USD. Am 9. Oktober 2018 beläuft sich der Wert eines Bitcoins auf 6'644 USD und die Marktkapitalisierung des Bitcoin auf gerundet 115 Mrd. USD, was bei 2047 Kryptowährungen einem Marktanteil von 52% entspricht.¹⁵ Sowohl der Wert eines Bitcoins als auch der Gesamtwert der sich in Umlauf befindenden Bitcoins hat sich vervielfacht. Wobei auch sehr viele andere virtuelle Währungen im Vergleich zu 2014 massiv an Wert zugelegt haben, so zum Beispiel Ripple und Litecoin. Dies macht die virtuellen Währungen attraktiv sowohl für Investoren als auch für Kriminelle.

1.3. Typologien virtueller Währungen

Virtuelle Währungen lassen sich grundsätzlich anhand zweier Charaktereigenschaften kategorisieren. Umtauschbare vs. nicht-umtauschbare virtuelle Währungen und zentralisierte vs. dezentralisierte virtuelle Währungen.

1.3.1. Umtauschbare vs. nicht-umtauschbare virtuelle Währungen

Umtauschbare virtuelle Währungen können in offizielle Währungen umgetauscht werden, zum Beispiel Bitcoin, Ether und Weitere. Nicht-umtauschbare virtuelle Währungen können nur innerhalb eines geschlossenen Systems zur Zahlung virtueller oder realer Güter genutzt werden und können nicht in offizielle Währungen umgetauscht werden, zum Beispiel Amazon coin, welcher nur für die Webseite von Amazon gebraucht werden kann und die Funktion eines Gutscheins besitzt.¹⁶

¹² Vgl. auch die Definition im Bericht des Bundesrates zu virtuellen Währungen in Beantwortung der Postulate Schwaab (13.3687) und Weibel (13.4070) vom 25. Juni 2014, 7-8.

¹³ SANSONETTI Riccardo, «Bitcoin: Virtuelle Währungen mit Chancen und Risiken», in Die Volkswirtschaft, 9-2014, S. 44-46.

¹⁴ Vgl. <https://www.coindesk.com/bitcoin-price-2014-year-review/> (zuletzt besucht am 14.05.2018).

¹⁵ Vgl. <https://coinmarketcap.com> (zuletzt besucht am 09.10.2018).

¹⁶ SERAINA GRÜNEWALD, «Währungs- und geldwäschereirechtliche Fragen bei virtuellen Währungen», in: Rolf H. Weber et. Al (Hrsg.), *Rechtliche Herausforderungen durch webbasierte und mobile Zahlungssysteme*, ZIK Bd. 61, Zürich/Basel/Genf 2015, 95.

1.3.2. Zentrale vs. dezentrale virtuelle Währungen

Alle nicht umtauschbaren virtuellen Währungen sind zentrale Währungen. Umtauschbare virtuelle Währungen können zentralisiert oder dezentralisiert sein. Zentrale virtuelle Währungen haben einen zentralen Verwalter, der die Währung herausgibt, die Nutzung regelt und das System kontrolliert. Er kann die Währung auch aus dem Verkehr nehmen. Beispiele für zentrale virtuelle Währungen sind: World of Warcraft gold oder Second Life «Linden dollars». Dezentrale Währungen sind immer umtauschbare virtuelle Währungen und besitzen keinen zentralen Verwalter, der das System kontrollieren kann. Währungen dieses Typs basieren auf der Lösung einer mathematischen Rechnung durch ein Netzwerk von Computern und werden auch Kryptowährungen genannt. Beispiele sind Bitcoin, Ripple und Litecoin.¹⁷

1.3.3. Funktionsweise der Technologie

Mit der Implementierung von Bitcoin Anfang 2009 wurde etwas Neuartiges geschaffen: Bitcoin ermöglicht eine gemeinschaftliche Buchführung mit Teilnehmern, die sich gegenseitig nicht vertrauen, sich nicht kennen und nicht wissen, wie viele andere Teilnehmer im System sind. Die Technologie, die dies ermöglicht, wird Blockchain genannt und erlaubt ein neues Datenverwaltungsmodell. Der Begriff Blockchain bezieht sich dabei darauf, dass Transaktionen in Blöcken gruppiert und gemeinsam bestätigt werden. Die Bestätigung wiederum hängt den Block mit den neuen Transaktionen an eine Kette von vorherigen Blöcken und baut somit inkrementell eine Transaktionshistorie auf.

Die Vielfalt der in der Praxis entstandenen Systeme sprengt den Begriff der Blockchain, weshalb der breitere Begriff der *Distributed Ledger Technology* (DLT) eingeführt wurde.

Die dezentrale Natur der Distributed Ledger Technologie ermöglicht es, Transaktionen direkt zwischen den Parteien ohne zwischengeschalteten Intermediär wie Banken oder Zahlungsdienstleister abzuwickeln (Peer-to-Peer). Die Transaktionen werden in einem dezentral geführten Register gespeichert. Zur Organisation und Speicherung der Datenstruktur haben sich die Teilnehmer deshalb auf (1) die gültigen Transaktionen und (2) ein gültiges Register zu einigen (Distributed Consensus).

Bei den Transaktionen erfolgt die Bestimmung der Gültigkeit i.d.R. dadurch, dass die Teilnehmer abstimmen, welche Transaktionen als "echt" und somit dem gültigen Register hinzuzufügen sind. Die Stimmkraft der abstimmenden Teilnehmer kann sich bei heutigen DLT-Modellen vorwiegend auf zwei Arten bestimmen, wobei auch eine Mischung der Systeme vorkommen kann:¹⁸

- *Proof of Work (Mining)*: Einige Systeme verwenden zur Konsensfindung für die Erstellung von Blöcken den *Proof-of-Work* Mechanismus. Dabei werden solange kryptographische Funktionen ausgeführt, bis das Resultat gewisse Eigenschaften aufweist. Man spricht von einem gültigen *Proof-of-Work* wenn die gesuchte Eigenschaft erfüllt ist. Die kryptographische Funktion macht es dabei unmöglich, die Gültigkeit des Proof-of-Work zu überprüfen ohne die Funktion tatsächlich auszuführen. Aber mit einer gültigen Eingabe ist es trivial deren Gültigkeit zu überprüfen. Dadurch wird der Teilnehmer gezwungen, durch wiederholtes ausprobieren (*Work*) eine gültige Eingabe zu erraten. Bei Bitcoin wendet man eine Einwegfunktion (konkret eine SHA-256-Hashfunktion) solange an bis die Ausgabe ein gewisses Präfix (konkret mehrere 0-Ziffern) aufweist.
- *Proof of Stake*: Zur Validierung der Transaktion wird durch einen Algorithmus ein Teilnehmer ausgewählt. Teilnehmer mit hohen Guthaben und/oder langer Haltefrist werden bevorzugt. Bei

¹⁷ FATF Report-Virtual Currencies, Key Definitions and Potential AML/CFT Risks, Juni 2014, 5.

¹⁸ LUZIUS MEISSER, Kryptowährungen: Geschichte, Funktionsweise, Potential, in: Rolf H. Weber et. al (Hrsg.), Rechtliche Herausforderung durch webbasierte und mobile Zahlungssysteme, ZIK Bd. 61, Zürich/Basel/Genf 2015, 82 f.

diesem Konzept werden i.d.R. nur am Anfang Token geschaffen und deren Anzahl nachträglich nicht erhöht. Die Entlohnung erfolgt daher über Transaktionsgebühren.

Da das Register, d.h. die Datenstruktur, dezentral ist, wird bei jedem oder mehreren Teilnehmern eine Kopie gespeichert und laufend gegenseitig nach den Regeln des Protokolls abgeglichen.¹⁹ Als wahr gilt dabei die Version, welche wiederum von der Mehrheit der Aufbewahrer der Datenstruktur, den sog. *Full (Blockchain) Nodes*²⁰, als wahr bestätigt wird.²¹

2. Kryptowährungen in der Praxis

2.1 Kryptowährungen als Finanzierungsinstrument

Seit 2017 ist ein markanter Anstieg von in der Schweiz durchgeführten oder angebotenen Initial Coin Offerings (ICO) feststellbar. Für ICOs bestehen gegenwärtig keine gesetzlich oder in der Lehre gefestigte Definitionen, gemeinhin kann man darunter jedoch die Schaffung eines Token sowie dessen erstmaliges Angebot gegenüber der Öffentlichkeit verstanden werden²². Das ICO dient dem ICO-Organisator i.d.R. der Verbreitung der Token und der Kapitalbeschaffung zu unternehmerischen Zwecken, die ausschliesslich über die *Distributed Ledger*- bzw. Blockchain-Technologie erfolgt. Bei einem ICO beteiligen sich die Investoren an einem blockchainbasierten Projekt des ICO-Organisators. Die Investoren überweisen finanzielle Mittel an den ICO-Organisator und erhalten im Gegenzug blockchainbasierte Token. Diese werden entweder auf einer in diesem Rahmen neu entwickelten Blockchain oder mittels eines sog. Smart Contract auf einer bereits bestehenden Blockchain geschaffen und dezentral gespeichert. Es handelt sich letztlich um eine Form des Crowdfunding ohne dazwischengeschaltete Plattform (vgl. Ziff. 2 unten). Als Synonyme werden auch *Token Sale* oder *Token Generating Event* verwendet. Teilnehmer an einem ICO investieren häufig in Projektanlagen bzw. Business-Ideen und hoffen auf eine erfolgreiche Projektrealisierung. Im Ergebnis sind ICOs traditionellen Finanzierungsrunden resp. Private Placements sehr ähnlich. Die über die emittierten Token entgegengenommenen finanziellen Mittel können dabei grundsätzlich einen Eigenkapital- oder einen Fremdkapitalcharakter aufweisen. Für gewöhnlich sollen die Tokeninhaber jedoch weder Aktionäre noch Gläubiger der Gesellschaft werden. In diesen Fällen können bei der Emission aufwendigen Dokumentationen (wie z.B. die Prospektpflicht) oftmals ausgewichen werden²³. Ebenfalls werden Transparenzvorschriften zu juristischen Personen umgangen. In Fällen, in denen die Token mit der Absicht zur Schaffung von kryptographischen Aktien ausgegeben werden, stellen sich grundsätzliche gesellschaftsrechtliche Fragen, inwiefern eine Aktionariatsstellung auf diesem Weg begründet werden kann.

ICOs sind für gewöhnlich so ausgestaltet, dass Investoren den neu auszugebenden Token erwerben können, indem sie Ethers (ETH) oder Bitcoins (BTC) auf eine dem ICO-Organisator zugehörigen Blockchain-Adresse (z.B. ein Smart Contract) übertragen werden. In einigen Fällen akzeptieren ICO-Organisatoren auch Zahlungen in Fiatgeld. Für die Teilnahme am ICO ist regelmässig eine vorgängige

¹⁹ LUZIUS MEISSER, a.a.O., 83 f.

²⁰ Aufbewahrer des *Blockchain Protocol* (inkl. des "Registers" der Transaktionen). Die *Full Blockchain Nodes* vergleichen stetig das *Blockchain Protocol* untereinander und stellen so sicher, dass keine falschen Transaktionen stattfinden können. Zudem finden Transaktionen über die *Full Blockchain Nodes* statt.

²¹ MARTIN HESS/PATRICK SPIELMANN, *Cryptocurrencies, Blockchain. Handelsplätze & Co. – Digitalisierte Werte unter Schweizer Recht*, in: Reutter, Thomas U. / Werlen, Thomas (Hrsg.): *Kapitalmarkt – Recht und Transaktionen XII*. Zürich: Schulthess 2017, S. 154.

²² Dabei laufen ICOs oftmals in verschiedenen Phasen ab. Dem an die breite Öffentlichkeit gerichteten Public ICO gehen in der Regel sog. Pre-Sales oder Private Sales voraus, in deren Rahmen sich lediglich ein beschränkter Teilnehmerkreis beteiligen kann.

²³ Eine Ausnahme hierzu stellt das Erfordernis der Erstellung eines Anleiheprospekts bei der Ausgabe von Anleiheobligationen gemäss Art. 1156 des Obligationenrechts dar.

Registrierung (z.T. mit Identifizierung) des Teilnehmers auf der Website des ICO-Organisators erforderlich, wobei in Bezug auf das Kundenonboarding noch kaum einheitliche Standards bestehen.

Dem ICO kann in der Form eines *Pre-Sales* eine private Platzierung der Token zu Vorzugskonditionen bei ausgewählten Investoren vorangehen. Im Kontext von ICOs werden bei Vorfinanzierungen und Vorverkäufen teilweise noch keine Token ausgegeben, sondern lediglich (bedingte)²⁴ Ansprüche auf einen noch zu schaffenden Token vermittelt.

Die nachfolgende Graphik²⁵ illustriert die markante Zunahme von ICO-Vorhaben global:



Einheitliche Daten zur Anzahl der weltweit stattgefundenen ICOs sowie den damit gesammelten Volumina lassen sich nicht genau ausmachen. Einer Studie von PWC Schweiz zufolge, fanden im vergangenen Jahr weltweit 450 ICOs statt, die Investitionssummen von rund CHF 4.6 Mrd. einbrachten. Die gesammelten Volumina betragen fast zwanzig Mal mehr als noch im Jahr 2016. Alleine in der Schweiz kamen mit 70 durchgeführten ICOs CHF 1 Mrd. zusammen.²⁶ Diese Zahlen verdeutlichen die Bedeutung des Schweizer Finanzplatzes im ICO-Markt. Die Schweiz ist weltweit ein Zentrum für ICOs. Insbesondere bei ICOs, welche im Jahre 2017 stattgefunden haben, wurde oft die Stiftungsform benutzt (siehe auch Tabelle unten). 2018 ist allerdings eine Zunahme der ICOs zu beobachten, die von Aktiengesellschaften oder von Gesellschaften mit beschränkter Haftung (GmbH) organisiert wurden. Die FINMA hat vor dem Hintergrund des starken Anstiegs von in der Schweiz durchgeführten ICO eine

²⁴ Z.B. ist in den "Terms of Token Sale" vorgesehen, dass bei Nichtzustandekommen des Projekts kein Anspruch auf entsprechende Token besteht.

²⁵ Die Graphik stammt von <https://www.coindesk.com/ico-tracker/> ("All-time Cumulative ICO Funding"; zuletzt besucht am: 27. Juli 2018).

²⁶ Vgl. <https://www.srf.ch/news/wirtschaft/finanzierung-mit-digitalgeld-millionen-generieren-mit-bitcoin-und-co>; mit Hinweis auf die PWC Studie (zuletzt besucht am: 27. März 2018). Z.B. wurden bei der TEZOS ICO (beendet am 14. Juli 2017) USD 228'590'404 gesammelt.

Wegleitung²⁷ publiziert, wie sie auf Basis des bestehenden Finanzmarktrechts ICOs aufsichtsrechtlich einordnet.

Die konkrete Ausgestaltung von ICOs unterscheidet sich im Einzelfall in technischer, funktionaler und ökonomischer Hinsicht sehr stark, sodass eine allgemeingültige Kategorisierung nicht möglich ist. Mit einigen ICOs werden z.B. Token geschaffen, die Funktionen von Geld übernehmen sollen und damit geeignet sind, als Zahlungsmittel im Sinne des Geldwäschereigesetzes (GwG) zu qualifizieren. In diesem Zusammenhang ist geplant, dass sich die Arbeitsgruppe des Bundesrates zu Blockchain/ICO²⁸, vertiefter mit den verschiedenen Konstellationen und rechtlichen Implikationen der verschiedenen Token-Modelle befasst.

Zahlungsmittel sind Instrumente, die Drittparteien die Übertragung von Vermögenswerten ermöglichen.²⁹ Eine einheitliche Begriffsdefinition existiert im Schweizer Recht nicht. Die Ausgabe von Zahlungsmitteln stellt allerdings eine dem GwG unterstellte Tätigkeit dar. Das Gesetz führt als Beispiele Kreditkarten und Reisechecks als Zahlungsmittel auf (Art. 2 Abs. 3 Bst. b GwG). Die exemplarische Aufzählung zeigt, dass regulatorisch von einem weiten Zahlungsmittelbegriff auszugehen ist.

Ein im Rahmen eines ICO ausgegebener Token qualifiziert als Zahlungsmittel im Sinne des Geldwäschereigesetzes, wenn er entweder tatsächlich oder der Absicht des Herausgebers nach als Zahlungsmittel für den Erwerb von Waren oder Dienstleistungen eingesetzt werden soll. Im Gegensatz zu Münzen oder Banknoten und Sichtguthaben bei der SNB sind Kryptowährungen nicht als gesetzliches Zahlungsmittel akzeptiert und in Schweizerfranken denominiert (z.B. BTC, ETH). Anders als etwa E-Geld sind Kryptowährungen nicht notwendigerweise eine Forderung gegenüber dem Emittenten. Sie existieren einzig als digitaler Code und es gibt kein materialisiertes Gegenstück in Form von Münzen oder Noten. Bestimmte Token entwickeln sich teilweise auch erst über die Zeit zu einer Kryptowährung, sobald die Akzeptanz als Zahlungsmittel gegeben ist. Es kann aber auch bereits im Zeitpunkt der ICO eine Kryptowährung vorliegen, wenn die Schaffung eines Zahlungsmittels beabsichtigt wird.

Die Zahlungsabwicklung folgt typischerweise folgendem (etwas vereinfacht dargestellten) Muster:

- (1) Der Schuldner gibt über sein Konto entweder direkt oder aber über einen Account bei einer Handelsplattform (vgl. Bst. d unten) die Empfänger-Adresse des Gläubigers und die Anzahl der zu übersendenden Token ein.
- (2) Die Informationen werden in das Blockchain-Netzwerk versendet.
- (3) Das Blockchain-Netzwerk bestätigt basierend auf dem im jeweiligen Protokoll angelegten Consensus-Mechanismus die Gültigkeit der Transaktion und die Gutschrift an die Adresse des Gläubigers.

Trotz grossen Kursschwankungen akzeptieren eine zunehmende Anzahl von Händlern (v.a. im Online-Handel oder Dienstleister im Informatikbereich) Kryptowährungen als Zahlungsmittel.³⁰

²⁷ Vgl. <https://www.finma.ch/de/news/2018/02/20180216-mm-ico-wegleitung/> (zuletzt besucht am: 29. März 2018).

²⁸ Bericht des Bundesrates „Rechtliche Grundlagen für Distributed Ledger-Technologie und Blockchain in der Schweiz“, 7. Dezember 2018.

²⁹ Vgl. FINMA-RS 2011/1 "Tätigkeit als Finanzintermediär nach GwG", Rz. 55.

³⁰ Am weitesten verbreitet dürfte noch immer der Bitcoin sein. Beispiele in der Schweiz sind die Einwohnerkontrolle der Stadt Zug sowie das Zuger Handelsregisteramt. Vgl. auch <https://bitcoin-stores.ch/> (zuletzt besucht am: 29. März 2018); diese Seite führt ein Schweizer Bitcoin Shop Verzeichnis und Bitcoin eShopping Branchenbuch und listet nur Geschäfte und Online-Shops in der Schweiz, die Bitcoins als Zahlungsmittel akzeptieren.

Gemäss Angaben von Coinmarketcap gibt es derzeit 2'094 Kryptowährungen weltweit.³¹ Unter den rund top-40 Kryptowährungen mit einer Marktkapitalisierung über USD 300 Mio. (Stand: 08.11.2018) weisen namentlich die folgenden Unternehmen einen Bezug zur Schweiz auf:

Rang	Name	Market cap. (Mia. USD)	Schweiz-Bezug
# 2	Ethereum (ETH)	21.7	Foundation Ethereum, Zug
# 8	Cardano (ADA)	1.9	Cardano Stiftung, Zug
# 18	Tezos (XTZ)	0.78	Tezos Stiftung, Zug
# 29	Lisk (LSK)	0.3	Lisk Stiftung, Zug
# 37	Icon (ICX)	0.2	Icon Stiftung, Zug

2.2 Wallet-Anbieter

Um Transaktionen über die DLT vornehmen zu können, wird ein kryptographisches Schlüsselpaar benötigt. Dieses besteht aus einem Public Key (PUK), der als Adresse dient (eine Art Kontonummer) und einem Private Key (PIK), der vollen Zugriff auf die Adresse gibt (vergleichbar mit der PIN). Entscheidendes Element für die Veranlassung einer Transaktion ist der PIK. Denn nur mit diesem kann eine Transaktion gültig signiert und damit ausgelöst werden. Geht der PIK verloren, geht auch die Verfügungsmacht über die Kryptowährung verloren. Entsprechend wichtig ist es, den PIK sicher aufzubewahren. Dies kann über eine sog. Wallet erfolgen. Gemeinhin kann darunter also Software verstanden werden, die es mittels eines Interface erlaubt, kryptographische Token zu verwalten.

Wallets können von entsprechenden Wallet-App-Entwicklern unterschiedlich ausgestaltet werden: Grundsätzlich kann zwischen *decentralized* wallet-Applikationen und *custody* wallet-Providern unterschieden werden. Bei ersteren handelt es sich typischerweise um dezentral organisierte Open Source-Projekte, welche nicht unbedingt einzelnen Unternehmen zugeordnet werden können. Die entsprechenden Software-Applikationen werden dabei oftmals kostenlos als Freeware zur Verfügung gestellt (z.B. Mycelium / Electrum, u.Ä.; auch als non-custodian wallets, private wallets oder self-hosted wallets bezeichnet). Entsprechende *Wallets* erlauben es Nutzern, selbst ihre *Keypairs* zu verwalten (abzugrenzen von sog. crypto *custodians* bzw. *custody wallet* Providern), d.h. der Entwickler hat in der Regel keine Kenntnis oder Zugriffsmöglichkeit auf die generierten Keypairs der App-Nutzer. Custody wallet-Provider unterhalten im Gegensatz dazu oft eine dauerhafte Kundenbeziehung und verwalten zu diesem Zweck auch die entsprechenden *Keypairs* (d.h. insbesondere auch die Private Keys der Kunden).

Anhand einer Studie der University of Cambridge³² aus dem Jahre 2017 lässt sich folgende grobe Abschätzung zum Markt der Wallet-Anbieter machen:

³¹ Vgl. <https://coinmarketcap.com/all/views/all/> (zuletzt besucht am: 12. November 2018).

³² Die Schätzungen basieren auf der [Global Cryptocurrency Benchmarking Study 2017](#) von Garrick Hileman & Michel Rauchs, Cambridge Center for Alternative Finance, University of Cambridge, Judge Business School (zuletzt besucht am: 28. März 2018).

- Es wird geschätzt, dass die Anzahl der Wallets von 8.2 Mio. im Jahr 2013 auf fast 35 Mio. im Jahr 2016 angestiegen ist.
- Im vergangenen Jahr waren schätzungsweise zwischen 5.8 und 11.5 Mio. Wallets aktiv.
- Ca. 80% der Wallet-Anbieter sollen entweder in Nordamerika oder Europa domiziliert sein, wobei nur 60% der Nutzer auch aus diesen Regionen stammen.
- Ca. 73% der Wallets kontrollieren keine PIK (Private Wallets), 15% sind Custodian Wallets und bei 12% der Wallets kann der Nutzer den Zugriff auf den PIK bestimmen.
- Knapp 40% der Wallets unterstützen mehrere Kryptowährungen.
- Mobile Wallet Apps sind am meisten verbreitet (65%), gefolgt von Desktop- (42%) und Internet-Wallets (38%).
- Die Abgrenzung zwischen Wallets und Handelsplattformen wird zunehmend unschärfer. Ungefähr die Hälfte der Wallets verfügt angeblich auch über eine Exchangefunktionalität (vgl. Ziff. 4.1. unten).
- Ca. 24% der Walletanbieter halten eine staatliche Lizenz. Sämtliche dieser Wallet-Anbieter unterstützen den Wechsel von Kryptowährung vs. Fiatgeld. Von den Wallet-Anbietern, die den Wechsel von Kryptowährung vs. Fiatgeld ermöglichen, halten jedoch nur 75% eine staatliche Lizenz.

Am 30. Mai 2018 haben das Europäische Parlament und der Rat der EU eine Änderung der 4. Geldwäschereirichtlinie verabschiedet.³³ Diese sieht neu u.a. vor, dass der Anwendungsbereich der Richtlinie auf Plattformen zum Umtausch virtueller Währungen sowie Anbieter von Custodian Wallets ausgedehnt wird, um Nutzer virtueller Währungen leichter identifizieren zu können.

Die FATF verfolgt die Themen um virtuelle Währungen und DLT im Rahmen der "Risk, Trends and Methods Group" (RTMG) und erarbeitet Empfehlungen. In einem Virtual Currencies Update (Oktober 2017) der RTMG hat diese die Rolle der Hosted Wallet-Anbieter, die auch technisch ungebildeten Nutzern den einfachen Transfer von virtuellen Währungen erlauben, sowie ICOs angesprochen. Diese Themen werden als zukünftige Herausforderungen und Diskussionsthemen benannt.

2.3 Wechselstuben und zentralisierte/dezentralisierte Handelsplattformen

Grundsätzlich kann zwischen Online-Wechselstuben und (zentralisierten und dezentralisierten) Handelsplattformen unterschieden werden. Beim Wechselgeschäft bieten die Wechsler den Kauf und Verkauf von Kryptowährungen direkt aus dem Eigenbestand an. Sie treten nicht als Vermittleragentur oder Marktplatz zwischen Käufern und Verkäufern von Kryptowährungen auf, sondern fungieren vielmehr im Sinne einer Wechselstube (Zweiparteienverhältnis). Wechselgeschäfte mit Kryptowährungen qualifizieren als finanzintermediäre Tätigkeit im Sinne des GwG.

Zentralisierte Handelsplattformen verfügen ähnlich wie traditionelle Handelsplätze über ein Orderbuch, Matching Rules und Ordertypen. Speziell ist, dass die Benutzer direkt auf der Plattform handeln (non-intermediated access) anstatt über einen regulierten Finanzintermediär (z.B. Bank oder Effekthändler) zu gehen. Der Benutzer deponiert seine Token entweder bei der Plattform oder nutzt ein Wallet, auf welches die Plattform Zugriff hat. Die Transaktionen laufen über die Plattform und die Token bleiben in der Regel im Zugriff der Plattform (Private Keys), bis der Benutzer die Token in eine andere Wallet überweisen lässt. Diese Handelsplattformen unterscheiden sich von Wechslern dadurch, dass sie eine Vermittlerfunktion übernehmen und somit ein Dreiparteienverhältnis vorliegt. Der Händler nimmt Gelder oder Kryptowährungen von Kunden entgegen und leitet diese an andere Nutzer weiter. Sie funktionieren

³³ Vgl. Richtlinie (EU) 2018/843 des Europäischen Parlaments und des Rates vom 30. Mai 2018 zur Änderung der Richtlinie (EU) 2015/849 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung, ABI. L 156 vom 19.06.2018, S.43.

also wie ein Devisenmarkt, an dem Devisenangebot und –nachfrage aufeinandertreffen und zum ausgehandelten Devisenkurs getauscht werden. Solche Handelsplattform qualifizieren als sog. Money Transmitter und sind entsprechend dem GwG unterstellt. Neben dieser Tätigkeit bieten viele Handelsplattformen auch den Kauf und Verkauf von Kryptowährungen aus dem Eigenbestand an und fungieren in dieser Hinsicht wie eine traditionelle Wechselstube. Der vorliegende Bericht konzentriert sich in diesem Zusammenhang auf Fragestellungen im Bereich der Geldwäschereigesetzgebung. Typischerweise bedürfen zentralisierte Handelsplattformen in der Schweiz jedoch zusätzlich Bewilligungen der FINMA.³⁴ In der Schweiz gibt es derzeit keine bewilligte Handelsplattform für Kryptowährungen.

Der Exchange-Sektor für Kryptowährungen ist der bedeutendste Markt und weist die grösste Population von Unternehmen auf, die in diesem Bereich operativ tätig sind. Per 12. November 2018 wurden gemäss Zahlen von Coinmarketcap weltweit auf insgesamt 15'840 "Märkten" 2094 Kryptowährungen gehandelt.³⁵ Auf derselben Website gibt es ein Ranking von 207 Handelsplattformen, die die grössten täglichen Handelsvolumen aufweisen.³⁶ Die – gemessen am Bitcoin-Handelsvolumen – aktuell fünf grössten Handelsplattformen sind Bifinex (HongKong), OKEEx (Belize/HongKong), Binance (HongKong), Huobi (Peking) und Bitflyer (Japan). In der Schweiz sind entsprechende Handelsplattformen derzeit in der Planungs- und Umsetzungsphase. Im Bereich des Sekundärmarkts sind demgegenüber bereits einige Broker (namentlich Bitcoin Suisse³⁷ und Bity³⁸), die das Wechselgeschäft betreiben tätig. Diese müssen nach geltendem Recht übereinen SRO-Anschluss oder eine Bewilligung der FINMA als direkt unterstellter Finanzintermediär (DUFI) verfügen, sofern sie aufgrund ihrer Tätigkeiten nicht ohnehin bereits eine andere Bewilligung nach den Finanzmarktgesetzen benötigen.

Die FATF hat in einer Guidance vom Juni 2015³⁹ insb. die Risiken beim Umtausch von Kryptowährungen in Fiatgeld hervorgehoben und auf die Notwendigkeit der Regulierung von VC-Exchanges hingewiesen. Dies in Anwendung der FATF Empfehlungen 14, 16 und 26.

2.4 Dezentralisierte Handelsplattformen

Wie zentralisierte Handelsplattformen führen auch dezentralisierte Handelsplattformen ein übliches Orderbuch, aber sie kontrollieren die Token-Wallet der Kunden nicht. D.h. die Plattform verfügt nicht über die Private Keys. Die Token werden dezentral auf den Wallets der Kunden gehalten und nicht gepoolt durch die Plattform verwahrt, was das Hacking-Risiko vermindern sollte. Das Settlement findet direkt auf der Blockchain mittels Smart Contract statt. Auch dezentralisierte Plattformen lassen ihre Privatkunden oft direkt als Teilnehmer zu.

Anders als bei bilateralen Handelsplattformen oder Wechselstuben wird eine vollständig dezentralisierte Plattform nie Gegenpartei eines Trades und im Unterschied zu zentralisierten Handelsplattformen erfolgt die Abwicklung der zusammengeführten Aufträge (nach Freigabe / Bestätigung des Trades) auf der Blockchain direkt zwischen den Benutzern der Plattform. Da letztlich unter Zuhilfenahme der Handelsplattform ein Transfer von Vermögenswerten stattfindet, stellt sich die Frage, ob die Plattform eine finanzintermediäre Dienstleistung im Sinne des GwG erbringt⁴⁰.

³⁴ Beim Handel von Tokens, welche als Effekten im Sinne der Finanzmarktinfrastrukturgesetzgebung qualifizieren, kommt insbesondere eine Bewilligung als multilaterales Handelssystem, oder eine Bewilligung als Effekthändler (mit oder ohne Zulassung zum Betrieb eines organisierten Handelssystems) in Betracht. Denkbar ist zudem auch eine Bewilligung als Bank, je nach gelagerter Tätigkeit der Plattform.

³⁵ Vgl. <https://coinmarketcap.com/> (zuletzt besucht am: 12. November 2018).

³⁶ Vgl. <https://coinmarketcap.com/exchanges/volume/24-hour/all/> (zuletzt besucht am: 28. März 2018).

³⁷ Vgl. <https://www.bitcoinsuisse.ch/> (zuletzt besucht am: 13. März 2018).

³⁸ Vgl. <https://bity.com/> (zuletzt besucht am: 13. März 2018).

³⁹ FATF Virtual Currencies – Guidance for a risk-based approach 6/2015.

⁴⁰ Bericht des Bundesrates „Rechtliche Grundlagen für Distributed Ledger-Technologie und Blockchain in der Schweiz“, 7. Dezember 2018, S. 137-151.

2.5 Off-chain Zahlungssysteme

Aufgrund der geringen Transaktionsgeschwindigkeiten über die Blockchain sind seit längerer Zeit Skalierungsbestrebungen im Gange. Eine Lösung für dieses Problem versprechen Anbieter von sog. "Off-chain Zahlungssystemen"⁴¹. Dabei handelt es sich um ein Netzwerk, in welchem die Nutzer Zahlungen an andere Nutzer des Netzwerks online (aber off-chain) vornehmen können. Das Zahlungssystem ist dezentral und hat keinen Zugriff auf die Vermögenswerte der Nutzer.

2.6 Kryptofonds

Neben der Möglichkeit direkt in Kryptowährungen zu investieren, sind auch Bestrebungen im Gange, die Nachfrage nach indirekten Investitionsmöglichkeiten zu bedienen. Verschiedene Akteure beabsichtigten die Lancierung eines Kryptofonds. Unter Kryptofonds versteht man gemeinhin kollektive Kapitalanlagen, welche ihr Fondsvermögen überwiegend oder ausschliesslich in Kryptowährungen oder andere Krypto-Assets anlegen. Sie werden geldwäschereirechtlich nicht anders behandelt als andere kollektive Kapitalanlagen, d.h. sie gelten als Finanzintermediäre, falls sie über eine Bewilligung als Fondsleistung, SICAV, KmGK oder SICAF verfügen⁴². Zurzeit gibt es keinen genehmigten Schweizer Kryptofonds.

3. Risikoanalyse

Parallel zur spektakulären Entwicklung der Krypto-Assets seit der Erfindung des Bitcoins im Jahr 2009 haben auch die Risiken einer kriminellen Verwendung zugenommen. Während Ökonomen und Regulierungsbehörden laufend auf die spekulativen Risiken von Investitionen in Kryptowährungen und vor allem in ICOs aufmerksam machen, denen Anlegerinnen und Anleger ausgesetzt sind⁴³, unterstreichen mehrere nationale und internationale Instanzen die Gefahr der Geldwäscherei und Terrorismusfinanzierung in Verbindung mit Kryptowährungen.⁴⁴ Der Bundesrat hatte dieses Risiko bereits in seinem Bericht von 2014 in Beantwortung der Postulate Schwaab (13.3687) und Weibel (13.4070) hervorgehoben.⁴⁵ Zwar hat die Zahl der Kryptowährungen in den letzten Jahren markant zugenommen und ihre Nutzung gewinnt immer mehr an Bedeutung. Aber dank den Erfahrungen, die die für die Prävention und Repression von Wirtschaftskriminalität zuständigen Behörden unterdessen gesammelt haben, können die Trends, die das Geldwäscherei- und Terrorismusfinanzierungsrisiko gegenwärtig prägen, besser erkannt werden. Die Beurteilung dieses Risikos beruht sowohl auf den Gefährdungen, die Kryptowährungen für die Integrität des Finanzsystems darstellen, als auch auf den Verwundbarkeiten, die dieses System kennzeichnen. Bei den Gefährdungen ist zu unterscheiden zwischen jenen, die untrennbar verbunden sind mit den Kryptowährungstechnologien, und jenen im Zusammenhang mit ihrer möglichen Verwendung für Wirtschaftsdelikte, für die auch Fiatgeld eingesetzt werden könnte, die aber durch die Nutzung von Kryptowährungen noch gefährlicher sind. Die Schwachstellen der Schweiz im Hinblick auf die Gefahr der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets, auf die später eingegangen wird, sind die gleichen wie jene der meisten anderen Länder, die ebenfalls mit diesem neuen und zunehmenden Risiko konfrontiert sind.

⁴¹ Vgl. z.B. die Lösung von [Liquidity Network](#) (zuletzt besucht am 12. Juli 2018).

⁴² Art. 2 Abs. 2 lit. b und lit. b^{bis} GwG.

⁴³ Vgl. beispielsweise die zahlreichen Warnungen, die seit 2014 von der amerikanischen *Securities and Exchange Commission* publiziert werden: <https://www.sec.gov/news/statements>.

⁴⁴ GAFI, *Virtual currencies. Key definitions and potential AML/CFT risks*, Juni 2014, <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>.

⁴⁵ Bericht des Bundesrates zu virtuellen Währungen in Beantwortung der Postulate Schwaab (13.3687) und Weibel (13.4070) vom 25. Juni 2014, <https://www.news.admin.ch/NSBSubscriber/message/attachments/35361.pdf>

3.1. Gefährdungen in Verbindung mit Krypto-Assets

3.1.1. Untrennbar mit der Krypto-Asset-Technologie verbundene Gefährdung

a. Anonymität der Transaktionen und schwierige Identifikation der wirtschaftlich Berechtigten

Die grösste Gefährdung durch Krypto-Assets ergibt sich aus der Anonymität der damit durchgeführten Transaktionen.

Zur Abwicklung von Kryptotransaktionen genügt es, lediglich über eine elektronische Geldbörse oder eine Wallet zu verfügen, die man dank zahlreichen Internet-Programmen ganz einfach und kostenlos einrichten kann. Ausser wenn es sich um eine Wallet handelt, die von einem spezialisierten Unternehmen verwaltet wird (*Custodian Wallets*), verläuft der Verfahren zur Einrichtung einer solchen elektronischen Geldbörse meistens anonym. Um eine Transaktion vorzunehmen, muss der Wallet-Inhaber lediglich mit seinem Private Key eine Überweisung an eine andere Adresse des gleichen Typs in Auftrag geben oder seine öffentliche Adresse einem anderen Nutzer bekannt geben, der die Wallet beispielsweise zur Bezahlung eines Einkaufs oder einer Dienstleistung belasten will. Bei Kryptowährungen wie dem Bitcoin, deren Technologie auf einer Kombination von asymmetrischer Verschlüsselung und Blockchain aufbaut, werden die Transaktionen aufgrund der tatsächlich in der betreffenden Wallet vorhandenen Vermögenswerte durch Miner entweder bestätigt oder eben nicht. Dabei sind die Transaktionen für alle Nutzer dieser Kryptowährung sichtbar. Die Transaktionen lassen sich somit vollumfänglich zurückverfolgen, aber die tatsächliche Identität der Person, die mit dieser Wallet verbunden ist, bleibt für die anderen Nutzer unbekannt. Ausserdem erlaubt dieses System zwar eine Identifizierung aller Transaktionen, die von einer bestimmten Adresse stammen oder an sie gerichtet sind. Die meisten Wallet-Programme erzeugen aber automatisch mehrere Adressen für die gleiche Wallet und ein Nutzer kann mehrere Wallets besitzen und für jede Transaktion eine andere nutzen, so dass es praktisch unmöglich wird, eine physische Person mit den von ihr veranlassten Transaktionen in Verbindung zu bringen.

Die Blockchain-Technologie wurde zudem, seit sie zur Einführung des Bitcoins geschaffen wurde, weiterentwickelt und gewährt gewissen Kryptowährungen unterdessen noch mehr Anonymität. Das gilt beispielsweise für Währungen wie den Bytecoin oder seinen Nachfolger Monero, die auf der CryptoNote-Technologie basieren: einem kryptographischen Verfahren, das sich auf die sogenannte «Ring Signature» stützt und sich von jenem der Bitcoins und Ethers unterscheidet. Diese Technologie erlaubt eine Gruppierung von Nutzern: Wenn einer von ihnen eine Transaktion in Auftrag gibt, ist es somit unmöglich zu wissen, welches Mitglied der Gruppe dies getan hat. Mit dem CryptoNote-Algorithmus kann ausserdem die Historie der Transaktionen vollständig verschleiert werden, dies im Gegensatz zur Blockchain beim Bitcoin, auf der die ganze Kette von Transaktionen von jedem Nutzer, der dies will, eingesehen werden kann. Schliesslich ermöglicht CryptoNote eine Stückelung der bei einer Transaktion übermittelten Summen über Drittkonten, so dass der tatsächliche Gesamtbetrag unsichtbar wird und nicht zurückverfolgt werden kann.

Ein solches Stückelungsverfahren kann im Übrigen von «Mischdiensten», die auch als Mixer oder Tumbler bezeichnet werden, durchgeführt werden, um die Anonymität von Transaktionen in Kryptowährungen zu erhöhen, die ebenso wie der Bitcoin die Blockchain-Technologie nutzen. Dabei werden die Kryptowährungen auf eine Plattform geschickt, die den Betrag zuerst in viele kleinere Summen aufteilt und an andere Adressen überweist, bevor die Gesamtsumme an die Adresse des Empfängers geleitet wird. Während insbesondere bei Bitcoins solche Mischdienste von externen Servern angeboten werden, haben gewisse erst vor kurzem entwickelte Krypto-Assets wie etwa Dash sie direkt in ihr Protokoll integriert, womit die mit Token-Transaktionen verbundene Anonymität weiter gestärkt wird. Die Anonymität ist aber auch bei den anderen Kryptowährungen bereits sehr gross, weshalb sie alle für Kriminelle besonders attraktiv sind.

Nicht zuletzt ermöglichen auch neu entwickelte Technologien zur Nutzung von Kryptowährungen, diese Anonymität zu stärken. Das gilt etwa für Prepaid-Debitkarten in Krypto-Assets und Krypto-Banknoten, wie sie vor kurzem von einem Zuger Unternehmen lanciert wurden, das auch über eine Niederlassung in Singapur verfügt.⁴⁶

Bezüglich Anonymität ist Bargeld mit einem ähnlichen Risiko verbunden wie Kryptowährungen.⁴⁷ Die Gefährdung, die von letzteren ausgeht, wird aber durch die technologiebedingte Schnelligkeit und Mobilität der Transaktionen verschärft. Im Gegensatz zum Bargeld können bei Kryptowährungen innert Sekunden enorme Summen von einem elektronischen Konto auf ein anderes verschoben werden, ohne dass man weiss, wer diese Transaktionen durchführt. Die involvierten Beträge können somit anonymen Nutzern überall auf der Welt fast unmittelbar zur Verfügung gestellt werden. Ausserdem kann der Inhaber einer Wallet den Private Key, der einem Dritten völlig anonym Zugriff auf seine elektronische Geldbörse gewährt, nach Belieben weitergeben. Auch diese Praxis lässt sich mit einer Übergabe von Bargeld von Hand zu Hand vergleichen, aber weil Kryptowährungen über Internet und völlig anonym weitergegeben werden können, steigt die damit verbundene Gefährdung. Die Gefahr von Geldwäscherei, die von Kryptowährungen ausgeht, ist also auf die Kombination von Anonymität, Schnelligkeit und Mobilität zurückzuführen.

b. Sicherheitslücken bei den grundlegenden Kryptowährungstechnologien

Die grundlegenden Technologien von Krypto-Assets – insbesondere Blockchain und ihre Folgetechnologien ebenso wie die asymmetrische Verschlüsselung – wurden entwickelt, um Transaktionen unter gleichzeitiger Gewährleistung der Anonymität vollständig absichern zu können. Dank der kollektiven Kontrolle durch die Miner können solche Transaktionen nur von Nutzern ausgeführt werden, die in ihrer Wallet tatsächlich über das Guthaben in Kryptowährung verfügen, das sie ausgeben wollen. Dank der asymmetrischen Verschlüsselung kann zudem nur der tatsächliche Inhaber der Wallet auf die dort gutgeschriebenen Vermögenswerte zugreifen, um Transaktionen durchzuführen. Wenn eine Transaktion von den Minern schliesslich validiert wurde, wird sie auf der Blockchain registriert und gilt als unwiderruflich. Ein solcher Eintrag kann nämlich nur gelöscht werden, wenn die gesamte Blockchain geändert wird. Dafür müsste man aber über mehr als die Hälfte der Mining-Leistung (*Hashrate*) für die betreffende Blockchain verfügen. Für die Bitcoin-Blockchain wäre dazu eine Rechnerleistung nötig, die schätzungsweise über 50-mal grösser ist als jene eines Unternehmens wie Google.

Diese Technologien sind aber trotzdem nicht unfehlbar. Da immer umfangreichere Proof-of-Work-Berechnungen verlangt werden, kann das Mining nämlich nicht mehr wie in der Anfangszeit der Kryptowährungen von einem einzigen Miner über seinen Computer durchgeführt werden, sondern erfordert eine Bündelung der Ressourcen und die Schaffung von Mining-Pools, dessen Mitglieder sich die Erträge teilen. Durch eine solche Zusammenlegung der Ressourcen droht aber auch die Gefahr, dass mehr als 50 Prozent der Hashrate einer Blockchain in den Händen eines einzigen Mining-Pools konzentriert werden, der dann die Blockchain nach Gutdünken verändern, Transaktionsdaten löschen oder fiktive Transaktionen durch die eigenen Miner bestätigen lassen könnte.⁴⁸ Diesbezüglich stellt die Entwicklung von immer leistungsstärkeren Prozessoren eine Gefahr dar. Diese Maschinen, die in der Regel für industrielle oder administrative Zwecke und nicht zum Schürfen von Kryptowährungen entwickelt werden, sind immer häufiger Zielscheibe von Hackern, die deren Rechenleistung für das Mining abzweigen wollen.

⁴⁶ Emmanuel Garessus, «Une société suisse veut émettre des billets de bitcoins», in *Le Temps*, 8. Mai 2018, <https://www.lemtemps.ch/economie/une-societe-suisse-veut-emettre-billets-bitcoins>; «Singapour : les premiers billets Bitcoins visent à favoriser l'adoption de l'actif», in *Crypto-France.com*, <https://www.crypto-france.com/singapour-premiers-billets-bitcoin/>.

⁴⁷ KGGT, *Bericht über die Bargeldverwendung und deren Missbrauchsrisiken für die Geldwäscherei und Terrorismusfinanzierung in der Schweiz*, Oktober 2018.

⁴⁸ DE PREUX Pascal et TRAJILOVIC Daniel, «Blockchain et lutte contre le blanchiment d'argent. Le nouveau paradoxe ?», in *Resolution LP*, https://resolution-lp.ch/wp-content/uploads/2018/02/064_L_14_De_Preux_Trajlilovic.pdf.

In anderen Fällen sind es die rechtmässigen Nutzer dieser Computer selbst, die sie zum Mining einsetzen. Dies war etwa im Februar 2018 der Fall, als Wissenschaftler des russischen staatlichen Nuklearzentrums in Sarow vom russischen Inlandsgeheimdienst FSB verhaftet wurden, als sie eben versuchten, das IT-System des Zentrums – einen der leistungsstärksten Computer der Welt – zum Schürfen von Bitcoins mit dem Internet zu verbinden.⁴⁹ Überdies sind die Mining-Erträge so hoch, dass es durchaus vorstellbar ist, dass Kriminelle zum Waschen ihrer Erträge aus illegalen Tätigkeiten massiv in den Kauf von Computern investieren und diese zum Aufbau von Mining-Farmen verwenden. Solche Beispiele zeigen, dass die Gefahr einer Konzentration von mehr als 50 Prozent der Hashrate einer Blockchain in einer Hand nicht nur theoretisch ist. Zwar dürften die wichtigsten Kryptowährungen zu hoch entwickelt sein, um Opfer einer solchen 51-Prozent-Attacke zu werden, aber bei neueren virtuellen Währungen war dies bereits der Fall. Dazu gehörten unlängst Verge, Monacoin oder auch Bitcoin Gold. Bei Letzterer gelang es einem Miner, die Kontrolle über die Blockchain zu übernehmen. Die hohen Kosten der Operationen zur Bündelung der erforderlichen Rechenleistung amortisierte er, indem er Bitcoins Gold entwendete, sie in andere Kryptowährungen umtauschte und die Transaktionen danach löschte, wodurch er die bereits umgetauschten Bitcoins Gold wieder zurückerhielt.⁵⁰

Zusätzlich zu dieser Gefährdung weisen die Technologien der Blockchain und der asymmetrischen Verschlüsselung, mehr als sich ihre Entwickler je vorstellen konnten, eine gewisse Anfälligkeit für Hackerangriffe auf. So können geschickte Hacker die Kontrolle über die Private Keys der Wallets von Dritten übernehmen, um dort nach Belieben Transaktionen vorzunehmen. Seit 2011 wurden mehrere Hackerangriffe auf Handels- und Speicherplattformen für Kryptowährungen gemeldet, bei denen oft Vermögenswerte im Gegenwert von mehreren Dutzend Millionen Dollar gestohlen wurden.⁵¹ Alleine im ersten Quartal 2018 erreichte die Summe der bei Hackerangriffen entwendeten Kryptowährungen einen Wert von umgerechnet 670 Millionen US-Dollar.⁵² Alle Kryptowährungen sind verwundbar und obwohl die meisten gemeldeten Fälle den Bitcoin betreffen, wurde der Rekord-Diebstahl im Januar 2018 bei einer anderen Kryptowährung erreicht: Damals gelang es Hackern, die in Japan ansässige Coincheck-Plattform um mehr als 500 Millionen XEM (die Kryptowährung des NEM-Netzes) zu erleichtern, was rund 530 Millionen US-Dollar entspricht.⁵³ Dieses Problem betrifft aber nicht nur Handels- und Speicherplattformen von virtuellen Währungen. Auch Wallets von einfachen Privatpersonen, die ohne einen E-Wallet-Anbieter verwaltet werden, können gehackt werden und die Verluste können hoch sein. Ein solcher Fall, von dem die Schweizer Behörden 2014 Kenntnis erhielten, kostete den Geschädigten fast 100'000 CHF.⁵⁴

Ebenso sind bestimmte Kryptowährungen wie etwa der Ether – nicht aber der Bitcoin – mit einer gewissen Anfälligkeit für das Abzweigen und nachfolgende Waschen von Geldern behaftet, weil sie die *Smart Contracts*-Technologie zulassen. Diese Technologie, die aus einer Weiterentwicklung der für den Bitcoin konzipierten Blockchain hervorgegangen ist und ursprünglich von Ethereum entwickelt wurde, beruht auf der Erarbeitung von Protokollen, die Vertragsbestimmungen automatisch ausführen. Massgebend sind dabei Computeralgorithmen, die festlegen, unter welchen Bedingungen welcher Entscheid getroffen werden muss. So können Verträge ausgeführt und Transaktionen auf der von ihnen erzeugten

⁴⁹ « Ils minaient des bitcoins dans un centre nucléaire », in *La Tribune de Genève*, 10. Februar 2018, <https://www.tdg.ch/faits-divers/lils-minaient-des-bitcoins-dans-un-centre-nucleaire/story/30448246>.

⁵⁰ « Bitcoin Gold : une attaque double dépense fait perdre plusieurs millions de dollars à des plateformes d'échanges », publiziert auf der Webseite von Crypto-France. <https://www.crypto-france.com/bitcoin-gold-attaque-double-depense-pertes-millions-dollars-plateformes-echange/>.

⁵¹ LOUBIRE Paul, « La très longue liste de vols de bitcoins par des hackers », in *Challenges*, 8. Dezember 2017, https://www.challenges.fr/finance-et-marche/la-tres-longue-liste-de-vols-de-bitcoins-par-des-hackers_518541.

⁵² « 670 millions de dollars de crypto-monnaies ont été dérobés au cours du premier trimestre 2018 », in *Crypto-France.com*, April 2018, <https://www.crypto-france.com/670-millions-dollars-crypto-monnaies-voles-premier-trimestre-2018/>.

⁵³ « Cryptomonnaie : la plateforme japonaise Coincheck victime d'un vol record », 29. Januar 2018, <http://www.rfi.fr/economie/20180129-coincheck-vol-cryptomonnaie-injonction-japon>.

⁵⁴ *Bericht des Bundesrates zu virtuellen Währungen in Beantwortung der Postulate Schwab (13.3687) und Weibel (13.4070) vom 25. Juni 2014*, <https://www.news.admin.ch/NSBSubscriber/message/attachments/35361.pdf>, cit., S. 22.

Blockchain überwacht werden, während gleichzeitig die mit dem menschlichen Handeln verbundenen Risiken der Willkür unterdrückt werden – weil der Grundsatz gilt, dass man nicht vom *Smart Contract*-Protokoll abweichen darf, das absolut rational und gerecht ist gegenüber allen und das somit zum Gesetz derjenigen wird, die diese Technologie nutzen («The code is the law»). Das Beispiel des DAO-Projekts zeigt allerdings, dass solche Protokolle, die als unfehlbar gelten, ebenfalls für gewisse Design-Fehler anfällig sind. Das DAO-Modell, mit dem die Utopie einer vollständig dezentralisierten und demokratischen Wirtschaft konkretisiert werden sollte, wurde 2016 auf der Ethereum-Blockchain gegründet. Es wurde vom Unternehmen DAI.LINK Sàrl von der Schweiz aus verwaltet und kann als eine Art dezentralisierter und automatisierter Anlagefonds definiert werden. Dabei konnten die Nutzer über Projekte abstimmen und eine Finanzierung gutheissen oder auch ablehnen, während die nachfolgenden Zahlungen dann automatisch über einen *Smart Contract* ausgeführt wurden. Aber aufgrund eines Programmierfehlers bei diesem *Smart Contract* konnte ein Nutzer die Vertragsbestimmungen für seine Zwecke nutzen, ohne den Vertrag selbst zu ändern. Auf diese Weise gelang es ihm, unter Einhaltung des Protokolls Token im Wert von insgesamt 53 Millionen US-Dollar abzuzweigen. Um diese Lücke zu beheben, mussten Nutzer gefunden werden, die damit einverstanden waren, die Blockchain zu ändern und alle Transaktionen zu löschen, die seit der missbräuchlichen Weiterleitung der Token vorgenommen worden waren. Obwohl dies den eigentlichen Grundsätzen der Blockchain widerspricht, wurde dieser Entscheidung von der Mehrheit der Nutzer unterstützt. Der Widerstand der Minderheit führte jedoch zu einem Hard Fork und damit zu einer Spaltung der Ethereum-Blockchain. *Smart Contracts* können also allen Vorsichtsmassnahmen ihrer Entwickler zum Trotz als Instrument zur Veruntreuung von Kryptowährungen dienen, die dann – wenn sie einmal abgezweigt sind – dank der Anonymität der Transaktionen auf der Blockchain gewaschen werden können. Das einzige Mittel dagegen bleibt bis heute eine Änderung der Blockchain selbst.

c. Gefährdungen in Verbindung mit dem Neuigkeitseffekt und der Unerfahrenheit der Nutzer

Die dritte Geldwäschereigefahr im Zusammenhang mit den Kryptowährungstechnologien ergibt sich aus der neuen Begeisterung für diese Art von Währung und der fehlenden Überwachung derjenigen, die sie nutzen und die mit den minimalen Vorsichtsmassnahmen, die es in diesem Bereich zu beachten gilt, oft wenig vertraut sind. Aufgrund ihrer relativen Neuartigkeit und ihrer vielfältigen Verwendungszwecke üben Kryptowährungen eine Anziehungskraft aus, die manchmal zu unüberlegtem Handeln verleitet und die Betrugsanfälligkeit erhöht. Der häufigste Risikofaktor ist Nachlässigkeit bei der Aufbewahrung der Private Keys, die Zugang zu den Wallets geben. Wenn diese Schlüssel nicht an ausreichend gesicherten Orten aufbewahrt werden, können sie einfach gestohlen und von Dritten verwendet werden, ohne dass diese dazu Hacking betreiben müssen. Aber abgesehen von diesem banalen Anfängerfehler gibt es auch raffiniertere Betrugsmethoden, die direkt mit der zunehmenden Verbreitung der Kryptowährungen verbunden sind und denen unerfahrene Nutzer zum Opfer fallen, die sich von der Neuartigkeit und den enormen Gewinnen, die sie sich von diesen virtuellen Währungen erhoffen, verleiten lassen.

Die Zahl der Kryptowährungen nimmt kontinuierlich zu und beläuft sich aktuell auf rund 2000, wobei etwa die Hälfte davon nicht mehr verwendet werden. Bei einigen von ihnen handelt es sich schlicht und einfach um Betrug. Dies betrifft meistens Kryptowährungen, die zwar auf der Blockchain-Technologie beruhen, aber nicht dezentralisiert sind. In solchen Fällen geben ihre Promotoren – eigentlich Betrüger – die Code-Basis nicht bekannt und schürfen vorgängig alle oder die meisten Token ab, deren Tauschwert sie dann selbst verwalten. Wenn solche Kryptowährungen von klar identifizierbaren und gut kontrollierten Institutionen verwaltet werden, können sie konkrete Vorteile im Kampf gegen die Finanzkriminalität bieten, weil die Promotoren die Identität ihrer Kunden leicht feststellen und gegebenenfalls die Finanzaufsichts- oder Strafverfolgungsbehörden darüber informieren können. Aber in vielen Fällen handelt es sich um Betrugereien, die zum sogenannten Ponzi- oder Schneeballsystem gehören, vor dem man sich eigentlich genau mit tatsächlich dezentralisierten Kryptowährungen schützen kann. Die MROS hat mehrere Verdachtsmeldungen im Zusammenhang mit Kryptowährungen erhalten, die offenbar in diese Betrugs-kategorie gehören. In allen Fällen liessen sich die Kunden von den fixen und hohen Erträ-

gen, die von den Promotoren versprochen wurden, blenden und kauften Token dieser Währungen. Danach wurden sie sofort dazu aufgefordert, in ihrem Freundeskreis neue Käufer zu werben. Es deutet aber alles darauf hin, dass in all diesen von der MROS erfassten Fällen die Erträge, die an die bestehenden Kunden ausbezahlt wurden, durch die Gelder von neuen Anlegern finanziert wurden, auch wenn die Pyramide bis anhin noch nicht eingestürzt ist. Dennoch haben die Behörden mehrerer Länder, darunter Deutschland, Italien oder auch Bulgarien, den Handel mit einer dieser Währungen aber bereits verboten. In der Schweiz hat die FINMA im September 2017 ebenfalls die rechtliche Liquidierung von Gesellschaften verfügt, die den E-Coin angeboten und verwaltet haben, der vermutlich auf einem derartigen kriminellen Muster beruht.⁵⁵

Ein ähnliches Betrugsrisiko für Anlegerinnen und Anleger könnte bei den ICOs vorhanden sein. Die jüngste Begeisterung für diese Art von Kapitalbeschaffung sowohl seitens der Anleger, die sich von den hohen Gewinnen, die die FinTech scheinbar prägen, blenden lassen, als auch der Start-ups, die Gelder für Projekte beschaffen wollen und von den herkömmlichen Anlageinstituten wohl nicht unterstützt würden, öffnet tatsächlich Tür und Tor für viele Betrugsmöglichkeiten. Ein häufiges und typisches Beispiel sind falsche ICOs, bei denen die angeblichen Entwickler eines Projekts Investitionsaufrufe lancieren, ohne wirklich mit der Entwicklung irgendeines Projekts begonnen zu haben. Die MROS hat kürzlich von einem solchen Fall erfahren.

Falsche ICO

Eine Online-Wechselstube meldete der MROS einen Fall, nachdem einer ihrer Kunden Opfer einer Abzockerei geworden war und sie darauf aufmerksam gemacht hatte. Der betreffende Kunde hatte in ein ICO-Projekt investiert, das von einer in einem anderen europäischen Land registrierten Gesellschaft organisiert wurde. Gegenstand dieses Projekts war die Entwicklung einer Wallet in einer physischen Form, ähnlich einer Debitkarte. Der Kunde, der in dieses scheinbar innovative Vorhaben investieren wollte, überwies dem Finanzintermediär eine Bitcoin-Summe. Diese sollte zunächst in Ether umgetauscht und dann der Wallet des Empfängers gutgeschrieben werden, die von einer Plattform nach ausländischem Recht gehostet wurde. Allerdings zeigte sich rasch, dass dieses ICO-Projekt ein Schwindel war. Die zuständigen Strafverfolgungsbehörden, denen dieser Fall übergeben wurde, weigerten sich jedoch, darauf einzutreten, und argumentierten, dass der zuständige Gerichtsstand nicht alleine aufgrund des Domizils des Finanzintermediär in der Schweiz liege.

Eine zweite Gefahr im Zusammenhang mit ICOs ergibt sich aus dem Rückzug der Promotoren aus einem Projekt, das deren Kapazitäten übersteigt. Die Promotoren könnten es vorziehen, Konkurs anzumelden, später neue Gesellschaften zu gründen und für deren Finanzierung erneut auf ICOs zurückzugreifen, statt an der Umsetzung des Projekts festzuhalten, für das sie die ursprüngliche ICO lanciert hatten.

Ein weiteres potenziell kriminelles Muster im Zusammenhang mit ICOs ist die Manipulation der Kurse von Token, die von ICO-Organisatoren herausgegeben werden. Ein solcher Verdacht betrifft die Zuger envion AG, die ein ICO zur Entwicklung von mobilen Mining-Farmen lancierte, dank denen der ökologische Fussabdruck des Minings vermindert werden sollte. Mehreren öffentlich zugänglichen Quellen zufolge soll der Direktor, der mit der Durchführung dieser ICO, die über 100 Millionen US-Dollar einbrachte, betraut war, illegal erzeugte Token herausgegeben und an Krypto-Börsen verkauft haben, um die Kontrolle über die Gesellschaft zu übernehmen. Aufgrund dieser Verdächtigungen brach der Kurs der ausgegebenen Tokens ein, so dass die Anleger riskieren, fast ihre gesamten Einlagen zu verlieren. Die FINMA hat ein Verfahren gegen die Emittenten dieser ICO eröffnet, das sich auf mögliche Verletzungen

⁵⁵ Medienmitteilung der FINMA vom 19. September 2017, <https://www.finma.ch/de/news/2017/09/20170919-mm-coin-anbieter/>

des Bankenrechts aufgrund einer allfällig unerlaubten Entgegennahme von Publikumseinlagen im Zusammenhang mit diesem ICO konzentriert.⁵⁶

Da bei vielen ICOs die Token, die die Anleger im Gegenzug für ihre Investitionen erhalten, nicht als Gesellschaftsanteile, sondern als vorrangige Nutzungsrechte gelten, könnten die angelegten Gelder bei einem Betrug unwiderruflich verloren sein, ausser für die Organisatoren der ICO. Da es bei den in letzter Zeit bekannt gewordenen ICOs oft um astronomische Summen geht, stellen derartige Betrügereien eine grosse Gefahr dar. Einigen Studien zufolge sind zwei Drittel der lancierten ICOs gescheitert oder stellten sich als Betrug heraus, wobei weltweit alleine in den ersten fünf Monaten des Jahres 2018 offenbar über 12 Milliarden US-Dollar durch ICOs beschafft worden sind.⁵⁷

d. Malware und Ransomware

Die Anonymität der Token und ihr elektronischer Träger machen sie zu einem privilegierten Instrument für Hacker, insbesondere im Zusammenhang mit Ransomware. Dafür gibt es im In- und Ausland zahlreiche Beispiele: Hacker attackieren Computer von Dritten, in der Regel Unternehmen, verschlüsseln die darauf befindlichen Dateien mit Schadsoftware und verlangen für deren Freigabe ein Lösegeld in Kryptowährung. Nach der Zahlung werden diese Lösegelder auf Wallets überwiesen, die in anderen Ländern registriert sind und von denen aus sie weitergeleitet oder umgetauscht werden können, wodurch eine strafrechtliche Verfolgung von solchen Erpressungen meist aussichtslos wird. Ein berühmtes Beispiel einer solchen Ransomware ist WannaCry, mit der im Mai 2017 die Daten von über 300'000 Computern in über 150 Ländern verschlüsselt werden konnten. Zur Entschlüsselung wurde ein Lösegeld in Bitcoins verlangt, das von einigen betroffenen Unternehmen auch bezahlt wurde. Die so erpressten Gelder wurden danach offenbar über Handelsplattformen in kleinen Tranchen in Monero umgetauscht – darunter auch von einer Plattform, die in Zug domiziliert ist. Da es sich bei dieser nicht um eine zentralisierte Handelsplattform handelt, die über einen Zugang zu den Wallets ihrer Nutzer verfügt, und auch nicht um eine dezentralisierte Plattform mit Verfügungsmacht, ist sie nicht dem GwG unterstellt. Deshalb hatte sie auch keine Überprüfungen vorgenommen, dank denen die kriminelle Herkunft der gewechselten Gelder hätte erkannt werden können. Die betreffende Plattform arbeitete aber bereits nach den ersten Hinweisen mit den Strafverfolgungsbehörden zusammen, um die Geldwäscherei zu blockieren.⁵⁸

e. Waschen von illegal erworbenen Krypto-Assets

Aufgrund ihrer intrinsischen Eigenschaften und vor allem der Anonymität, die sie bieten, können Kryptotechnologien auf vielerlei Arten zum Waschen von illegal erworbenen Token missbraucht werden. Allerdings ist darauf hinzuweisen, dass in gewissen Fällen nicht zweifelsfrei feststeht, ob der illegale Erwerb von Krypto-Assets mit einer Straftat und damit einer Vortat zur Geldwäscherei gleichzusetzen ist. Aufgrund der fehlenden Rechtsprechung zu dieser Frage ist nicht klar, ob 51-Prozent-Attacken oder das Abzweigen von Token über *Smart Contracts* selbst strafrechtlich relevant sind, da die Urheber dieser Aktionen in beiden Fällen nur die Möglichkeiten der Blockchain- und *Smart Contracts*-Technologien nutzen, die allen Nutzern zur Verfügung stehen. Hingegen stellen der Diebstahl oder die Erpressung

⁵⁶ FARINE Mathilde, «La FINMA enquête sur une ICO à 100 millions de francs», in *Le Temps*, 26. Juli 2018, <https://www.letemps.ch/economie/finma-enquete-une-ico-100-millions-francs>; FINMA, Medienmitteilung vom 26. Juli 2018, <https://www.finma.ch/de/news/2018/07/20180726-mm-envion/>

⁵⁷ FARINE Mathilde, «Comment investir dans les cryptomonnaies», in *Le Temps*, 22. Juli 2018, <https://www.letemps.ch/economie/investir-cryptomonnaies>; FAUCETTE James, GRASECK Betsy und SHAH Sheena, *Update : Bitcoin, Cryptocurrencies and Blockchain*, Morgan Stanley, 1. Juni 2018, S. 35, <https://www.macrobusiness.com.au/wp-content/uploads/2018/06/82012860.pdf>

⁵⁸ SUBERG William, «Bitcoin exchange ShapeShift helps police as WannaCry attacker converts to monero», in <https://cointelegraph.com/news/bitcoin-exchange-shapeshift-helps-police-as-wannacry-attacker-converts-to-monero>; EUROPOL, *2017 Virtual Currencies Money Laundering Typologies*, 2017, S. 11.

von Token ebenso wie ihr Erwerb durch Anlegerbetrug eindeutig Wirtschaftsverbrechen und Vortaten zur Geldwäscherei dar.

Die Geldwäschereihandlungen hängen von den IT-Fähigkeiten der Kriminellen ab. Das System der Peer-to-Peer-Validierung der Transaktionen bietet nämlich eine gewisse Gewähr für eine Eigenkontrolle. Wallets, auf denen abgezweigte Summen gutgeschrieben werden, können auf eine schwarze Liste gesetzt und die damit verbundenen Transaktionen von der Nutzergemeinschaft abgelehnt werden, so dass die gestohlenen Vermögenswerte oft nicht genutzt werden können. Damit eine Wallet aber auf die schwarze Liste kommt, müssen die Mitglieder der Nutzergemeinschaft die kriminelle Herkunft der darauf gutgeschriebenen Werte erst feststellen, was gemäss Auskunft der Polizei nur selten geschieht.

Zum Waschen von illegal erworbenen Krypto-Assets nutzen Kriminelle oft Darknets, wo Tokens von krimineller Herkunft auf dort gehosteten dezentralisierten Handelsplattformen zu manchmal unterbewerteten Preisen verkauft werden können. Diese Art der Geldwäscherei kam offenbar bei den XEM zum Einsatz, die von der Krypto-Börse Coincheck gestohlen wurden: Über 40 Prozent der entwendeten XEM konnten auf solchen Plattformen gegen Bitcoins umgetauscht und so rasch abgesetzt werden.⁵⁹ Mischdienste stellen ebenfalls ein besonders grosses Hindernis für die Identifizierung von illegal erworbenen Bitcoins dar, weshalb Kriminelle, die die unlautere Herkunft ihrer Kryptowährungen vertuschen wollen, sehr oft darauf zurückgreifen. Aber auch Umtauschen in andere Kryptowährungen, Abheben an Krypto-Geldautomaten oder Spielen in Online-Casinos sind Möglichkeiten, um illegal erworbene Krypto-Assets zu waschen.⁶⁰ Eine andere Technik der Geldwäsche besteht darin, bei anerkannten Anbietern von elektronischen Geldbörsen im Namen von sogenannten Money Mules, die mit falschen Dokumenten ausgestattet sind, Wallets zu eröffnen. Von dort aus werden die Vermögenswerte auf Bankkonten überwiesen, die auch auf den Namen von Money Mules eröffnet wurden, über die aber die Kriminellen dank falschen Dokumenten ebenfalls die Kontrolle haben.⁶¹

3.1.2. Gefahren einer betrügerischen Nutzung von Kryptowährungen

Kryptowährungen sind nicht nur aufgrund ihrer Technologie mit grossen Gefahren verbunden. Ebenso können sie für wirtschaftskriminelle Aktivitäten genutzt werden, die nicht spezifisch auf Kryptowährungen ausgerichtet sind, für die aber solche Währungen aufgrund ihrer Anonymität, der Schnelligkeit der Transaktionen und dem Fehlen von Finanzintermediären bei der Abwicklung von Transaktionen von besonderem Interesse sind.

a. Terrorismusfinanzierung mittels Kryptowährungen

Bis anhin wurden weltweit erst wenige Fälle von Terrorismusfinanzierung mittels Kryptowährungen gemeldet. Terrororganisationen und ihre Anhänger bevorzugen offenbar andere Arten der Finanzierung und andere Zahlungsmittel.⁶² Deshalb stufte das Vereinigte Königreich das tatsächliche Terrorismusfinanzierungsrisiko durch digitale Währungen als gering ein.⁶³ Das Ausmass der Gefährdung wird aber

⁵⁹ «Coincheck : les pirates servaient déjà parvenus à blanchir 40% des 500 millions de XEMs dérobés», <https://www.crypto-france.com/coincheck-pirates-blanchiment-xems/>.

⁶⁰ FANUSIE Yaya und ROBINSON, Tom, *Bitcoin laundering: an analysis of illicit flows into digital currency services*, Center on Sanctions & Illicit Finance et ELLIPTIC, 12. Januar 2018.

⁶¹ EUROPOL, *2017 Virtual Currencies Money Laundering Typologies*, 2017, S. 8.

⁶² European Parliament, *Virtual currencies and terrorist financing : assessing the risks and evaluating responses*, Mai 2018, [http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU\(2018\)604970_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf).

⁶³ HM Treasury et Home Office, *National risk assessment of money laundering and terrorist financing 2017*, London, 2017, S. 38,

durch zahlreiche Diskussionen über die Nutzung von Kryptowährungen deutlich, die internationale Anhängerinnen und Anhänger des Islamischen Staates (IS) auf sozialen Netzwerken führen, wo die Erfahrensten unter ihnen eigentliche Schulungen zur Verwendung von Krypto-Assets anbieten.⁶⁴ In diesem Kontext wurde auch zu Spenden in Kryptowährung zur Finanzierung des IS aufgerufen, was die besondere Gefahr des Token-Crowdfundings hinsichtlich der Terrorismusfinanzierung unterstreicht.⁶⁵ Offenbar nutzte eine salafistische palästinensische Terrororganisation diese Technik, um sich zu finanzieren.⁶⁶ Obwohl bis anhin keine Belege dafür erbracht werden konnten, behaupten mehrere Journalisten ebenso wie die Anti-Terror-Organisation Ghost Security Group, dass Bitcoin-Wallets zur Finanzierung der letzten Terroranschläge in Frankreich und Indonesien beigetragen haben und dass der Islamische Staat über mehrere solche Wallets verfügt, auf denen Vermögenswerte in der Höhe von mehreren Millionen US-Dollar gutgeschrieben sind.⁶⁷ Die Einfachheit und Anonymität von Kryptotransaktionen, mit denen Vermögenswerte rasch von einem Ort der Welt an einen anderen verschoben werden können, stellt somit eine grosse Gefährdung in Bezug auf eine Terrorismusfinanzierung dar, auch wenn dieses Risiko im Moment eher theoretisch als tatsächlich erwiesen ist. Eine ähnliche Gefährdung, die sich bis anhin aber noch nicht bestätigt hat, könnte von den ICOs ausgehen, deren Gewinne zur Terrorismusfinanzierung verwendet werden könnten. Organisationen der extremen Rechten, die oft misstrauisch sind gegenüber den herkömmlichen Finanzinstituten, die ihrer Überzeugung nach von Juden kontrolliert werden, greifen jedoch vor allem in den Vereinigten Staaten immer häufiger auf Kryptowährungen und insbesondere Kapitalbeschaffungen in Kryptowährungen zurück. So können sie herkömmliche Zahlungssysteme umgehen, von denen sie aufgrund ihrer Aktivitäten oft ausgeschlossen sind. Es gibt jedoch noch keine Belege dafür, dass solche Organisationen jemals Krypto-Assets zur Terrorismusfinanzierung eingesetzt hätten.⁶⁸

In der Schweiz wurde noch kein einziger Fall von Terrorismusfinanzierung mittels Kryptowährungen gemeldet. Die MROS hat jedoch von einer ausländischen Partnerstelle Informationen über solche Verdachtsfälle erhalten. Banktransaktionen von Fiatgeld aus verschiedenen europäischen Ländern, darunter auch der Schweiz, wurden einem Konto in dem Land gutgeschrieben, dessen FIU die MROS verständigt hatte. Nachdem das Geld auf dieses Konto überwiesen worden war, wurde es in Bitcoins umgetauscht und offenbar zur Finanzierung von terroristischen Aktivitäten verwendet. Da es keine gesetzliche Grundlage gibt, dank der aufgrund einer Anfrage einer ausländischen FIU bei Finanzintermediären Informationen eingefordert werden können, konnte die MROS in diesem Fall keine weitergehenden Abklärungen treffen. Aber alleine die Meldung eines solchen Verdachts zeigt die grosse Gefährdung, die Krypto-Assets hinsichtlich der Terrorismusfinanzierung darstellen. Sie ermöglichen potenziell einen raschen und anonymen Transfer von grossen Summen, die zur Finanzierung von Terrororganisationen bestimmt sind, können aber auch von einfachen Anhängern solcher Organisationen genutzt werden, die Terroranschläge verüben wollen. In dieser Hinsicht sind sie insofern besonders gefährlich, als sie zum illegalen Kauf des erforderlichen Materials im Darknet verwendet werden können.

b. Kryptowährungen als Zahlungsmittel für illegale Güter und Dienstleistungen

Digitale Plattformen, die illegale Güter und Dienstleistungen zum Kauf oder Verkauf anbieten und in Darknets zu finden sind, greifen mit Vorliebe auf Kryptowährungen zurück. Der Bitcoin war während

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/655198/National_risk_assessment_of_money_laundering_and_terrorist_financing_2017_pdf_web.pdf.

⁶⁴ BRANTLY Aaron, «Financing Terror Bit by Bit», in *CTC Sentinel*, vol. 7, no 10, Oktober 2014, S. 4, <https://ctc.usma.edu/financing-terror-bit-by-bit/>.

⁶⁵ WILE Rob, «Supporter of extremist group ISIS explains how bitcoin could be used to fund Jihad», in *Business Insider Australia*, 8. Juli 2014, <https://www.businessinsider.com.au/isis-supporter-outlines-how-to-support-terror-group-with-bitcoin-2014-7>.

⁶⁶ European Parliament, *Virtual currencies and terrorist financing...*, cit., S. 29.

⁶⁷ IRWIN Angela S.M. et MILAD, George, «The use of crypto-currencies in funding violent jihad», in *Journal of Money Laundering Control*, vol. 19, no 4, 2016, S. 410-411.

⁶⁸ European Parliament, *Virtual currencies and terrorist financing...*, cit., S. 30.

langer Zeit die am häufigsten verwendete Währung auf solchen Plattformen. Unterdessen steigt aber offenbar die Bedeutung des Moneros, der eine grössere Anonymität und eine Nicht-Rückverfolgbarkeit der Transaktionen gewährleistet. Krypto-Assets sind das wichtigste Zahlungsmittel in Darknets, wo sich Kriminelle mit verbotenem pornografischem und vor allem kinderpornografischem Material, Waffen, Nummern von gestohlenen Kreditkarten und insbesondere Drogen eindecken können. Letztere werden zunehmend über solche illegalen digitalen Plattformen gehandelt, obwohl Polizeiquellen zufolge ein überwiegend grosser Teil des Drogenhandels nach wie vor in Bargeld abgewickelt wird.⁶⁹

Transaktionen im Darknet lassen sich nur schwer nachverfolgen. Einerseits nutzen Netzwerke wie etwa TOR, die Zugang zum Darknet geben, verschiedene Server (*Nodes*) und damit auch immer wieder andere IP-Adressen, so dass es extrem schwierig wird, die tatsächliche IP-Adresse eines Nutzers zu identifizieren. Andererseits werden Transaktionen in Darknets über Mischdienste durchgeführt, die zwischen dem Verkäufer und dem Käufer der illegalen Güter oder Dienstleistungen stehen, was ein zusätzliches Hindernis für die Identifikation sowohl des einen als auch des anderen darstellt. Und schliesslich kann eine Wallet zwar auf die schwarze Liste gesetzt werden, weil sie Vermögenswerte erhalten hat, die aus illegalem Handel in Darknets stammen. Aber auf der Blockchain ist nicht ersichtlich, ob eine Transaktion im oder ausserhalb des Darknets erfolgt ist. Tatsächlich ist es heute so, dass ein Nutzer einen Fehler begehen und beispielsweise auf einer Drittseite im Internet seine verschlüsselte Adresse oder andere persönliche Daten veröffentlichen muss, damit die Anonymität der Transaktionen in den Darknets verloren geht. Durch geduldiges Abgleichen können die Strafverfolgungsbehörden in solchen Fällen verschiedene Kryptotransaktionen den Wallets eines bestimmten Nutzers und manchmal einer identifizierten Person zuordnen.⁷⁰

Zwar dienen Darknets nicht ausschliesslich kriminellen Aktivitäten, aber die Möglichkeit, dort unter dem Schutzmantel einer schwer durchdringbaren Anonymität Waffen, anderes Kriegsmaterial oder Anleitungen zur Herstellung von Sprengkörpern zu kaufen, verstärkt die von Krypto-Assets ausgehende Gefahr einer Terrorismusfinanzierung. Allerdings ist auch hier noch kein solcher Fall in der Schweiz nachgewiesen worden. Bezüglich der Geldwäscherei hingegen hängt das Risiko damit zusammen, dass Erträge aus illegalen Verkäufen in Kryptowährungen wieder in den legalen Kreislauf eingespeist werden. In der Schweiz wurden mehrere solche Fälle gemeldet. Meist nutzen die Verkäufer von illegalen Produkten im Darknet Online-Wechselstuben – manchmal solche, die in der Schweiz niedergelassen sind –, um ihre Kryptowährungen in Fiatgeld umzutauschen. Wenn es sich um einfache Gelegenheitsverkäufer handelt, geht es oft um geringfügige Summen. Aber die Beträge können auch beträchtlich sein, etwa, wenn Organisatoren eines Drogen- oder Waffenhandels oder Administratoren einer illegalen Online-Handelsplattform involviert sind, wie der nachfolgende Fall zeigt, den die MORS 2017 behandelt hat.

Waschen von Geld aus einem illegalen Online-Handel mittels Kryptowährungen

Eine Online-Wechselstube meldete der MROS einen Verdacht gegen einen ihrer Kunden. In der Presse wurde der betreffende Kunde namentlich genannt und berichtet, es handle sich um den Administrator einer illegalen Online-Handelsplattform, der dank der Zusammenarbeit der Bundespolizeien zweier nordamerikanischer Staaten und eines asiatischen Landes aufgespürt werden konnte. Der Mann, der seit mehreren Jahren in eben diesem asiatischen Land wohnhaft gewesen war und nun dort verhaftet wurde, hatte mit dem Verkauf von illegalen Produkten, vor allem Waffen und Drogen, auf der von ihm betriebenen Plattform in einem Darknet ein beträchtliches Vermögen gemacht. Um die in Bitcoins erzielten Gewinne zu waschen, hatte er die Online-Wechselstube genutzt, die schliesslich Meldung erstattete. Diese hatte ihm Fiatgeld für seine Bitcoins gegeben, das er vor allem

⁶⁹ Siehe auch HAEDERLI Alexandre und STÄUBLE Mario, «De la drogue livrée en courrier A. Comment fonctionne le marché des stupéfiants sur le Darknet», in *La Tribune de Genève*, 02.05.2018, https://www.tdg.ch/extern/interactive_wch/darknet/.

⁷⁰ AL JAWAHERI Husam, AL SABAH Mashaël, BOSHMAF Yazan et ERBAD Aiman, "When a small leak sinks a great ship: deanonymizing Tor hidden service users through bitcoin transactions analysis", in *arXiv*: 1801.07501v2, April 2018, <https://arxiv.org/abs/1801.07501>.

in Immobilien in mehreren Ländern und in Luxusprodukte investiert hatte. Aufgrund der in den Darknets verwendeten Mischdienste war es nicht mehr möglich, die Transaktionen zu analysieren und den kriminellen Ursprung der gewechselten Summen zu eruieren. Die ausländischen Behörden, die Strafverfahren gegen ihn eingeleitet hatten, konnten aber dank der Informationen aus der Analyse seiner Computer dennoch Vermögenswerte in der Höhe von mehreren Dutzend Millionen US-Dollar in Kryptowährung beschlagnahmen und einziehen.

Dieser Fall zeigt: Sogar wenn die Identität der Person, die den Umtausch von Kryptowährungen in Fiatgeld vorgenommen hat, bekannt ist und sogar wenn es sich bei der betreffenden Kryptowährung um den Bitcoin handelt, bei dem alle Transaktionen zurückverfolgt werden können, ist eine Identifizierung der kriminellen Herkunft der Vermögenswerte aufgrund der Anonymität rund um die Wallets fast unmöglich.

c. Der Rückgriff auf Kryptowährungen beim Phishing

Bei den zahlreichen Gaunereien, die in die Kategorie betrügerischer Missbrauch einer Datenverarbeitungsanlage gehören, sind immer öfter auch Krypto-Assets involviert. Zwar wird in der überwiegenden Mehrheit solcher Fälle noch immer mit Fiatgeld operiert, aber eine Prüfung der Verdachtsmeldungen an die MROS belegt, dass bei dieser Vortat zur Geldwäscherei zunehmend auf Kryptowährungen zurückgegriffen wird. Zwei Hauptvarianten dieser Art von Kriminalität zeigen, wie Token zum Waschen von betrügerisch erlangten Vermögenswerten verwendet werden. Bei der ersten Variante nutzen Kriminelle gehackte elektronische Zugangsdaten zu Bankkonten von Dritten, um von dort aus Fiatgeld auf Konten von Privatpersonen zu überweisen, die Kryptowährungen verkaufen möchten. Sobald Letztere die Summe in Fiatgeld erhalten haben, überweisen sie die so gekauften Kryptowährungen auf eine Wallet, die ihnen angegeben wurden. Allerdings gehört diese Wallet nicht den wirtschaftlich Berechtigten der Konten, von denen das Fiatgeld missbräuchlich abgebucht wurde. In der Regel können aber die wirtschaftlich Berechtigten der Wallet, der die Werte gutgeschrieben wurden, aufgrund der damit verbundenen Anonymität von den Strafverfolgungsbehörden nicht identifiziert werden, so dass die gegen sie eingeleiteten Strafverfahren eingestellt werden müssen. Bei der zweiten, raffinierteren Variante wird ein Money Mule eingesetzt, auf dessen Konto die aus gehackten Geschäftsbeziehungen abgezogenen Vermögenswerte überwiesen werden. Die Money Mules, die meist durch einen falschen Arbeitsvertrag oder mit anderen betrügerischen Vorwänden geködert werden, kaufen dann im Auftrag der Kriminellen Kryptowährungen und schreiben sie den Wallets gut, die ihnen angegeben werden. Bei beiden Varianten können durch die Verwendung von Kryptowährungen klassische kriminelle Muster perfektioniert werden: Die *Paper Trail* wird dank der Anonymität der Inhaber der Krypto-Wallets vernebelt, die in der Regel in anderen Ländern als der Schweiz registriert sind, was eine Strafverfolgung in solchen Fällen noch schwieriger macht als bei herkömmlichen Phishing-Fällen.

d. Investition von Geldern krimineller Herkunft in Krypto-Assets

Die Anonymität der Krypto-Assets und die Möglichkeiten zur Geldwäscherei, die sich durch Kryptotransaktionen und das Wechseln solcher Währungen bieten, machen sie bei Kriminellen, die ihre illegal erworbenen Gelder investieren und auf diese Weise waschen wollen, immer beliebter.⁷¹ Die zunehmende Häufigkeit, mit der Krypto-Assets zum Waschen von Geldern aus Internet-Betrügereien eingesetzt werden, veranschaulicht diesen Trend. Es können jedoch Erträge aus allen möglichen Vortaten zum Kauf von Krypto-Assets verwendet werden. Diesbezüglich sind die ICOs mit einem ähnlichen Risiko behaftet und es ist nicht ausgeschlossen, dass Gelder krimineller Herkunft darin investiert werden. Ein Hinweis dafür ist die hohe Zahl von Verdachtsmeldungen an die MROS durch Organisatoren von ICOs, die

⁷¹ EUROPOL, *2017 Virtual Currencies Money Laundering Typologies*, 2017, p. 12; FANUSIE Yaya et ROBINSON, Tom, *Bitcoin laundering: an analysis of illicit flows into digital currency services*, Center on Sanctions & Illicit Finance et ELLIPTIC, 12. Januar 2018, S. 5.

entdeckten, dass ihre Kunden zur Eröffnung der Geschäftsbeziehung gestohlene oder gefälschte Identitätspapiere verwendet hatten. Gegenwärtig scheint aber die Vortat, deren Gewinne am häufigsten durch den Kauf von Krypto-Assets gewaschen werden, der von kriminellen Organisationen kontrollierte Drogenhandel zu sein. Die in diesem Bereich aktiven kriminellen Netzwerke nutzen Kryptowährungen nicht nur zum Verkauf von Drogen in den Darknets, sondern immer häufiger auch, um ihre illegal erlangten Erträge aus Europa in die exportierenden Regionen zurückzuführen. Dabei zeigt sich, wie einfach rasche und umfangreiche grenzüberschreitende Transfers von Token dank diesen Systemen sind, wie ein kürzlich von Europol behandelter Fall belegt. Mitglieder eines kriminellen Netzwerks, die in Europa aus Kolumbien importiertes Kokain verkauften, hatten Money Mules angestellt und sie beauftragt, Bargeld aus dem Drogenhandel an Bitcoin-Geldautomaten umzutauschen. Diese Bitcoins sollten sie dann auf Wallets überweisen, die ebenfalls von Money Mules kontrolliert wurden, die ihrerseits für die Drogen-Exporteure in Kolumbien arbeiteten.⁷² Die amerikanischen Behörden stellen ebenfalls eine zunehmende Nutzung von Kryptowährungen durch kriminelle Organisationen fest, die im Drogengeschäft in den Vereinigten Staaten, Europa und Australien aktiv sind und die ihre Erträge aus diesem illegalen Handel in den Kauf von Bitcoins investieren.⁷³ In der Schweiz wurde zwar bis anhin noch kein solcher Fall aufgedeckt, aber es nicht ausgeschlossen, dass solche Fälle auftauchen werden. In diesem Zusammenhang könnte die zunehmende Verbreitung von Bitcoin-Geldautomaten insofern eine Gefährdung darstellen, als sie auch von Kriminellen, die in anderen Bereichen als im Drogenhandel aktiv sind, für ihre Zwecke genutzt werden könnten.

3.2. Die Verwundbarkeiten der Schweiz angesichts der Gefahr der Geldwäscherei und Terrorismusfinanzierung durch Kryptowährungen

Die bis hierhin dargelegten Aspekte belegen die grosse Gefahr, die Kryptowährungen im Bereich der Geldwäscherei und Terrorismusfinanzierung darstellen. Diese Gefährdung hat sich zwar noch nicht in einer hohen Zahl von nachgewiesenen Fällen niedergeschlagen, aber das bedeutet nicht, dass das Risiko gering ist. Die Verwundbarkeit des Finanzsystems gegenüber dieser Gefährdung ist nämlich erheblich und im Übrigen nicht spezifisch für die Schweiz. Nicht dazu zählt aber die rechtliche Qualifikation von Krypto-Assets: In der Schweiz werden Krypto-Assets von den Strafverfolgungsbehörden in der Regel als eine von mehreren Arten von Vermögenswerten behandelt, die zur Geldwäscherei beitragen können. Diese Sichtweise entspricht auch jener der FINMA, die mit der Aufsicht über die Finanzmärkte beauftragt ist.

3.2.1. Verwundbarkeiten von Finanzintermediären, die Kryptotransaktionen durchführen

Nach Auffassung der FINMA sind in der Schweiz alle Arten von Finanzintermediären, die Kryptotransaktionen durchführen, dem GwG unterstellt. Dies gilt für Online-Wechselstuben, die Kryptowährungen gegen Fiatgeld tauschen, zentralisierte Handelsplattformen für verschiedene Krypto-Assets – von denen jedoch keine in der Schweiz registriert ist –, Anbieter von *Custodian Wallets*, dezentralisierte Handelsplattformen für verschiedene Krypto-Assets, die in die Transaktionen ihrer Kunden eingreifen können, oder auch Gesellschaften, die ICOs lancieren und dabei Token ausgeben, die als Zahlungsmittel dienen können.

⁷² Koos Couvée, «European traffickers pay colombian cartels through bitcoin ATMs : Europol Official», in ACAMS Moneylaundering.com, 28. Februar 2018, <https://www.moneylaundering.com/news/european-traffickers-pay-colombian-cartels-through-bitcoin-atms-europol-official/>.

⁷³ U.S. Department of Justice and Drug Enforcement Administration, *2017 National Drug Threat Assessment*, Oktober 2017, S. 130; TZANETAKIS Meropi, «Comparing cryptomarkets for drugs: a characterisation of sellers and buyers over time», in *International Journal of Drug Policy*, vol. 56, Juni 2018, S. 176-186.

Allerdings können die Nutzer aufgrund des dezentralisierten Charakters der Technologie, die den meisten Kryptowährungen zugrunde liegt, Transaktionen oft auch ohne Finanzintermediäre durchführen, was eine erhebliche Verwundbarkeit im System zur Bekämpfung der Geldwäscherei darstellt. So entziehen sich die Anbieter von *Non-custodian Wallets* und die dezentralisierten Handelsplattformen für Kryptowährungen, die nicht in die von ihren Kunden angeordneten Transaktionen eingreifen können, der Reglementierung. Tatsächlich greifen Gesellschaften, die solche Dienstleistungen anbieten, in keinem Zeitpunkt in die von den Nutzern vorgenommenen Transaktionen ein und üben daher auch keine finanzintermediäre Tätigkeit aus. Dies gilt insbesondere für dezentralisierte Handelsplattformen für Kryptowährungen.⁷⁴ Das vorgenannte Beispiel, in dem eine solche Schweizer Gesellschaft Bitcoins, die mit der Ransomware *WannaCry* beschafft wurden, gegen Moneros umgetauscht hatte, ohne die Urheber der Transaktionen oder die kriminelle Herkunft der umgetauschten Tokens zu erkennen, verdeutlicht diese Verwundbarkeit. Folglich entzieht sich ein grosser Teil der Kryptotransaktionen⁷⁵ jeder Kontrolle.

Im Übrigen scheinen sich nicht alle Finanzintermediäre, die sich mit Kryptotransaktionen beschäftigen, gleichermassen bewusst zu sein, dass sie dem GwG und den damit verbundenen Sorgfaltspflichten unterstellt sind. Auch erfüllen sie diese Pflichten nicht immer auf angemessene Weise, kennen ihre Kunden nicht immer genau und sind trotz ihrer Bereitschaft zur Zusammenarbeit mit den Strafverfolgungsbehörden nicht in der Lage, Informationen zur Identität ihrer Kunden oder zur Herkunft der Token zu liefern, mit denen sie handeln. Die zunehmende Zahl der Verdachtsmeldungen von auf den Handel mit Kryptowährungen spezialisierten Gesellschaften, die bei der MROS eingehen, deuten jedoch auf ein wachsendes Bewusstsein dieser Finanzintermediäre für ihre Sorgfaltspflichten hin. Ebenso veröffentlichte die FINMA im Februar 2018 eine Wegleitung zu IOCs, in der definiert wird, unter welchen Bedingungen Gesellschaften, die auf diese Form der Kapitalbeschaffung in Kryptowährung zurückgreifen, als Finanzintermediäre gelten. Die MROS stellt fest, dass seit der Publikation dieser Wegleitung mehr Verdachtsmeldungen von solchen Gesellschaften eingegangen sind.

Aber selbst wenn sich alle Finanzintermediäre ihrer Sorgfaltspflichten bewusst wären, bliebe die Wirksamkeit dieser Vorsichtsmassnahmen zwangsläufig beschränkt, weil Kryptotransaktionen transnational sind und über Dienstleistungsgesellschaften laufen, die in sehr vielen Ländern registriert sind. Beispielsweise werden in der Schweiz registrierte Online-Wechselstuben oft von ausländischen *Custodian Wallet*-Anbietern, die im Auftrag ihrer Kunden handeln, mit dem Umtausch von Kryptowährungen beauftragt. In solchen Fällen hat die Schweizer Plattform keinen Zugang zu den KYC-Daten des Kunden der ausländischen Plattform, für die sie diesen Umtausch vornimmt, und kennt somit die Identität des Kunden nicht. Ebenso und aufgrund der Anonymität der Kryptotransaktionen haben die Finanzintermediäre, die solche Transaktionen im Auftrag ihrer Kunden durchführen, keine Möglichkeit zu prüfen, ob die Wallets, aus denen die von ihnen gehandelten Werte stammen oder auf die sie Überweisungen vornehmen, tatsächlich den Personen gehören, die von ihren Kunden angegeben wurden. Um diese Verwundbarkeit zu vermindern, konzentrieren sich gewisse Finanzintermediäre auf die Vermögensverwaltung ihrer Kunden und verzichten auf Tätigkeiten im Zusammenhang mit dem Zahlungsverkehr zugunsten von Dritten. Ausserdem akzeptieren sie anonyme Kryptowährungen nur nach äusserst genauen Abklärungen und nur für Kunden, die sie gut kennen.

Solche Bemühungen sind besonders wertvoll, denn im Grunde sind die einzigen Kryptotransaktionen, die eine Identifizierung der wirtschaftlich Berechtigten der involvierten Werte ermöglichen, ihr Kauf oder Verkauf gegen Fiatgeld. Online-Wechselstuben, die solche Transaktionen durchführen, sind sich ihrer Sorgfaltspflichten bewusst, kommen ihnen nach und liefern bei Bedarf die ihnen zur Verfügung stehenden Informationen an die Strafverfolgungsbehörden, ebenso wie dies alle herkömmlichen Finanzintermediäre tun. Nach Ansicht der zuständigen Polizei- und Justizbehörden sind solche Online-Wechselstuben die einzigen an Kryptotransaktionen beteiligten Finanzintermediäre, die ihnen genaue Angaben zur Identität der wirtschaftlich Berechtigten der betreffenden Werte liefern können. Dies schützt sie aber

⁷⁴ Vgl. unten Ziffer 4.1.4.

⁷⁵ "76% of incorporated wallet providers do not have a license", HILEMAN Garrick et RAUCHS Michel, *Global Cryptocurrency Benchmarking Study*, Cambridge, Center for Alternative Finance/University of Cambridge, 2017, S.62.

nicht umfassend vor Betrug. Sie haben nämlich keinerlei Möglichkeit, die Identität der wirtschaftlich Berechtigten von Wallets zu überprüfen, denen sie im Auftrag ihrer Kunden Beträge gutschreiben. Wenn ein Kunde seine Token gegen Fiatgeld verkaufen will, stehen dem Finanzintermediär zudem nur wenige Mittel zur Verfügung, um eine allfällige kriminelle Herkunft dieser Token nachzuweisen. Bei Kryptowährungen wie dem Bitcoin, bei denen alle Transaktionen zurückverfolgt werden können, kann er anhand einer Kettenanalyse (*chain analysis*) zwar überprüfen, ob die Wallet des Kunden tatsächlich die Bitcoins enthält, die dieser verkaufen will, und möglicherweise erkennen, ob die betreffenden Vermögenswerte über einen Mischdienst gelaufen sind oder – was seltener ist – über eine geblockte Wallet. Hingegen kann er nicht herausfinden, ob es der Kunde selbst ist, der diesen Mischdienst oder die geblockte Wallet genutzt hat, oder ob er die betreffenden Token erst nach diesen verdächtigen Etappen auf legale Weise erworben hat.

Ausserdem bieten die Verfahren der Online-Wechselstuben zur Kontoeröffnung oft einen gewissen Handlungsspielraum für Kriminelle, die mithilfe von Token widerrechtlich erlangte Gelder waschen wollen. Die MROS kennt Fälle, in denen solche Schweizer Finanzintermediäre eine Verdachtsmeldung auf Geldwäscherei einreichten, weil Geschäftsbeziehungen mithilfe von gestohlenen Identitätsdokumenten eröffnet worden waren. Da das Verfahren zur Kontoeröffnung häufig über Internet erfolgt, konnte ein solcher Identitätsdiebstahl zuvor nicht entdeckt werden. Eine ähnliche Verwundbarkeit betrifft auch Gesellschaften, die ICOs anbieten und die als Finanzintermediäre gelten. Alle bisherigen Meldungen von solchen Gesellschaften an die MROS gründeten auf dem Verdacht, dass bei der Eröffnung der Geschäftsbeziehungen gefälschte Dokumente im Spiel waren. So meldete eine Gesellschaft, die ein ICO durchführte, der MROS über 100 Geschäftsbeziehungen mit investitionswilligen Anlegern, die gefälschte Identitätspapiere vorgelegt hatten. Dies bestärkte den Verdacht, dass die in das ICO investierten Summen krimineller Herkunft sein könnten.

Überdies müssen die am Handel mit Krypto-Assets beteiligten Online-Wechselstuben genau wie herkömmliche Wechselstuben ihre Sorgfaltspflichten bei Geldwechselgeschäften erst ab einem Betrag von 5000 Franken auf ihre Kunden anwenden (Art. 51 Abs. 1 Bst. 1 GwV-FINMA, SR 955.033.0). Dies lässt Spielraum für zahlreiche, völlig anonyme Wechselvorgänge unterhalb dieses Schwellenwertes. Die zunehmende Verbreitung von Krypto-Geldautomaten verschärft diese Verwundbarkeit noch, wie mehrere bei der MROS eingegangene Verdachtsmeldungen bestätigen.

Aufteilung der Summen bei Kryptowährungskäufen

Eine Plattform für Zahlungsdienstleistungen, die Zahlungen in Krypto-Assets akzeptiert, richtete eine Verdachtsmeldung an die MROS und gab an, ein und derselben Wallet seien Bitcoin-Summen gutschrieben worden, die innert kurzer Zeit durch elf Bezüge an Automaten gekauft worden waren, wobei jedes Mal der erlaubte Höchstbetrag bezogen worden war. Die meldende Plattform kannte den wirtschaftlich Berechtigten der kreditierten Wallet nicht – was darauf hindeutet, dass sich Finanzintermediäre, die Kryptotransaktionen ohne Wechsel in Fiatgeld durchführen, ihrer Due-Diligence-Pflichten oft nicht bewusst sind. Zur Identifikation der Person(en), die diese Wechselgeschäfte durchgeführt hat oder haben, standen der MROS einzig die Schweizer Mobiltelefonnummern zur Verfügung. Mobilnetzbetreiber, die solche Telefonnummern herausgeben, sind zwar durch das Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF, SR 780.1) gesetzlich zur Identifikation ihrer Kunden verpflichtet. In diesem Fall waren sie ihrer Pflicht aber nicht nachgekommen und die Telefonnummern waren unter Fantasienamen wie etwa Donald Duck registriert. Da im BÜPF keine strafrechtlichen Sanktionen für solche Versäumnisse der Mobilnetzbetreiber vorgesehen sind, konnten sie nicht geahndet werden. Die MROS hatte also keine Möglichkeit, die Inhaber dieser Telefone ausfindig zu machen. Da ihr ausserdem auch Informationen zur Herkunft der Vermögenswerte fehlten, die gegen Bitcoins gewechselt worden waren, musste sie die Untersuchungen einstellen. In diesem Fall hatte der Finanzintermediär die verdächtigen Transaktionen sehr wohl erkannt und sie der MROS auch ordnungsgemäss gemeldet. Weil aber die Mittel zur Identifikation des Inhabers der Wallet fehlten, der die Beträge gutschrieben wurden, konnten die Untersuchungen nicht

weitergeführt werden. Die am 1. Januar 2018 in Kraft getretene Änderung des BÜPF, die für solche Verstösse gegen die Pflicht zur Identifikation der Kunden seitens der Mobilnetzbetreiber strafrechtliche Sanktionen vorsieht, sollte die in diesem Fall noch mögliche totale Anonymität der Transaktionen aufheben. Sie kann aber nicht verhindern, dass ein Mobiltelefon von jemand anderem als dem rechtmässigen Inhaber, beispielsweise von einem Dieb, für kriminelle Zwecke verwendet wird.

Finanzintermediäre, die sich mit Transaktionen von Krypto-Assets beschäftigen, sind somit sehr verwundbar gegenüber der Gefährdung der Geldwäscherei und Terrorismusfinanzierung. Im Übrigen wird die Verwundbarkeit des Finanzplatzes Schweiz durch die begrenzte Zahl solcher Finanzintermediäre noch verstärkt, was aber auch für andere Länder gilt. Die Tatsache, dass es nur wenige Gesellschaften gibt, die im Bereich der Finanzintermediation für Kryptowährungen aktiv sind, impliziert nämlich, dass unzählige Transaktionen direkt zwischen den Nutzern ablaufen. Dabei greifen sie auf Plattformen zurück, die nur Programme zur Verfügung stellen, die die Nutzer ohne ihre Intervention verwenden können, und die daher nicht als Finanzintermediäre gelten. Mit wenigen Ausnahmen wie etwa den Vereinigten Staaten, Japan und seit kurzem auch Malaysia sind zudem die Anbieter von *Custodian Wallets* in den meisten Ländern noch nicht der Geldwäschereigesetzgebung unterstellt. Dies macht es Schweizer Nutzern einfach, für Krypto-Geschäfte und potenziell auch zur Geldwäscherei die Dienste von Finanzintermediären in Anspruch zu nehmen, die in anderen Ländern registriert sind, in denen die Geldwäscherei-Gesetze für sie nicht gelten oder kaum angewendet werden. In dieser Hinsicht ist die Tatsache, dass die herkömmlichen Grenzen der Strafgerichtsbarkeit im Internet verwischt sind, eines der wichtigsten Elemente, das die Repression der Token-Finanzkriminalität behindert.

3.2.2. Die schwierige Repression von Geldwäscherei und Terrorismusfinanzierung durch Kryptowährungen

Die mit der Repression von Cyberkriminalität und insbesondere von Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets beauftragten Polizei- und Justizbehörden sehen sich mit zahlreichen Hindernissen konfrontiert, wobei diese nicht spezifisch mit dem Finanzplatz Schweiz zusammenhängen, sondern für alle Länder gelten. Aufgrund der Anonymität rund um Token-Transaktionen ist es extrem schwierig, verdächtige Transaktionen und die wirtschaftlich Berechtigten der involvierten Wallets zu identifizieren. In dieser Hinsicht bietet die Kettenanalyse nur eine sehr beschränkte Hilfe. Zum einen ist eine solche Analyse nur bei Kryptowährungen möglich, bei denen die Rückverfolgbarkeit der Transaktionen auf ihrer Blockchain vorgesehen ist, und kann bei völlig anonymen Token wie etwa Monero oder Verge gar nicht durchgeführt werden. Zum andern wird die *Paper Trail* durch einen dazwischen geschalteten Mischdienst endgültig unterbrochen, und dies auch bei verfolgbaren Kryptowährungen wie dem Bitcoin. Und selbst wenn die betreffenden Vermögenswerte durch eine Kettenanalyse nachverfolgt werden können, ist das Problem nicht gelöst: Diese Analyse sagt nämlich nichts aus über die wirtschaftlich Berechtigten der in die Transaktionen verwickelten Wallets, über die allenfalls kriminelle Natur einer Transaktion im Zusammenhang mit einer Geldwäschereihandlung oder über die IP-Adressen der Computer, die für diese Transaktionen verwendet wurden. Mit gewissen Kettenanalyse-Programmen können die zwischen verschiedenen Wallets durchgeführten Transaktionen allerdings relativ genau abgeglichen werden, wodurch sich mit einer sehr hohen Wahrscheinlichkeit feststellen lässt, ob ihr wirtschaftlich Berechtigter immer derselbe ist. Ausserdem können diese Programme auch anzeigen, wenn eine der Wallets, die für die Transaktionen verwendet wurden, aus irgendeinem Grund auf die schwarze Liste gesetzt wurde, etwa weil jemand Vermögenswerte aus dem Verkauf von illegalen Gütern oder Dienstleistungen im Darknet darauf überwiesen hat.

Fehlt jedoch eine solche Anzeige, dann gibt es in einer Kettenanalyse keinen Unterschied zwischen einer illegalen oder im Darknet durchgeführten Transaktion und einer legalen Transaktion. Um eine Transaktion identifizieren zu können, die zum Waschen von Geldern aus Verkäufen im Darknet gedient haben könnte, sind die Polizeibehörden zudem meist gezwungen, diese illegalen Märkte zu infiltrieren,

dort die Pseudonyme der Kriminellen ausfindig zu machen und zu hoffen, dass diese einen Fehler begehen, dank dem ihre Anonymität durchbrochen werden kann. Ein solcher Fehler wäre beispielsweise, wenn sie auf einer öffentlichen Webseite Informationen preisgeben, die sich abgleichen lassen, so dass ihre Identität und ihre Kontrolle über eine bestimmte Wallet ermittelt werden kann. Das Erkennen von betrügerischen Token-Transaktionen, die nicht aus einem Darknet stammen, ist noch schwieriger, weil die Strafverfolgungsbehörden in diesem Fall nicht *a priori* wissen, auf welchen Bereich sie ihre Recherchen konzentrieren sollen. Die MROS erhält Meldungen von Finanzintermediären, die jedoch bei der Analyse der Transaktionen auf die gleichen Schwierigkeiten stossen wie die Strafverfolgungsbehörden. Sie erstatten denn auch in den meisten Fällen Meldung, weil einer ihrer Kunden Opfer eines Betrugs geworden ist und deshalb Strafanzeige oder Beschwerde eingereicht hat oder weil bei der Eröffnung der Geschäftsbeziehungen gestohlene oder gefälschte Identitätspapiere verwendet worden sind.

Sobald eine verdächtige Transaktion als erkannt wurde, ist der wirtschaftlich Berechtigte der damit verbundenen Werte zu identifizieren. Diese Identifikation ist laut den konsultierten Justizbehörden durch Informationen möglich, die von den Finanzintermediären geliefert werden. Es kann aber sein, dass eine zweifelhafte Transaktion ohne Finanzintermediär ausgeführt wurde oder, falls ein Finanzintermediär involviert war, dieser über keine Informationen darüber verfügte. Schliesslich werden verdächtige Transaktionen oft vor allem von Handelsplattformen für Krypto-Assets ausgeführt, die nicht in der Schweiz registriert sind. In solchen Situationen bleibt den Strafverfolgungsbehörden nur die Hoffnung, dass der mutmassliche Kriminelle einen Fehler begeht, dank dem der Schleier seiner Anonymität gelüftet werden kann, oder dass sich der Informationsaustausch der Polizei und Justiz mit ihren ausländischen Partnerstellen als produktiv erweist. Die internationale Rechtshilfe ist zwar zweifellos eines der wirksamsten Instrumente zur Repression der Kriminalität im Zusammenhang mit Kryptowährungen, aber sie wird oft durch die Schnelligkeit der grenzüberschreitenden Transaktionen ausser Gefecht gesetzt. Hinzu kommt, dass auch bei einer Identifikation der Wallets mit Guthaben von verdächtiger Herkunft und ihrer wirtschaftlich Berechtigten eine Beschlagnahme der darauf deponierten Vermögenswerte nur dann möglich ist, wenn die Strafverfolgungsbehörden über die Private Keys zu diesen Wallets verfügen. Mit ein wenig Glück besitzt ein kooperationsbereiter Anbieter einer *Custodian Wallet* diesen Schlüssel und übergibt ihn der Justiz. Aus der Sicht der helvetischen Behörden muss dieser Anbieter aber in der Schweiz registriert sein, was nur sehr selten der Fall ist. Ebenso kann ein Krimineller, gegen den bereits ein Strafverfahren eingeleitet wurde, den Private Key seiner Wallet preisgeben und damit den Weg freimachen für die Beschlagnahme und Einziehung der darauf deponierten Vermögenswerte. Wenn aber keiner dieser Fälle eintritt, ist der Erlös aus der Geldwäscherei mittels Kryptowährungen für die Strafverfolgungsbehörden zumindest beim heutigen Stand der Technologie unwiderruflich verloren.

In den meisten Fällen gelingt es den Polizei- und Justizbehörden ausserdem nicht, die Anonymität der Kryptotransaktionen und der Wallets, auf denen diese virtuellen Gelder deponiert sind, zu durchbrechen. Ebenso lässt sich nicht einfach feststellen, ob die Lancierung einer neuen Kryptowährung oder einer ICO einfach auf einem Scam beruht. Es kann zwar entsprechende Verdachtsmomente geben, aber oft lässt sich nichts beweisen. Schliesslich führen auch die unklaren Grenzen der strafgerichtlichen Zuständigkeiten im Internet zu erheblichen Problemen bezüglich des Gerichtsstands, die zur Trägheit des internationalen Rechtshilfeprozesses hinzukommen. Daraus ergeben sich zahlreiche Hindernisse für die Verfolgung von Geldwäscherei und Terrorismusfinanzierung mittels Kryptowährungen, die erklären, weshalb in vielen Verdachtsfällen auf Geldwäscherei durch Kryptowährungen, die von der MROS an eine Staatsanwaltschaft weitergeleitet wurden, eine Nichtanhandnahmeverfügung erlassen wurde. Als häufigster Grund dafür wurde genannt, dass es nach Abschluss der Voruntersuchungen nicht möglich war, die wirtschaftlich Berechtigten der Wallets, die Kryptowährungen mit verdächtiger Herkunft enthalten, zu identifizieren.

3.3. Bilanz der Risikoanalyse

Die Zahl der Verdachtsfälle auf Geldwäscherei durch Kryptowährungen, die den Schweizer Behörden gemeldet wurden, hat zwar zugenommen, ist aber immer noch so klein, dass eine Evaluation des damit

verbundenen Risikos schwierig ist. Die wenigen Fälle könnten ein reales, aber letztlich geringes Risiko widerspiegeln, das sich aus einer zwar expandierenden, aber immer noch neuen Technologie ergibt, die nur sehr selten zu kriminellen Zwecken der Geldwäscherei oder Terrorismusfinanzierung genutzt wird. Ebenso könnte die geringe Zahl der Meldungen aber auch auf Schwachstellen bei der Abklärung eines Verdachts und der Identifizierung der Fälle von Geldwäscherei und Terrorismusfinanzierung durch Token zurückzuführen sein. Wie dem auch sei: Die grosse Gefährdung, die von Kryptowährungen ausgeht, hat sich bestätigt und die Verwundbarkeiten der Schweiz in diesem Bereich sind erheblich, auch wenn sie alle Länder betreffen. Diesbezüglich ist darauf hinzuweisen, dass die unklaren Grenzen der strafgerichtlichen Zuständigkeiten im Internet ein besonders hohes Risiko darstellen, ohne dass man sagen könnte, dass dies ein spezifisch schweizerisches Phänomen ist. Ein Nutzer, der anonym bleiben will, um beispielsweise Transaktionen in Zusammenhang mit einem kriminellen Muster durchzuführen, kann problemlos auf Dienstleister im Krypto-Geschäft zurückgreifen, die in einem Land registriert sind, in dem sie nicht der Geldwäschereigesetzgebung unterstellt sind oder diese nicht wirksam angewendet wird, auch wenn er selbst von einem Land aus tätig ist, in dem sehr strenge Regelungen zur Geldwäschereibekämpfung gelten.

4. Risikomindernde Faktoren

Die Gefährdung durch Kryptowährungen ist zwar gross und die Verwundbarkeiten sind erheblich, aber es gibt mehrere risikomindernde Faktoren. Einige davon wurden bereits erwähnt und hängen mit den Technologien zusammen, die den Kryptowährungen zugrunde liegen. Bei Diebstählen oder der betrügerischen Abzweigung von Token können die Nutzer die Wallets, auf die diese Werte überwiesen werden, identifizieren und auf eine schwarze Liste setzen, womit jede Geldwäscherei unterbunden wird. Ebenso können Anfängerfehler, die von ehrlichen Nutzern begangen werden, auch Kriminellen unterlaufen. Nach Ansicht der zuständigen Strafverfolgungsbehörden lässt sich die Verwendung von Kryptowährungen für die Geldwäscherei daher am besten unterbinden, wenn die Urheber solcher Verbrechen Fehler begehen, dank denen sie identifiziert und wenn möglich ausser Gefecht gesetzt werden können. Neben diesen Faktoren, die zur Verminderung der technologiebedingten Risiken beitragen, bemühen sich die Schweizer Behörden aber auch um die Entwicklung von möglichst effizienten Instrumenten, mit denen das Geldwäscherei- und Terrorismusfinanzierungsrisiko im Zusammenhang mit Kryptowährungen eingedämmt werden kann. Dazu zählt vor allem und trotz der Grenzen, die einer nationalen Regelung dieser transnationalen Problematik gesetzt sind, die in der Schweiz besonders weitreichende Unterstellung der im Kryptogeschäft tätigen Finanzintermediäre unter das GwG, obwohl sich dadurch nicht verhindern lässt, dass Kryptotransaktionen mehrheitlich über Dienste laufen, die nicht zur Finanzintermediation zählen. Beispiele dafür sind etwa Anbieter von *Non-Custody-Wallets* oder dezentralisierte Handelsplattformen, die nicht dem GwG unterstellt oder im Ausland registriert sind.

4.1. Aufsichtsrechtliche Einordnung der Krypto-Anwendungsfälle

4.1.1. Initial Coin Offerings

Werden im Rahmen eines ICOs⁷⁶ Token ausgegeben, die tatsächlich oder der Absicht des Organisers nach als Zahlungsmittel für den Erwerb von Waren oder Dienstleistungen akzeptiert werden und/oder der Geld- und Wertübertragung dienen sollen, stellt dies aus geldwäschereirechtlicher Sicht eine unterstellungspflichtige Ausgabe von Zahlungsmitteln gemäss Art. 2 Abs. 3 lit. b GwG i.V.m. Art. 4 Abs. 1 lit. b GwV dar.

Aus dem GwG ergeben sich verschiedene Sorgfaltspflichten und die Pflicht, sich entweder einer SRO anzuschliessen oder direkt der FINMA für die GwG-Aufsicht zu unterstellen. Gemäss Praxis der FINMA

⁷⁶ Die FINMA hat ihre Praxis zur aufsichtsrechtlichen Einordnung von ICOs mit der [Wegleitung für Unterstellungsanfragen betreffend Initial Coin Offerings \(ICO\) vom 16. Februar 2018](#) bekanntgegeben.

gilt diese Pflicht als eingehalten, wenn die Entgegennahme der Mittel durch einen in der Schweiz dem GwG unterstellten Finanzintermediär erfolgt und dieser die Sorgfaltspflichten einhält.

Die Identifizierungspflicht der Vertragspartei gemäss Art. 3 GwG stellt einen elementaren Grundsatz der Geldwäschereiprävention dar. Grundsätzlich gilt die Identifizierungspflicht ab CHF 0. Die GwV-FINMA, die VSB 16 sowie SRO-Reglemente sehen jedoch für bestimmte Geschäfte und bis zu bestimmten Betragsschwellen risikoorientiert den gänzlichen Verzicht oder eine erleichterte Identifizierung vor. Für die Herausgabe von Zahlungsmittel im Rahmen eines ICOs sieht die FINMA die Möglichkeit für eine erleichterte Identifizierung bei einem Investitionsbetrag von CHF 0 bis CHF 3'000 (einfache Kopie des Ausweises) vor.⁷⁷ Erst ab CHF 3'000 ist eine vollständige Identifizierung vorzunehmen. Eine solche Erleichterung rechtfertigt sich aufgrund der einem ICO inhärenten Risiken. Bei einem ICO besteht das grösste Risiko darin, dass es sich um einen Scam handelt oder der ICO-Organisator die Gelder zur Terrorismusfinanzierung verwendet.⁷⁸ Ein weiteres Risiko ist die Möglichkeit, dass Gelder aus krimineller Herkunft in ein ICO investiert werden können.⁷⁹ Mit der Unterstellung von ICOs, bei denen Zahlungs-Token ausgegeben werden, wird das GwG-Risiko adäquat adressiert.

Generell kann festgestellt werden, dass ICOs traditionellen Finanzierungsrunden resp. Private Placements von juristischen Personen sehr ähnlich sind. Da die Tokeninhaber i.d.R. jedoch weder Aktionäre noch Gläubiger der Gesellschaft werden, können bei der Emission einerseits aufwendige und kostspielige Dokumentationen (wie z.B. die Prospektpflicht) und andererseits Transparenzvorschriften zu juristischen Personen umgangen werden.

4.1.2. Wallet-Anbieter

Ein Wallet-Anbieter, den Private Key des Kunden verwahrt (sog. Custody Wallet-Anbieter), ermöglicht das Senden und Empfangen von Kryptowährungen und erbringt damit eine unterstellungspflichtige Dienstleistung für den Zahlungsverkehr im Sinne des GwG (Art. 2 Abs. 3 lit. b GwG i.V.m. Art. 4 Abs. 1 lit. a GwV). Die Funktion und Risikosituation sind ähnlich wie beim Money Transmitter. Insbesondere können Kryptowährungen dazu dienen, rasch und unkompliziert Vermögenswerte rund um den Globus zu schicken. Es besteht das Risiko, dass damit Sanktionen umgangen und Terroristen finanziert werden.

Entsprechende Wallet-Anbieter müssen sich entweder einer SRO anschliessen oder direkt der FINMA für die GwG-Aufsicht zu unterstellen. Da Wallet-Anbieter die Transaktionen geografisch nicht einschränken können, gilt gemäss Praxis der FINMA, wie bei Auslandüberweisungen durch Money Transmitter grundsätzlich eine Identifizierungspflicht ab CHF 0. Aufgrund der Analogie zu den New Payment Methods ist auch bei Wallet-Anbieter eine erleichterte Identifizierung (einfache Kopie des Ausweises) zulässig, wenn der Wallet-Anbieter das Transaktionsvolumen auf CHF 500 pro Monate und CHF 3'000 pro Kalenderjahr begrenzt.

Mit der Unterstellung der Custody Wallet-Anbieter wird den GwG-Risiken nur teilweise Rechnung getragen.⁸⁰ Der grosse Teil der Wallet-Anbieter kontrollieren keine Private Keys der Kunden (Non-Custody Wallet-Anbieter, vgl. Ziff. 2.2. oben). Unter der geltenden Rechtslage wäre eine Unterstellung höchstens mit einer extensiven Auslegung von Art. 4 Abs. 1 lit. a GwV möglich, wonach eine Dienstleistung für den Zahlungsverkehr vorliegt, wenn der Finanzintermediär die Überweisung der liquiden Finanzwerte im Namen und Auftrag der Vertragspartei "anordnet". Die FINMA hat eine entsprechende Auslegung geprüft und ist zum Schluss gekommen, dass dies mit der Systematik des GwG bzw. der Konzeption des

⁷⁷ In sinngemässer Anwendung von Art. 12 Abs. 2 lit. d GwV-FINMA.

⁷⁸ Vgl. oben Ziffer 3.1.1.c.

⁷⁹ Vgl. oben Ziffer 3.2.1.

⁸⁰ Vgl. MROS-Fall unter Ziff. 3.2.1, der mangels Identifizierungspflicht des Wallet-Anbieters nicht weiterverfolgt werden konnte.

Begriffs der Finanzintermediation, der auf die Verfügungsmacht über fremde Vermögenswerte abstellt, nicht vereinbar ist.

4.1.3. Wechselstuben und zentralisierte Handelsplattformen

Beim Wechselgeschäft bieten die Wechsler den Kauf und Verkauf von Kryptowährungen direkt aus dem Eigenbestand an. Wechselgeschäfte mit Kryptowährungen qualifizieren als finanzintermediäre Tätigkeit im Sinne des GwG (vgl. Art. 2 Abs. 3 lit. c GwG i.V.m. Art. 5 Abs. 1 lit. a GwV).

Das GwG-Risiko bei Wechslern im Kryptobereich ist ähnlich wie beim herkömmlichen Wechselgeschäft, d.h. geringer als im Zahlungsverkehr, da die Vermögenswerte beim Kunden nur ausgetauscht und nicht an Dritte übertragen werden. Vor diesem Hintergrund wendet die FINMA im Zusammenhang mit der Identifizierungspflicht den bestehenden Schwellenwert für Wechsler von CHF 5'000 auch im Kryptobereich an. Im Kryptogeschäft stellt allerdings die Abgrenzung des Wechselgeschäfts (mit gänzlichem Verzicht auf die Identifizierung bis CHF 5'000 pro Transaktion) von der Dienstleistung im Zahlungsverkehr eine Herausforderung dar. Beim herkömmlichen Wechsel an einem Schalter kann sich der Finanzintermediär sicher sein, dass es sich wirklich um ein Wechselgeschäft handelt, sieht er die Person, der er den Wechselbetrag übergibt, doch direkt vor sich. Im Internet weiss der Wechsler hingegen nicht, ob die vom Kunden angegebene Empfänger-Wallet diesem auch gehört, oder es die Wallet einer Drittperson ist (womit eine Überweisung, also risikoreicherer Zahlungsverkehr, vorliegen würde). Der Wechsler im Kryptobereich muss deshalb durch geeignete Massnahmen sicherstellen, dass nur ein Zweipartei-Verhältnis besteht, um vom erhöhten Schwellenwert von CHF 5'000 profitieren zu können. Wie er diese Vorgabe umsetzt, ist ihm selber überlassen.

Anders als Wechselstuben übernehmen zentralisierte Handelsplattformen eine Vermittlerfunktion zwischen den Nutzern der Plattform. Der Händler nimmt Gelder oder Kryptowährungen von Kunden entgegen und leitet diese an andere Nutzer weiter. Solche Handelsplattform qualifizieren als Money Transmitter und sind entsprechend dem GwG unterstellt. Gemäss Praxis der FINMA gilt für die Handelsplattformen der gleiche Schwellenwert wie für Custody Wallet-Anbieter (vgl. Ziff. 4.1.2 oben).

4.1.4. Dezentralisierte Handelsplattformen

Im Unterschied zu zentralisierten Handelsplattformen erfolgt bei dezentralisierten Handelsplattformen die Abwicklung der zusammengeführten Aufträge (nach Freigabe / Bestätigung des Trades) auf der Blockchain direkt zwischen den Nutzern der Plattform⁸¹. Da letztlich unter Zuhilfenahme der Handelsplattform ein Transfer von Vermögenswerten stattfindet, stellt sich die Frage, ob die Plattform eine finanzintermediäre Dienstleistung für den Zahlungsverkehr im Sinne des GwG erbringt.

Für GwG-Unterstellung einer solchen Handelsplattform ist es entscheidend, ob der Plattformbetreiber Verfügungsmacht über die gehandelten Kryptowährungen erlangt oder nicht. Dies ist grundsätzlich oft der Fall, da die Plattform zur Sicherstellung des geordneten Handels die Aufträge (in welcher Form auch immer) bestätigen oder zur Ausführung freigeben muss bzw. sperren kann. Um sicherzustellen, dass alle abgeschlossene Trades ordentlich abgewickelt werden können, behält sich der Betreiber ausserdem oft die Möglichkeit zu intervenieren vor und vom Benutzer beantragte Rückzahlungen der im Rahmen des Settlement Smart Contracts verwahrten Kryptowährungen nicht freizugeben. Gemäss Praxis der FINMA unterstehen dezentralisierte Handelsplattformen grundsätzlich dem GwG.

Nur wenn die dezentralisierte Handelsplattform überhaupt keine Interventionsmöglichkeit über die Abwicklung der abgeschlossenen Trades hat (z.B. reines Zurverfügungstellen eines für das Settlement notwendigen Escrow Smart Contract ohne Eingriffsmöglichkeiten der Plattform), ist sie nicht dem GwG

⁸¹ Der Transfer kann auch mittels off-chain Zahlungssystemen geschehen. Dabei hat das Zahlungssystem bzw. der Betreiber keine Verfügungsmacht über die Vermögenswerte der Nutzer. Die Nutzer transferieren, unter Zuhilfenahme der Zahlungssystem-Infrastruktur, Kryptowährungen untereinander.

unterstellt. Wie bei den Non-Custody Wallet-Anbietern sieht die FINMA unter der geltenden Rechtslage auch hier keine Möglichkeit solche Handelsplattformen dem GwG zu unterstellen.

4.1.5. Mining

Das Schürfen bzw. Mining von Kryptowährungen in der Schweiz ist nach den Finanzmarktgesetzen nicht bewilligungspflichtig. In Bezug auf den Verkauf der durch das Mining erhaltenen Kryptowährungen kann eine geldwäschereirechtlich relevante Handelstätigkeit vorliegen, namentlich wenn der Handel auf fremde Rechnung erfolgt.

4.1.6. Übersichtstabelle über die verschiedenen Arten von Krypto-Asset-Dienstleistungen und ihre Unterstellung unter das GwG

Kategorie der Dienstleistungen	Unterstellung unter das GwG	Keine Unterstellung unter das GwG	Unterstellung unter das GwG unter bestimmten Bedingungen
ICOs			Dem GwG unterstellt, wenn beim ICO Token ausgegeben werden, die mit Zahlungsmitteln gleichgestellt werden können (Zahlungs-Token)
<i>Custodian Wallet-Anbieter</i>	In jedem Fall dem GwG unterstellt		
<i>Non-Custodian Wallet-Anbieter</i>		Nicht dem GwG unterstellt	
Online-Wechselstuben	Ebenso wie herkömmliche Wechselstuben dem GwG unterstellt		
Zentralisierte Handelsplattformen	In jedem Fall dem GwG unterstellt		
Dezentralisierte Handelsplattformen			Dem GwG unterstellt, wenn sie die Möglichkeit haben, in die Transaktionen ihrer Nutzer einzugreifen, um beispielsweise eine Transaktion zu blockieren

Miner		Nicht dem GwG unterstellt	
-------	--	------------------------------	--

4.2. Die internationale Zusammenarbeit

Wie bereits ausgeführt, sind die Schweizer Strafverfolgungsbehörden gegenüber der Finanzkriminalität mittels Kryptowährungen und vor allem gegenüber der Gefahr, dass diese zur Geldwäscherei und Terrorismusfinanzierung genutzt werden könnten, relativ machtlos. In diesem Bereich scheinen die Kriminellen immer einen Schritt voraus zu sein. Die Strafverfolger können aber auf herkömmliche und sehr nützliche Instrumente zurückgreifen, insbesondere auf die Zusammenarbeit mit ihren europäischen Partnerstellen.

Polizei- und Justizbehörden sind sich einig, dass die internationale polizeiliche und justizielle Rechtshilfe ebenso effizient ist bei der Verfolgung von Finanzkriminalität mittels Kryptowährungen wie in anderen Bereichen. Dank dieser Art der internationalen Zusammenarbeit, an der die schweizerische Justiz und Polizei umfassend beteiligt sind, konnten international die grössten Erfolge bei der Repression von Finanzkriminalität mittels Kryptowährungen und vor allem in der Bekämpfung der Geldwäscherei erzielt werden.⁸² Dazu zählt insbesondere die Schliessung der grössten illegalen Marktplätze in Darknets wie etwa Silkroad, Hansa oder auch Alpha Bay. Die hiesigen Justiz- und Polizeibehörden arbeiten oft an diesen umfangreichen Operationen mit, die zuweilen auch zu Verurteilungen in der Schweiz führen.

Verurteilung eines im Darknet aktiven Cyber-Kriminellen in der Schweiz

Im Rahmen von koordinierten Operationen der Polizei- und Justizbehörden mehrerer Länder gegen den Online-Schwarzmarkt Silk Road 2 erhielt die Schweiz ein internationales Rechtshilfegesuch zu einer von der Schweiz aus verwalteten Webseite dieses illegalen und über ein Darknet zugänglichen Marktes. Ausländischen Polizeibehörden war es im Rahmen ihrer Untersuchungen gelungen, die IP-Adresse zu identifizieren, worauf der zuständige kantonale Staatsanwalt ein Strafverfahren einleitete. Schliesslich wurden international koordiniert in mehreren Ländern gleichzeitig Hausdurchsuchungen durchgeführt. In der Schweiz konnte dabei in der Wohnung, in der sich der identifizierte Anschluss befand, der gesuchte Server beschlagnahmt und der Entwickler und Webmaster der beanstandeten Webseite für illegale Verkäufe identifiziert werden. Die polizeilichen Untersuchungen ergaben zudem, dass er fiktive illegale Waren zum Verkauf angeboten hatte. Dabei hatte er in wenigen Monaten rund 125'000 US-Dollar in der Form von Bitcoins eingenommen, die er beim Spielen auf Online-Poker-Webseiten allerdings fast vollständig wieder verloren hatte. Er besass aber auf einer Wallet noch etwa 20 Bitcoins aus seiner kriminellen Aktivität. Der Beschuldigte zeigte sich bereit, mit der Justiz zusammenzuarbeiten, und übergab dieser den Private Key dieser Wallet, so dass der darauf befindliche Betrag beschlagnahmt und eingezogen werden konnte. Der Beschuldigte wurde danach wegen Betrugs verurteilt.

Neben den Bestimmungen des Bundesgesetzes über internationale Rechtshilfe in Strafsachen (IRSG, SR 351.1) bildet das von der Bundesversammlung genehmigte und durch Bundesbeschluss vom 18. März 2011⁸³ umgesetzte Übereinkommen des Europarates über die Cyberkriminalität eine wichtige gesetzliche Grundlage für die Regelung der justiziellen und polizeilichen Zusammenarbeit in diesem

⁸² «Significant law enforcement actions», in European Parliament, *Virtual currencies and terrorist financing : assessing the risks and evaluating responses*, Mai 2018, S. 85, [http://www.europarl.europa.eu/Reg-Data/etudes/STUD/2018/604970/IPOL_STU\(2018\)604970_EN.pdf](http://www.europarl.europa.eu/Reg-Data/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf).

⁸³ <https://www.admin.ch/opc/de/official-compilation/2011/6293.pdf>

Bereich. Es erlaubt der Polizei der verschiedenen Unterzeichnerstaaten namentlich, sich direkt an ausländische Unternehmen zu wenden, um die für ihre Untersuchungen notwendigen Daten einzufordern (Art. 32). Die angefragten Unternehmen sind zwar nicht verpflichtet, solche Anfragen zu beantworten, aber gemäss den zuständigen Polizeibehörden arbeiten mehrere von ihnen aktiv an solchen Verfahren mit, sofern die nationale Gesetzgebung, der sie unterstellt sind, dies erlaubt. Ausserdem können die angefragten Unternehmen dank diesem rechtlichen Instrument auch bei einer Verweigerung der Auskunft dazu verpflichtet werden, die Daten, die Gegenstand des Gesuchs waren, im Hinblick auf ein ordnungsgemässes Rechtshilfegesuch besonders sorgfältig aufzubewahren. Laut zuständigen Polizeibehörden hat sich dieses Instrument als besonders wichtig erwiesen. Zudem zeigt die Praxis, dass die angefragten Unternehmen, sofern es sich bei ihnen um Finanzintermediäre handelt, ihren FIU aufgrund solcher Anfragen Verdachtsmeldungen senden können. Diese Informationen können der MROS danach spontan übermittelt werden.

Das Umgekehrte gilt ebenfalls: Schweizer Intermediäre, die von ausländischen Polizeien kraft Artikel 32 des Übereinkommens des Europarates über die Cyberkriminalität kontaktiert werden, antworten diesen zwar nicht immer direkt, liefern jedoch stets die verlangten Informationen an die MROS, die sie an ihre ausländischen Partnerstellen weiterleitet. Im Übrigen schickt die MROS ihren ausländischen Partnerstellen auch Informationensuchen und unaufgeforderte Informationen zu Verdachtsfällen der Geldwäscherei durch Kryptowährungen. Zum heutigen Zeitpunkt ist es allerdings noch zu früh für eine Auswertung der Ergebnisse.

4.3. Technologische Fortschritte zugunsten der Strafverfolgungsbehörden

Beim jetzigen Stand der Technologie sind die Instrumente der Kettenanalyse für die Ermittler, die der Geldwäscherei und Terrorismusfinanzierung mittels Kryptowährungen auf der Spur sind, zwar erst eine teilweise Hilfe. Aber dies könnte sich schnell ändern. Mehrere Forschungsprojekte lassen nämlich hoffen, dass in naher Zukunft bedeutende Fortschritte in diesem Bereich erzielt werden. So sind gegenwärtig mehrere Gesellschaften an der Entwicklung von Informatikinstrumenten, die eine Rekonstruktion der *Paper Trail* von Kryptotransaktionen, die über Mixer-/Tumbler-Dienste laufen, ermöglichen sollen. Auf internationaler Ebene beteiligt sich die Schweiz zudem am TITANIUM-Projekt (*Tools for the Investigation of Transaction in Underground Markets*), an dem Computerforscher und Strafverfolgungsbehörden mehrerer Länder unter der Leitung von INTERPOL zusammenarbeiten. Ziel dieses Projekts ist die Entwicklung eines Instrumentes, mit dem die Transparenz der Kryptotransaktionen auf den Märkten im Darknet verbessert werden kann. Mittel dazu ist insbesondere eine simultane Analyse von Blockchains verschiedener Kryptowährungen, damit die Anonymität ihrer Nutzer durchbrochen werden kann.⁸⁴

4.4. Diverses

Zusätzlich zu den bis hierhin genannten Massnahmen haben mehrere Behörden verschiedene Initiativen ergriffen, um die Finanzkriminalität durch Kryptowährungen und vor allem die Geldwäscherei und Terrorismusfinanzierung effizienter bekämpfen zu können. Dazu zählen beispielsweise Bemühungen zur Schulung der betroffenen Behörden. Staatsanwälte, Polizisten und Finanzanalysten der MROS werden dadurch zunehmend für die Problematik der Kryptowährungen und der damit verbundenen potenziellen Kriminalität sensibilisiert. Zur Ausbildung der Polizisten gehören namentlich Kurse über Cyberkriminalität, die vom Schweizer Polizei-Institut angeboten werden. Ein solcher Ansatz ist besonders wichtig, und zwar nicht nur, weil ein umfassendes Fachwissen in diesem Bereich unerlässlich ist, um

⁸⁴ <https://www.interpol.int/News-and-media/News/2017/N2017-069>.

die technischen Möglichkeiten von Kryptowährungstechnologien für die Geldwäscherei und Terrorismusfinanzierung zu verstehen, sondern auch zu deren Repression. Diese Ansätze, die noch in den Kinderschuhen stecken, sollten systematisiert und vertieft werden. In dieser Hinsicht stellt der Aufbau von auf Cyberkriminalität spezialisierten Brigaden in den verschiedenen Kantonspolizeien einen wichtigen Fortschritt dar.

Ein weiteres Beispiel einer Initiative im Kampf gegen das Geldwäscherei- und Terrorismusfinanzierungsrisiko im Zusammenhang mit Kryptowährungen ist die Bildung einer Arbeitsgruppe zu diesem Thema innerhalb der Bundesanwaltschaft. Mehrere kantonale Staatsanwaltschaften haben ebenfalls Pools von Staatsanwälten gebildet, die auf solche Fragen spezialisiert sind.

Alle diese Initiativen gipfelten im Sommer 2018 in der Schaffung einer nationalen Plattform zur justiziel- len und polizeilichen Zusammenarbeit – dem Cyberboard –, dem Vertreterinnen und Vertreter der wich- tigsten Akteure im Kampf gegen die Cyberkriminalität in der Schweiz angehören: KKJPD, KKPKS, Schweizerische Staatsanwälte-Konferenz (SSK), fedpol, Bundesanwaltschaft, Schweizerische Krimi- nalprävention (SKP), SVS, NDB und ISB. Die modular aufgebaute Plattform soll eine Zusammenarbeit dieser Akteure und eine Koordination ihrer Aktionen ermöglichen, um die Cyberkriminalität effizienter zu bekämpfen. Beispielsweise vereint das erste Modul, der Cyber-CASE, Staatsanwälte und Kantons- und Bundespolizisten, die auf die Cyberkriminalität spezialisiert sind, sowie Vertreter von MELANI. Die- ses Modul, das seit dem 6. Juli 2018 aktiv ist, hat den Auftrag, in operativen Fällen die Koordination zwischen Staatsanwaltschaft und Polizei von Bund und Kantonen ebenso wie den Erfahrungs- und Wissensaustausch zwischen ihnen sicherzustellen.

Ebenso behält die Eidgenössische Spielbankenaufsicht (ESBK) das Problem der Geldwäscherei durch Krypto-Assets im Auge, da es die Casinos betreffen könnte. Diese bis anhin inexistente Gefährdung könnte mit der Aufhebung des Verbots von Online-Spielen auftauchen, die das Schweizer Volk mit der Zustimmung zum neuen Bundesgesetz über Geldspiele am 10. Juni 2018 gutgeheissen hat. Im Rah- men der Aufsicht der ESBK über solche Online-Spiele wird sich zeigen, ob spezifische Massnahmen gegen eine allfällige missbräuchliche Nutzung von Kryptowährungen in diesem Bereich ergriffen werden müssen. Die ESBK besitzt nach Artikel 76 Absatz 2 des Entwurfs der Geldspielverordnung (VGS), der sich derzeit im Hinblick auf seine Genehmigung durch das Parlament in der Vernehmlassung befindet, die Kompetenz, gewisse Zahlungsmittel zu verbieten. Die ESBK behält sich deshalb vor, bei bestimmten Kryptowährungen davon Gebrauch zu machen, sollte sich dies als notwendig erweisen.

5. Crowdfundingplattformen

5.1. Erscheinungsformen

Bereits vor dem Aufkommen der ICOs wurde im Internet via Crowdfunding-Plattformen Geld gesammelt. Der Begriff Crowdfunding bezeichnet die Finanzierung eines Projekts durch eine Vielzahl von Geldgebern. Ziel ist es, über die Masse Projekte zu finanzieren, die von Geldnehmern in der Regel im Internet auf einer Crowdfunding-Plattform aufgeschaltet werden. Eine Crowdfunding-Plattform ist grundsätzlich dafür verantwortlich, die Crowdfunding-Website zu betreiben und die damit verbundene Projektaufschaltung, -koordination bzw. das Zusammenführen von Geldgeber und Geldnehmern zu ermöglichen. Dabei nehmen die Plattformen je nach Geschäftsmodell verschiedene (weitere) Tätigkeiten wahr. Viele Plattformen nehmen dabei z.B. Gelder entgegen und leiten diese weiter. Dies teilweise erst, nachdem eine gewisse Gesamtsumme innert einer Frist erreicht worden ist. Wird die Gesamtsumme nicht innert Frist erreicht, haben die Plattformen i.d.R. eine Rücküberweisungspflicht an die Geldgeber. Es gibt verschiedene Formen der mittels Crowdfunding gewährten Unterstützung (wobei die Definitionen und Begriffe variieren bzw. allenfalls weitere Begriffe verwendet werden können):

- a) Crowddonating: Die Geldgeber stellen den Geldnehmern eine bestimmte Summe als Spende ohne Gegenleistung zur Verfügung. Es wird nicht erwartet, dass der überlassene Geldbetrag zurückerstattet wird.
- b) Crowdsupporting: Die Geldgeber stellen den Geldnehmern eine bestimmte Summe als Spende mit einer Gegenleistung ideeller oder bloss geringer materieller Natur (z.B. signiertes Exemplar der produzierten CD) zur Verfügung. Es wird i.d.R. nicht erwartet, dass der überlassene Geldbetrag zurückerstattet wird.
- c) Crowdlending (Beteiligung am Fremdkapital): Bei dieser Form werden sowohl eine Rückerstattung des überlassenen Geldes als auch regelmässige Zinszahlungen vereinbart. Privatrechtlich handelt es sich insoweit um Darlehensverträge.
- d) Crowdinvesting (Zurverfügungstellung von Eigenkapital): Dabei handelt es sich um eine Gesellschaftsfinanzierung, bei der als Gegenleistung für die Überlassung des Geldes Beteiligungsrechte und gegebenenfalls eine Beteiligung am Erfolg versprochen wird.

Auch die jüngere Erscheinungsform des ICO ist im Grunde ein Crowdfunding. Die Unterschiede liegen in der Praxis darin, dass beim klassischen Crowdfunding in der Regel eine Plattform (Intermediär) zwischen Geldgeber und Geldnehmer steht und die Gelder in FIAT übertragen werden. Bei ICOs wird meist keine Plattform dazwischengeschaltet, sondern die Geldgeber zahlen direkt an den Geldnehmer. Zudem wird oft – aber weitaus nicht immer – der Geldbetrag in Kryptowährungen entgegengenommen.

5.2. Risikoanalyse

Ebenso wie bei den Krypto-Assets ist es gegenwärtig auch bei den Online-Crowdfunding-Plattformen schwierig, das Geldwäscherei- und Terrorismusfinanzierungsrisiko zu evaluieren, weil die Zahl der von den Schweizer Behörden erfassten Fälle sehr gering ist. Die Gefahren solcher Plattformen sind jedoch erwiesen. Sie ergeben sich aus der Anonymität, die dadurch verschärft wird, dass diese Plattformen im Internet operieren. Dadurch wird über Crowdfunding-Plattformen die Teilnahme an Projekten über die Landesgrenzen hinaus ermöglicht.⁸⁵ Besonders ausgeprägt sind die Bedrohungen beim Crowddonating. Gelder können über soziale Medien oder formelle Crowddonating-Plattformen von betrügerischen

⁸⁵ ADVANCED FINANCIAL CRIME PROFESSIONALS WORLDWIDE (ACAMS), *Financial Institutions and Crowdfunding*, K.M. Veldhuizen-Koeman, 2016, p. 6 et seq., [http://files.acams.org/pdfs/2016/Financial Institutions and Crowdfunding K. Veldhuizen.pdf](http://files.acams.org/pdfs/2016/Financial%20Institutions%20and%20Crowdfunding%20K.%20Veldhuizen.pdf).

gemeinnützigen Organisationen unter dem Deckmantel der humanitären Hilfe gesammelt werden. Wie mehrere Meldungen an die MROS zeigen, können solche Kapitalbeschaffungen ebenso wie ICOs einem Investorenbetrug gleichkommen, wenn das angeblich zu finanzierende Projekt gar nicht umgesetzt wird und die Organisatoren die Spenden für sich selbst behalten. Die Hauptbedrohung liegt aber darin, dass die gesammelten Gelder als materielle Unterstützung für sog. Foreign Terrorist Fighters (für Flugtickets, Mobilkommunikation etc.) oder als Geldmittel für die Ausführung von Terroranschlägen dienen können.⁸⁶

Im Bericht der FATF zu Emerging Terrorist Financial Risks wird ausgeführt, dass Geldgebern häufig nicht bewusst ist, für was ihre über soziale Medien (inklusive Crowdfunding-Plattformen) gespendeten Gelder schlussendlich verwendet werden, was ein Risiko bedeutet, welches Terrorismusorganisationen ausnutzen können⁸⁷. Die Bedrohung der Terrorismusfinanzierung dürfte sich kurzfristig erhöhen, da die Popularität dieser Systeme wächst und sie häufiger benutzt werden. Zwar mögen Transaktionen verfolgbar sein, den eigentlichen Endnutzer bzw. Begünstigten zu identifizieren ist jedoch schwierig, wenn die Crowdfunding-Plattform keine KYC-Pflichten wahrnimmt. Gemäss der FATF ist derzeit nicht klar, inwiefern Terroristengruppen und ihre Unterstützer diese Technologien ausnutzen. Die Nutzung organisierter Crowdfunding-Techniken stellt ein aufkommendes Terrorismusfinanzierungsrisiko dar. Crowdfunding ist gefährdet, für illegale Zwecke genutzt zu werden, auch für Fälle, in denen ein falscher Zweck einer Funding-Kampagne angegeben wird. Individuen und Organisationen, welche Gelder zur Unterstützung von Terrorismus und Extremismus sammeln wollen, dürften behaupten, dass sie sich in legitimen wohltätigen oder humanitären Aktivitäten engagieren und zu diesem Zwecke gemeinnützige Organisationen etablieren. Die FATF zeigt in einer Fallstudie auf, dass die kanadische FIU Beispiele hat, dass Personen, welche im Zusammenhang mit terroristischen Straftaten überprüft wurden, versucht haben, das Land zu terroristischen Zwecken zu verlassen und dazu vorgängig Crowdfunding-Webseiten benutzt haben.

Die französische Tracfin weist auf die erheblichen Risiken der Terrorismusfinanzierung durch Crowddonating hin. Sie beschreibt auch einen Fall, bei welchem die Analyse einer Crowddonating-Plattform ergeben hat, dass gewisse Geldflüsse aus sensiblen geographischen Zonen kamen und der insgesamt gespendete Betrag im Vergleich zur Art des finanzierten Projekts ungewöhnlich schnell zustande kam. Bei einigen der Projekte auf dieser Plattform gab es offenbar Verbindungen zu radikalen Islamisten⁸⁸. Seit dem Inkrafttreten der «Ordonnance n°2016-1635 du 1er décembre 2016 renforçant le dispositif français de lutte contre le blanchiment et le financement du terrorisme» per Ende 2016 ist der Status als «intermédiaire en financement participatif» nicht mehr fakultativ, sondern obligatorisch für sog. «plateformes de dons», d.h. Crowddonating-Plattformen. Diese müssen nun die Regeln zur Geldwäschereibekämpfung und Bekämpfung der Terrorismusfinanzierung einhalten.⁸⁹

Weiter berichtet die Association of Certified Anti-Money Laundering Specialists ACAMS von einem Fall, in welchem zwei Personen einer französischen Charity-Kampagne Terrorismusfinanzierung in Syrien angelastet wird. Über die Kampagnenseite wurde u.a. für syrische Kinder gesammelt. Obwohl Nahrungsmittel und medizinisches Material nach Syrien geliefert wurde, sind viele dieser Lieferungen auch dazu benutzt worden, um Gelder an Dschihadistengruppen strömen zu lassen. Gemäss der ACAMS ist die Anzahl der Berichte zu illegalen Aktivitäten mit Bezug zu Crowdfunding der US-Behörde FinCEN

⁸⁶ Siehe zum Thema Terrorismusfinanzierung: FATF, *Emerging Terrorist Financing Risks*, Octobre 2015 (<http://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf>).

⁸⁷ *Ibid.*, p. 6, 31 et seq.

⁸⁸ TRACFIN, *Tendances et analyse de risques de blanchiment de capitaux et de financement du terrorisme en 2015*, 2015, <https://www.economie.gouv.fr/tracfin/tendances-et-analyse-des-risques-en-2015>.

⁸⁹ Vgl. Art. L548-2, II und Art. L561-2, 4° des Code monétaire et financier, <https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006072026>.

zwar noch tief, nimmt aber stetig zu. Die Durchsicht und die Analyse dieser Meldungen zeigen, dass insbesondere Crowdsupporting-Plattformen zu Geldwäscherei-Zwecken benutzt werden.⁹⁰

In der Schweiz sind bisher keine Fälle eines Missbrauchs einer Crowdfunding-Plattform bekannt. Bei der MROS sind keine entsprechenden Meldungen eingegangen. Dies könnte aber auch damit zusammenhängen, dass viele Plattformen heute nicht dem GwG unterstellt sind und keine Meldungen erstatten können. Auf dem Markt sind einige grössere Crowddonating- und Crowdsupporting-Plattformen ohne GwG-Unterstellung tätig, die trotzdem die angemeldeten Projekte und die Geldnehmer vorgängig einer Prüfung unterziehen. Diese Aspekte stellen eine echte Verwundbarkeit der Schweiz in diesem Bereich dar.

5.3. Risikomindernde Faktoren

Die Unterstellungspflicht unter das GwG ist unter anderem in Art. 2 Abs. 3 GwG sowie in der Geldwäschereiverordnung (GwV; SR 955.01) geregelt. Darunter fallen Personen, die berufsmässig fremde Vermögenswerte annehmen oder aufbewahren oder helfen, sie anzulegen oder zu übertragen, insbesondere Personen, die Dienstleistungen für den Zahlungsverkehr erbringen (Art. 2 Abs. 3 Bst. b GwG). Eine Dienstleistung für den Zahlungsverkehr liegt insbesondere vor, wenn der Finanzintermediär im Auftrag seiner Vertragspartei liquide Finanzwerte an eine Drittperson überweist und dabei diese Werte physisch in Besitz nimmt, sie sich auf einem eigenen Konto gutschreiben lässt oder die Überweisung der Werte im Namen und Auftrag der Vertragspartei anordnet oder wenn er das Geld- oder Wertübertragungsgeschäft durchführt (Art. 2 Abs. 3 Bst. b GwG i.V.m. Art. 4 GwV; vgl. auch FINMA-Rundschreiben 2011/1, Rz. 58). Liegt eine Dienstleistung für den Zahlungsverkehr vor und ist der Finanzintermediär berufsmässig tätig (Art. 7 GwV), hat er die Sorgfaltspflichten nach Art. 3 - 7 GwG einzuhalten.

Nicht als Finanzintermediation gilt die Inkassotätigkeit. Dem Inkasso liegt ein zwei- oder mehrseitiges Rechtsgeschäft zugrunde, in welches der Inkassobeauftragte i.d.R. nicht involviert ist. Die mit dem Inkasso betraute Person zieht im Auftrag des Gläubigers fällige Forderungen ein. Die Beauftragte handelt entweder als direkte Stellvertreterin des Gläubigers oder tritt gegenüber dem Schuldner in eigenem Namen auf. Eine GwG-Unterstellung der Inkassotätigkeit würde in der Regel weitgehend leerlaufen, weil die Inkassounternehmen mangels vertraglicher Beziehung zu den Schuldnern nicht verpflichtet werden könnten, diese gemäss Art. 3 GwG zu identifizieren.⁹¹ Ausnahmsweise unterhält der Beauftragte Vertragsbeziehungen sowohl zum Gläubiger der Forderung als auch zum Schuldner. In solchen Fällen kann gemäss FINMA-RS 2011/1 Rz. 9 gleichwohl eine Inkassotätigkeit vorliegen. Entscheidend ist, in wessen Auftrag die Überweisung resp. Weiterleitung vorgenommen wird, was anhand von Indizien zu eruieren ist. Typischerweise wird dabei die Dienstleistung vom Auftraggeber entschädigt.

Da Crowdfundingplattformen i.d.R. fremde Gelder entgegennehmen und an die zu finanzierenden Projekte weiterleiten, liegt grundsätzlich eine unterstellungspflichtige Dienstleistung für den Zahlungsverkehr vor (vgl. Art. 2 Abs. 3 lit. b GwG i.V.m. Art. 4 Abs. 1 lit. a GwV). Im aktuellen Rechtsrahmen ist es jedoch möglich, die Ausprägung der Crowddonating-Plattformen bewilligungsfrei zu betreiben. Namentlich können Betreiber von Crowddonating- und Crowdsupporting-Plattformen die Inkassoausschussausnahme gemäss Art. 2 Abs. 2 lit. a Ziff. 2 GwV für sich beanspruchen. In der Schweiz sind damit bislang grundsätzlich nur Crowdlending- und Crowdinvesting-Plattformen (d.h. die Geldgeber erhalten Zinsen oder Dividenden) dem Geldwäschereigesetz unterstellt (Art. 2 Abs. 3 GwG), da bei diesen Plattformen die Geldflüsse in beide Richtungen zwischen Geldgeber und Geldnehmer laufen und somit kein Inkassoauftrag nur des Geldgebers vorliegen kann. Die übrigen Plattformen sind in der Regel so ausgestaltet

⁹⁰ ADVANCING FINANCIAL CRIME PROFESSIONALS WORLDWIDE (ACAMS), *Crowdfunding: The New Face of Financial Crime?*, Financial Institutions and Crowdfunding, 2017, p. 14 et seq., http://files.acams.org/pdfs/2017/Crowdfunding_The_New_Face_of_Financial_Crimes_S.Sessoms.pdf.

⁹¹ Vgl. FINMA-RS 2011/1, Rz. 8; Praxis der Kontrollstelle für die Bekämpfung der Geldwäscherei zu Art. 2 Abs. 3 GwG vom 29. Oktober 2008, Ziff. 4.1, S. 31 (https://www.finma.ch/FinmaArchiv/gwg/d/dokumentationen/publikationen/gwg_auslegung/pdf/59402.pdf), welche als Grundlage für die VBF diente; BGE 2A.62/2007, Erw. 8.

(namentlich hinsichtlich ihrer AGB sowie der Geldflüsse), dass sie von der Inkassoausnahme gemäss Art. 2 Abs. 2 Bst. a Ziff. 2 GwV Gebrauch machen können.

Am 1. August 2017 wurden in der BankV Erleichterungen für Finanzmarktteilnehmer eingeführt, von welchen auch das Crowdfunding stark profitieren kann.⁹² Die Anpassungen haben jedoch keinen Einfluss auf die Anwendbarkeit des GwG auf Crowdfundingplattformen.⁹³

⁹² "Nimmt der Betreiber von Crowdfunding-Plattformen die Gelder nicht bloss zur Weiterleitung innerhalb von 60 Tagen an den Projektentwickler entgegen (vor dem 1. August 2017 waren praxisgemäss max. 7 Arbeitstage erlaubt), sondern verbleiben sie aus anderen Gründen für längere Zeit auf den Konten des Plattformbetreibers, um beispielsweise das Vorhandensein der Gelder bei Ablauf einer längeren Sammelfrist zu gewährleisten, so ist bei einer gewerbsmässigen Tätigkeit grundsätzlich vorgängig eine Bewilligung nach Bankengesetz erforderlich. Seit 1. August 2017 ist in diesen Fällen wegen fehlender Gewerbsmässigkeit dann keine Bewilligung nötig, wenn nicht mehr als CHF 1 Mio. zur Weiterleitung entgegengenommen werden. Dabei müssen die Projektfinanzierer allerdings über die fehlende Beaufsichtigung der Plattform durch die FINMA und die nichtbestehende Einlagensicherung informiert werden" (Faktenblatt der FINMA zu Crowdfunding, Stand: 1. August 2017).

⁹³ Erläuterungen zur Änderung der Bankenverordnung (Fintech) des Eidgenössischen Finanzdepartements (EFD) vom 5. Juli 2017, Ziff. 1.1.3.

6. Schlussfolgerungen / Empfehlungen

6.1. Schlussfolgerungen aus der Analyse der Risiken im Zusammenhang mit Krypto-Assets

Die Gefahr der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets ist gross, auch wenn die Zahl der nachgewiesenen Fälle in der Schweiz bis anhin beschränkt ist. Sie gründet auf der Anonymität der Token-Transaktionen und äussert sich sowohl in der kriminellen Ausnutzung von Design-Fehlern bei den Kryptowährungen als auch im Investorenbetrug vor allem bei ICOs und der Nutzung von Kryptowährungen für Ransomware-Zahlungen. Die Verwendung von Kryptowährungen stellt aber auch in sonstigen kriminellen Mustern eine Gefahr dar: Terrorismusfinanzierung, Waschen von Geldern aus dem Verkauf von illegalen Dienstleistungen und Produkten, Phishing-Betrügereien oder auch Drogenhandel, insbesondere durch kriminelle Organisationen. Aufgrund ihrer Anonymität eignen sich Kryptowährungen besonders gut für die Geldwäscherei.

In der Schweiz ist die Zahl der Fälle, in denen nachweislich Token zur Geldwäscherei verwendet wurden, nicht sehr hoch und im Bereich der Terrorismusfinanzierung sogar Null. Das mit Kryptowährungen verbundene Risiko lässt sich folglich nur schwer evaluieren, aber die Verwundbarkeiten der Schweiz in Bezug auf diese Gefährdung sind erheblich, wenn auch nicht spezifisch für den Finanzplatz Schweiz.

Aufgrund der Anonymität der Kryptotransaktionen ist eine Identifikation von Token aus krimineller Herkunft und ihrer wirtschaftlich Berechtigten für die Strafverfolgungsbehörden und die Finanzintermediäre, die mit ihnen handeln, äusserst kompliziert. Wegen der dezentralisierten Struktur der Kryptowährungstechnologien entzieht sich zudem eine Vielzahl von Transaktionen jeder Kontrolle: Diese Technologien erlauben einen anonymen Handel und Umtausch von Kryptowährungen ohne Finanzintermediäre und oft ohne dass festgestellt werden kann, aus welchem Land die Transaktionen angeordnet wurden. Diese Feststellung unterstreicht die entscheidende Verantwortung, die den Plattformen für den Wechsel zwischen Fiatgeld und Krypto-Assets zukommt: Sie sind zum heutigen Zeitpunkt offenbar die einzigen Finanzintermediäre, die ihre Sorgfaltspflichten gegenüber ihren Kunden wahrnehmen können, auch wenn diese Vorsichtsmassnahmen nur eine beschränkte Wirkung haben.

Rechtliche Anpassungen zur Verminderung des Geldwäscherei- und Terrorismusfinanzierungsrisikos im Zusammenhang mit Kryptowährungen können zwar in Betracht gezogen werden.⁹⁴ Die Schweizer Behörden haben es aber verstanden, die Instrumente anzupassen, die ihnen die bestehende Gesetzgebung schon heute bietet. So sind alle Gesellschaften, die finanzintermediäre Dienstleistungen im Token-Bereich anbieten, dem GwG unterstellt, sogar die Anbieter von *Custodian Wallets*, dezentralisierte Handelsplattformen, die in die von ihren Kunden angeordneten Transaktionen eingreifen können, sowie gewisse ICOs, die in anderen Ländern nicht in den Bereich der Finanzintermediation gehören. Die Anbieter von *Non-custodian Wallets* und dezentralisierte Plattformen, die keine Möglichkeit haben, in die Transaktionen ihrer Kunden einzugreifen, entziehen sich aber dem Dispositiv der Geldwäschereibekämpfung. Überdies sind sich offenbar nicht alle dem GwG unterstellten Finanzintermediäre ihrer Sorgfaltspflichten gleichermassen bewusst.

Auch die Strafverfolgungsbehörden bemühen sich, Kriminalität im Zusammenhang mit Kryptowährungen mit den ihnen zur Verfügung stehenden Mitteln zu ahnden. Zu den wichtigsten Instrumenten zählen zweifellos die internationale Zusammenarbeit und die justizielle und polizeiliche Rechtshilfe mit ihren ausländischen Partnerstellen. Aber die Schnelligkeit der Transaktionen, mit der Token krimineller Herkunft innert Sekunden und mit nur wenigen Klicks von einem Ort auf dem Globus an einen anderen

⁹⁴ Vgl. dazu Empfehlungen im Bericht des Bundesrates „Rechtliche Grundlagen für Distributed Ledger-Technologie und Blockchain in der Schweiz“, 7. Dezember 2018.

verschoben werden können, ohne dass die Urheber dafür von ihrem Computer aufstehen müssen, macht diese Zusammenarbeit oft vergeblich.

Durch den transnationalen Charakter der Gefahren der Geldwäscherei und Terrorismusfinanzierung durch Kryptowährungen müssen die wichtigsten Massnahmen zur Verminderung des damit verbundenen Risikos auf internationaler Ebene koordiniert werden, auch wenn sich das Ausmass dieses Risikos bis anhin nur schwer evaluieren lässt. Der Einsatz der Schweiz innerhalb der GAFI für eine internationale Harmonisierung der Regelungen für Gesellschaften, die am Handel und an Transaktionen von Krypto-Assets beteiligt sind, stellt eine angemessene Antwort auf diese Herausforderung dar. Ohne eine solche Harmonisierung droht jedes Rechtshilfegesuch ans Ausland aussichtslos zu sein. Zudem könnte jede Verschärfung der schweizerischen Gesetzgebung kontraproduktiv sein und einfach dazu führen, dass neue Tätigkeiten, für die neue Sorgfaltspflichten gelten würden, die Schweiz verlassen und in ein anderes Land umziehen würden.

Neben dem Engagement der Schweiz auf der internationalen Bühne tragen auch mehrere nationale und kantonale Initiativen dazu bei, das Geldwäscherei- und Terrorismusfinanzierungsrisiko durch Krypto-Assets im Rahmen des Möglichen zu vermindern. Die wichtigste ist die Schaffung des Cyberboards im Juni 2018: einer nationalen Plattform zur justiziellen und polizeilichen Zusammenarbeit im Bereich der Cyberkriminalität. Die Schulung von Schweizer Polizistinnen und Polizisten im Bereich der wirtschaftlichen Cyberkriminalität, die Bildung einer spezialisierten Arbeitsgruppe innerhalb der BA und die auf finanzielle Cyberkriminalität spezialisierten Brigaden der Kantonspolizeien stellen aber ebenfalls wichtige Fortschritte dar. Kombiniert mit der engen justiziellen, polizeilichen und administrativen Zusammenarbeit zwischen der Schweiz und ausländischen Staaten sind sie die stärksten Waffen im Kampf gegen die erhöhte Gefahr, die Krypto-Assets im Bereich der Geldwäscherei und Terrorismusfinanzierung darstellen.

6.2. Schlussfolgerungen und Empfehlungen zur Analyse der Risiken von Crowdfunding-Plattformen

Das mit dem Online-Crowdfunding verbundene Risiko betrifft im Wesentlichen die Terrorismusfinanzierung. Bis anhin wurde von den Schweizer Behörden zwar noch kein solcher Fall erfasst, aber die Schweiz weist in diesem Bereich Schwachstellen auf, die sinnvoll wären zu beheben.

Die geltende Regulierung trägt den festgestellten Risiken insgesamt nicht angemessenen Rechnung. Eine Anpassung auf regulatorischer Ebene ist zu prüfen. Dabei steht das ausdrückliche Unterstellen von Crowddonating-Plattformen und Crowdsupporting-Plattformen in der GwV im Vordergrund. Ohne eine solche Anpassung wären geldsammelnde Plattformen (Intermediäre), im Gegensatz zu Crowdlending- und Crowdinvestingplattformen, vom GwG ausgenommen, während derjenige, der für sich selber Geld sammelt (ICO), unter Umständen (Ausgabe eines Zahlungstokens) heute bereits unterstellt ist. Das GwG knüpft in seiner Konzeption allerdings an die Kontrolle von Geldflüssen durch Intermediäre an. Zudem würde damit dem Risiko der Zweckentfremdung und missbräuchlicher Verwendung der gesammelten Gelder nicht vorgebeugt.

7. Bibliographie

ADVANCED FINANCIAL CRIME PROFESSIONALS WORLDWIDE (ACAMS), *Financial Institutions and Crowdfunding*, K.M. Veldhuizen-Koeman, 2016, http://files.acams.org/pdfs/2016/Financial_Institutions_and_Crowdfunding_K_Veldhuizen.pdf.

ADVANCING FINANCIAL CRIME PROFESSIONALS WORLDWIDE (ACAMS), *Crowdfunding: The New Face of Financial Crime?*, Financial Institutions and Crowdfunding, 2017, S. 14 ff, http://files.acams.org/pdfs/2017/Crowdfunding_The_New_Face_of_Financial_Crimes_S.Sessoms.pdf.

AL JAWAHERI Husam, AL SABAH Mashael, BOSHMAF Yazan et ERBAD Aiman, "When a small leak sinks a great ship: deanonymizing Tor hidden service users through bitcoin transactions analysis", in *arXiv*: 1801.07501v2, April 2018, <https://arxiv.org/abs/1801.07501>.

ANONYME, « Singapour : les premiers billets Bitcoins visent à favoriser l'adoption de l'actif », in *Crypto-France.com*, <https://www.crypto-france.com/singapour-premiers-billets-bitcoin/>.

ANONYME, « Ils minaient des bitcoins dans un centre nucléaire », in *La Tribune de Genève*, 10. Februar 2018, <https://www.tdg.ch/faits-divers/Ils-minaient-des-bitcoins-dans-un-centre-nucleaire/story/30448246>.

ANONYME, « Bitcoin Gold : une attaque double dépense fait perdre plusieurs millions de dollars à des plateformes d'échanges », in *Crypto-France*, <https://www.crypto-france.com/bitcoin-gold-attaque-double-depense-perdes-millions-dollars-plateformes-echange/>.

ANONYME, « 670 millions de dollars de crypto-monnaies ont été dérobés au cours du premier trimestre 2018 », in *Crypto-France.com*, April 2018, <https://www.crypto-france.com/670-millions-dollars-crypto-monnaies-voles-premier-trimestre-2018/>.

ANONYME, « Cryptomonnaie : la plateforme japonaise Coincheck victime d'un vol record », 29. Januar 2018, <http://www.rfi.fr/economie/20180129-coincheck-vol-cryptomonnaie-injonction-japon>.

ANONYME, « Coincheck : les pirates servaient déjà parvenus à blanchir 40% des 500 millions de XEMs dérobés », <https://www.crypto-france.com/coincheck-pirates-blanchiment-xems/>.

BRANTLY Aaron, « Financing Terror Bit by Bit », in *CTC Sentinel*, vol. 7, no 10, Oktober 2014, S. 4, <https://ctc.usma.edu/financing-terror-bit-by-bit/>.

Bundesrat, *Bericht des Bundesrates zu virtuellen Währungen in Beantwortung der Postulate Schwab (13.3687) und Weibel (13.4070) vom 25. Juni 2014*, <https://www.news.admin.ch/NSBSubscriber/message/attachments/35361.pdf>

Bundesrat, *Rechtliche Grundlagen für Distributed Ledger-Technologie und Blockchain in der Schweiz*, 7. Dezember 2018. Abrufbar unter: www.admin.ch > Dokumentation > Medienmitteilungen > Medienmitteilung vom 14. Dezember 2018 (Stand: 14.12.2018).

Code monétaire et financier français, version consolidée au 1er octobre 2018, <https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006072026>.

DE PREUX Pascal et TRAJILOVIC Daniel, « Blockchain et lutte contre le blanchiment d'argent. Le nouveau paradoxe ? », in *Resolution LP*, https://resolution-lp.ch/wp-content/uploads/2018/02/064_L_14_De_Preux_Trajilovic.pdf.

European Parliament, *Virtual currencies and terrorist financing : assessing the risks and evaluating responses*, Mai 2018, [http://www.europarl.europa.eu/Reg-Data/etudes/STUD/2018/604970/IPOL_STU\(2018\)604970_EN.pdf](http://www.europarl.europa.eu/Reg-Data/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf);

EUROPOL, *2017 Virtual Currencies Money Laundering Typologies*, 2017.

FANUSIE Yaya et ROBINSON, Tom, *Bitcoin laundering: an analysis of illicit flows into digital currency services*, Center on Sanctions & Illicit Finance et ELLIPTIC, 12. Januar 2018.

FARINE Mathilde, "Comment investir dans les cryptomonnaies", in *Le Temps*, 22. Juli 2018, <https://www.letemps.ch/economie/investir-cryptomonnaies>.

FARINE Mathilde, « La FINMA enquête sur une ICO à 100 millions de francs », in *Le Temps*, 26. Juli 2018, <https://www.letemps.ch/economie/finma-enquete-une-ico-100-millions-francs>.

FAUCETTE James, GRASECK Betsy et SHAH Sheena, *Update : Bitcoin, Cryptocurrencies and Blockchain*, Morgan Stanley, 1. Juni 2018, S. 35, <https://www.macrobusiness.com.au/wp-content/uploads/2018/06/82012860.pdf>

FATF, *National Money Laundering and Terrorist Financing Risk Assessment*, 2013, [http://www.fatf-gafi.org/media/fatf/content/images/National ML TF Risk Assessment.pdf](http://www.fatf-gafi.org/media/fatf/content/images/National_ML_TF_Risk_Assessment.pdf).

FATF, *Virtual currencies. Key definitions and potential AML/CFT risks*, Juni 2014, <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>.

FATF, *Virtual currencies. Guidance for a risk-based approach*, 2015, <http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf>.

FATF, *FATF Fintech & RegTech Initiative*, [http://www.fatf-gafi.org/fintech-regtech/?hf=10&b=0&s=desc\(fatf_releasedate\)](http://www.fatf-gafi.org/fintech-regtech/?hf=10&b=0&s=desc(fatf_releasedate)).

FINMA, Medienmitteilung der FINMA vom 19. September 2017, <https://www.finma.ch/de/news/2017/09/20170919-mm-coin-anbieter/>.

FINMA, Medienmitteilung vom 26. Juli 2018, <https://www.finma.ch/de/news/2018/07/20180726-mm-en-vion/>

GARESSUS Emmanuel, « Une société suisse veut émettre des billets de bitcoins », in *Le Temps*, 8. Mai 2018, <https://www.letemps.ch/economie/une-societe-suisse-veut-emettre-billets-bitcoins>.

GRÜNEWALD Seraina, « Währungs- und geldwäschereirechtliche Fragen bei virtuellen Währungen », in Rolf H. Weber *et. al* (Hrsg.), *Rechtliche Herausforderungen durch webbasierte und mobile Zahlungssysteme*, ZIK Bd. 61, Zürich/Basel/Genf 2015.

HAEDERLI Alexandre et STÄUBLE Mario, « De la drogue livrée en courrier A. Comment fonctionne le marché des stupéfiants sur le Darknet », in *La Tribune de Genève*, 2. Mai 2018, https://www.tdg.ch/extern/interactive_wch/darknet/.

HESS Martin et SPIELMANN Patrick, « Cryptocurrencies, Blockchain. Handelsplätze & Co. – Digitalisierte Werte unter Schweizer Recht », in: Reutter, Thomas U. / Werlen, Thomas (Hrsg.): *Kapitalmarkt – Recht und Transaktionen XII*. Zürich: Schulthess 2017, S. 145-202.

HILEMAN Garrick und RAUCHS Michel, *Global Cryptocurrency Benchmarking Study*, Cambridge, Center for Alternative Finance/University of Cambridge, 2017.

HM Treasury et Home Office, *National risk assessment of money laundering and terrorist financing 2017*, London, 2017, S. 38, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/655198/National_risk_assessment_of_money_laundering_and_terrorist_financing_2017_pdf_web.pdf.

IRWIN Angela S.M. et MILAD, George, « The use of crypto-currencies in funding violent jihad », in *Journal of Money Laundering Control*, vol. 19, no 4, 2016, S. 410-411.

KGGT, *Bericht über die Bargeldverwendung und deren Missbrauchsrisiken für die Geldwäscherei und Terrorismusfinanzierung in der Schweiz*, Oktober 2018. Publikation vorgesehen am 18. Dezember 2018. Dann abrufbar unter: www.admin.ch > Dokumentation > Medienmitteilungen > Medienmitteilung vom 18. Dezember 2018.

Koos Couvée, « European traffickers pay colombian cartels through bitcoin ATMs : Europol Official », in ACAMS Moneylaundering.com, 28. Februar 2018, <https://www.moneylaundering.com/news/european-traffickers-pay-colombian-cartels-through-bitcoin-atms-europol-official/>.

LOUBIRE Paul, « La très longue liste de vols de bitcoins par des hackers », in *Challenges*, 8. Dezember 2017, https://www.challenges.fr/finance-et-marche/la-tres-longue-liste-de-vols-de-bitcoins-par-des-hackers_518541.

MEISSER Luzius, „Kryptowährungen: Geschichte, Funktionsweise, Potential“, in WEBER Rolf H. *et al* (Hrsg.), *Rechtliche Herausforderung durch webbasierte und mobile Zahlungssysteme*, ZIK Bd. 61, Zürich/Basel/Genf 2015.

SANSONETTI Riccardo, «Bitcoin: Virtuelle Währungen mit Chancen und Risiken», in *Die Volkswirtschaft*, 9-2014, S. 44-46.

SUBERG William, « Bitcoin exchange ShapeShift helps police as WannaCry attacker converts to monero », in <https://cointelegraph.com/news/bitcoin-exchange-shapeshift-helps-police-as-wannacry-attacker-converts-to-monero>.

TRACFIN, *Tendances et analyse de risques de blanchiment de capitaux et de financement du terrorisme en 2015*, 2015, <https://www.economie.gouv.fr/tracfin/tendances-et-analyse-des-risques-en-2015>.

TZANETAKIS Meropi, “Comparing cryptomarkets for drugs: a characterisation of sellers and buyers over time”, in *International Journal of Drug Policy*, vol. 56, Juni 2018, S. 176-186.

U.S. Department of Justice and Drug Enforcement Administration, *2017 National Drug Threat Assessment*, Oktober 2017.

US Securities and Exchange Commission, <https://www.sec.gov/news/statements>.

WILE Rob, « Supporter of extremist group ISIS explains how bitcoin could be used to fund Jihad », in *Business Insider Australia*, 8. Juli 2014, <https://www.businessinsider.com.au/isis-supporter-outlines-how-to-support-terror-group-with-bitcoin-2014-7>.