Kryptowährungen als Risiko für die öffentliche Sicherheit und Terrorismusbekämpfung

Gefahrenanalyse und Probleme der Regulierung

Dr. Daniel Eisermann
Berlin, April 2020

BERLIN RISK

COUNTER EXTREMISM PROJECT

Rechtlicher Hinweis

Berlin Risk wurde von Counter Extremism Project (CEP) mit der vorliegenden Studie beauftragt. Es wurde jede Anstrengung unternommen, die Genauigkeit der in diesem Bericht enthaltenen Informationen zu überprüfen. Sämtliche Bewertungen und Einschätzungen beruhen auf einer Beurteilung aus heutiger Sicht und können sich in Zukunft verändern. Es wird keine Gewähr für die Richtigkeit der Feststellungen oder ausgesprochenen Empfehlungen übernommen, ebenso wenig im Hinblick auf unvorhergesehene Veränderungen, welche die Bewertungen und Empfehlungen der Studie beeinflussen. Berlin Risk übernimmt auch keine Haftung für jegliche Forderungen und Schäden, die aus einer unerlaubten Weitergabe von Informationen, die in dem Bericht enthalten sind, resultieren. Außerdem übernimmt Berlin Risk Ltd. ausdrücklich keine Haftung für jegliche direkten oder indirekten Verluste, die mit dem Inhalt der Studie oder der darauf bezogenen Kommunikation in Zusammenhang stehen könnten.

Berlin Risk

Berlin Risk ist ein Beratungsunternehmen, das Kunden bei der Einschätzung politischer Risiken und der Erfüllung von Compliance-Anforderungen unterstützt. Dies umfasst Geschäftspartnerprüfungen und Fragen der Bekämpfung von Korruption, Geldwäsche, Betrug und die Verhinderung von Steuerhinterziehung. Zu den Kunden zählen Finanzinstitutionen, Unternehmen und Investoren sowie öffentliche Institutionen, Anwaltskanzleien und Nichtregierungsorganisationen.

Berlin Risk, das an den Standorten Berlin und Frankfurt am Main vertreten ist, ist Mitglied des europäischen Konsortiums BCF Partners.

Weitere Informationen sind hier zu finden: *www.berlinrisk.com*

Counter Extremism Project (CEP)

Das Counter Extremism Project (CEP) ist eine gemeinnützige, überparteiliche internationale Organisation, die das Ziel verfolgt, der Bedrohung durch extremistische Ideologien entgegenzuwirken und pluralistisch-demokratische Kräfte zu stärken. CEP befasst sich mit Extremismus in jeglicher Form – dazu gehören sowohl islamistischer Extremismus/Terrorismus als auch Rechts- und Linksextremismus/Terrorismus. CEP übt dazu durch eigene Recherchen und Studien Druck auf finanzielle und materielle Unterstützungsnetzwerke von extremistischen und terroristischen Organisationen aus, arbeitet den Narrativen von Extremisten und Terroristen sowie ihren Rekrutierungstaktiken im Internet entgegen, entwickelt bewährte Praktiken (good practices) zur Reintegration von Extremisten und Terroristen, und wirbt für effektive Regulierungen und Gesetze.

Neben Büros in den Vereinigten Staaten verfügt CEP über Standorte in Berlin, London und Brüssel. Die Aktivitäten von CEP werden geleitet von einer internationalen Gruppe ehemaliger Politiker, leitender Regierungsbeamter und Diplomaten. CEP unterstützt politische Entscheidungsträger bei der Ausarbeitung von Gesetzen und Vorschriften zur wirksamen Prävention und Bekämpfung von Extremismus und Terrorismus zu unterstützen, insbesondere auch im Bereich der Bekämpfung der Finanzierung des Terrorismus.

Weitere Informationen sind hier zu finden: *www.counterextremism.com/German*

Cryptocurrencies as Threats to Public Security and Counter Terrorism: Risk Analysis and Regulatory Challenges

Berlin, April 2020

English Summary

The rise of Bitcoin and other cryptocurrencies poses new challenges for the fight against money laundering and terrorist financing (AML/CFT). Cryptocurrencies provide their users with the opportunity to make global payments that are beyond the control of financial regulators and security authorities. In addition, there is a growing risk that terrorist financiers may evade state surveillance and tap into new sources of funding.

Recent evidence demonstrates that terrorist groups and their supporters have become increasingly familiar with the new technology. Terrorists use it to launder money or try to find new sources of finance, as a number of recent examples of fundraising by terrorist groups illustrate. We are still at an early stage of the development of this new threat, but the technical capabilities and capacities of terrorist groups close to ISIS or Hamas, for example, are progressing rapidly. For example, there have been several reported cases of terrorist groups using automatic address-generating software for cryptocurrency wallets to call for donations. None of these new addresses, which have not yet received payments, can be found on the blockchain.

Consequently, the long held assumption that Bitcoin may not be suitable for illegal activities due to traceability or lack of liquidity is put into question. Various technical means are available to cryptocurrency users to conceal financial flows and protect against forensic analysis of the blockchain, such as the use of anonymizing services called ‘mixers’ or ‘tumblers’. Furthermore, cryptocurrencies known as Privacy Coins allow increased technical protection and encryption of the identity of the sender and the recipient of funds.

In mid-2019, governments agreed on a joint response at the level of the Financial Action Task Force (FATF), the international standard setter in the field. The new FATF recommendations are aimed at an effective regulation of crypto exchanges, the crucial interface between the sphere of cryptocurrencies and fiat currencies. AML/CFT standards that apply to traditional financial transactions should, as far as possible, also cover blockchain financial services. Ultimately, the plan is to put an end to anonymous crypto transactions. The Wire Transfer Rule, also called the ‘Travel Rule’, requires states to take precautions to ensure that Virtual Asset Service Providers (VASPs) monitor and share customer data among themselves and with the relevant government authorities.

At present, the crypto industry is faced with the task of finding technological solutions to operationalize these new compliance standards and establish appropriate Know Your Customer (KYC), due diligence and reporting procedures.

Both governments and companies have one year to comply with the new rules. In the European Union, the adoption of the new FATF recommendations coincided with the need to implement the latest EU anti-money laundering directive (AMLD5). In Germany, new legal rules on crypto assets came into force on 1 January 2020. Crypto companies are now obliged to fulfil KYC requirements and report suspicious transactions to the German financial intelligence unit (FIU). Germany and other countries seem to be on the right track to prevent the practice of anonymous crypto transactions, which poses serious security risks. It should be noted, however, that a legal, and yet unregulated crypto payment system still exists. Additional regulation is required, in particular regarding the use of unhosted wallets.

The study makes a number of recommendations aimed at increasing the effectiveness of the agreed measures. Countries like Germany continue to face the difficult task of keeping pace with the high speed at which crypto technology is developing. It is therefore essential to increase the expertise and technical capabilities available to German regulatory authorities. The overlap of responsibilities between various German authorities in the area of AML/CFT should be reduced and ideally eliminated. The relevant functions, including prosecutorial responsibilities, expertise and capacity, should be pooled and integrated where possible.

Regulators must also pay attention to and demand more efforts from crypto companies in terms of regulatory compliance and testing of emerging industry procedures. Both sides should cooperate to find an appropriate way to comply with the new FATF rules. Finally, investigating authorities and VASPs should consult each other and develop typologies and indicators for terrorist financing methodologies and potential asset storage operations in the field of crypto transactions.

Recently, there have been first initiatives at the EU level to harmonize the entire crypto sector more effectively. Germany should actively participate in this, but in the meantime, it should not fail to catch up in the area of AML/CFT and develop its own structures and capacities with regard to cryptocurrencies without waiting for EU regulations to materialize.

1 Vorbemerkung

Diese Studie handelt von den speziellen Herausforderungen, die mit dem weltweiten Aufkommen von Bitcoin und anderen Kryptowährungen für den Bereich der Bekämpfung der Geldwäsche und Terrorismusfinanzierung (AML/CFT) [1] verbunden sind. Der zweitgenannte Punkt, den man als Spezialfall der Geldwäschebekämpfung auffassen kann, soll dabei im Vordergrund stehen. Genauer besehen ist die Terrorismusfinanzierung als ein gesondertes Phänomen zu betrachten, das aus praktischen Gründen meist im engen Kontext mit Geldwäsche betrachtet wird.

Unter Terrorismusfinanzierung ist im weitesten Sinne die Bereitstellung oder Sammlung finanzieller Mittel zu verstehen, die ganz oder teilweise zu terroristischen Zwecken verwendet werden oder verwendet werden sollen.[2] Dies kann die Unterstützung von Einzeltätern und Terrorgruppen betreffen, die oftmals sogar öffentlich auftreten und ihre politische Propaganda verbreiten, ebenso wie die Finanzierung konkreter Anschläge bzw. der Vorbereitungen für Gewaltakte und andere Straftaten durch Terroristen. Anders als bei ‚normaler' Geldwäsche, um einen weiteren Unterschied hervorzuheben, spielen bei der Terrorismusfinanzierung schon kleinere Geldmittel eine Rolle, wie sie etwa für die Beschaffung einer Tatwaffe benötigt werden.

Bezüglich der Kryptowährungen – gemeint sind kryptographisch abgesicherte digitale Zahlungsmittel, die auf der Blockchain-Technologie basieren[3] – geht es zunächst darum, sich mit einigen grundlegenden Fakten und verschiedenen Merkmalen des Kryptofinanzsektors vertraut zu machen, die für die Fragestellung relevant sind. Im nächsten Schritt ist das Risikopotenzial zu prüfen, wieweit Bitcoin und andere Kryptowährungen im Zusammenhang mit Terrorismusfinanzierung tatsächlich als gefährlich eingestuft werden müssen. Liegen bereits konkrete Erfahrungen vor, was die Nutzung von Kryptowerten durch terroristische Gruppen und Organisationen betrifft? Haben Terroristen und ihre Unterstützer damit begonnen, die neue Technologie anzuwenden, um auf diese Weise der Überwachung durch staatliche Behörden auszuweichen und sich neue Finanzierungsquellen zu erschließen?

In den letzten Jahren wurde eine international abgestimmte Reaktion vor allem auf Ebene der Europäischen Union, der Financial Action Task Force (FATF) sowie der G7 verabredet, um die Regulierung des Kryptosektors auf verschiedenen Ebenen voranzutreiben. Diese Bemühungen sollen hier aus der spezifischen AML/CFT-Perspektive heraus näher betrachtet werden. Welche Maßnahmen wurden beschlossen, und welche Handlungsaufträge lassen sich daraus für die staatliche Seite und die betroffenen deutschen Kryptounternehmen ableiten?

[1] Die Abkürzung steht für Anti-Money Laundering / Combating the Financing of Terrorism.
[2] Eine ausführliche Definition enthält z.B. das Strafgesetzbuch (§ 89c Terrorismusfinanzierung). https://www.gesetze-im-internet.de/stgb/__89c.html
[3] Zur näheren Begriffsbestimmung siehe den nächsten Abschnitt.

Die Studie endet mit einer Reihe von Empfehlungen. Die Vorschläge zielen darauf ab, die Wirksamkeit der geplanten Schritte im Bereich der Bekämpfung der Geldwäsche und Terrorismusfinanzierung zu erhöhen. Kryptowährungen bilden heute einen so faszinierenden wie umstrittenen Bereich der Finanzwelt. Deutschland und seine Partner stehen vor der nicht einfachen Aufgabe, Schritt zu halten mit dem hohen Tempo, mit der sich die den Kryptowerten zugrunde liegende Technologie weiterentwickelt.

2 Die Blockchain-Technologie verändert die Finanzwelt

Die Entwicklung der Kryptowährungen, die im Jahr 2008 mit der Veröffentlichung des Bitcoin White Paper[4] begann, steht auch ein Jahrzehnt später relativ gesehen in einer frühen Phase. Die Verbreitung des Kryptogeldes ist, zumindest im Vergleich zu den sogenannten Fiatwährungen[5], noch begrenzt. Einige Webseiten, darunter coinmarketcap.com, gaben mit Stand von Anfang Februar 2020 an, dass sich die Gesamtkapitalisierung der bis zu 2500 einzelnen Kryptocoins auf rund 270 Milliarden Dollar beläuft. Die meisten Kryptocoins führen dabei nur ein Schattendasein. Dagegen beträgt, auf alle Kryptowährungen bezogen, der weltweite Marktanteil von Bitcoin derzeit mehr als 60 Prozent. Der Bitcoin-Anteil an allen Kryptotransaktionen, die einen vermuteten kriminellen Hintergrund aufweisen, soll sogar deutlich höher liegen. Schätzungen von Experten belaufen sich auf bis zu 95 Prozent.[6]

Wenn nachfolgend von Kryptowährungen oder Kryptowerten die Rede ist, ist dies überwiegend mit Bitcoin gleichzusetzen. Von den Gründen dafür, dass auch Terroristen Bitcoins bevorzugen, wird noch die Rede sein. Terminologisch gesehen, verwenden die seit Januar 2020 in Deutschland geltenden neuen gesetzlichen Regelungen, mit denen die jüngste EU-Geldwäscherichtlinie umgesetzt wird[7], den von der Richtlinie definierten neutralen Begriff ‚Kryptowerte'. Die Änderungsrichtlinie zur Vierten EU-Geldwäscherichtlinie (zumeist Fünfte Geldwäscherichtlinie genannt) definiert Kryptowerte umständlich als „digitale Darstellung eines Werts, die von keiner Zentralbank oder öffentlichen Stelle emittiert wurde oder garantiert wird und nicht zwangsläufig an eine gesetzlich festgelegte Währung angebunden ist und die nicht den gesetzlichen Status einer Währung oder von Geld besitzt, aber von natürlichen oder juristischen Personen als

[4] Satoshi Nakamoto [Pseudonym des unbekannten Bitcoin-Erfinders]: Bitcoin: A Peer-to-Peer Electronic Cash System https://bitcoin.org/bitcoin.pdf
[5] Als Fiatwährungen werden von Regierungen festgelegte Zahlungsmittel bezeichnet, die nicht an den Preis eines Rohstoffs wie Gold oder Silber gebunden sind. Der Begriff ‚fiat' leitet sich vom lateinischen Wort für ‚gemacht werden' bzw. ‚entstehen' ab.
[6] Diese Angabe („95% of the cryptocurrency cases law enforcement investigates") stammt aus einem TV-Interview mit Jonathan Levin, Mitgründer von Chainalysis, einer führenden Firma für Blockchain-Forensik (Bitcoin Accounts for 95% of Cryptocurrency Crime, Says Analyst, fortune.com, 24.4.2019) https://fortune.com/2019/04/24/bitcoin-cryptocurrency-crime/
[7] Von den im Januar 2020 in Kraft getretenen Änderungen betroffen sind vor allem das Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäschegesetz) und das Gesetz über das Kreditwesen.

Tauschmittel akzeptiert wird[8] und die auf elektronischem Wege übertragen, gespeichert und gehandelt werden kann."[9]

Dazu muss man wissen, dass Kryptowährungen rechtlich gesehen keine Währungen sind, weil sie nicht von einem Staat oder einer Zentralbank herausgegeben werden.[10] Der Basler Ausschuss für Bankenaufsicht legt Wert auf die Feststellung, dass Krypto-Vermögenswerte die Standardfunktionen des Geldes als Tauschmittel oder Wertspeicher nicht zuverlässig erfüllen.[11] So sprechen Politiker und Regulierer lieber von Kryptowerten bzw. Krypto-Assets. Unter diesen Begriff fallen nicht nur Kryptowährungen, sondern auch andere digitale Token, die verschiedenste Vermögenswerte abbilden können.

Mit dem Begriff Token wird jede digitale Wertmarke bezeichnet, die ein Wertobjekt repräsentiert oder die Nutzung bestimmter Dienste zulässt. Oftmals wird Token als Oberbegriff verwendet, der Kryptocoins miteinschließt.[12] Digitale Token können grundsätzlich jedes beliebige vorhandene Wertobjekt darstellen, etwa eine Immobilie, Aktien und andere Wertpapiere (Security Token). Ferner können sie den Zugang zu einer bestimmten Software oder Dienstleistung gewähren (Utility Token). Bei der Ausgabe digitaler Token dominiert übrigens bisher das Ethereum-Netzwerk, das verbunden ist mit Ether, der nach Marktwert zweitgrößten Kryptowährung. Die Programmiermöglichkeiten von Ethereum erleichtern die sogenannten Smart Contracts (das sind Programme, die automatisierte Rechtsgeschäfte ermöglichen) und damit eine detailgenaue Beschreibung und Erzeugung von Token aller Art.[13]

Der Handel mit Security Token, die ebenso wie Kryptogeld-Guthaben als Vermögens-speicher dienen können, ist offensichtlich relevant für die Geldwäschebekämpfung. Trotzdem stehen digitale Token für das hier behandelte Thema weniger im Fokus. Stattdessen wirken sich technische Design-Unterschiede zwischen Bitcoin und anderen Kryptowährungen auf die Bekämpfung von Geldwäsche und Terrorismusfinanzierung aus. Um der Klarheit willen wird im Weiteren meist von Kryptowährungen die Rede sein. Das entscheidende Kriterium ist, dass diese Cryptocurrencies an den dafür vorgesehenen Handelsplattformen gegen Fiatgeld getauscht werden können. Genau an diesem Punkt setzen auch die bisher geplanten Regulierungsmaßnahmen von staatlicher Seite an.

---

[8] Im geänderten deutschen Kreditwesengesetz wird hinzugefügt: „oder Anlagezwecken dient".
[9] 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 und zur Änderung der Richtlinien 2009/138/EG und 2013/36/EU https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32018L0843&from=DE
[10] Kryptowährungen werden in Deutschland rechtlich als „immaterielle Wirtschaftsgüter" behandelt.
[11] Basel Committee on Banking Supervision: Statement on crypto-assets, 13.3.2019 https://www.bis.org/publ/bcbs_nl21.htm
Der Basler Ausschuss setzt sich aus Vertretern von Zentralbanken und Bankenaufsichtsbehörden der G10-Staaten zusammen.
[12] Der Begriff Token ist von den älteren physischen Token abgeleitet. Das sind z.B. spezielle Münzen bzw. Wertmarken für die Nutzung des öffentlichen Verkehrs oder Jetons in Spielcasinos. Mit einem Token Sale oder der Tokenisierung eines Vermögenswerts wird bezweckt, Wertobjekte ähnlich effizient über das Internet zu versenden, wie dies bei Kryptogeld der Fall ist.
[13] Aaron Koenig: Die dezentrale Revolution. Wie Bitcoin und Blockchain Wirtschaft und Gesellschaft verändern, FinanzBuch Verlag, München 2019, S. 99f.

Bitcoin (der Name meint zugleich die Werteinheit und das Protokoll zur sicheren Speicherung und Übertragung der Bitcoins) und den meisten anderen Kryptowährungen liegt die Blockchain-Technologie zugrunde. Die Blockchain funktioniert als dezentrale und nahezu fälschungssichere Datenbank, die über das Internet von einem Peer-to-Peer-Netzwerk verwaltet wird. Die Anwender von Bitcoin und den meisten Kryptowährungen, die an Bitcoin angelehnt sind, verwenden einen privaten Schlüssel, der nur ihnen selbst bekannt ist, und einen öffentlichen Schlüssel. Für den öffentlichen Schlüssel können Nutzer ein oder mehrere Pseudonyme wählen, um während der öffentlichen Transaktion ihre Privatsphäre zu schützen. Im Ergebnis wird ein Zahlungsverkehr ohne Finanzintermediär ermöglicht, bei dem erfolgte Transaktionen in einem dezentralen Transaktionsbuch („distributed ledger“) [14] nachverfolgt werden können. Die Blockchain ist die bekannteste Distributed-Ledger-Technologie. Vereinfachend werden beide Begriffe häufig synonym verwendet. [15] Sämtliche Transaktionen, für die eine Blockchain ausgelegt ist, werden chronologisch erfasst und verschlüsselt. Nach einem gesicherten Verifizierungsverfahren entstehen neue Informationsblöcke, die nacheinander in die bestehende Kette eingefügt werden.

Kryptowährungen hatten bisher allerdings mit hohen Wertschwankungen zu kämpfen. Nach 2017, dem ‚Jahr des Bitcoin‘, stürzte die führende Kryptowährung ab, wobei es die meisten Konkurrenten, auch Altcoins genannt, zumeist noch deutlich stärker traf. Auch wenn sich der Bitcoin-Kurs danach wieder erholt hat, wird seitdem oft die Frage gestellt, ob Kryptowährungen nicht primär ein riskantes Spekulationsobjekt sind. Demgegenüber stehen jedoch die Vorteile, die der Krypto-Zahlungsverkehr verheißt. Es handelt sich um eine extrem innovative Finanztechnologie, die grenzüberschreitende Transaktionen ohne Zeitverlust möglich macht. Eine der attraktiven Anwendungsmöglichkeiten ist der direkte und nahezu kostenfreie Transfer von Währungsäquivalenten in ärmere Staaten, in welchen vielen Empfängern keine Bankinfrastruktur zur Verfügung steht. Generell gehen die Meinungen über die Vorzüge der ganzen Technologie auseinander. Im September 2017 nannte der Chef von JPMorgan, Jamie Dimon, Bitcoin öffentlich einen „Betrug“, änderte jedoch bald danach seine Meinung wieder. Im Februar 2019 kündigte Dimon sogar an, die amerikanische Großbank wolle sich mit an die Spitze der Entwicklung setzen und einen an den Dollar gekoppelten digitalen Coin einführen.[16]

2.1 Die Vision vom „Geld ohne Staat”

Nicht zu übersehen ist eine große Schattenseite. Kryptowährungen verschaffen ihren Nutzern die Gelegenheit, Zahlungen bei Bedarf abseits vom Zugriff der Finanzaufsicht und der Sicherheitsbehörden vorzunehmen. Damit entsteht ein Widerspruch zwischen

[14] Distributed Ledger kann wörtlich mit ‚verteiltes Kassenbuch‘ bzw. ‚verteiltes Register‘ übersetzt werden.
[15] So werden in der Blockchain-Strategie der Bundesregierung beide Ausdrücke, Blockchain und Distributed-Ledger-Technologien, gleichbedeutend verwendet.
[16] Matt Egan: Jamie Dimon hated bitcoin. Now JPMorgan is getting ahead of the crypto revolution, CNN, 15.2.2019 https://cnn.com/2019/02/15/investing/jpmorgan-bitcoin-crypto-jamie-dimon/index.html

dem technischen und funktionalen Design des virtuellen Geldes und dem Grundprinzip einer wirksamen Regulierung des Finanzverkehrs.

Das verwundert nicht, wenn man die politische Stoßrichtung berücksichtigt, die dem Bitcoin-Projekt seit Beginn zugrunde liegt. Der deutsche Bitcoin-Aktivist Aaron Koenig veröffentlichte schon im Jahr 2015 ein Buch, das die Nähe des Ansatzes von Bitcoin, dem „Geld ohne Staat", zur Österreichischen Schule der Volkswirtschaft in den Mittelpunkt rückt. Deren theoretisches Ideal ist auf eine maximale Freiheit privater Eigentumsrechte gerichtet. Jeder staatlichen Aktivität und Kontrolle wird Misstrauen entgegengebracht. Dies erstreckt sich auch auf das Gebiet der Finanzen. So kritisieren die ‚Austrians' die ab den 1930er Jahren in den westlichen Ländern eingeleitete Abkehr von einer goldgedeckten Währung zugunsten staatlich kontrollierter Fiatwährungen. Regierungen bzw. Zentralbanken werde dadurch eine praktisch unbegrenzte Geldschöpfung und Verschuldung ermöglicht.[17] Im Vorwort zu dem erwähnten Buch, das der FDP-Politiker Frank Schäffler beisteuerte, heißt es, Friedrich August von Hayek und Bitcoin seien „wie Vater und Sohn". Bitcoin setze von Hayeks Ziel eines freien Währungswettbewerbs unter Einschluss privater Währungen in einer Weise um, die sich dieser nicht habe vorstellen können.[18]

Christoph Bergmann, dem eine aufschlussreiche Darstellung der Geschichte von Bitcoin zu verdanken ist, formuliert ähnlich. Der unbekannte Bitcoin-Erfinder habe ein Geld erschaffen, das „die kühnsten Träume der ‚Österreicher' übertrifft."[19] Diese waren früher häufig (oder sind es heute noch) Verfechter einer goldgedeckten Währung. Angelehnt an die Verhältnisse beim Gold, ist bei Kryptowährungen der Bitcoin-Familie die Beschränkung der virtuellen Geldmenge. Außerdem gibt es die sogenannten Miner, die für die Verifizierung der abgelaufenen Transaktionen Rechnerleistung zur Verfügung stellen und dafür mit neu ‚geschürften' Bitcoins belohnt werden.

Die libertären Vorstellungen, denen Anhänger der Österreichischen Schule oftmals anhängen, sind bei vielen Vertretern der Bitcoin- und Kryptogemeinde in Nordamerika und Europa anzutreffen. Haben Liberale meist ein differenziertes Staatsverständnis, nehmen Libertäre vielfach eine geradezu staatsfeindliche Haltung ein. Die Rolle staatlicher Institutionen, aber auch der etablierten Banken und zentral kontrollierter Konzerne, soll soweit möglich zurückgedrängt werden. In dieser Gedankenwelt steht das Ziel größtmöglicher individueller Freiheit im Vordergrund. Dies soll ausdrücklich die Option einschließen, finanzielle Transaktionen unbehindert von staatlicher Kontrolle oder dem negativ beurteilten Einfluss der Zentralbanken auszuführen.

[17] Auf Nachweise wird hier verzichtet. Die Österreichische Schule, die ursprünglich auf die von Carl Menger in den 1870er Jahren begründete Grenznutzenschule zurückgeht, hat im 20. Jahrhundert in Europa und den USA verschiedenste Ausprägungen erfahren. Als berühmtester Vertreter gilt Friedrich August von Hayek (1899-1992).
[18] Frank Schäffler, Vorwort, in: Aaron Koenig: BITCOIN – Geld ohne Staat: Die digitale Währung aus Sicht der Wiener Schule der Volkswirtschaft, FinanzBuch Verlag, München 2018 (4. Aufl.), S. 9-13. Schäffler nimmt Bezug auf von Hayeks im Jahr 1976 erschienenes Buch „Entnationalisierung des Geldes".
[19] Christoph Bergmann: Bitcoin. Die verrückte Geschichte vom Aufstieg eines neuen Geldes, Moby Verlagshütte, Nersingen 2019 (2. Aufl.), S. 145

Man muss einschränken, dass es daneben zahlreiche Akteure im Kryptobereich gibt, die ideologisch ganz anders bzw. unpolitisch ausgerichtet sind. Darunter sind Investoren oder z.B. Betreiber von Kryptounternehmen, die kommerzielle Interessen verfolgen. Und natürlich gibt es selbst unter Ökonomen, die in der Tradition der Österreichischen Schule stehen, manche Bitcoin-Skeptiker. Aus Sicht ihrer Befürworter sind Kryptowährungen jedenfalls nicht bloß als technisch ausgereiftes digitales Geld zu verstehen. Vielmehr sollen sie in Konkurrenz zu staatlichen Fiatwährungen treten und deren Vorherrschaft beenden. Und es sind nicht nur die Kryptowährungen – auch mit anderen diskutierten Blockchain-Anwendungen sind ähnliche Ideen verbunden, die auf das Zurückdrängen staatlicher Einflüsse abzielen. Die Blockchain-Technologie, so das zugespitzte Argument von Kritikern, sei in Wahrheit „eine als Technik getarnte Ideologie“.[20]

Ungeachtet der latenten politischen Konnotationen, haben westliche Regierungen den Aufstieg der Kryptowährungen lange Zeit nicht behindert, sondern abwartend beobachtet. Eine gewisse Anerkennung und teilweise Faszination für die neue Technologie spielten hier eine Rolle. Mit dem Aufkommen der Blockchain-Technologie werden Hoffnungen auf signifikante technische und ökonomische Veränderungen verbunden. Beim Weltwirtschaftsforum hält man die Einschätzung für realistisch, dass bis 2027 ein Zehntel des globalen Bruttoinlandsprodukts auf Blockchains gespeichert sein wird.[21]

Entsprechend stehen die Chancen einer künftigen „Token-Ökonomie“ im Mittelpunkt der im September 2019 veröffentlichten Blockchain-Strategie der Bundesregierung. Nicht nur in Deutschland tendiert die Politik jedoch dahin, den Fokus bei diesem Zukunftsthema nicht bei den Kryptowährungen bzw. Krypto-Token, sondern „jenseits von Bitcoin“ [22] zu suchen und andersgelagerte Anwendungsmöglichkeiten zu befürworten. Die Bundesregierung möchte, so heißt es in der Blockchain-Strategie, unter anderem eine Blockchain-basierte Energieanlagenanbindung an eine öffentliche Datenbank oder die Erprobung Blockchain-basierter Verifikation von Hochschulzertifikaten fördern. Untersucht werden soll, ob Blockchain-Technologie die Transparenz bei Liefer- und Wertschöpfungsketten erhöhen kann. Eine Abwehrhaltung gegen die Kryptowerte kommt darin zum Ausdruck, dass die Bundesregierung sich dagegen einsetzen will, dass Stablecoins – und das gilt implizit damit für die ‚instabilen‘ Kryptowährungen – eine Alternative zu staatlichen Währungen werden.[23]

Zugleich ist angekündigt, das deutsche Recht für elektronische Wertpapiere zu öffnen, was sich zunächst nur auf elektronische Schuldverschreibungen erstrecken soll. Ein entsprechendes Gesetz soll bis Ende der Legislaturperiode in Kraft treten. [24] Im

[20] Michael Seemann: Digitaltechnologie Blockchain. Eine als Technik getarnte Ideologie, 15.3.2018 https://www.deutschlandfunkkultur.de/digitaltechnologie-blockchain-eine-als-technik-getarnte.1005.de.html?dram:article_id=413022
[21] Margaret Leigh Sinrod: Still don't understand the blockchain? This explainer will help, 9.3.2018 https://www.weforum.org/agenda/2018/03/blockchain-bitcoin-explainer-shiller-roubini/
[22] Blockchain-Strategie der Bundesregierung. Wir stellen die Weichen für die Token-Ökonomie, S. 3 www.blockchain-strategie.de
[23] Ebd., S. 8
[24] „Politik zu zaghaft. Gesetzentwurf für Blockchain verzögert sich“, Frankfurter Allgemeine Zeitung, 15.11.2019

Gegensatz zur eher zögernden Haltung, die in Deutschland vorherrscht, hat Liechtenstein, das für eine kryptofreundliche Haltung bekannt ist, als erstes europäisches Land ein Blockchain-Gesetz beschlossen, das Anfang 2020 in Kraft trat. Es bleibt abzuwarten, ob der damit verbundene ehrgeizige Versuch, eine einheitliche Rechtsgrundlage für die Token-Ökonomie zu schaffen, Schule macht.[25]

Trotz vieler interessanter Ideen und Projekte sind Kryptowährungen bislang die einzige kommerziell erfolgreiche Anwendung der Blockchain-Technologie. Unterdessen stören sich nicht nur in westlichen Ländern die Politik und die Regulierer daran, dass die angestrebte Anonymität finanzieller Transaktionen ein Leitprinzip der meisten Kryptowährungen bildet. Von Anhängern der Kryptoszene wird die Gefahr zumeist vernachlässigt oder geleugnet, dass mit dem Wachstum potenziell anonymer Kryptowährungen unweigerlich der Geldwäsche und Terrorismusfinanzierung Tür und Tor geöffnet wird. Der Regulierung im AML/CFT-Bereich begegnet die Kryptoszene überwiegend skeptisch. Dahinter wird ein Versuch von Seiten der Regierungen vermutet, die gesamte Dynamik hinter dem Aufstieg der Kryptocoins zu aufzuhalten.

Diese Argumentation vermischt sich bei Bitcoin-Anhängern gelegentlich mit dem Eingeständnis der politischen Sprengkraft der Kryptowährungen. In seinem Buch über die Geschichte des Bitcoin räumt Christoph Bergmann ein, die Bitcoin-Szene habe lange Zeit, bis ungefähr 2017, mit der Gefahr eines weltweiten Bitcoin-Verbots gerechnet.[26] Langfristig drohe den Regierungen mit dem Aufstieg der Kryptowährungen weltweit die Kontrolle der Finanzströme zu entgleiten. Die Möglichkeiten zur Steuerflucht würden radikal vereinfacht. Finanzsanktionen oder Anordnungen, Geld einzufrieren, könnten zukünftig aufgrund mangelnder Jurisdiktion ins Leere laufen. Nicht überraschend sei daher, dass sich besonders Staaten, die von Sanktionen betroffen oder bedroht sind wie z.B. der Iran, Nordkorea und nicht zuletzt China[27] besonders für die Blockchain-Technologie interessierten. Die Vormacht der traditionellen Finanzinstitutionen wird herausgefordert. Was bedeuten die Regeln gegen Geldwäsche und Terrorismusfinanzierung noch, fragt Bergmann, wenn es in Zukunft keine Intermediäre mehr benötige, um sie umzusetzen?[28] Kryptobörsen und Handelsplattformen, so lautet eine naheliegende Antwort, müssen letztlich zu Helfern der Strafverfolgung werden – und dazu verpflichtet werden, einen ähnlichen Beitrag wie traditionelle Finanzinstitute zu leisten.

2.2 Die Rolle der Kryptobörsen und Handelsplattformen

Die Grundtendenz von Bitcoin und anderen Kryptowährungen geht dahin, die Stellung der Intermediäre, also der Finanzinstitute, im Zahlungsverkehr überflüssig zu machen.

[25] Christopher Klee: Durchbruch im Crypto Country: Liechtenstein verabschiedet Blockchain Act, BTC-Echo, 3.10.2019 https://www.btc-echo.de/durchbruch-im-crypto-country-liechtenstein-verabschiedet-blockchain-act/
[26] Bergmann: Bitcoin. Die verrückte Geschichte vom Aufstieg eines neuen Geldes, S. 282
[27] Siehe z.B. die Meldung „China emittiert Blockchain-Anleihe“, Frankfurter Allgemeine Zeitung, 11.12.2019
[28] Bergmann: Bitcoin. Die verrückte Geschichte vom Aufstieg eines neuen Geldes, S. 263ff.

Der Handel und Umgang mit Kryptowährungen sind praktisch gesehen für die Nutzer aber immer noch anspruchsvoll. Und tatsächlich sind deshalb sogar neue spezialisierte Intermediäre entstanden. So besteht ein Paradox der bisherigen Entwicklung der Kryptowährungen darin, dass bis zum Jahr 2018 nach Ansicht von Experten 99 Prozent der Kryptotransaktionen über zentralisierte Kryptobörsen abgewickelt wurden. Der oft vorhergesagte Trend hin zu den dezentralisierten Exchanges, welche dem Grundgedanken der Blockchain-Technologie besser entsprechen, hatte bis dahin anscheinend noch nicht eingesetzt.[29] Die derzeitige Marktdominanz zentralisierter Handelsplattformen, an denen Kryptogeld typischerweise auch gegen Fiatwährungen getauscht wird, begünstigt daher den in Aussicht genommen Regulierungsrahmen.

Die vielfältigen Varianten von bestehenden Kryptobörsen (Exchanges) und Handelsplattformen können an dieser Stelle nur kurz skizziert werden. Ein Unterschied zwischen Kryptobörsen und dezentralen Handelsplattformen besteht darin, ob die Nutzer ihren privaten Schlüssel kontrollieren, wie das bei den dezentralen Exchanges der Fall ist, oder nicht. Eine andere wichtige Unterscheidung richtet sich danach, ob jeweils nur Kryptowährungen gehandelt werden können oder ob auch der Umtausch zwischen Fiatwährungen und Kryptogeld ermöglicht wird. Solche Fiat-zu-Krypto-Börsen werden in der Fachsprache als Fiat On-Ramps bezeichnet. Um dort Kryptogeld zu erwerben, ist es erforderlich, dass Kunden etablierte Zahlungswege nutzen, typischerweise Überweisungen vom Bankkonto oder mit Kreditkarte. Für Kunden der Kryptobörsen bedeuten diese Schnittstellen ein Sicherheitsrisiko, weil die privaten Schlüssel der Adressen, auf die Bitcoins eingezahlt werden, von den Börsenbetreibern gehalten werden.

Die Geschichte der Kryptowährungen kennt viele Fälle gehackter Kryptobörsen. Kriminellen ist es wiederholt gelungen, Sicherheitslücken auszunutzen und von Kundenadressen Kryptogeld in großer Höhe abzuzweigen.[30] So wurden z.B. im August 2016 von der in Hongkong ansässigen Bitfinex-Börse fast 120.000 Bitcoins im Wert von damals 60 Millionen Dollar geraubt. Die Täter blieben unbekannt. Der erste berühmte Fall betraf die japanische Börse Mt.Gox, über die Anfang 2014 der Großteil des weltweiten Bitcoin-Handelsvolumens abgewickelt wurde. Bei diesem ebenfalls bis heute nicht aufgeklärten Hack verschwand eine Summe von 740.000 Bitcoins, rund 6 Prozent aller damals existierenden Bitcoins und nach heutigem Kurs umgerechnet ein größerer Milliardenwert.[31]

Was die Bekämpfung von Geldwäsche und Terrorismusfinanzierung betrifft, bieten Fiat On-Ramps auf der anderen Seite den Vorteil, dass sie den für Finanzinstitute geltenden Regeln für Geldwäschebekämpfung unterliegen. Kunden müssen entsprechend im Sinne der KYC-Erfordernisse (Know your customer) durch Vorlage von Dokumenten usw.

[29] Nathan Sexer: State of Decentralized Exchanges, 2018 https://media.consensys.net/state-of-decentralized-exchanges-2018-276dad340c79
[30] In der Darstellung von Robert A. Küfner (Das Krypto-Jahrzehnt. Was seit dem ersten Bitcoin alles geschehen ist – und wie digitales Geld die Welt verändern wird, Börsenbuchverlag, Kulmbach 2018) sind verschiedene Fälle erwähnt, darunter auch Bitfinex (S. 138).
[31] Andrew Norry: The History of the Mt Gox Hack: Bitcoin's Biggest Heist, blockonomi.com, 7.6.2019 https://blockonomi.com/mt-gox-hack/

identifiziert werden. Dies ist nicht zwingend der Fall bei den reinen Kryptobörsen, an denen Kryptowährungen untereinander getauscht werden können.

Bisher überwog bei diesen Exchanges oftmals eine ‚weichere' Praxis, Identitätsprüfungen wurden gar nicht oder jedenfalls nachlässiger als bei den Fiat On-Ramps vorgenommen. Kriminellen eröffnet das die Möglichkeit, verdächtige finanzielle Transaktionen teilweise im nichtregulierten Bereich durchzuführen. Die im Jahr 2019 beschlossene Einführung eines neuen regulatorischen Rahmens für den Kryptosektor sieht deshalb vor, die Anforderungen für Kryptobörsen und das damit verbundene Kryptoverwahrgeschäft, wie der neue deutsche Terminus lautet, soweit möglich den für Finanzinstitute geltenden Regeln anzunähern. Hierauf ist später näher einzugehen.

Es liegt auf der Hand, dass die Fiat On-Ramps sich als Ansatzpunkt für regulatorische Eingriffe anbieten. Effektive Maßnahmen im AML/CFT-Bereich lassen sich am einfachsten an den Stellen durchführen, wo Geld in normaler Währung in Kryptocoins umgewechselt wird und umgekehrt. Aber dies scheint nur eine Momentaufnahme. Je mehr der direkte Handel zwischen Kryptowährungen voranschreitet und sich generell die Verwendung von Kryptogeld als Zahlungsmittel auch im Güter- und Warenhandel ausbreitet, desto schneller dürfte die Bedeutung der Fiat-zu-Krypto-Börsen zurückgehen.

Eine weitere wichtige Unterscheidung erfolgt zwischen hergebrachten Kryptobörsen und solchen dezentralen Exchanges bzw. Plattformen, bei denen es möglich ist, Kryptocoins direkt zwischen Sender und Empfänger zu handeln, also ohne notwendige Vermittlung eines Intermediärs. Es gibt dann keine zentralen Server, auf denen die Kryptowerte liegen. Unerwünschte Angreifer werden so besser abgehalten – und zugleich ist staatlichen Behörden der Zugriff erschwert. Preise können zwischen Auftraggeber und Empfänger festgelegt werden. Allerdings findet der Handel immer noch so weit unter Aufsicht statt, als dass die Plattformen Informationen über die Identität von Auftraggeber und Empfänger und Art und Umfang der Transaktion sammeln. Diese dezentralen Kryptobörsen entsprechen der ursprünglichen Philosophie von Bitcoin und gelten in der Kryptogemeinde schon länger als die Zukunft des Handels mit Bitcoin und anderen Kryptowährungen.[32]

Schließlich gibt es den außerbörslichen OTC-Handel mit Kryptowerten (OTC ist die Abkürzung für ‚over the counter', übersetzt etwa ‚über den Ladentisch'), der auf spezieller Software basiert und bei dem Handelsplattformen überhaupt nicht mehr zwischengeschaltet sind. Bisher gehen Experten davon aus, dass Peer-to-Peer-Transfers nur einen relativ geringen Anteil am gesamten Kryptozahlungsverkehr haben, was sich in Zukunft jedoch ändern könnte. Eine der Besonderheiten solcher Transaktionen besteht darin, dass sie sich nicht auf den Wechselkurs einer Kryptowährung auswirken. Bei OTC-Trades können riesige Vermögenswerte den Besitzer wechseln. Die Handelspartner bleiben weitgehend anonym bzw. identifizieren sich nur gegenseitig. Bisher greifen theoretisch vorstellbare regulatorische Maßnahmen

[32] Phillip Horch: Dezentrale Börsen: Die Zukunft von Bitcoin, BTC-Echo, 29.9.2018 https://www.btc-echo.de/dezentrale-boersen-die-zukunft-von-bitcoin/

an dieser Stelle ins Leere. Ein denkbares Verbot des praktisch anonymen OTC-Kryptohandels erscheint wenig praktikabel. Es lässt sich aus heutiger Sicht nicht genau sagen, wie die Regulierungsbehörden auf diesen Trend am besten reagieren sollen.

Westliche Sicherheitsfachleute sind der Auffassung, die Rolle des OTC-Handels in Bezug auf Geldwäsche und Terrorismusfinanzierung werde derzeit noch vernachlässigt. Die Behörden seien sich grundsätzlich dieses Risikos bewusst, doch sei dieser neue Trend noch nicht genug im öffentlichen Fokus. Die Gefahr könnte schnell steigen, wenn der Kryptowährungsmarkt weiterwächst. Den westlichen Sicherheitsbehörden stünden teilweise schon spezielle Analysemethoden zur Verfügung, doch bleibe es schwierig, so die Warnung eines amerikanischen Fachmanns, den OTC-Kryptohandel genügend im Auge zu behalten.[33]

Wie intransparent das Geschehen am Kryptowährungsmarkt ist, bestätigte sich bei einem Vorgang am 6. September 2019, der international Schlagzeilen machte. In einem einzigen Trade erwarb ein Unbekannter 94.504 Bitcoins im Wert von rund einer Milliarde Dollar. Vom Wert her war dies die bislang größte Transaktion in der Geschichte der Blockchain-Währungen. Rund 0,5 Prozent aller existierenden Bitcoins wechselten den Besitzer. Die näheren Umstände des Vorgangs blieben im Dunklen. Experten vermuten dahinter den Versuch einer Kursmanipulation. Analysten fanden anscheinend nur heraus, dass ein erheblicher Teil der Bitcoins von Adressen stammte, die bei Huobi Global registriert sind, einer Kryptobörse mit Sitz in Singapur.[34]

Neben Kryptobörsen oder Handelsplattformen in Staaten, in denen der Kryptobereich bisher kaum reguliert wird, stehen Geldwäschern und Terrorismusfinanzierern weitere Wege offen, unbeobachtet vorzugehen. Zu erwähnen sind die mehr als 5.000 Bitcoin-Geldautomaten, von denen es bisher aber nur sehr wenige in Deutschland gibt. Kunden müssen sich erst bei Umtauschbeträgen von mehr als 500 Euro mit ihrem Ausweis identifizieren.[35] Weitere Schwachstellen aus Sicht der Geldwäschebekämpfung sind Prepaid-Debitkarten und Online-Gaming-Seiten, die Bitcoin oder andere Kryptowährungen als Zahlungsmittel zulassen. Schließlich ist in den letzten Jahren eine Gruppe neuer Kryptowährungen entstanden, sogenannte Privacy Coins, die explizit auf den Schutz der Privatsphäre und damit die Anonymität der durchgeführten Transaktionen abstellen.

[33] Interview, September 2019.
[34] Anthony Cuthbertson: Billion worth of bitcoin and no one knows why, The Independent, 13.9.2019 https://www.independent.co.uk/life-style/gadgets-and-tech/news/bitcoin-mystery-trade-cryptocurrency-market-transaction-blockchain-a9103611.html ; Daniel Eckert / Holger Zschäpitz: Wer steckt hinter dem Megatrade? Eine Milliardenorder für Bitcoin hat den Markt aufgeschreckt, Welt am Sonntag, 22.9.2019
[35] Im Mai 2019 standen in Deutschland erst vier solcher Bitcoin-Automaten. Phillip Horch: BTC kaufen: Bitcoin-Automaten (ATM) jetzt auch in Deutschland, in: BTC Echo, 2.5.2019 https://www.btc-echo.de/btc-kaufen-bitcoin-automaten-atm-nun-auch-in-deutschland/

2.3 ‚Pseudonymität' und die Möglichkeit der Blockchain-Analyse

Den Gefahren, die von Bitcoin und ähnlichen Kryptowährungen ausgehen, lässt sich entgegenhalten, dass die durchgeführten Transaktionen keineswegs anonym verlaufen. Stattdessen bietet Bitcoin nur den Schutz der sogenannten Pseudonymität. Prinzipiell machen Bitcoin-Nutzer ihr Finanzgebaren transparent und verwenden eine öffentliche Adresse. Sämtliche Transaktionen sind in der Blockchain dokumentiert. Folglich kann jede Transaktion zurückverfolgt werden. Dies umfasst die Anzahl an Coins, die erworben bzw. verkauft wurden. In der Bitcoin-Wallet bleiben auch die einzelnen verwendeten Bitcoins identifizierbar. Meistens müssen verschiedene ‚Münzen' kombiniert werden, und es fallen in der virtuellen Geldbörse ‚Münzsplitter' an, die bei nachfolgenden Transaktionen wieder verschmelzen können.[36] All diese Informationen lassen sich jedoch nicht ohne weiteres einem bestimmten Individuum zuordnen, zumal Nutzer dazu übergehen können, verschiedene Pseudonyme oder laufend wechselnde Wallet-Adressen zu verwenden.

Gelingt es, an irgendeiner Stelle die Verbindung zu einer bestimmten Person nachzuweisen – am einfachsten, wenn jemand öffentlich, etwa in den sozialen Medien, eine Adresse für Zahlungen bekannt gemacht hat – dann sieht die Sache anders aus. Dann lassen sich grundsätzlich sämtliche Bitcoins und Wallets ermitteln, die die betreffende Person jemals verwendet hat. Wurde nur eine Wallet verwendet, liegen praktisch alle Bitcoin-Transaktionen, die jemand ausgeführt hat, offen zutage. Eine umfassendere Analyse kann schließlich die Verbindungen zwischen verschiedenen benutzten Wallets aufzeigen. Seit mehreren Jahren sind spezialisierte Firmen auf dem Markt, die anbieten, die Bitcoin-Blockchain zu analysieren, durchgeführte Transaktionen forensisch zu untersuchen und schließlich die Inhaber der Bitcoin-Konten zu ermitteln. Staatliche Behörden in den USA und einigen anderen Staaten nutzen diesen spezialisierten Service bereits, um Geldwäsche zu verfolgen. Auch hinsichtlich der Terrorfinanzierung können Forscher durch eine Nachverfolgung der Kryptotransaktionen mehr über Finanzierungsmethoden und eventuell die Identität von Angehörigen der Terrornetzwerke erfahren.

Technisch versierten Experten gegenüber, ob es sich um Mitarbeiter staatlicher Stellen oder von diesen beauftragte Analysefirmen handelt, müssen Kriminelle also damit rechnen, dass die vermeintliche Anonymität von Kryptotransaktionen aufgehoben wird.[37] Für eine Zuordnung zu einer Person durch eine Untersuchung der Blockchain kommt es letztlich darauf an, mit welchem zeitlichen und sonstigen Aufwand die Ermittler bei der forensischen Analyse zu Werke gehen. Das Ausmaß der verfügbaren Informationen ließe sich noch steigern, soweit der Austausch von Benutzerinformationen zwingend vorgeschrieben wird.

[36] Bergmann: Bitcoin. Die verrückte Geschichte vom Aufstieg eines neuen Geldes, S. 284ff.
[37] Cynthia Dion-Schwarz, David Manheim, Patrick B. Johnston: Terrorist Use of Cryptocurrencies. Technical and Organizational Barriers and Future Threats, RAND Corporation, Santa Monica 2019, S. 24ff. https://www.rand.org/pubs/research_reports/RR3026.html

Selbst wenn eine Wallet ermittelt wird, von der im Ausland verdächtige Transaktionen erfolgen, bleibt die Schwierigkeit, solche Geldflüsse aufzuhalten bzw. Kryptowerte einzufrieren oder zu beschlagnahmen. Solange dafür keine weltweiten Regeln existieren, müssen Strafverfolgungsbehörden bei dem betreffenden Staat einen Antrag auf Rechtshilfe (MLA [38] request) stellen. Für eine effektive Bekämpfung der Terrorismusfinanzierung stellt dieses Verfahren kein adäquates Mittel dar, weil die Beantwortung zu lange dauern würde.[39]

Trotz der Möglichkeit einer nachträglichen forensischen Analyse der Blockchain können Bitcoin-Nutzer ihrerseits Schutzvorkehrungen treffen. Ihnen, darunter den Kriminellen, stehen technische Mittel und Wege zur Verfügung, die Zahlungsströme bei Bitcoin und anderen Kryptowährungen hochkomplex und unübersichtlich zu gestalten.

Die Anonymisierung der Transaktionen erfordert allerdings einigen technischen Aufwand, etwa die Nutzung von Anonymisierungsdiensten, die „Mixer“ oder „Tumbler“ genannt werden, oder der Software Darkwallet, die bereits entsprechende Funktionen umfasst.[40] Um Krypto-Schwarzgeld zu verschleiern, werden, etwa im Falle von Bitcoin, Einzelbeträge durch eine Abfolge von Adressen geschleust und anschließend neu zusammengefügt. Am Ende steht dann wieder scheinbar ‚sauberes‘ Kryptogeld. Im Verlauf der ganzen Operation werden verschiedene Darknet-Adressen[41] verwendet. Das Geld landet nach vielen Umwegen auf einer regulierten Kryptobörse und kann in Fiatgeld umgetauscht werden.

Mit Verwendung der Mixer wird gleichsam das „technische Bankgeheimnis“ gewahrt.[42] Demjenigen, der Kryptotransaktionen ausführt, wird es ermöglicht, sein ohne Einsatz der Mixer-Dienste theoretisch für jedermann transparentes (d.h. durch eine Blockchain-Analyse nachvollziehbares) Nutzerverhalten möglichst zu verschleiern. Dieses Bestreben ist für jeden sinnvoll, der um die eigene Sicherheit im Krypto-Zahlungsverkehr besorgt ist. Am Rande sei vermerkt, dass bereits Fälle von Entführungen und Überfällen bekannt wurden, die sich anscheinend gezielt gegen Menschen richteten, die dafür bekannt sind, Bitcoin zu besitzen. Viele reiche Bitcoiner, so ist zu lesen, lebten inzwischen in Furcht und seien um ihre persönliche Sicherheit besorgt.[43] Auch weniger vermögende Bitcoin-Verwender dürften ähnlich denken.

Auf der anderen Seite wird durch die Verwendung von Mixern der Rechercheaufwand bei der Analyse von Transaktionen mit potenziell kriminellem Hintergrund deutlich

[38] Mutual Legal Assistance (MLA)
[39] Auf Einzelheiten im Zusammenhang mit einer sogenannten MLA request ist hier nicht näher einzugehen.
[40] Bundesministerium der Finanzen (Hg.): Erste Nationale Risikoanalyse. Bekämpfung von Geldwäsche und Terrorismusfinanzierung 2018/2019, S. 127 https://www.nationale-risikoanalyse.de
[41] Mit dem Begriff Darknet sind Netzwerke im Internet gemeint, die Zugriffsprotokolle verwenden, die eine anonyme Nutzung ermöglichen, etwa indem die IP-Adressen der Verbindungen verschleiert werden.
[42] Für diesen Hinweis sei Dr. Hans-Jakob Schindler (Counter Extremism Project) gedankt.
[43] Einige Beispiele und Nachweise finden sich bei Bergmann: Bitcoin. Die verrückte Geschichte vom Aufstieg eines neuen Geldes, S. 261f.

erschwert. Die Anwender, in ihrem Streben nach mehr als ‚Pseudonymität', erschweren Geldwäschebekämpfern und Steuerbehörden die Arbeit. Dieser Widerspruch ist ein gutes Beispiel dafür, wie das Aufkommen von Kryptowährungen das bestehende Finanzsystem vor komplexe Probleme stellt, für die es derzeit noch keine zufriedenstellenden Lösungen gibt.

3 Die Nutzung von Kryptowährungen durch Kriminelle und terroristische Gruppen

Kryptowährungen stellen die Bekämpfung von Geldwäsche und Terrorismusfinanzierung (AML/CTF) vor fundamental neue Herausforderungen. Grundsätzlich verringern sie die Rolle traditioneller Finanzintermediäre, also vor allem der Banken, die ihre kundenbezogenen Sorgfaltspflichten beachten. Kriminellen Nutzern von Kryptowerten wird eine Möglichkeit eröffnet, unter falschem Namen nahezu anonym zu handeln. Die typischen Phasen der Geldwäsche finden auch im Falle der Kryptowährungen Anwendung. Werte aus verdächtiger Herkunft werden durch Umtausch ins Bitcoin-Finanzsystem eingespeist, dort wird die Rückverfolgung der Mittel absichtsvoll verschleiert, bevor ein Umtausch in Fiatgeld die Mittel in den legalen Geldkreislauf zurückführt.[44]

Kryptowährungen stehen daher schon länger im Fokus der Sicherheitsbehörden. Seit den Anfängen von Bitcoin haben sich Kriminelle für Kryptowährungen interessiert. Transaktionen in Kryptowährungen wurde seitdem regelmäßig eine latente Nähe zu dunklen Geschäften und Geldwäsche unterstellt. So sind auch schon Fälle bekanntgeworden, in denen beispielsweise Entführer die Zahlung von Lösegeld in Bitcoin bzw. anderer Kryptowährung verlangt haben. Hinzu kam eine ganze Reihe von Skandalen, in denen es kriminellen Hackern gelang, technische Schwächen und mangelnde Sicherheitsvorkehrungen einzelner Kryptobörsen auszunutzen und hohe Bitcoin-Beträge oder andere Kryptowerte zu entwenden. Nicht nur der schon erwähnte Fall um die Börse Mt. Gox (2014), mit dem sich Strafverfolger bis heute befassen, hat die Einsicht reifen lassen, dass das Geschehen an den Kryptobörsen neu geordnet werden muss.[45]

Als größter Betrugsfall im Zusammenhang mit einer angeblichen Kryptowährung gilt der OneCoin-Skandal. In zahlreichen Medienberichten wird Ruja Ignatova, die bulgarische Erfinderin von OneCoin, als Haupttäterin beschrieben. Bis zum Jahr 2017 soll OneCoin weltweit von Investoren mehr als 4 Milliarden Dollar eingesammelt haben, die als verschwunden gelten. Der spektakuläre Kriminalfall weist Verbindungen nach

[44] Zur rechtlichen Betrachtung siehe die kürzlich veröffentliche Dissertation von Johanna Grzywotz: Virtuelle Kryptowährungen und Geldwäsche, Duncker & Humblot, Berlin 2019
[45] Andrew Norry: The History of the Mt Gox Hack: Bitcoin's Biggest Heist, blockonomi.com, 7.6.2019 https://blockonomi.com/mt-gox-hack/

Deutschland, wo Ignatova länger gelebt hat, und in mehrere Kontinente auf.[46] Während der Verbleib Ignatovas ungeklärt ist, wurde ihr Bruder Konstantin Ignatov, der als Mittäter gesucht wurde, im Frühjahr 2019 in den USA festgenommen. Der Fall OneCoin betrifft jedoch keine wirkliche Kryptowährung. OneCoin basiert nicht auf der Blockchain-Technologie, sondern gleicht dem bekannten Pyramidenspiel oder Ponzi-System. Konnten die ersten Anleger noch Gewinne machen, weil sich immer mehr Investoren beteiligten, standen am Ende nur noch hohe Verluste für zahlreiche Betrugsopfer.

3.1 Die Einschätzungen von Sicherheitsexperten

Die Kryptowährungen stellen die Strafverfolgung vor große praktische Herausforderungen. In Deutschland gingen bei der deutschen FIU im Jahr 2018 rund 570 Verdachtsmeldungen überwiegend von Verpflichteten der Kreditinstitute ein, bei denen es um Auffälligkeiten im Zusammenhang mit Kryptowährungen ging. [47] Bei konkreten Verdachtshinweisen ergeben sich (im Vergleich mit dem klassischen Zahlungsverkehr) besondere Schwierigkeiten – etwa wenn es darum geht, die wirtschaftlich Berechtigten von Krypto-Vermögenswerten zu ermitteln oder den kriminellen Hintergrund einer Transaktion aufzudecken. Ferner gibt es ohne Kenntnis des privaten Schlüssels nicht die Möglichkeit, die auf einer Wallet deponierten Vermögenswerte zu beschlagnahmen oder einzufrieren.

Oftmals führt die Spur zu ausländischen Handelsplätzen. Der zumeist grenzüberschreitende Charakter der Kryptotransaktionen erfordert internationale Rechtshilfegesuche oder eine internationale polizeiliche Zusammenarbeit, um eine vermutete Wirtschaftskriminalität zu ahnden. Schweizer Regierungsexperten gelangten zu dem Schluss, dass die Strafverfolgungsbehörden häufig vom Tempo der Kryptotransaktionen überholt werden; hinzu träten dann noch Probleme bezüglich der zuständigen Gerichtsbarkeit.[48]

Nach Berechnungen einer Anfang 2018 publizierten Studie, die sich auf eine Datenauswertung des Londoner Blockchain-Analyseunternehmens Elliptic stützte, konzentrierte sich von 2013 bis 2016 ein beträchtlicher Teil der Bitcoin-bezogenen Geldwäsche-Aktivitäten auf Europa.[49] Hierbei wurden die verschiedensten Formen von

---

[46] Milliarden-Betrug mit falscher Kryptowährung, FAZ, 17.11.2019 https://www.faz.net/aktuell/wirtschaft/die-macher-der-kryptowaehrung-onecoin-sollen-anleger-um-milliarden-betrogen-haben-16489799.html

[47] Financial Intelligence Unit: Jahresbericht 2018, S. 36 https://www.zoll.de/SharedDocs/Downloads/DE/Links-fuer-Inhaltseiten/Fachthemen/FIU/fiu_jahresbericht_2018.pdf?__blob=publicationFile&v=3
Auf die Rolle der deutschen FIU wird in Abschnitt 5 näher eingegangen.

[48] Schweizerische Eidgenossenschaft (Hg.): 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), Oktober 2018, S. 35 https://www.newsd.admin.ch/newsd/message/attachments/56167.pdf

[49] Yaya J. Fanusie / Tom Robinson: Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services, 12.1.2018 https://www.fdd.org/wp-content/uploads/2018/01/MEMO_Bitcoin_Laundering.pdf

Bitcoin-Umtauschdiensten und Wechselstellen (conversion services) berücksichtigt, also z.B. neben den Exchanges auch Darknet-Aktivitäten, soweit Erkenntnisse darüber vorlagen. Im letzten erfassten Jahr 2016 betrug der Anteil für Europa mehr als 56 Prozent (im gesamten Zeitraum 37 Prozent), während der Rest großteils auf Umtauschdienste entfiel, die nicht regional zugeordnet werden konnten. Demgegenüber waren die nachzuweisenden entsprechenden Aktivitäten in Nordamerika und Asien (7 bzw. 3 Prozent) gering. Der Grund für diesen erstaunlichen Befund ist den Autoren zufolge in der laxen bis fehlenden Regulierung und Überwachung der Handelsplattformen in Europa zu sehen.

Elliptic meldete außerdem im September 2019, dass derzeit Bitcoin im Wert von 829 Millionen Dollar (was 0,5 Prozent aller Bitcoin-Transaktionen im Jahr 2019 entspricht) im Dark Web verwendet werden.[50] Schließlich veröffentlichte die US-Firma CipherTrace einen Bericht, wonach, auf das ganze Jahr 2019 hochgerechnet, Betrüger und andere Kriminelle im Kryptobereich insgesamt 4,3 Milliarden Dollar umgesetzt haben. [51] Vermutlich haben Terrorfinanzierer daran nur einen äußerst geringen Anteil. Genauere Zahlen sind nicht bekannt. Dabei ist jedoch zu beachten, dass es kein Vermögen braucht, um Terrorangriffe zu finanzieren. Selbst sehr große Angriffe können relativ kostengünstig sein. Der Abschluss-bericht der Sonderkommission der US-Regierung zu den Terroranschlägen vom 11. September 2001 („The 9/11 Commission Report“) stellte fest, dass es zwischen 400.000 und 500.000 Dollar kostete, um die mit entführten Passagierflugzeugen durchgeführten Terrorattacken auf New York und Washington zu planen und durchzuführen.[52]

Kürzlich wurde ein erster Fall in Deutschland bekannt, bei dem eine terroristische Handlung mit einer Kryptotransaktion in Verbindung gebracht wird. Im Oktober 2019 stufte das bayerische Landeskriminalamt nachträglich das Attentat vom 22. Juli 2016, bei dem ein 18-jährige Schüler im Münchener Olympia-Einkaufszentrum neun Menschen tötete und fünf weitere verletzte, als rechtsradikal motiviert ein. Lange Zeit war von einem Amoklauf die Rede gewesen. Das Münchener Landgericht sah es bereits 2018 als erwiesen an, dass der Täter eine Pistole und Munition über das Darknet erworben hatte und verurteilte den geständigen Waffenhändler zu einer Haftstrafe.[53] Schon kurz nach dem Attentat hieß es in Medienberichten, die sich auf laufende Ermittlungen stützten, der Schüler habe unter fremdem Namen in einem Darknet-Forum angekündigt, die Waffe mit Bitcoin zu bezahlen.[54] Mit Terrorismusfinanzierung hat der Fall jedoch nur am Rande zu tun, denn der Täter selbst erfuhr keine finanzielle Unterstützung für seine Tat.

---

[50] Elliptic: Bitcoin Money Laundering: How Criminals Use Crypto (And How MSBs Can Clean Up Their Act), 18.9.2019 https://www.elliptic.co/our-thinking/bitcoin-money-laundering

[51] Cryptocurrency Anti-Money Laundering Report, 2019 Q3, November 2019 https://ciphertrace.com/wp-content/uploads/2019/12/CipherTrace-Cryptocurrency-Anti-Money-Laundering-Report-2019-Q3-2.pdf

[52] 9/11 Commission Report (Executive Summary) https://govinfo.library.unt.edu/911/report/911Report_Exec.htm

[53] dpa-Meldung vom 19.1.2018 („Sieben Jahre Haft für Waffenhändler vom Münchner Amoklauf“) https://www.op-marburg.de/Mehr/Hessen/Sieben-Jahre-Haft-fuer-Waffenhaendler-vom-Muenchner-Amoklauf

[54] Siehe besonders Max Hoppenstedt: Der Fall „Maurächer“ und die Darknet-Waffe des David S, vice.com, 26.5.2016 https://www.vice.com/de/article/wnxvvy/der-fall-mauraecher-und-die-darknet-waffe-des-david-s

Trotz vereinzelter Meldungen, wonach Terrorgruppen sich mit dem Thema Kryptowährungen beschäftigen bzw. bereits erste entsprechende Transaktionen nachgewiesen wurden, herrschte bislang die Auffassung vor, das Thema Kryptowährungen sei im Zusammenhang mit der Terrorismusbekämpfung noch nicht relevant. Handelt es sich womöglich um eine übertriebene Gefahr, und welche Erkenntnisse liegen darüber vor, dass Kryptowährungen für Terroristen und ihre Unterstützer wenig attraktiv sind? Gibt es möglicherweise aktuelle Trends und Entwicklungen, welche eine solche Einschätzung mit Fragezeichen versehen?

Erst vor wenigen Monaten hat die Bundesregierung näher Stellung genommen. Im Oktober 2019 wurde die „Erste Nationale Risikoanalyse zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung“ veröffentlicht. [55] Dieser Bericht der Bundesregierung, der als Kernelement des risikobasierten Ansatzes im Sinne der Vierten EU-Geldwäscherichtlinie gilt, stuft die Bedrohung durch Geldwäsche und Terrorismusfinanzierung in Deutschland als mittel-hoch ein, was der zweithöchsten Gefahrenstufe entspricht. In einem eigenen kurzen Kapitel geht der Bericht ausdrücklich auf die Rolle der Kryptowährungen ein.[56] Da „einfachere anonyme Zahlungsmittel (etwa in erster Linie Bargeld)“, wie es heißt, die Geldwäsche mit viel geringerem Aufwand ermöglichten, wird die Geldwäschebedrohung durch Kryptowerte mit mittel-niedrig bewertet.

Das spezielle Risiko der Nutzung von Kryptowährungen für die Terrorismusfinanzierung wird gegenwärtig sogar nur mit niedrig eingestuft. Begründet wird dies in der Nationalen Risikoanalyse damit, die Nutzung von Bargeld verglichen mit „pseudonymen Kryptowerten“ lasse keine Nachverfolgung zu und sei deutlich einfacher zu handhaben. Daher geht die Bundesregierung davon aus, dass vor allem Bargeldkuriere den Geldtransfer von Terrororganisationen besorgen und daneben Hawala [57] und Geldtransferdienstleister eine wichtige Rolle spielen. Hinsichtlich der Terrorismusfinanzierung haben die staatlichen Stellen dagegen bisher keine sicheren Erkenntnisse darüber, ob Kryptowerte „in größerem Umfang“ genutzt würden.

Es fällt auf, wie die niedrige Risikobewertung gleichzeitig mit einer Reihe von Einschränkungen versehen wird. So soll die Entwicklung genau beobachtet werden, da eine Steigerung des Risikopotenzials nicht auszuschließen sei. Dies betreffe den Umtausch von Kryptowährungen untereinander und namentlich solche

---

9/11 Commission Report (Executive Summary)
https://govinfo.library.unt.edu/911/report/911Report_Exec.htm

[55] Bundesministerium der Finanzen (Hg.): Erste Nationale Risikoanalyse. Bekämpfung von Geldwäsche und Terrorismusfinanzierung 2018/2019 https://www.nationale-risikoanalyse.de
An der Risikoanalyse haben seit Ende 2017 insgesamt 35 Bundes- und Landesbehörden mitgearbeitet.

[56] Erste Nationale Risikoanalyse, S. 114-116

[57] Mit Hawala wird ein in der islamischen Welt verbreitetes informelles Zahlungsverfahren bezeichnet, bei dem Transaktionen mit Bargeld erfolgen. Geld wird z.B. in Deutschland ein- und im Ausland ausgezahlt, ohne dass es direkt übermittelt wird. Stattdessen gleichen Händler am Sender- und Empfängerort die Salden untereinander ab, die unterschiedliche Transaktionen betreffen. In Deutschland ist Hawala-Banking ohne Zulassung der BaFin verboten. Weltweit werden auf diese Weise, so die Einschätzung der Bundesregierung, jährlich etwa 200 Milliarden Dollar transferiert. Erste Nationale Risikoanalyse, S. 56

Kryptowährungen, die Nutzern eine größtmögliche Anonymität böten. Privacy Coins bzw. „anonyme Kryptowerte“, namentlich Monero, erlangten, zunehmend größere Akzeptanz im Darknet und könnten zur wichtigen Alternative zu Bitcoin werden.

Ferner räumt der Bericht ein, auch bei älteren Kryptowährungen wie Bitcoin sei eine Entwicklung in Richtung hin zu mehr Anonymität zu beobachten. Festgestellt wird, dass Kryptowährungen „abseits entsprechender Spendenaufrufe und fehlender Erkenntnisse hinsichtlich des dadurch tatsächlich generierten Spendenaufkommens“ bisher nur in Einzelfällen für die Terrorismusfinanzierung genutzt würden.[58] Schließlich wird daran angeknüpft, dass Kryptowährungen heute meist weniger als Zahlungsmittel, sondern als Spekulationsobjekt mit der Gefahr hoher Wertschwankungen fungieren. Eine Ausbreitung der Stablecoins jedoch, einer Kategorie von Kryptowährungen, die auf Wertstabilität angelegt sind, könnte, so der Bericht, die Risiken für Geldwäsche und Terrorismusfinanzierung erhöhen.[59]

Der Eindruck liegt nahe, dass die Nationale Risikoanalyse in Ermangelung sicherer Erkenntnisse das Thema Kryptowährungen recht knapp behandelt. Die große Dynamik, die der Materie innewohnt, wird jedoch anerkannt. Auf die speziellen Risiken der Kryptowährungen im Kontext der Geldwäschebekämpfung wird die Bundesregierung mit Sicherheit noch ausführlich zurückkommen.

Aufschlussreich in dem Zusammenhang ist der Vergleich mit dem bereits im Jahr 2018 von der Schweiz veröffentlichten speziellen National Risk Assessment, das auf das „Risiko der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets und Crowdfunding“ fokussiert.[60] Die Schweizer Behörden, heißt es zu Beginn der Zusammenfassung, hätten bislang kein Beispiel von Terrorismusfinanzierung mittels Kryptowerten und nur einzelne Fälle von Geldwäsche erfasst. Somit bestehe Ungewissheit gegenüber den tatsächlich vorhandenen Risiken. Doch gelangt das National Risk Assessment zu dem 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“.[61]

Im Bericht wird weiter erläutert, die Schweizer FIU, die Meldestelle für Geldwäscherei, habe bereits Hinweise auf Verdachtsfälle von einer ausländischen Partnerstelle erhalten. Dabei ging es um Banktransaktionen von Fiatgeld aus mehreren Ländern, darunter der Schweiz, die einem Konto in demjenigen Staat gutgeschrieben wurden, dessen FIU den Alarm ausgelöst hatte. Das auf dem Konto eingegangene Geld wurde dem Vernehmen nach in Bitcoin umgetauscht und zur Finanzierung terroristischer Aktionen benutzt. Schon die Meldung eines solchen Verdachts, wird argumentiert, belege die Gefährdung,

[58] Erste Nationale Risikoanalyse, S. 115
[59] Erste Nationale Risikoanalyse, S. 115
[60] Schweizerische Eidgenossenschaft (Hg.): 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), Oktober 2018
https://www.newsd.admin.ch/newsd/message/attachments/56167.pdf
[61] National Risk Assessment (NRA): Risiko der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets und Crowdfunding, S. 4

die Kryptowerte für die Terrorismusfinanzierung darstellen. Grundsätzlich sei ein schneller und anonymer Transfer von Mitteln möglich, mit denen Terrororganisationen von Anhängern unterstützt werden könnten.[62]

3.2 Kryptowährungen und Terrorismusfinanzierung – ein zunehmendes Risiko

Bisher vorliegende Studien stimmen darin überein, dass es bisher nur eine kleine Anzahl öffentlich dokumentierter und bestätigter Fälle von Terrorismusfinanzierung mit Kryptowährungen gibt.[63] Auf einige wichtige Fallbeispiele ist an dieser Stelle näher einzugehen. Dabei hat sich erwiesen, dass sich sowohl die den Kryptowährungen zugrunde liegende Technologie als auch die Fähigkeiten terroristischer Gruppen weiterentwickeln. Wie schon gesagt, ist die Situation auf dem Gebiet sehr dynamisch und das von der Verwendung von Kryptowährungen ausgehende Risikopotenzial beträchtlich.

Die Vorgehensweise bei der Finanzierung terroristischer Aktivitäten unterscheidet sich teilweise von Zielen und Methoden von Geldwäschern und anderen Kriminellen, denen es in erster Linie um die Verschleierung finanzieller Transaktionen geht. Auch Terroristen geht es um die Finanzierung durch kriminelle Einkommensquellen, darunter z.B. den illegalen Drogen- und Waffenhandel. In der Praxis stellt sich, so die Erfahrung, häufig heraus, dass im Bereich der Terrorismusfinanzierung die Geldbeträge „sehr gering sind und daher leicht durch das Raster der Indizien fallen“. Außerdem stammen diese Mittel häufig aus nachvollziehbaren legalen Quellen, wie Lohn oder Ersparnissen.[64]

Eine weitere Besonderheit liegt darin, dass Terroraktivisten daran Interesse haben, ein Fundraising zu betreiben, um von Unterstützern Spenden zur Unterstützung der Organisation zu erhalten. Die Verwendung der Mittel, die so eingeworben werden bzw. aus anderen Quellen beschafft werden, können dann für den Kauf von Material zur Unterstützung von Terroranschlägen und jedwede finanzielle Unterstützung von Angriffsaktionen genutzt werden. Zur operativen Unterstützung kommt noch die Verwendung von Mitteln zur laufenden Unterstützung einer terroristischen Vereinigung einschließlich Personalkosten, Gelder für allgemeine Sicherheit und Kommunikation.[65]

---

[62] National Risk Assessment (NRA): Risiko der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets und Crowdfunding, S. 28

[63] Cynthia Dion-Schwarz, David Manheim, Patrick B. Johnston: Terrorist Use of Cryptocurrencies. Technical and Organizational Barriers and Future Threats, RAND Corporation, Santa Monica 2019, S. 55; Policy Department for Citizens' Rights and Constitutional Affairs: Virtual currencies and terrorist financing: assessing the risks and evaluating responses, Mai 2018, S.9 (Verfasser der im Auftrag des EU-Parlaments erstellten Studie waren Tom Keatinge, David Carlisle, und Florence Keen vom Londoner Royal United Services Institute) http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2018)604970

[64] Erste Nationale Risikoanalyse, S. 57, 61

[65] Einen Überblick zu Methoden und Besonderheiten der Terrorfinanzierung geben Cynthia Dion-Schwarz, David Manheim, Patrick B. Johnston: Terrorist Use of Cryptocurrencies. Technical and Organizational Barriers and Future Threats, RAND Corporation, Santa Monica 2019, S. 7ff.

Weil die in der Vergangenheit verfolgten Strategien zur Bekämpfung der Terrorismusfinanzierung (CTF) sich teilweise als wirksam erwiesen haben, ist gut zu verstehen, warum Kryptowährungen für terroristische Organisationen interessant sind. Dafür sind mehrere Gründe verantwortlich. Von der angestrebten Anonymität abgesehen, sind dies eine unkomplizierte Handhabung und Abwicklung von Kryptotransaktionen, deren relative Sicherheit und schnelle Durchführung sowie eine zunehmende Verbreitung von Kryptowährungen. Keine der vorhandenen Kryptowährungen erfüllt alle diese Funktionen in vollkommener Weise. Gäbe es eine nahezu perfekte Kryptowährung, würden Kriminelle hiervon zweifellos intensiv Gebrauch machen. Die bisher bekannt gewordenen Fälle in Verbindung mit Terrorismusfinanzierung bestätigen den Befund, dass unter den Kryptowährungen Bitcoin eindeutig im Vordergrund steht.

Eine weitere Herausforderung für die Kontrollbehörden besteht in der Schwierigkeit, aufgrund der fehlenden Jurisdiktion erkannte Gelder und Finanzflüsse zu beschlagnahmen, aufzuhalten oder einzufrieren. Daher besteht oft für potenzielle Finanzierer des Terrorismus kaum Verfolgungsdruck in diesem Bereich.

Dem Thema Kryptowährungen haben sich Terroristen anfangs nur vorsichtig genähert. Im Herbst 2015 warnte Ghost Security (auch GhostSec), eine angebliche Antiterror-Hackerinitiative, die aus dem „Anonymous"-Netzwerk hervorging, erstmals davor, dass sich Terrorgruppen wie der Islamische Staat (IS)[66] für Bitcoin interessierten. Die Gruppe behauptete, sie habe Bitcoin-Konten aufgespürt, mit welchen der IS Operationen finanziere. Von einem Gesamtwert von 4,7 bis 15,6 Millionen Dollar war die Rede, was einem Anteil zwischen 1 bis 3 Prozent des (vom US-Finanzministerium seinerzeit auf jährlich zwischen 468 und 520 Millionen Dollar geschätzten) Gesamtbudgets des IS entsprochen hätte.[67] Die in dem Bericht genannten Angaben waren aber nicht belegt und wurden bald in Frage gestellt. Sicher scheint, dass frühe Experimente der Terroristen mit Bitcoin im Darknet oder hinter privaten Chat-Kanälen stattfanden.

In der Folgezeit erschienen immer wieder Berichte über die mögliche Verwendung von Kryptowährungen durch Terrorgruppen. Schon kurz nach Erstarken des IS in Syrien und Irak begannen Anhänger der Organisation sich für Finanzierungsmöglichkeiten mittels Bitcoin zu interessieren. So wurde im August 2015 ein amerikanischer Teenager, Ali Shukri Amin, in Virginia zu einer langen Gefängnisstrafe verurteilt, der über Twitter dem IS Empfehlungen gegeben hatte, wie sich die Organisation mittels Bitcoin finanzieren könnte.[68]

---

[66] Der arabische Name des Islamischen Staates lautet ad-daula al-islāmīya (abgekürzt Daesh). In westlichen Medien wurde die Organisation meist als Islamischer Staat im Irak und der Levante (ISIL), Islamischer Staat in Irak und Syrien (ISIS) oder Islamischer Staat (IS) bezeichnet. Die letzte Form überwiegt in deutschen Quellen.

[67] Siehe u.a. Heather Nauert (FoxNews.com), 25.11.2015, ISIS parks its cash in Bitcoin, experts say https://bgr.com/2015/11/25/isis-parks-its-cash-in-bitcoin-experts-say/

[68] financemagnates.com, 30.8.2015 https://www.financemagnates.com/cryptocurrency/news/teen-who-advised-on-funding-isis-with-bitcoin-gets-11-years-in-prison/

In der Praxis kam es dann zunächst zu Anfängerfehlern. Davon zeugt der erste konkrete Fall, der im Jahr 2016 bekannt wurde. Damals rief eine Gruppe im Gazastreifen, Ibn Taymiyya Media Center (ITMC), öffentlich auf Twitter und Telegram zu Bitcoin-Spenden auf, um eine Finanzierungskampagne namens Jahezona (arabisch etwa: „Rüstet uns aus“) zu unterstützen.[69] Diese ITMC gilt als Medienflügel des Mujahideen Shura Council (MSC), einer Sammlung salafistisch-dschihadistischer Gruppen in Gaza, die von der amerikanischen Regierung als Terrororganisation bezeichnet wird.[70] Obwohl das MSC hauptsächlich auf Israel abzielt, unterstützt seine Führung den IS. Die Jahezona-Kampagne lief schon seit 2015. Die Kampagne veröffentlichte regelmäßig Grafiken, die die von der Gruppe gewünschten Waffen und Munition sowie die dafür anfallenden Kosten zeigten. Im Juni 2016 wurde erstmals auf die Möglichkeit verwiesen, in Bitcoin zu bezahlen; außerdem erschienen bei Twitter Infografiken mit QR-Codes, die auf eine Bitcoin-Adresse verwiesen. Nachweislich gingen darauf zwei Transaktionen Anfang Juli 2016 ein. Der Gesamtwert belief sich auf 0,929 Bitcoin (540 Dollar nach damaligem Wert).

Nicht auszuschließen ist, dass die Organisatoren diese Transaktionen selbst durchführten, um die Bitcoin-Adresse zu testen. Obwohl die Kampagne also kaum Erfolg hatte, zeigte sich daran, wie Terroristen mit der neuen Technologie experimentierten, um sich neue Finanzierungsquellen zu erschließen. Der kritische Fehler, den die Aktivisten machten, bestand darin, öffentlich eine Bitcoin-Adresse anzugeben und sich auf der Blockchain transparenter zu machen, als dies sicher beabsichtigt war. Eine Gruppierung, die sich auf eine oder mehrere Adressen bezieht, öffnet sich zumindest teilweise einer Prüfung. Sicherheitsexperten können in einem solchen Fall erkennen, dass hinter eingehenden Transaktionen eine Person steht, die Terroristen Geld sendet. Und mittels der von einem Bitcoin-„Spendenkonto“ ausgehenden Transaktionen wird man der Organisation nachspüren können, die Geld empfängt und an andere Adressen weiterleitet (ohne diese Gelder jedoch aufhalten oder ohne spezialisierte Dienste die tatsächliche Identität der Spender und Empfänger ermitteln zu können).

Eine vom Europäischen Parlament in Auftrag gegebene Studie zum Thema Krypto-währungen und Terrorismusfinanzierung hob den Fall von al-Sadaqah hervor, einer in Syrien aktiven dschihadistischen Organisation. [71] Diese Gruppe, die als Wohltätigkeitsorganisation auftritt, führte gegen Ende 2017 eine Crowdfunding-Kampagne über al-Qaida nahestehende Social-Media-Kanäle und den Messaging-Dienst Telegram durch. In deren Verlauf erhielt al-Sadaqah 0,075 Bitcoin (nach damaligem Wert 803 Dollar) für ihre Bitcoin-Adresse. Die Kampagne hatte zunächst dazu aufgerufen, dass Unterstützer anonym und sicher mit Bitcoin spenden sollten. Wochen später, nachdem der Vorfall Beachtung fand, erklärte die Organisation auf Twitter,

[69] Yaya Fanusie: The New Frontier in Terror Fundraising, in: Bitcoin, The Cipher Brief, 24.8. 2016 https://www.thecipherbrief.com/column_article/the-new-frontier-in-terror-fundraising-bitcoin
[70] Office of Foreign Asset Control, Specially Designated National Update, 19.8.2014 https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20140819.aspx
[71] Sadaqah bedeutet im Arabischen „Wohltätigkeit“ und bezieht sich auf die Freiwilligkeit der Gabe.

künftig könnten auch Privacy Coins wie Monero und Dash verwendet werden, um die Mudschahedin in Syrien zu unterstützen.[72]

Zum Jahresende 2017 wurde ein weiterer Fall bekannt. Zoobia Shahnaz, eine in Pakistan geborene US-Staatsbürgerin, wurde wegen Bankbetrugs und Verschwörung zur Geldwäsche angeklagt. Nach Angaben des US-Justizministeriums hatte Shahnaz, die sich später für schuldig bekannte, mit mehr als einem Dutzend durch Betrug erworbenen Kreditkarten rund 62.000 Dollar in Bitcoin und anderen Kryptowährungen gekauft bzw. wieder in Dollar zurückgetauscht und anschließend begonnen, Geldbeträge zur Unterstützung des IS zu überweisen.[73] Einige Stimmen wollen den Fall eher als Beleg dafür sehen, dass Terroristen und ihre Unterstützer zur direkten Nutzung von Kryptowerten eher Abstand halten. Jedenfalls ging es darum, mit Hilfe der zwischengeschalteten Kryptotransaktionen die kriminelle Herkunft der Gelder zu verschleiern, die danach für terroristische Zwecke genutzt werden sollten.

Unterdessen zeigte sich im Nahen und Mittleren Osten, wie die Terroristen dazulernen. Wie das Recherchenetzwerk Bellingcat berichtete, begann eine syrische dschihadistische Gruppierung aus der Region Idlib namens Malhama Tactical im Juni 2018 mit öffentlicher Werbung um Bitcoin-Spenden. Neu war in diesem Fall der veränderte Ansatz für die Spendenwerbung. Tweets mit der Bitcoin-Adresse der Gruppe wurden bald wieder gelöscht. Stattdessen wurden potenzielle Spender gebeten, Malhama Tactical über Direktnachrichten zu kontaktieren, um eine Spendenadresse mitgeteilt zu bekommen. Ob dieses Vorgehen, das inzwischen auch weitere Terrorgruppen gewählt haben, eine besonders wirksame Methode ist, Spenden anzuziehen, bleibt offen.[74] Die Nachverfolgung möglicher Kryptotransaktionen wird damit jedoch erschwert. Um in dieser Richtung nachzuforschen, müssten Ermittler eigene Tarnaccounts anlegen und mit den Terrorgruppen Verbindung aufnehmen. [75]

Inzwischen ist eine weitere wichtige Neuerung zu beobachten. Im April 2019 wurde berichtet, die Kassam-Brigaden, der militärische Arm der palästinensischen Hamas, hätten ihre Anhänger bereits seit Januar des gleichen Jahres zu Spenden in digitaler Währung aufgerufen. Die Kassam-Brigaden und die Hamas werden von der EU offiziell als Terrororganisation eingestuft. [76] Ursprünglich sollten Spender an eine einzelne

[72] Policy Department for Citizens' Rights and Constitutional Affairs: Virtual currencies and terrorist financing: assessing the risks and evaluating responses, Mai 2018, S.34 (Verfasser der Studie waren Tom Keatinge, David Carlisle, und Florence Keen vom Royal United Services Institute) http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2018)604970
[73] United States Department of Justice, 26.11.2018 https://www.justice.gov/usao-edny/pr/long-island-woman-pleads-guilty-providing-material-support-isis
[74] Generell spielt die Nutzung sozialer Medien für die Terrorismusfinanzierung mittels Crowdfunding eine zunehmende Rolle. Tom Keatinge / Florence Keen: Social Media and Terrorist Financing. What are the Vulnerabilities and How Could Public and Private Sectors Collaborate Better?, Global Research Network on Terrorism and Technology: Paper No. 10 (RUSI), London 2019 https://rusi.org/sites/default/files/20190802_grntt_paper_10.pdf
[75] Brenna Smith: The Evolution Of Bitcoin In Terrorist Financing, 9.8.2019 https://www.bellingcat.com/news/2019/08/09/the-evolution-of-bitcoin-in-terrorist-financing/
[76] Zur Liste der Personen, Vereinigungen und Körperschaften, deren Gelder eingefroren und gegen die verstärkte Maßnahmen der polizeilichen und justiziellen Zusammenarbeit angewendet werden, siehe den Beschluss (GASP) 2019/1341 des Rates vom 8.8.2019 https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019D1341&from=en

Bitcoin-Adresse oder Wallet spenden. Wie jedoch Recherchen der Analysefirma Elliptic zeigten, wurde die betreffende Finanzierungs-Website inzwischen dahingehend modifiziert, dass mit jedem Seitenaufruf automatisiert eine neue eindeutige Bitcoin-Spendenadresse generiert wird. Keine dieser neuen Einzeladressen, die selbst keine Beträge erhalten haben, ist auf der Blockchain zu finden. Um eine dieser neu generierten Adressen auf die Blockchain zu setzen, müssten die Ermittler selbst an die Hamas spenden. Anders gesagt gehört auf diese Weise jede neue Spende zu einer neuen Wallet, die nur der Spender selbst je zuvor gesehen hat. Die innovative Fundraising-Kampagne der Hamas, heißt es, habe in den ersten vier Monaten ein Spendenaufkommen von 7.400 Dollar erzielt.[77]

Etwa gleichzeitig wurde entdeckt, dass auch der Islamische Staat (IS) bzw. dessen Medienseite al-Furqan mittels der gleichen adressengerierenden Software um Bitcoin-Spenden wirbt. Es ist nicht sicher, welche der beiden Organisationen für die technologische Weiterentwicklung ursprünglich verantwortlich ist. Die New York Times berichtete im August 2019 ebenfalls von der neuen als alarmierend eingestuften Entwicklung.[78] Amerikanische Experten, so dieser Bericht, gehen davon aus, dass die Erträge aus solchen einzelnen Spendenkampagnen sich vermutlich im Bereich von jeweils mehreren Zehntausend Dollar bewegen dürften.

Ein Großteil der neuen Erkenntnisse über die verstärkte Nutzung von Kryptowährungen durch Terroristen ist schließlich in einem umfangreichen Bericht des amerikanischen Terrorexperten Steven Stalynski enthalten.[79] Der neue Trend wird darin auch mit der Zerschlagung des „Islamischen Staates“ im Verlauf des Syrien-Krieges in Zusammenhang gebracht. Die flüchtigen IS-Kämpfer seien inzwischen ohne festes Territorium und darum stärker als zuvor an Kryptotransaktionen interessiert.

Eine israelische Analysefirma namens Whitestream berichtete, sie habe Hinweise gefunden, die belegen, dass die Bombenanschläge am Ostersonntag 2019 in Sri Lanka, bei denen 253 Menschen getötet und 485 weitere Personen verletzt wurden, wesentlich durch Bitcoin-Transaktionen finanziert wurden.[80] Der IS, der den Anschlag für sich reklamierte, nutzte offenbar die kanadische Kryptobörse CoinPayments. In Bitcoin-Wallets, die dem IS zugeordnet werden, sollen die Guthaben nur einen Tag vor den Osterangriffen von 500.000 auf 4,5 Millionen Dollar gestiegen sein. Direkt nach den

[77] Reuters, 26.4.2019 https://uk.reuters.com/article/us-crypto-currencies-hamas/hamas-shifts-tactics-in-bitcoin-fundraising-highlighting-crypto-risks-research-idUKKCN1S20FA
[78] Nathaniel Popper: Terrorists Turn to Bitcoin for Funding, and They’re Learning Fast, The New York Times, 18.8.2019 https://www.nytimes.com/2019/08/18/technology/terrorists-bitcoin.html
[79] Steven Stalinsky: The Coming Storm – Terrorists Using Cryptocurrency, 21.8.2019 https://www.memri.org/reports/coming-storm-%E2%80%93-terrorists-using-cryptocurrency
Stalinsky ist Direktor des Middle East Media Research Institute (MEMRI), das sich auf die Beobachtung islamischer Medien des Nahen Ostens konzentriert. Die NGO mit Sitz in Washington wird teilweise als neokonservativ und der israelischen Regierung nahe stehend beschrieben.
[80] Roy Katsiri: Bitcoin donations to ISIS soared day before Sri Lanka bombings, Globes (Israel), 2.5.2019 https://en.globes.co.il/en/article-exclusive-isis-funded-sri-lanka-bombings-with-bitcoin-donations-1001284276

Anschlägen seien sie, so die Whitestream-Experten, wieder auf 500.000 Dollar zurückgegangen.[81]

Die Kassam-Brigaden und der IS werden nicht die letzten Extremisten sein, die diese technologisch fortgeschrittene Form der Finanzierung nutzen. Von daher ist die frühere Annahme, Bitcoin sei aufgrund von Rückverfolgbarkeit und mangelnder Liquidität für illegale Aktivitäten wenig geeignet, ernsthaft in Frage gestellt. Terrororganisationen haben vielmehr scheinbar einen Weg gefunden, die genutzten Finanzierungswege anonym zu gestalten – gelingt es ihnen auch, ein schnelle Auszahlung bzw. den Umtausch in Fiatwährungen zu organisieren, könnten Bitcoin und andere Kryptowährungen neben Bargeld zu einem zweiten Grundpfeiler der Terrorismusfinanzierung werden.

Finanzmittel, die in Kryptowährungen gebunden sind, sind nur schwer zu ermitteln, insbesondere wenn Gelder in Wallets nur aufbewahrt werden. Weiterhin bleibt es eine Herausforderung für die Sicherheitsbehörden, inkriminierte Krypto-Vermögenswerte zu beschlagnahmen oder einzufrieren. Diese Assetklasse stellt daher für Terrororganisationen eine potenziell attraktive Methode dar, Finanzmittel zu verwahren, mit denen nicht unbedingt Profit erzielt werden soll, sondern die in erster Linie vor staatlichem Zugriff geschützt werden müssen. Dies gilt in erhöhtem Maße für Terrororganisationen, die wie z.B. IS, Hezbollah oder die Taliban regelmäßig große Budgets verwalten.

3.3 Messaging-Dienste auf Blockchain-Basis?

Ein wichtiger Nebenaspekt in dem Zusammenhang sind fortgeschrittene Messaging-Dienste, die ebenfalls mit Methoden der kryptographischen Verschlüsselung funktionieren. Die Experten von Counter Extremism Project (CEP) haben hierzu schon im Jahr 2017 einen Bericht veröffentlicht, der die wachsende Nutzung von Telegram durch verschiedene Terrorgruppen aufzeigt.[82] Telegram ist ein kostenloser, Cloud-basierter Instant-Messaging-Dienst. Die Basis des Entwicklerteams soll sich nach Eigenangaben in Dubai befinden. Der Hauptgründer ist der Internet-Milliardär Pawel Durow, der teilweise als „russischer Mark Zuckerberg“ bezeichnet wurde und auch Russland populärstes soziales Netzwerk VK (vk.com) gegründet hat. Durow musste aus Russland emigrieren. Sein erklärtes Ziel lautete, eine App zu konstruieren, auf der Menschen miteinander kommunizieren können, ohne dass staatliche Stellen mitlesen können.[83]

[81] Bei den Anschlägen in Sri Lanka (21.4 2019) wurden mehrere Kirchen und Hotels durch Selbstmordattentäter angegriffen. Die dortigen Behörden machen eine srilankische islamistische Gruppierung und Dschihadisten, die Verbindungen zum internationalen Terrorismus aufwiesen, für die Angriffe verantwortlich. Bitcoin donations to ISIS soared day before Sri Lanka bombings, Globes (Israel), 2.5.2019 https://en.globes.co.il/en/article-exclusive-isis-funded-sri-lanka-bombings-with-bitcoin-donations-1001284276

[82] Counter Extremism Project (Hg.): Terrorists on Telegram, Mai 2017 https://www.counterextremism.com/terrorists-on-telegram

[83] Christian Steiner: Wie Telegram-Gründer Pawel Durow die Geschichte besiegen will, Neue Zürcher Zeitung, 20.4.2018 https://www.nzz.ch/wirtschaft/telegram-gruender-durow-will-die-geschichte-besiegen-ld.1378493

Tatsächlich nutzen Terroristen den geschützten Chat-Verkehr beispielsweise für Zwecke des Fundraising. Telegram fungierte außerdem als eine der Medienplattformen, auf der Material des IS verbreitet wurde.

Inzwischen hat auf internationaler Ebene eine Gegenreaktion eingesetzt, die den Druck auf die Telegram-Betreiber erhöhte, gegen den Missbrauch vorzugehen und Sicherheitsmaßnahmen zu planen und einzubauen. Parallel dazu verklagte die US-Börsenaufsicht Telegram im Oktober 2019 und forderte, Telegrams Blockchain-Projekt Telegram Open Network (TON) zu verschieben. Durow und andere Verantwortliche wurden aufgefordert, in den USA vor Gericht auszusagen.[84] In der Zwischenzeit haben Telegram und andere Internetunternehmen auf Geheiß von Europol und europäischen Staaten damit begonnen, zahlreiche Konten von IS-Anhängern zu sperren. Der IS hat darauf trotzig reagiert und Unterstützern geraten, auf andere Plattformen auszuweichen.[85]

Im Dezember 2019 erschienen Medienberichte, wonach der IS derzeit aktiv eine Blockchain-basierte Messaging-App testet, die verschiedene Vorteile aus Sicht der Terroristen bietet, darunter eine scheinbar sichere und anonyme Kommunikation sowie ein manipulationssicheres Archiv, in dem der IS seine Propagandavideos speichern kann. Die Messaging-App nennt sich BCM („Because Communication Matters“). Hinter BCM steht ein von David Xueling Li, einem chinesischen Milliardär, gegründetes Unternehmen mit Sitz auf den Britischen Jungferninseln. Ob die App wirklich aus Sicht des IS die Nachfolge von Telegram antreten kann, bleibt abzuwarten. Ein Schlüsselaspekt von BCM, den andere Plattformen nicht bieten, ist eine integrierte Wallet, mit der man Kryptowährungen wie Bitcoin und Ethereum nutzen kann.[86]

Das Unternehmen spricht auch davon, eine eigene Kryptobörse aufbauen zu wollen, um den weltweiten anonymen Kryptozahlungsverkehr zu vereinfachen. Unter Sicherheitsaspekten ist dies bedenklich. Einige Fachleute äußerten jedoch Zweifel hinsichtlich der Ankündigungen von BCM. Den Regierungen wird außerdem Zeit verbleiben, um wie im Fall von Telegram nötigenfalls Gegenmaßnahmen zu ergreifen. Die Diskussion über Messaging-Dienste ist somit ein anschauliches Beispiel dafür, wieviel Aufmerksamkeit neueste technologische Trends erfordern, wenn Terroristen zunehmend Geschmack an Kryptowährungen und Blockchain-Anwendungen finden.

---

[84] Telegram Founder Durov Should Testify in SEC Case Over Gram Token: Judge, coindesk,com, 26.11.2019 https://www.coindesk.com/telegram-founder-durov-to-testify-in-sec-case-over-gram-token

[85] Defiant Message From ISIS In Response To Campaign Against Its Presence On Telegram, Other Platforms, MEMRI, 2.12.2019 https://www.memri.org/reports/defiant-message-isis-response-campaign-against-its-presence-telegram-other-platforms

[86] Der erste Artikel, der eine weitere Berichterstattung auslöste, stammt von David Gilbert: ISIS Is Experimenting with This New Blockchain Messaging App, vice.com, 13.12.2019 https://www.vice.com/en_us/article/v744yy/isis-is-experimenting-with-this-new-blockchain-messaging-app

4 Die Antwort der Regierungen: ein koordinierter Regulierungsansatz

Das Aufkommen von Bitcoin und anderen Kryptowährungen ist ein weltweites Phänomen. Kryptowährungen sind nicht wie Fiatgeld in bestimmten Staaten verankert, sondern bestehen als Technologie im globalen Cyberspace. Die Kryptocoins mit ihrem großen Entwicklungspotenzial stellen, wie bereits dargelegt, den Kampf gegen Geldwäsche und Terrorismusfinanzierung (AML/CFT) vor neuartige Herausforderungen. Dazu kommt die Geschwindigkeit der technologischen Veränderungen. So überrascht es nicht, dass die Regulierung des Krypto-Zahlungsverkehrs erst am Anfang steht. Einige Zeit verging, bis die ersten Regierungen anfingen, sich dieser komplizierten Materie anzunehmen. Vielfach fehlt es in vielen Staaten auf Regierungsebene an einer ausreichenden Zahl von Fachleuten, die das Thema verfolgen, entsprechende Expertise entwickeln sowie über entsprechende technische Möglichkeiten verfügen.

Die wachsende Sorge aus Sicht der Sicherheitsbehörden besteht darin, dass Kryptowährungen eine sich entwickelnde Technologie sind, die sich bereits in einer bestimmten Nische des Finanzsektors durchgesetzt hat. Das hat dazu geführt, dass kriminelle Akteure und Terrororganisationen wie der IS, damit begonnen haben, mit der neuen Technologie zu experimentieren. Sie benutzen die neue Technologie zur Geldwäsche oder versuchen, sich neue Finanzquellen zu erschließen, wie die aktuellen Beispiele vom Fundraising terroristischer Gruppen zeigen. Zugleich ist zu beobachten, dass man sich in dieser Hinsicht noch in einem frühen Stadium befindet. Aus diesem Grund ist es unerlässlich, dass die nationalen Sicherheitsakteure, seien es Finanzbehörden, Strafverfolgungsbehörden oder Nachrichtendienste, die neue Herausforderung annehmen. Letztlich müssen sie in die Lage versetzt werden, mit der neuen Technologie genauso intelligent umzugehen wie ihre Gegner.

4.1 Die neuen Empfehlungen der FATF (Juni 2019)

Eine wirksame Antwort auf die neuen Herausforderungen sollte soweit möglich auf internationaler Ebene abgestimmt werden. Dabei ist es nicht das erste Mal, dass die Regulierer im AML/CFT-Bereich mit Problemen konfrontiert sind, die eine globale Koordination und Zusammenarbeit erfordern. Maßgeblicher Standardsetzer auf diesem Gebiet ist seit langem die Financial Action Task Force (FATF), ein von westlichen Ländern gegründetes zwischenstaatliches Gremium, das fortlaufend aktualisierte Empfehlungen und dazugehörige Auslegungsgrundsätze zur Regulierung der Geldwäsche- und Terrorismusfinanzierungsbekämpfung veröffentlicht. [87] Die Pariser

[87] Die im Jahr 1989 gegründete Financial Action Task Force (on Money Laundering) – übersetzt „Arbeitsgruppe für finanzielle Maßnahmen gegen Geldwäsche“ – hat ihren Sitz bei der OECD in Paris. Mitglieder der FATF sind derzeit 37 Staaten und zwei internationale Organisationen (die EU und der Golf-Kooperationsrat). Zu den Mitgliedern zählen neben vielen meist westlichen Staaten auch China, das derzeit mit Xiangmin Liu den Präsidenten der FATF stellt, Indien und Russland.

Institution, deren Empfehlungen sich als weltweiter Standard etabliert haben, übernimmt die Rolle des Antreibers der Regulierung in diesen Bereichen. Oftmals fließen die zunächst unverbindlichen Empfehlungen der FATF mit einiger Verzögerung in die Gesetzgebung vieler Staaten ein. Ähnlich wie der Financial Stability Board[88], eine Organisation, die für die Überwachung der finanziellen Stabilitätsrisiken zuständig ist und derzeit ebenfalls dem Thema Kryptowerte größere Aufmerksamkeit schenkt, berichtet die FATF regelmäßig an die Gruppe der zwanzig wichtigsten Industrie- und Schwellenländer (G20).

Kryptowerte sind bereits seit Jahren Teil der Empfehlungen der FATF. Zunächst war das Vorgehen noch etwas zurückhaltend. Die FATF stellte allgemein eine Lizenzierungspflicht für Virtual Asset Service Provider (VASP) zur Diskussion. Damit sind die Anbieter von Diensten für virtuelle Vermögen einschließlich Kryptobörsen gemeint. Im Oktober 2018 entschied die FATF dann auf Aufforderung der G20-Finanzminister, in ihre Standards künftig auch spezifische Vorgaben für Kryptowerte (virtual assets) aufzunehmen.[89] Wenig später kündigten die G20-Staaten auf ihrem Gipfeltreffen in Buenos Aires an, Kryptowerte im Einklang mit den FATF-Standards zu regulieren.[90] Zugleich wurde der Ball an die FATF zurückgespielt mit dem Auftrag, konkrete Vorgaben für die Regulierung von Kryptowerten zu erarbeiten. Die FATF hat inzwischen ihre Empfehlungen entsprechend überarbeitet[91] und am 21. Juni 2019 einen ausführlichen Leitfaden zu Krypto-Vermögenswerten und -Dienstleistern veröffentlicht.[92] Kurz darauf bestätigten die Staats- und Regierungschefs der G20 auf dem Gipfel in Osaka die Anwendung der FATF-Standards auf Kryptowährungen und Virtual Asset Service Provider. Zugleich stellten sie eine Umsetzung des Regelwerks im Sinne des FATF-Leitfadens in Aussicht.[93]

Im Kern geht es um eine weltweit koordinierte Regulierung der Kryptobörsen, der entscheidenden Schnittstelle zwischen der Sphäre der Kryptowährungen und den Fiatwährungen. Im Wesentlichen heißt dies, dass die bestehenden Regeln gegen Geldwäsche und Terrorfinanzierung zukünftig auch auf Blockchain-Finanzdienstleistungen angewendet werden. Die FATF räumt den Staaten ein Jahr Zeit ein, um die Empfehlungen anzunehmen. Eine entsprechende Überprüfung ist für Juni

[88] Der Financial Stability Board, der in dieser Form seit 2009 existiert, ist bei der Bank für Internationalen Zahlungsausgleich (BIZ) in Basel angesiedelt. Die Organisation befasst sich als Standardsetzer im Bereich Kryptowährungen mit Regulierungsfragen und finanziellen Stabilitätsrisiken, die sich nicht auf die speziellen Aspekte des Kampfs gegen Geldwäsche und Terrorismusfinanzierung beziehen.
[89] FATF: Regulation of virtual assets 19.10.2018 https://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets.html
[90] G20 Leaders' Declaration: Building Consensus for Fair and Sustainable Development, 1.12.2018. siehe Nr. 25 http://www.g20.utoronto.ca/2018/2018-leaders-declaration.html
[91] FATF (Hg.): International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. The FATF Recommendations, Paris 2012-2019 www.fatf-gafi.org/recommendations.html
[92] FATF (Hg.): Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, Juni 2019 www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html
[93] G20 Osaka Leaders' Declaration, 29.6.2019, siehe Nr. 17 http://www.g20.utoronto.ca/2019/2019-g20-osaka-leaders-declaration.html

2020 vorgesehen.[94] Auf einer Plenarsitzung im Oktober 2019 griff die Organisation das Thema erneut auf. Zugleich wurden sich die Mitgliedsländer einig darüber, wie die Überprüfung der notwendigen Schritte zur Umsetzung der neuen Anforderungen erfolgen werde. Festgestellt wurde außerdem, dass – in Anspielung auf Projekte wie Libra[95] – auch neu aufkommende virtuelle Währungen wie die sogenannten Stablecoins unter die neue Regulierung fallen würden.[96] Nicht gemeint damit sind mögliche künftige staatliche digitale Währungen auf Blockchain-Basis, die anscheinend einen gesonderten Status erhalten werden.

Derzeit steht die Umsetzung der vereinbarten Regulierungsmaßnahmen an. Auch wenn betont wird, wie dies bei allen Empfehlungen der FATF der Fall ist, dass die neuen Krypto-Leitlinien nicht verbindlich seien und die Zuständigkeit der nationalen Behörden nicht außer Kraft setzten, bleibt den Regierungen kaum eine Wahl. Staaten, die den neuen regulatorischen Rahmen nicht übernehmen, müssen damit rechnen, von der FATF auf eine „schwarze Liste" gesetzt zu werden. Staaten, die negativ beurteilt werden, riskieren im schlimmsten Fall, den Zugang zum globalen Finanzsystem zu verlieren.[97] Inwieweit alle Staaten und hinsichtlich der technischen Umsetzung die Virtual Asset Service Provider den engen Zeitplan einhalten können, wird sich zeigen. Die einzelnen Staaten behalten außerdem einen gewissen Interpretationsspielraum bei der Umsetzung der Richtlinien.

Wie sehen die wichtigsten Beschlüsse aus? Die geänderte FATF-Empfehlung 15 verlangt von den Staaten, dass Krypto-Dienstleister (VASPs), die in ihrem Zuständigkeitsbereich tätig sind, zur Bekämpfung der Geldwäsche und der Terrorismusfinanzierung verpflichtet werden. Diese müssen entsprechend reguliert und lizenziert werden sowie einem wirksamen staatlichen Aufsichtssystem unterliegen. In einer mitveröffentlichten Auslegungshilfe[98], die in der G20-Erklärung ausdrücklich mit erwähnt wurde, heißt es, die Staaten sollten von den Krypto-Dienstleistern verlangen, Informationen zu den von ihnen abgewickelten Transaktionen zu sammeln. Die betreffenden Daten müssen mit den auf der Gegenseite einer Transaktion einbezogenen Dienstleistern ausgetauscht werden. Kundendaten sind den zuständigen Behörden auf Verlangen zu übermitteln.

Die Empfehlung 16 (Wire Transfer Rule) sieht weiter vor, die Staaten sollten Vorsorge treffen, dass Banken bzw. Krypto-Dienstleister Informationen zu Absender und

[94] FATF: Public Statement on Virtual Assets and Related Providers, 21.6.2019 http://www.fatf-gafi.org/publications/fatfrecommendations/documents/public-statement-virtual-assets.html
[95] Zu der von Facebook geplanten virtuellen Währung (Libra) und der Diskussion um Stablecoins siehe Abschnitt 4.4
[96] Outcomes FATF Plenary, 16-18 October 2019 https://www.fatf-gafi.org/publications/fatfgeneral/documents/outcomes-plenary-october-2019.html
[97] Auf der schwarzen Liste der FATF befinden sich aktuell Nordkorea und der Iran (FATF: Public Statement, 18.10.2019 https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/public-statement-october-2019.html). Daneben gibt es eine im Oktober 2019 aktualisierte Liste von derzeit 12 Staaten, die „strategische Mängel" aufweisen. https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/fatf-compliance-october-2019.html
[98] Interpretative Note to Recommendation 15, in: The FATF Recommendations, S. 70-71

Empfänger auf mögliche fehlende Angaben hin überwachen. Im Einzelnen werden folgende Informationen für jede Transaktion benötigt:[99]

- der Name des Auftraggebers
- die Kontonummer des Auftraggebers, wenn ein solches Konto zur Abwicklung der Transaktion verwendet wird (z.B. die Krypto-Wallet)[100]
- die physische (geografische) Anschrift des Auftraggebers oder die nationale Identifikationsnummer oder die Kundenidentifikationsnummer, die den Auftraggeber gegenüber dem auftraggebenden Institut eindeutig identifiziert, oder das Geburtsdatum und den Geburtsort
- der Name des Begünstigten
- die Kontonummer des Begünstigten, wenn ein solches Konto zur Abwicklung der Transaktion verwendet wird (z.B. die Krypto-Wallet)

Ferner müssen Krypto-Dienstleister geeignete Prozesse entwickeln und sicherstellen, dass ihre Kunden keine illegalen Aktivitäten betreiben. Die als Krypto-Dienstleister eingestuften Unternehmen unterliegen damit künftig ähnlichen Anforderungen wie herkömmliche Banken und Finanzdienstleister. Allerdings ergeben sich einige offene Punkte. So besteht bisher auf nationaler wie internationaler Ebene noch kein System (wie z.B. im Falle von Swift im Interbankenverkehr), mit dessen Hilfe Identifikationsdaten zum Zahlungsverkehr auf der Blockchain zuverlässig übermittelt werden können. So ist es praktisch unmöglich, einen Begünstigten zu identifizieren, der beispielsweise eine neugeschaffene, nicht-depotpflichtige (non-custodian) Bitcoin-Wallet nutzt.

Von der Überwachung ausgenommen bleiben Kryptotransaktionen, die zwischen Wallets erfolgen, die nicht der Aufsicht des betreffenden Staates unterliegen. Die Nutzer von Kryptowährungen, die selbst unmittelbar keiner Regulierung unterliegen, behalten daher die Möglichkeit, schwächer regulierte Kryptobörsen zu nutzen oder Peer-to-Peer-Transaktionen vorzunehmen (bei reinen Krypto-Krypto-Zahlungen), die nicht erfasst werden. Im ungünstigen Fall werden die neuen Regeln Peer-to-Peer-Transfers über nicht depotpflichtige Wallets attraktiver machen, was die Verfolgung und Kontrolle für die Behörden wesentlich erschweren würde. Im konkreten Fall könnte ein Auftraggeber Kryptocoins von einer Börse an eine nicht-depotpflichtige Wallet senden, deren privaten Key allein der Nutzer kontrolliert. Von dieser Wallet würden die Coins danach an eine andere Plattform geschickt mit dem Ergebnis, dass keiner der am Anfang und Ende beteiligten Krypto-Dienstleister beide Seiten der Transaktion überschauen könnte.

Was die Ausübung der kundenbezogenen Sorgfaltspflichten (im Sinne des „Know your customer“ bzw. KYC) angeht, hat die FATF für Krypto-Dienstleister eine niedrige Schwelle eingezogen. Dem liegt die Einschätzung zugrunde, dass Kryptotransaktionen in erhöhtem Maße anfällig sind für eine Nutzung im Zusammenhang mit Geldwäsche und Terrorismusfinanzierung. Entsprechende Prüfungen bei gelegentlichen Transaktionen

[99] FATF (Hg.): Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, S.29 (Nr. 114)
[100] Im Original „VA wallet”

sollen schon ab einem Mindestwert von mehr als 1.000 Dollar oder Euro erfolgen.[101] In Deutschland entspricht dieser Schwellenwert den bereits für die Überwachung von Geldtransfers geltenden Bestimmungen des Geldwäschegesetzes. Dazu muss man ergänzen, dass die meisten etablierten Kryptobörsen anscheinend bereits heute KYC-Prüfungen, darunter die Identitätsprüfung des Auftraggebers (z.B. um den Namen mit Sanktionslisten abzugleichen), bei eingehenden Transaktionen ab 1.000 Dollar oder Euro vornehmen. Nach den neuen FATF-Regeln würde dies jedoch künftig auch ausgehende Transaktionen betreffen. [102] Die FATF verzichtete darauf, näher auf Umgehungshandlungen einzugehen, d.h. innerhalb welcher Zeitspanne Transaktionen unter dem Schwellenwert anfallen müssen, um eine Überprüfung auszulösen. [103]

Die FATF geht andererseits noch weiter und legt den Staaten nahe, Überprüfungen der Kryptotransaktionen im Sinne des risikobasierten Ansatzes sogar bereits bei auffälligen Transaktionen unterhalb der Mindestschwelle von 1.000 Euro vorzusehen. [104] Ein Unterschreiten der Mindestschwelle ist laut FATF insbesondere dann angezeigt, sobald Verdachtsmomente bezüglich Geldwäsche und Terrorismusfinanzierung vorliegen. Erinnert sei an die in jüngster Zeit durchgeführten Fundraising-Kampagnen von Terrorgruppen, bei denen sich die Gesamteinnahmen aus zahlreichen Kleinspenden zusammensetzten.

Es waren sicher auch die Erkenntnisse darüber, dass das Fehlen eines wirksamen Regelwerks erhöhte Geldwäsche-Aktivitäten im Umfeld von Handelsplattformen speziell in Europa begünstigt hat,[105] welche die amerikanische Regierung veranlassten, auf die Verabredung strenger Regeln zu drängen. Die erweiterten FATF-Empfehlungen laufen darauf hinaus, im Wesentlichen einen von der zuständigen im US-Finanzministerium angesiedelten Behörde, dem Financial Crimes Enforcement Network (FinCEN), entwickelte Praxis der Krypto-Regulierung zu übernehmen. Bereits im Jahr 2013 wirkte FinCEN darauf hin, die im Bank Secrecy Act verankerte sogenannte Travel Rule auf Krypto-Handelsplattformen auszudehnen. [106] Die amerikanische Travel Rule, die sich

[101] Interpretative Note to Recommendation 15, in: The FATF Recommendations, S. 71, Nr. 7a (Bezugnehmend auf Empfehlung 10 bzw. Customer Due Diligence): „The occasional transactions designated threshold above which VASPs are required to conduct CDD is USD/EUR 1 000". Im Vergleich dazu liegt die von der FATF empfohlene Schwelle bei Transaktionen in Fiatwährungen bei 15.000 Dollar oder Euro.
[102] Colin Harper: FATF Finalizes Crypto Guidelines, Recommends Exchanges Share Client Data, Bitcoin Magazine, 21.6.2019 https://bitcoinmagazine.com/articles/fatf-finalizes-crypto-guidelines-recommends-exchanges-share-client-data
[103] Nina-Luisa Siedler / Susi Förschler: FATF recommends regulating and monitoring Virtual Asset Service Providers, DWF Spotlight, 22.8.2019 https://www.dwf.law/Legal-Insights/2019/August/Regulation-of-virtual-asset-service-providers
[104] FATF (Hg.): Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, S.25 (Nr. 95)
[105] Siehe die bereits früher erwähnte Studie von Yaya J. Fanusie und Tom Robinson: Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services, 12.1.2018 https://www.fdd.org/wp-content/uploads/2018/01/MEMO_Bitcoin_Laundering.pdf
[106] Die Travel Rule wurde erstmals 1996 von FinCEN als Teil der Anti-Geldwäsche-Normen eingeführt, die für alle US-Finanzinstitute gelten. Seit März 2013 wurde der Geltungsbereich der Vorschrift auf Krypto-Exchanges erweitert. Siehe die aktuelle FinCEN Guidance: Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies, 9.5.2019 https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf

bislang auf einen Schwellenwert von 3.000 Dollar bezog, entspricht mit wenigen Abweichungen weitgehend der Wire Transfer Rule der FATF.[107] Im November 2019 hat Kenneth Blanco, der Direktor von FinCEN, bekräftigt, seine Regierung verlange von Krypto-Exchanges und Wallet-Providern eine strikte Einhaltung der verschärften neuen Vorgaben. Schließlich gibt es im US-Kongress Bestrebungen, den gesamten Bereich der Kryptowährungen, der in den Vereinigten Staaten (jenseits der Geldwäsche-Problematik) bislang nicht einheitlich gesetzlich geregelt ist, in einem sogenannten „Crypto-Currency Act of 2020“ umfassend zu reformieren.[108]

4.2 Erhöhte Anforderungen an Compliance und Technologie

Während die staatlichen Behörden, so heißt es im ‚Easy Guide‘, mit dem die FATF über die Regulierung im Kryptobereich informiert, ihr Wissen um die neue Technologie erweitern müssen, ist es Aufgabe der Kryptounternehmen, sich über das finanzielle Regelwerk zu unterrichten, das zukünftig für ihren Bereich gilt. Um dann in aller Deutlichkeit hinzuzufügen: „Es liegt an der Branche selbst, die Technologie zu entwickeln, um den Anforderungen der FATF gerecht zu werden, insbesondere wenn es darum geht, Informationen über Auftraggeber und Begünstigten sicher zu sammeln und zu übermitteln.“[109]

Dies bedeutet eine große Veränderung, nachdem die Kryptobranche in der Vergangenheit verglichen mit traditionellen Finanzinstituten nur geringen regulatorischen Aufwand hatte. Kaum eines der in dem Sektor tätigen Unternehmen wird umhinkommen, zusätzliches Personal für den Bereich Compliance und Geldwäschebekämpfung abzustellen. Die neuen Regeln werden für alle Unternehmen greifen, die mit digitalen Währungen und Krypto-Token arbeiten, was Kryptobörsen, dezentrale Plattformen, Custodians (Wallet-Provider), Mixer-Dienste und Krypto-Hedgefonds einschließt. Jedes Unternehmen muss KYC-Regeln umsetzen, die es ermöglichen, verdächtige Aktivitäten, die z.B. auf Terrorismusfinanzierung hindeuten, rechtzeitig zu erkennen und die Informationen mit anderen Dienstleistern und staatlichen Stellen zu teilen. [110] Gesammelte Kundeninformationen müssen wenigstens fünf Jahre lang gespeichert

[107] Ein Unterschied ist z.B. dass in den USA auch Daten über die Höhe des übersandten Betrages (transmittal amount) ausgetauscht werden. Ein tabellarischer Vergleich zwischen der Travel Rule des Bank Secrecy Act (USA) und der FATF-Empfehlung findet sich bei CipherTrace: Cryptocurrency Anti-Money Laundering Report, 2019 Q3, November 2019, S. 11 https://ciphertrace.com/wp-content/uploads/2019/12/CipherTrace-Cryptocurrency-Anti-Money-Laundering-Report-2019-Q3-2.pdf

[108] Jason Brett: Congress Considers Federal Crypto Regulators In New Cryptocurrency Act Of 2020, forbes.com, 19.12.2020 https://www.forbes.com/sites/jasonbrett/2019/12/19/congress-considers-federal-crypto-regulators-in-new-cryptocurrency-act-of-2020/#57eb0f4d5fcd

[109] FATF (Hg.): Virtual Assets: What, When and How? (Easy Guide to FATF Standards and Methodology), ohne Datum (Dezember 2019) http://www.fatf-gafi.org/media/fatf/documents/bulletin/FATF-Booklet_VA.pdf

[110] Die Ausweitung der Verpflichteten erhöht zusätzlich die Notwendigkeit, Aufwuchs und Spezialisierung der entsprechenden staatlichen Stellen voranzutreiben. Diese müssen in die Lage versetzt sein, komplexe Vorgänge im Bereich des Kryptozahlungsverkehr zu ermitteln und gegebenenfalls zur Anklage zu bringen.

werden.[111] Schließlich müssen die Unternehmen Möglichkeiten vorsehen, im Ernstfall eingreifen zu können, also z.B. Transaktionen an inkriminierte Wallets zu unterbinden oder im Zusammenspiel mit Strafverfolgungsbehörden Krypto-Guthaben einzufrieren.[112]

Sobald sich die Anwendung der Wire Transfer Rule abzeichnete, gab es erschreckte Reaktionen. Schon im April 2019, als die wichtigsten Vorschläge der FATF bekannt wurden, äußerte Jonathan Levin Bedenken, ein Mitgründer der namhaften Beratungsfirma Chainalysis. Kryptowerte seien grundsätzlich so konzipiert, sagte Levin, dass man Zahlungen vornehmen könne, ohne den Empfänger zu identifizieren. Gelder könnten in eine persönliche Wallet transferiert werden, die gar nicht in der Lage sei, Kundenidentifikationsdaten entgegenzunehmen. [113] Daher könnten die neuen Regulierungsschritte dazu führen, dass viele Plattformen den Betrieb einstellen müssten, da derzeit noch keine Technologie existiere, um entsprechende Informationen zu übermitteln. Levin gab weiter zu bedenken, dass eine Gängelung prinzipiell kooperativer Krypto-Exchanges die Nutzer dazu verleiten könnte, vermehrt zu dezentralen oder P2P-Plattformen abzuwandern. Damit würde aber die Transparenz verringert, von der die Ermittler bisher profitierten.

Daneben gab es versöhnliche Stimmen. Nüchtern betrachtet erscheinen manche Befürchtungen übertrieben. Der Hauptanreiz etwa für Bitcoin-Nutzer liegt nicht darin, sich staatlicher Aufsicht zu entziehen, sondern Transaktionen kostengünstig und schnell auszuführen. Phil Liu, Chief Legal Officer des kalifornischen Krypto-Hedgefonds Arca, kommentierte die Veröffentlichung der neuen FATF-Empfehlungen damit, Krypto-Fachleute machten gerne eine große Sache daraus, der Regierung Kundendaten zu überlassen. Er sehe aber „nicht viele Disruptionen für legitime Nutzer, wenn der Vorschlag umgesetzt wird“.[114]

Einleuchtender sind die ökonomischen Sorgen der jungen Branche, die zahlreiche kleinere Firmen und Startups einschließt. Die eingeleitete Regulierungswelle im Kryptobereich, dürfte die Kosten angesichts zusätzlicher Compliance-Maßnahmen und der fälligen technologischen Aufrüstung in die Höhe treiben. Somit wird sich die Schwelle, um als Unternehmen im Krypto-Finanzsektor zu operieren, erhöhen, und manche Geschäftsmodelle werden in Zukunft nicht mehr funktionieren. Die Gewinnmargen dürften sich in vielen Fällen verringern, und in der Kryptobranche werden vielleicht teilweise Bedingungen einziehen, wie sie bisher die traditionelle Finanzwelt kennt.

---

[111] FATF (Hg.): Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, S. 27 (Nr. 102)
[112] FATF (Hg.): Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, S. 29 (Nr. 114)
[113] Nikhilesh De: ‘Onerous’ FATF Recommendations Harmful for Crypto Transparency: Chainalysis, 12.4.2019 https://www.coindesk.com/chainalysis-onerous-fatf-recommendations-harmful-for-crypto-transparency
[114] Zitiert nach Lukas Hofer: FATF veröffentlicht neue Krypto-Richtlinien – Bedrohung oder Chance?, ico.li (Liechtenstein), 24.6.2019 https://www.ico.li/de/fatf-veroffentlicht-neue-krypto-richtlinien/

Als Hauptproblem bleibt die technologische Umsetzung der Wire Transfer Rule der FATF. Im November 2019, kamen Softwareentwickler verschiedener Firmen bei einer von der Analysefirma CipherTrace organisierten Konferenz, an der auch US-Regierungsexperten teilnahmen, zu dem Schluss, die Kryptobranche tue sich schwer mit der Forderung der FATF, alle Vorgaben bis Juni 2020 vollständig umzusetzen. Trotzdem seien die Krypto-Unternehmen auf dem richtigen Weg, zumindest vorläufige Lösungen zu finden.[115] Einen Monat zuvor hatte John Roth, Chief Compliance Officer der US-Kryptobörse Bittrex, negativer geklungen. Seines Wissens halte bislang niemand in der Branche die Travel Rule ein. Die große Schwierigkeit bestehe darin, erklärte er sinngemäß, dass man sich auf einen neuen Industriestandard einigen müsse. Neue und noch nicht in der Praxis erprobte technische Lösungen müssten imstande sein, die Geschwindigkeit und das hohe Datenvolumen zu bewältigen.[116]

CipherTrace publizierte einen Bericht für das dritte Quartal 2019, der erstmals einen Blick auf die KYC-Praxis von Krypto-Handelsplattformen in der ganzen Welt zulässt.[117] Demnach lassen die Legitimationsprüfungen weiter stark zu wünschen übrig. Die Unternehmen seien schlecht vorbereitet auf die Übernahme der FATF-Regeln. Zwei Drittel der 120 wichtigsten Exchanges verfolgten keine konsequente KYC-Politik, geschweige denn dass sie die demnächst verbindliche Wire Transfer Rule einhielten. Ändere sich nichts an dem alarmierenden Befund, müssten viele Exchanges mit Konsequenzen rechnen. Ein Drittel aller Plattformen lasse immer noch den Handel mit Privacy Coins wie Zcash und Monero zu. Umgekehrt habe der Großteil der Exchanges jedoch schon damit begonnen, Privacy Coins aus dem Angebot zu nehmen. Privacy Coins, darunter Monero, behindern die Rückverfolgung von Transaktionen erheblich. In der Folge können Krypto-Dienstleister der Wire Transfer Rule nur bedingt Folge leisten, die vorsieht, dass Krypto-Dienstleister Einsicht in die Konten und Handelsaktivität der Kunden nehmen. Für die Exchanges wäre es praktisch unmöglich, die Herkunft von Privacy Coins zu ermitteln, die auf Börsen-Wallets der Kunden überwiesen wurden.

Das europäische Analysehaus Crystal, das zum niederländischen Blockchain-Unternehmen Bitfury gehört, veröffentlichte im September 2019 einen Bericht über die historischen Bitcoin-Finanzströme zwischen den weltweiten Kryptobörsen. Darin ging es auch um die Frage, wie sich die FATF-Regeln künftig auf den Bitcoin-Zahlungsverkehr auswirken werden. Die Forscher sagen voraus, dass die Zahl der Exchanges, die von unbekannten Herkunftsländern operieren, deutlich zurückgehen wird, da sie nach den FATF-Regeln ohne offizielle Registrierung und Lizenz nicht mehr legal operieren können. Die Travel Rule (bzw. Wire Transfer Rule) werde die Einhaltung der Börsenvorschriften zweifellos komplizierter machen, doch die Gefahr eines weltweiten kriminellen

[115] Valentina Kirilova: CipherTrace conference sheds light on FATF 'Travel Rule' for user info, LeapRate.com, 22.11.2019 https://www.leaprate.com/cryptocurrency/blockchain/ciphertrace-conference-sheds-light-on-fatf-travel-rule-for-user-info/
[116] Henry Linver: FATF AML Regulation: Can the Crypto Industry Adapt to the Travel Rule?, Cointelegraph, 10.10.2019 https://cointelegraph.com/news/fatf-aml-regulation-can-the-crypto-industry-adapt-to-the-travel-rule
[117] Cryptocurrency Anti-Money Laundering Report, 2019 Q3, November 2019 https://ciphertrace.com/wp-content/uploads/2019/12/CipherTrace-Cryptocurrency-Anti-Money-Laundering-Report-2019-Q3-2.pdf

Missbrauchs von Kryptowerten könnte sich am Ende erheblich verringern, lautet die optimistische Prognose.[118]

4.3 Umsetzung der Fünften EU-Geldwäscherichtlinie

In der Europäischen Union fiel die Übernahme der neuen FATF-Empfehlungen mit der Umsetzung der jüngsten EU-Geldwäscherichtlinie zusammen. Im Mai 2018 war die Änderungsrichtlinie zur Vierten Geldwäscherichtlinie verabschiedet worden, die meist als Fünfte Geldwäscherichtlinie (AMLD5) bezeichnet wird.[119] Der Anwendungsbereich der Richtlinie wird künftig auf Plattformen zum Umtausch virtueller Währungen sowie Wallet-Provider ausgedehnt, um Nutzer von Kryptowährungen leichter identifizieren zu können. Die Umsetzung in nationales Recht musste bis zum 10. Januar 2020 erfolgen. Deutschland kam dieser Pflicht rechtzeitig nach. Die Neuregelungen, die vor allem das Geldwäsche- und das Kreditwesengesetz betrafen, traten Anfang 2020 in Kraft.[120]

Die Verschärfung der Sorgfaltspflichten gemäß der Fünften EU-Richtlinie ist an zwei Stellen besonders relevant aus Sicht der Terrorfinanzierungsbekämpfung. So wird u.a. verlangt, dass die Verpflichteten Hintergrund und Zweck aller Transaktionen untersuchen sollen, die ungewöhnlichen Transaktionsmuster folgen und keinen offensichtlichen wirtschaftlichen oder rechtmäßigen Zweck haben. Um zu entscheiden, ob diese Transaktionen oder Tätigkeiten verdächtig sind, sollen die Verpflichteten bestehende Geschäftsbeziehungen besser überwachen. Der neu eingefügte Artikel 18a sieht außerdem vor, bei Transaktionen, an denen Drittländer mit hohem Risiko beteiligt sind, zusätzliche Informationen einzuholen.[121]

In der öffentlichen Diskussion des deutschen Umsetzungsgesetzes kam das Thema Kryptowerte nur relativ am Rande vor. Viele der neuen Vorschriften betrafen schließlich andere Branchen wie den Edelmetallhandel, den Erwerb von Immobilien (Offenlegung der wirtschaftlich Berechtigten) oder verschärfte Prüfpflichten für Notare. Die Änderungen im Kryptobereich zielen vor allem auf einen Punkt. Das Kryptoverwahrgeschäft, wie der neue deutsche Terminus lautet, wird künftig als Finanzdienstleistung eingestuft. [122] Jede Form des Handels mit Kryptowerten wird

[118] Bitfury Crystal (Hg.): Report on International Bitcoin Flows 2013- 2019, September 2019 https://crystalblockchain.com/assets/reports/International%20Bitcoin%20Flows%20Report%20for%202013-2019%20-%20by%20Crystal%20Blockchain,%20Bitfury.pdf
[119] 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 und zur Änderung der Richtlinien 2009/138/EG und 2013/36/EU https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32018L0843&from=DE
[120] Gesetz zur Umsetzung der Änderungsrichtlinie zur Vierten EU-Geldwäscherichtlinie, 12.12.2019 https://www.bundesfinanzministerium.de/Content/DE/Standardartikel/Themen/Internationales_Finanzmarkt/2019-07-31-bekaempfung-geldwaesche.html
[121] Für einen Überblick der Änderungen und zur Entwicklung der bisherigen EU-Geldwäscherichtlinien siehe die Zusammenfassung von Regula Heinzelmann: Die 5. EU-Geldwäscherichtlinie in der Umsetzung, haufe.de, 5.9.2018 https://www.haufe.de/compliance/recht-politik/geldwaescherichtlinie_230132_468208.html
[122] Merkblatt: Hinweise zum Tatbestand des Kryptoverwahrgeschäfts, 2.3.2020 https://www.bafin.de/dok/13710900

erlaubnispflichtig, und die Anbieter werden künftig von der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) beaufsichtigt.[123] Dabei stand auch schon vor Einführung des Kryptowertes als Finanzinstrument der gewerbliche Handel mit Kryptowährungen unter Erlaubnisvorbehalt der BaFin. Diese Verwaltungspraxis war jedoch in Frage gestellt worden. So urteilte das Berliner Kammergericht im Jahr 2018, der nicht erlaubte Bitcoin-Handel sei keine Straftat und die BaFin habe ihren Aufgabenbereich überspannt.[124] Die gesetzliche Neuregelung hat diese Unklarheit ausgeräumt.

In Deutschland ansässige Dienstleister, die virtuelle Währungen in Fiatgeld und zurücktauschen, sowie Wallet-Provider werden zugleich in den Kreis der geldwäscherechtlich Verpflichteten aufgenommen, die höhere Sorgfaltspflichten erfüllen und Verdachtsfälle melden müssen. Dazu muss man wissen, dass der Bundesregierung im August 2019 nur drei Unternehmen bekannt waren, die hierzulande im Kryptoverwahrgeschäft aktiv sind.[125] Es wird allerdings mit einem deutlichen Anstieg gerechnet.

Mit Einführung der neuen EU-Geldwäscheregeln in Verbindung mit der Wire Transfer Rule der FATF haben die Europäer, so kann man es verstehen, mit mehrjähriger Verzögerung Grundzüge des amerikanischen Anti-Geldwäsche-Regelwerks bezüglich Kryptowährungen übernommen. Wobei die Amerikaner an einer wichtigen Stelle weitergehen als die Europäer. In den Vereinigten Staaten unterliegt nämlich auch der Krypto-Krypto-Zahlungsverkehr der Aufsicht, während die EU in diesen Bereich der Krypto-Transaktionen (also ohne direkten Bezug zu Fiatwährungen) vorerst nicht regulierend eingreift.[126]

Die Europäische Union hat bisher keine spezifische Gesetzeslage für Kryptowährungen vorgesehen. Dabei besteht allgemein Einigkeit, dass eine nationale Regulierung im Kryptobereich lediglich eine Brückenlösung darstellen kann. Die Bundesregierung signalisiert inzwischen, was eine weitere Regulierung betreffe, etwa hinsichtlich spezieller Krypto-Token wie Security Token oder geplante Stablecoins wie Libra, eine angekündigte Regulierung im EU-Rahmen abwarten zu wollen.[127] Der Vizepräsident der Europäischen Kommission, Valdis Dombrovskis, hat im Oktober 2019 tatsächlich einen neuen Legislativvorschlag angekündigt, für den es noch keinen Zeitplan gibt. Hierin kam

[123] Die BaFin kündigte an, dass im Jahr 2020 „Distributed-Ledger-Technologie (DLT) und die auf ihr basierenden Kryptowerte" einen Schwerpunkt der Aufsicht der Behörde darstellen werden. BaFin: Aufsichtsschwerpunkte 2020, Bonn und Frankfurt am Main, Dezember 2019, S. 9ff. https://www.bafin.de/SharedDocs/Downloads/DE/Broschuere/dl_Aufsichtsschwerpunkte2020.pdf?__blob=publicationFile&v=4

[124] Markus Frühauf: Regelungen bedrohen Bitcoin und Co., Frankfurter Allgemeine Zeitung, 24.7.2019 https://www.faz.net/aktuell/finanzen/digital-bezahlen/kampf-gegen-geldwaesche-regeln-fuer-geschaefte-mit-kryptowaehrung-16299333.html

[125] „Drei Betreiber im Kryptoverwahrgeschäft", 29.8.2019 https://www.bundestag.de/presse/hib/655760-655760

[126] Serhii Mokhniev: European AML Regulations Follow the US Path With a Six-Years' Delay, Cointelegraph, 30.11.2019 https://cointelegraph.com/news/european-aml-regulations-follow-the-us-path-with-a-six-years-delay

[127] Politik zu zaghaft. Gesetzentwurf für Blockchain verzögert sich, Frankfurter Allgemeine Zeitung, 15.11.2019

der Kurswechsel zum Ausdruck, den vor allem die breite öffentliche Diskussion um Facebooks geplante Libra-Währung ausgelöst hat. Dabei hatte sich der lettische EU-Kommissar bislang gegen die Regulierung digitaler Währungen ausgesprochen. Inzwischen hat er sich der Auffassung angeschlossen, dass ein Umdenken der EU-Mechanismen zur Bekämpfung der Finanzkriminalität erforderlich ist.[128]

Ein von der Kommission eingesetztes EU-Expertengremium, das regulatorische Hindernisse für finanzielle Innovationen identifizieren sollte, hat im Dezember 2019 einen Bericht vorgelegt, der auch eine Reihe von Empfehlungen enthält, die sich auf den Kryptobereich beziehen.[129] Letztlich wird eine umfassende Harmonisierung auf dem Gebiet gefordert, angefangen mit den Risiken, die sich aus dem Fehlen einer gemeinsamen Taxonomie bezüglich Kryptowerten und den daher fragmentierten nationalen Ansätzen zur Klassifizierung von Kryptowerten im Rahmen von EU-Vorschriften und nationalen Rechtsvorschriften ergeben. Die Anforderungen an die kundenbezogenen Sorgfaltspflichten (KYC-Prozesse) sollten, so die Empfehlung, vollständig vereinheitlicht werden, gerade im Hinblick auf die Bestimmungen zur Erfassung von Kundendaten. Für einen einheitlichen EU-Ansatz auf dem Gebiet der Kryptowerte wird das grundlegende Prinzip formuliert, „dass für Tätigkeiten, die die gleichen Risiken verursachen, die gleichen Regeln gelten sollten, um eine Fragmentierung in dieser Hinsicht zu vermeiden“.[130]

Es ist vermutlich kein Zufall, dass sich der stellvertretende französische Notenbankchef Denis Beau kürzlich im Verlauf einer Rede über die Rolle der Kryptowerte im Zahlungssystem auf den gleichen Grundsatz – auf Englisch „same activities, same risks, same rules” – berief.[131] Man muss an der Stelle hinzufügen, wenn in diesem Zusammenhang von Risiken die Rede ist, sich dies auf finanzielle Stabilitätsrisiken ebenso wie die Bekämpfung der Geldwäsche und Terrorismusfinanzierung erstreckt. Eine weitere Harmonisierung der EU-Geldwäscheregeln ist jedenfalls sehr wahrscheinlich.

4.4 Die politische Diskussion um Stablecoins

Die internationale Beschäftigung mit dem Thema Kryptowährungen erfuhr seit Sommer 2019 beträchtlichen Auftrieb durch die Ankündigung von Facebook, in Gemeinschaft mit einer Reihe anderer Unternehmen eine eigene Blockchain-basierte Kryptowährung namens Libra zu gründen.[132] Diese soll durch Anbindung an einen Währungskorb relative

[128] Moritz Draht: EU-Kommissar Dombrovskis fordert eindeutige Gesetzgebung für Krypto-währungen, BIT-Echo, 9.10.2019 https://www.btc-echo.de/eu-kommissar-dombrovskis-fordert-eindeutige-gesetzgebung-fuer-kryptowaehrungen/
[129] Expert Group on Regulatory Obstacles to Financial Innovation (ROFIEG): Thirty Recommendations on Regulation, Innovation and Finance. Final Report to the European Commission, 13.12.2019 https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/191113-report-expert-group-regulatory-obstacles-financial-innovation_en.pdf
[130] Thirty Recommendations on Regulation, Innovation and Finance. S. 58
[131] Denis Beau: The role of cryptoassets in the payment system, Official Monetary and Financial Institutions Forum (OMFIF) Meeting, London, 15.10.2019 https://www.bis.org/review/r191015b.htm
[132] Libra Whitepaper (deutsche Fassung) https://libra.org/de-DE/white-paper

Stabilität erlangen und damit einen Hauptnachteil bestehender Kryptowährungen, also deren hohe Volatilität bzw. großen Wertschwankungen, vermeiden. Ein nutzerfreundlicher ‚Stablecoin' mit starker finanzieller Rückendeckung, so die Erwartung, könnte zu einer attraktiven digitalen Währung aufsteigen. Gerade Menschen in den Schwellen- und Entwicklungsländern sollten Gefallen an einer wertstabilen Parallelwährung finden, welche die eigenen nationalen Fiatwährungen in den Schatten stellt. Im Unterschied zu führenden Kryptowährungen wie Bitcoin oder Ethereum würden die Mitglieder der in der Schweiz beheimateten Libra Association die neue digitale Währung nicht als offenes Netzwerk betreiben. Dies hätte anscheinend den technischen Vorteil, im Vergleich z.B. zu Bitcoin die Transaktionsgeschwindigkeit der Digitalwährung wesentlich zu steigern bei gleichzeitig niedrigem Energieverbrauch.[133]

Inzwischen ist das Projekt ins Stocken geraten, mehrere beteiligte Firmen sind wieder abgesprungen. Wegen des politischen Widerstands nicht nur der amerikanischen Regierung wurden die Pläne abgeschwächt, bis zuletzt nur noch von einem ‚globalen Zahlungssystem' anstelle einer neuen Währung die Rede war. Die meisten Staaten wollen offenkundig einen Machtverlust, der mit der Schwächung bestehender staatlicher Währungen einhergeht, verhindern und argumentieren mit der notwendigen Stabilität des internationalen Finanzsystems. Die Zugkraft der hinter Libra stehenden Idee wurde aber deutlich, als mehrere Regierungen ankündigten, eine eigene staatliche Digitalwährung ins Leben zu rufen. Auch Bundesfinanzminister Olaf Scholz sprach davon, Europa müsse den digitalen Euro vorantreiben, um das Feld nicht anderen Staaten oder Privatanbietern zu überlassen.[134] Am weitesten fortgeschritten sind die Vorbereitungen in China. Dort hat die Regierung ein Pilotprojekt für eine weltweit erste staatliche Digitalwährung lanciert.[135]

Auf der anderen Seite bestehen Zweifel, ob Notenbanken ernsthaft daran interessiert sind, eigene Kryptowährungen einzuführen. Bei der Europäischen Zentralbank sollen derzeit noch keine Vorarbeiten geplant sein.[136] Eher im Sinne der Politik scheint es, durch Ankündigungen eines Stablecoin die Banken dahin zu bringen, den ineffizienten und teuren grenzüberschreitenden Zahlungsverkehr zu verbessern. Ob es sich um Ablenkungsmanöver handelt oder nicht, die Regierungen möchten dem Libra-Projekt gerne den Wind aus dem Segel nehmen. Längst haben Großbanken wie JPMorgan und UBC eigene Pläne für digitale Stablecoins angekündigt. Übrigens bestanden schon vor der Ankündigung von Facebook, wie leicht vergessen wird, private Stablecoins, darunter Tether, die aktuell vierthäufigste Kryptowährung, die ebenfalls das Ziel der Wertstabilität

[133] Wolfgang Prinz: Die Idee hinter Libra ist wichtig für Deutschland, Frankfurter Allgemeine Zeitung, 7.12. 2019 (aktualisierte Online-Fassung vom 10.12.) https://www.faz.net/aktuell/finanzen/finanzmarkt/facebook-plant-eine-weltumspannende-digitale-waehrung-16522969.html
[134] Interview in der Wirtschaftswoche, 3.10.2019 https://www.wiwo.de/politik/deutschland/finanzminister-scholz-sehr-sehr-kritisch-gegenueber-libra/25084172.html
[135] Mike Orcutt: Pilottest für Chinas staatliche Kryptowährung, Technology Review, 19.12.2019 https://www.heise.de/tr/artikel/Pilottest-fuer-Chinas-staatliche-Digitalwaehrung-4615207.html
[136] Martin Arnold: Central bank talk of launching cryptocurrencies is all bluff, Financial Times, 5.12.2019 https://www.ft.com/content/5988c3f4-15e6-11ea-9ee4-11f260415385

(beispielsweise durch Anbindung an den Dollar oder an einen Korb von Kryptowährungen) verfolgen.[137]

Vorsorglich kündigte die FATF im Oktober 2019 an, dass Stablecoins und deren Provider ebenfalls ihren Standards zur Geldwäschebekämpfung unterliegen würden.[138] Eine weitere Befassung der FATF mit dem Thema ist geplant. Dabei sind Sicherheitsaspekte von der Stablecoin-Diskussion so lange kaum berührt, wie die angekündigten Projekte noch im Raum schweben und ihre Ausgestaltung offen ist. Zudem ist es kaum einzusehen, warum Terroristen und andere Kriminelle bevorzugt auf eine staatlich kontrollierte Kryptowährung oder ein von Regierungsseite stark beeinflusstes digitales Zahlungssystem (Libra) zugreifen sollten. Anders sähe es aus, wenn von Sanktionen bedrohte Außenseiterstaaten wie Iran oder Nordkorea die Einführung von Digitalwährungen ernsthaft ins Auge fassen. Bislang besteht die Bedeutung der Diskussion um Libra oder staatliche Digitalwährungen offenbar darin, dass sich die Weltöffentlichkeit an die Normalität von Kryptowährungen allmählich gewöhnt. Der Aufstieg von Libra oder einem digitalen Euro könnte deshalb auch Bitcoin und anderen Kryptocoins zu neuem Auftrieb verhelfen. Eine größere Verbreitung der Kryptowährungen insgesamt könnte dann wiederum das Ausmaß der möglichen Nutzung durch Kriminelle oder Terrorgruppen erhöhen.

5 Die nächsten Schritte

Aufgrund der schnellen technischen Entwicklungen im Bereich von Kryptowährungen und den weiterwachsenden technischen Fähigkeiten verschiedener Terrororganisationen ist zu erwarten, dass diese Form der Terrorismusfinanzierung kurz- bis mittelfristig an Bedeutung gewinnen wird. Unverkennbar besteht daher Bedarf, das volle Potenzial für die terroristische Nutzung von Kryptowährungen zu verstehen. Und es stellt sich die Frage, wie staatliche Regulierungs- und Aufsichtsbehörden am besten auf diese Entwicklungen reagieren sollten.

In den letzten zwei Jahren ist die Regulierung des Krypto-Finanzsektors weltweit in Bewegung geraten. Erkenntnisse über die wachsenden Gefahren, die von den nicht nur in Europa kaum oder gar nicht überwachten Krypto-Finanzströmen für die Bekämpfung der Geldwäsche und Terrorismusfinanzierung ausgehen, haben erste Regulierungsschritte notwendig gemacht. Mit der Umsetzung der FATF-Empfehlungen von Juni 2019 ist jetzt ein erster wichtiger Schritt getan. Die vereinbarten Maßnahmen zielen darauf ab, Kryptobörsen auf der ganzen Welt analog zu traditionellen Finanzinstituten zu behandeln. Deutschland und andere Staaten sind auf dem richtigen

[137] Alex Anderson: Stablecoins for Beginners. What they are, how they work and where to buy them, Selbstverlag 2019 (Amazon Fulfillment, ISBN 9781077031005)
[138] Money laundering risks from “stablecoins” and other emerging assets, 18.10.2019 https://www.fatf-gafi.org/publications/fatfgeneral/documents/statement-virtual-assets-global-stablecoins.html

Weg, die bislang tolerierte, aber wegen der vorhandenen signifikanten Sicherheitsrisiken gefährliche Praxis tendenziell anonymer Kryptotransaktionen zu unterbinden.

Eine große Schwierigkeit liegt jedoch in der hohen Geschwindigkeit, mit der sich die zugrunde liegende Technologie verändert. Es wäre eine Täuschung zu glauben, der aktuelle Regulierungsansatz, der sich auf die Kryptobörsen bzw. auf die Schnittstellen zwischen Fiatgeld und Kryptowerten konzentriert, biete eine ausreichende Lösung. Die Regulierer werden weiterhin den technologischen Entwicklungen hinterherlaufen. Unterschiede zwischen dem Bankenzahlungsverkehr und dem Krypto-Finanzsektor werden bestehen bleiben. Die Staaten müssen daher ihren Regulierungsansatz in den nächsten Jahren fortentwickeln und ‚feintunen'. Dabei hoffen sie auf die Mitwirkung der Kryptounternehmen, die daran interessiert sind, ihr Geschäftsmodell anzupassen und zu erhalten.

Aus Sicht der deutschen staatlichen Akteure und der betroffenen Kryptobranche stehen also weitere Aufgaben bevor. Einige Probleme im Zusammenhang mit Kryptowährungen wurden bisher vernachlässigt und einige der bereits identifizierten Schwachstellen noch nicht beseitigt. Die folgenden Empfehlungen setzen hier an. Zu bedenken ist auch, dass sich hierzulande ein innovativer Blockchain-Sektor herausgebildet hat, der aus einer konsistenten Regulierung Vorteile ziehen kann.

1. Deutschland sollte parallel vorgehen – also eine Regulierung des Kryptosektors im EU-Rahmen unterstützen, aber in der Zwischenzeit nicht zögern, das eigene Regelwerk in AML/CFT-Fragen dort anzupassen, wo es nötig erscheint.

Mittlerweile zeichnen sich, auch unter dem Eindruck der Debatte um staatliche Stablecoins, neue Initiativen auf EU-Ebene ab, den gesamten Kryptobereich stärker zu harmonisieren. Erkenntnisse aus dem Umgang mit Kryptowährungen und elektronischen Geldbörsen (Wallets) beeinflussen die Diskussion über neue Normen in der Geldwäschebekämpfung. Daher läge es eigentlich nahe, an diesen Bemühungen teilzuhaben und vorläufig darauf zu verzichten, die eigenstaatliche Regelsetzung voranzutreiben. Im Zuge der Online-Konsultation zur Erarbeitung der Blockchain-Strategie der Bundesregierung gab es übrigens unter den Unternehmen ganz unterschiedliche Auffassungen darüber, ob eine Regulierung auf europäischer oder nationaler Ebene vorzuziehen sei.[139]

Schließlich ist nochmals an den Zeitfaktor zu erinnern. Andreas Krautscheid, der Hauptgeschäftsführer des Bankenverbandes, machte im Kontext der Libra-Diskussion darauf aufmerksam, dass es seinerzeit bei der EU-Zahlungsdiensterichtlinie fast acht Jahre von der Idee zur Umsetzung gedauert habe.[140] Davon abgesehen kann die eventuelle Einrichtung einer weiteren EU-Behörde keine vordringliche Lösung sein,

[139] Online-Konsultation zur Erarbeitung der Blockchain-Strategie der Bundesregierung. Gesammelte Stellungnahmen, die zwischen dem 20. Februar und 30. März 2019 eingegangen sind (siehe z.B. S. 186, 212, 380, 814) https://www.blockchain-strategie.de
[140] Andreas Krautscheid: Interview mit der Wirtschaftswoche, 31.10.2019 https://bankenverband.de/newsroom/reden_und_interviews/interview-wiwo-ak-libra/

zumal ungewiss wäre, welche Befugnisse an eine solche zentrale Stelle übertragen werden könnten.

2. Es ist unerlässlich, die vorhandene Expertise bei den staatlichen Stellen zu erhöhen und das Nebeneinander an Zuständigkeiten in der Geldwäschebekämpfung insbesondere im Kryptobereich zu verringern.

Die Bekämpfung von Geldwäsche und Terrorismusfinanzierung ist in Deutschland nicht durchgehend wirksam und kostengünstig organisiert. Grundsätzlich gibt es eine Arbeitsteilung durch die Sicherheits- und Strafverfolgungsbehörden des Bundes und der Länder. Dabei liegt die Strafverfolgung im Bereich der Geldwäsche maßgeblich in der Verantwortung der Länder, praktisch gesehen bei den jeweils zuständigen Staatsanwaltschaften, die durch die Polizeibehörden und die Zollfahndung unterstützt werden. Im Bereich der Terrorismusfinanzierungsbekämpfung sieht die Arbeitsteilung ein Zusammenwirken von Staatsanwaltschaften und Sicherheitsbehörden des Bundes und der Länder vor.[141]

Die Zentralstelle für die Sammlung und Auswertung von Verdachtsmeldungen im Zusammenhang mit Geldwäsche oder Terrorismusfinanzierung ist die Financial Intelligence Unit (FIU), die als eigenständige Behörde (mit Hauptsitz in Köln) in die Generalzolldirektion eingebettet ist.[142] Von der FIU werden Verdachtsmeldungen zentral entgegengenommen und untersucht. Die FIU soll wichtige Fälle herausfiltern und an die zuständigen Strafverfolgungsbehörden weiterreichen.[143]

Im Bereich der Terrorismusfinanzierungsbekämpfung sieht es zunächst so aus, dass die FIU alle terrorismusrelevanten Meldungen sofort an das Bundesamt für Verfassungsschutz zur Kenntnis weitergibt, das gegebenenfalls die betroffenen Landesämter für Verfassungsschutz einschaltet. Das Ergebnis der operativen Analyse leitet die FIU bei Sachverhalten mit Staatsschutzrelevanz an die zuständige Strafverfolgungsbehörde (Staatsschutzabteilung bei den Landeskriminalämtern oder Staatsanwaltschaft).[144]

Vorgesehen ist derzeit, die FIU durch den vermehrten Zugriff auf relevante Datenbestände im Zusammenhang mit Geldwäsche und Terrorismusfinanzierung zu stärken. Die Behörde wirkt allerdings überlastet und ist stark in die Kritik geraten. Die Rede ist von einer „Aufklärungsmisere“. In der Berichterstattung wird meist ein Zusammenhang hergestellt mit einer womöglich fragwürdigen Reorganisation im Sommer 2017. Bis dahin war das Bundeskriminalamt für die FIU zuständig gewesen. Insgesamt trafen im Jahr 2018 77.252 (2017: 59.845) Verdachtsmeldungen ein. Wie im

[141] Die spezialisierte Staatsanwaltschaft des Bundes bei Straftaten im Zusammenhang mit Terrorismusfinanzierung ist der Generalbundesanwalt beim Bundesgerichtshof. Letztlich entscheidet die Einstufung bzw. Bedeutung des jeweiligen Falls darüber, ob Bundes- oder Landesbehörden die Zuständigkeit übernehmen. Siehe dazu Erste Nationale Risikoanalyse, S.52f.
[142] Die offizielle (wenig gebräuchliche) Bezeichnung lautet Zentralstelle für Finanztransaktionsuntersuchungen.
[143] Erste Nationale Risikoanalyse, S. 39ff.
[144] Erste Nationale Risikoanalyse, S. 51

August 2019 bekannt wurde, hatte sich zum damaligen Zeitpunkt ein Rückstau von mehr als 46.000 nicht abgeschlossenen Verfahren angehäuft.[145]

Die FIU registrierte, wie schon an anderer Stelle erwähnt, im Jahr 2018 „rund 570" Verdachtsmeldungen von Verpflichteten, die im Zusammenhang mit Kryptowährungen stehen. Mit der Ausweitung des Kreises der Verpflichteten infolge der Umsetzung der Fünften EU-Geldwäscherichtlinie sei mit einem starken Anstieg der Verdachtsmeldungen in diesem Bereich zu rechnen, gab die Behörde selbst zu bedenken. [146]

Zu diesen bestehenden großen Problemen kommt hinzu, dass es bei Verdachtsmeldungen häufig an Gesprächspartnern bei staatlichen Stellen fehlt, die sich mit dem Kryptozahlungsverkehr auskennen und auf Verdachtsmeldungen in dem Bereich reagieren. Wie der Experte eines Krypto-Dienstleisters mitteilte, besteht derzeit bei Verdachtsmeldungen, die Kryptowährungen betreffen, auf dem Meldebogen lediglich die Option, anzugeben, ob es sich um Bitcoin oder eine andere Kryptowährung handele.[147] Es steht zu vermuten, dass die meisten Ermittler mit Hinweisen auf eine der zahlreichen anderen Kryptowährungen ohnehin wenig anzufangen wissen.

Das Fehlen qualifizierter Experten trifft wohlgemerkt die gesamte Blockchain-Branche. Laut einer im Jahr 2019 durchgeführten Unternehmensbefragung herrscht die Erwartung, dass in Deutschland auf Dauer ein deutlicher Mangel an Blockchain-Experten droht.[148] Auch in Zukunft wird nicht zu erwarten sein, dass es möglich ist, in jedem Landeskriminalamt und jeder Staatsanwaltschaft Ermittler mit Kenntnissen über Kryptowährungen zu etablieren. Daher erscheint es sinnvoll, dass Bund und Länder einen gemeinsamen Pool von Spezialisten einrichten, auf den z.B. die Strafverfolgungsbehörden zugreifen können. [149] Ein solches zentrales Analysezentrum könnte bei der FIU angesiedelt sein. Für eine Übergangszeit könnten auch Partner aus dem privaten Sektor hinzugezogen werden. Blockchain-Analysetools sind im kommerziellen Sektor schon entwickelt und eingesetzt und ermöglichen eine genaue Überwachung des Kryptowährungsbereichs. Solche technischen Fähigkeiten sollten auf jeden Fall Teil der Instrumente der Finanzaufsichtsbehörden werden.

---

[145] Diese Angabe entstammt der Antwort der Bundesregierung auf eine schriftliche Anfrage des FDP-Abgeordneten Markus Herbrand, siehe Jan Willmroth: Der Stapel wächst, Süddeutsche Zeitung, 8.10.2019 https://www.sueddeutsche.de/wirtschaft/zoll-der-stapel-waechst-1.4631795

[146] Financial Intelligence Unit: Jahresbericht 2018, S.36 https://www.zoll.de/SharedDocs/Downloads/DE/Links-fuer-Inhaltseiten/Fachthemen/FIU/fiu_jahresbericht_2018.pdf?__blob=publicationFile&v=3

[147] Interview, September 2019.

[148] Bitkom e.V. (Hg.): Blockchain in Deutschland – Einsatz, Potenziale, Herausforderungen. Studienbericht 2019, S.38 https://www.bitkom.org/Bitkom/Publikationen/Blockchain-Deutschland-Einsatz-Potenziale-Herausforderungen

[149] Eventuell bietet sich ein Vergleich an mit der Zentralstelle zur Bekämpfung der Internet- und Computerkriminalität (ZIT), die im Jahr 2010 als Gießener Außenstelle der Staatsanwaltschaft Frankfurt am Main eingerichtet wurde. Die ZIT ist erster Ansprechpartner des Bundeskriminalamtes für Internetstraftaten bei noch ungeklärter örtlicher Zuständigkeit in Deutschland oder bei Massenverfahren gegen eine Vielzahl von Tatverdächtigen bundesweit. https://staatsanwaltschaften.hessen.de/staatsanwaltschaften/gsta-frankfurt-am-main/aufgabengebiete/zentralstelle-zur-bekämpfung-der

3. Die Behörden müssen von Krypto-Anbietern Compliance-Erfahrungen und Prozesse verlangen und diese nachprüfen. Beide Seiten sollten bei der Suche nach einem geeigneten und kostengünstigen Weg kooperieren, um die neuen FATF-Regeln einzuhalten.

Die bis Juni 2020 verpflichtende Anwendung der Wire Transfer Rule durch die betroffenen Krypto-Unternehmen und ihre Überwachung durch die Aufsichtsbehörden sind Test dafür, ob das neue Regelwerk funktioniert. Für Deutschland steht einiges auf dem Spiel, da schon die Vorarbeiten für die im Dezember 2020 anstehende FATF-Länderprüfung anlaufen. Im Vordergrund steht die Frage, ob die vereinbarten Vorschriften im AML/CFT-Bereich auch bei der Strafverfolgung effektiv angewendet werden. [150] Dann werden die deutschen Stellen u.a. nachweisen müssen, ob Verdachtsmeldungen, die Kryptotransaktionen betreffen, hierzulande wirksam nachgegangen wird.

Die rechtzeitige technische Umsetzung der Wire Transfer Rule bereitet jedoch international Schwierigkeiten, wie bereits erklärt wurde. Eine nachhaltige Lösung sollte in jedem Fall kostengünstig sein und somit Kunden davon abhalten, in einen weniger regulierten Bereich abzuwandern, also z.B. ein Peer-to-Peer-Netzwerk zu nutzen. [151] Konkrete Punkte auf der Agenda sollten z.B. hohe Anforderungen an die Technik bei Video- und Online-Identifizierungen sein und eine ausführliche Definition der verstärkten Sorgfaltspflichten für Krypto-Geschäftsbeziehungen mit erhöhten Risiken. Die Ermittlungsbehörden und die Krypto-Unternehmen sollten sich über für den Krypto-Finanzverkehr typische Verdachtsindikatoren abstimmen.

Ein positives Signal ist die Ankündigung, dass unter Mitarbeit aller zuständigen Behörden laufend aktualisierte Typologien für den Bereich der Terrorismusfinanzierung erarbeitet werden sollen, um eine bessere Informationsversorgung der Verpflichteten zu erreichen. [152] In Beachtung der typischen Besonderheiten in diesem Gebiet sollte der Verwendung von Mindestschwellenwerten bei Kryptotransaktionen (den 1.000 Dollar oder Euro nach den Vorgaben der FATF) keine zu große Bedeutung zukommen. Die Finanzierung terroristischer Gruppierungen und Operationen findet oft durch eine Vielzahl an Transaktionen mit geringen Beträgen statt.

Beispiele aus den Vereinigten Staaten lehren, dass die Krypto-Unternehmen an einem guten Verhältnis zu den Strafverfolgungsbehörden interessiert sind. Ein befragter Mitarbeiter einer dezentralen Handelsplattform gab zu verstehen, dass es in den USA kaum eine staatliche Behörde gebe, die sich nicht für den Krypto-Zahlungsverkehr zuständig fühle bzw. in konkreten Fällen um Mitwirkung bitte. Zugleich würden

[150] Die letzte entsprechende Evaluierung fand im Jahr 2010 statt. Siehe die Information des Bundesministeriums der Justiz und für Verbraucherschutz (Hg.): Kampf gegen Geldwäsche und Terrorfinanzierung. FATF Länderprüfung Deutschland 2020 – Informationen zum Ablauf der Prüfung https://www.bmjv.de/SharedDocs/Publikationen/DE/Geldwaesche.html
[151] Anton Moiseienko / Kayla Izenman: From Intention to Action. Next Steps in Preventing Criminal Abuse of Cryptocurrency, RUSI Occasional Paper, September 2019, S. 25 https://rusi.org/publication/occasional-papers/intention-action-next-steps-preventing-criminal-abuse-cryptocurrency
[152] Erste Nationale Risikoanalyse, S. 61

amerikanische Kryptobörsen mit staatlichen Behörden vertrauensvoll kooperieren. Über Transaktionen von staatlicherseits angefragten verdächtigen Personen würden Informationen mitgeteilt, auch wenn nicht immer eindeutig sei, ob die (dezentralen) Börsen hierzu verpflichtet seien. Unternehmen können hierzu eigene interne Regeln festlegen. Eine solche Selbstregulierung ist vor dem Hintergrund zu sehen, dass es den Krypto-Anbietern darum gehen muss, eine Reputation zu entwickeln, welche den Rufen nach schärferer Regulierung des Kryptohandels entgegenwirkt.[153]

4. Das politische Ziel, anonyme Transaktionen zu unterbinden, ist noch nicht erreicht. Ein legaler nichtregulierter Krypto-Zahlungsverkehr besteht fort. Zusätzlicher Regulierungsbedarf besteht bezüglich der Verwendung nicht gehosteter Wallets.

Die neuen FATF-Vorgaben fokussieren auf den Krypto-Zahlungsverkehr zwischen Intermediären bzw. Kunden, die mit an Bitcoin-Kryptobörsen gehosteten Wallets Transaktionen veranlassen. Für andere Zahlungswege, die vermutlich an Bedeutung zunehmen, reicht das nicht aus. Wenn in Zukunft viele Firmen Kryptowährung als Zahlungsmittel akzeptieren, dürfte es viele neue Risiken und Geldwäschebedenken geben. Daneben bestehen Regulierungslücken infolge nicht gehosteter Wallets. Die Wire Transfer Rule greift tatsächlich dann, wenn die Wallets beider Seiten bei einer Börse gehostet sind. Sobald ein Kunde Bitcoin an eine nicht gehostete Wallet sendet (die sich im Besitz einer Einzelperson befindet, ohne dass eine persönliche ID an einer Börse registriert ist), löst die Transaktion die Regel nicht aus. So kann immer noch Geld aus dem regulierten Markt herausgezogen werden.[154]

Das Nachbarland Schweiz ist teilweise weitergegangen, als die FATF-Standards verlangen. Laut einer am 26. August 2019 veröffentlichten Mitteilung der Schweizer Finanzmarktaufsicht (Finma)[155] dürfen von der Finma beaufsichtigte Institute demnach „Kryptowährungen oder andere Token grundsätzlich nur an externe Wallets ihrer eigenen, bereits identifizierten Kunden schicken und auch nur von solchen Kryptowährungen oder Token entgegennehmen. Finma-Beaufsichtigte dürfen keine Token von Kunden von anderen Instituten empfangen oder zu Kunden von anderen Instituten senden."

Diese im weltweiten Maßstab strenge Praxis soll solange gelten, als im Rahmen des entsprechenden Zahlungssystems zum Absender oder Empfänger keine zuverlässigen Angaben übermittelt werden können. Es wäre zu prüfen, ob diese konsequente Praxis nicht von Deutschland übernommen werden kann.

Besiegelt zu sein scheint über kurz oder lang das Schicksal der sogenannten Privacy Coins wie Monero. Die Entwicklung scheint hier faktisch auf ein Nutzungsverbot im

[153] Interview, Oktober 2019
[154] Yaya Fanusie: The Travel Rule Is Not Enough If Crypto Gets Adopted, forbes.com, 30.10.2019 https://www.forbes.com/sites/yayafanusie/2019/10/30/the-travel-rule-is-not-enough-if-crypto-gets-adopted/#6dbc7b0921e3 Fanusie bezieht sich auf die amerikanische Travel Rule, die sich in dieser Hinsicht praktisch nicht von der Wire Transfer Rule unterscheidet.
[155] FINMA-Aufsichtsmitteilung: Konsequente Geldwäschereibekämpfung im Blockchain-Bereich, 26.8.2019 https://finma.ch/de/news/2019/08/20190826-mm-kryptogwg

Zahlungsverkehr auf Ebene der Kryptobörsen hinauszulaufen, wenn die von der FATF geforderten Informationen von den Exchanges schon aus technischen Gründen nicht gesammelt werden können. Ausschließlich im unregulierten Peer-to-peer-Bereich könnte diese (beinahe) anonyme Zahlungsmethode weiterverwendet werden.[156] Wenn sämtliche regulierten Kryptobörsen die FATF-Richtlinien einhalten werden, können sie Privacy Coins nicht mehr zum Handel anbieten. Somit wird es in Zukunft sehr schwierig werden, Privacy Coins zu erwerben oder zu handeln bzw. in Fiatwährung umzuwandeln. Die Verwendung solcher Kryptowährungen könnte unter Umständen sogar bereits einen Anfangsverdacht begründen.

Die Regulierer stehen auch künftig vor der nicht leichten Aufgabe, einen Mittelweg einzuschlagen. Im Einklang mit den Sicherheitsbehörden haben sie Interesse daran, dass sich Kunden nicht veranlasst sehen, auf relativ weich regulierte Kryptobörsen außerhalb von Europa und Nordamerika auszuweichen. Kriminelle würden ohnehin Wege suchen und finden, die Weiterentwicklung der Technologie auszunutzen und stärker dazu tendieren, den regulierten Bereich ganz zu meiden. Stattdessen sollten Regierungen die Kryptobranche zur Kooperation ermutigen. Regulierungsmaßnahmen sollten der jungen Branche genug Luft zum Atmen geben. Im Gegenzug sollten staatliche Behörden erwarten, dass Kryptounternehmen ihren nötigen Beitrag zur Bekämpfung der Geldwäsche und Terrorismusfinanzierung leisten.

[156] Verschiedene Blockchain-Analysefirmen bieten ausdrücklich auch eine Untersuchung von Privacy Coins wie Monero an. Eine vollständige sichere Anonymität kann bislang keine Kryptowährung garantieren.

6 Literatur

Die Liste umfasst eine Auswahl der verwendeten Publikationen und Medienberichte. Ebenso aufgenommen wurden einige Beschlüsse und Stellungnahmen internationaler Organisationen und staatlicher Stellen, die auf die bestehende oder geplante Regulierung von Kryptowerten Bezug nehmen.

Basel Committee on Banking Supervision: Statement on crypto-assets, 13.3.2019 https://www.bis.org/publ/bcbs_nl21.htm

Basel Committee on Banking Supervision: Discussion paper. Designing a prudential treatment for crypto-assets. Issued for comment by 13 March 2020, December 2019 https://www.bis.org/bcbs/publ/d490.pdf

Beau, Denis: The role of cryptoassets in the payment system, Official Monetary and Financial Institutions Forum (OMFIF) Meeting, London, 15.10.2019 https://www.bis.org/review/r191015b.htm

Bergmann, Christoph: Bitcoin. Die verrückte Geschichte vom Aufstieg eines neuen Geldes, Moby Verlagshütte, Nersingen 2019 (2. Aufl.)

Bitfury Crystal (Hg.): Report on International Bitcoin Flows 2013-2019, September 2019 https://crystalblockchain.com/assets/reports/International%20Bitcoin%20Flows%20Report%20for%202013-2019%20-%20by%20Crystal%20Blockchain,%20Bitfury.pdf

Bitkom e.V. (Hg.): Blockchain in Deutschland – Einsatz, Potenziale, Herausforderungen. Studienbericht 2019 https://www.bitkom.org/Bitkom/Publikationen/Blockchain-Deutschland-Einsatz-Potenziale-Herausforderungen

Brett, Jason: Congress Considers Federal Crypto Regulators In New Cryptocurrency Act Of 2020, forbes.com, 19.12.2020 https://www.forbes.com/sites/jasonbrett/2019/12/19/congress-considers-federal-crypto-regulators-in-new-cryptocurrency-act-of-2020/#57eb0f4d5fcd

Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) (Hg.): Aufsichtsschwerpunkte 2020, Bonn und Frankfurt am Main, Dezember 2019 https://www.bafin.de/SharedDocs/Downloads/DE/Broschuere/dl_Aufsichtsschwerpunkte2020.pdf?__blob=publicationFile&v=4

Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) (Hg.): Merkblatt: Hinweise zum Tatbestand des Kryptoverwahrgeschäfts, 2.3.2020 https://www.bafin.de/dok/13710900

Bundesministerium der Finanzen (Hg.): Erste Nationale Risikoanalyse. Bekämpfung von Geldwäsche und Terrorismusfinanzierung 2018/2019, Oktober 2019 https://www.bundesfinanzministerium.de/Content/DE/Downloads/Broschueren_Bestellservice/2019-10-19-erste-nationale-risikoanalyse_2018-2019.html

Bundesministerium der Justiz und für Verbraucherschutz (Hg.): Kampf gegen Geldwäsche und Terrorfinanzierung. FATF Länderprüfung Deutschland 2020. Informationen zum Ablauf der Prüfung, ohne Datum (November 2019) https://www.bmjv.de/SharedDocs/Publikationen/DE/Geldwaesche.html

Bundesministerium für Wirtschaft und Energie / Bundesministerium der Finanzen (Hg.): Blockchain-Strategie der Bundesregierung. Wir stellen die Weichen für die Token-Ökonomie, ohne Datum (September 2019) www.blockchain-strategie.de

Chainalysis: Terrorism Financing in Early Stages with Cryptocurrency But Advancing Quickly, 17.1.2020 https://blog.chainalysis.com/reports/terrorism-financing-cryptocurrency-2019

Ciphertrace (Hg.): Cryptocurrency Anti-Money Laundering Report, 2019 Q3, November 2019 https://ciphertrace.com/wp-content/uploads/2019/12/CipherTrace-Cryptocurrency-Anti-Money-Laundering-Report-2019-Q3-2.pdf

Counter Extremism Project (Hg.): Terrorists on Telegram, Mai 2017 https://www.counterextremism.com/terrorists-on-telegram

Dion-Schwarz, Cynthia / Manheim, David / Johnston, Patrick B.: Terrorist Use of Cryptocurrencies. Technical and Organizational Barriers and Future Threats, RAND Corporation, Santa Monica 2019 https://www.rand.org/pubs/research_reports/RR3026.html

Draht, Moritz: EU-Kommissar Dombrovskis fordert eindeutige Gesetzgebung für Kryptowährungen, BIT-Echo, 9.10.2019 https://www.btc-echo.de/eu-kommissar-dombrovskis-fordert-eindeutige-gesetzgebung-fuer-kryptowaehrungen/

Eidgenössische Finanzmarktaufsicht FINMA: Aufsichtsmitteilung: Konsequente Geldwäschereibekämpfung im Blockchain-Bereich, 26.8.2019 https://finma.ch/de/news/2019/08/20190826-mm-kryptogwg

Elliptic: Bitcoin Money Laundering: How Criminals Use Crypto (And How MSBs Can Clean Up Their Act), 18.9.2019 https://www.elliptic.co/our-thinking/bitcoin-money-laundering

Expert Group on Regulatory Obstacles to Financial Innovation (ROFIEG): Thirty Recommendations on Regulation, Innovation and Finance. Final Report to the European Commission, 13.12.2019 https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/191113-report-expert-group-regulatory-obstacles-financial-innovation_en.pdf

Fanusie, Yaya J.: The New Frontier in Terror Fundraising, in: Bitcoin, The Cipher Brief, 24.8.2016 https://www.thecipherbrief.com/column_article/the-new-frontier-in-terror-fundraising-bitcoin

Fanusie, Yaya J. / Robinson, Tom: Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services, 12.1.2018 https://www.fdd.org/wp-content/uploads/2018/01/MEMO_Bitcoin_Laundering.pdf

Fanusie, Yaya J.: The Travel Rule Is Not Enough If Crypto Gets Adopted, forbes.com, 30.10.2019 https://www.forbes.com/sites/yayafanusie/2019/10/30/the-travel-rule-is-not-enough-if-crypto-gets-adopted/#6dbc7b0921e3

Financial Action Task Force (FATF) (Hg.): International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. The FATF Recommendations, Paris 2019 www.fatf-gafi.org/recommendations.html

Financial Action Task Force (FATF): Money laundering risks from “stablecoins” and other emerging assets, 18.10.2019 https://www.fatf-gafi.org/publications/fatfgeneral/documents/statement-virtual-assets-global-stablecoins.html

Financial Action Task Force (FATF) (Hg.): Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, Juni 2019 www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html

Financial Action Task Force (FATF): Public Statement on Virtual Assets and Related Providers, 21.6.2019 http://www.fatf-gafi.org/publications/fatfrecommendations/documents/public-statement-virtual-assets.html

Financial Action Task Force (FATF) (Hg.): Virtual Assets: What, When and How? Easy Guide to FATF Standards and Methodology, Dezember 2019 http://www.fatf-gafi.org/media/fatf/documents/bulletin/FATF-Booklet_VA.pdf

Financial Crimes Enforcement Network (FinCEN) (Hg.): FinCEN Guidance: Application of FinCEN’s Regulations to Certain Business Models Involving Convertible Virtual Currencies, 9.5.2019 https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf

Financial Intelligence Unit (Hg.): Jahresbericht 2018, Köln, Juli 2019 https://www.zoll.de/SharedDocs/Downloads/DE/Links-fuer-Inhaltseiten/Fachthemen/FIU/fiu_jahresbericht_2018.pdf?__blob=publicationFile&v=3

Gilbert, David: ISIS Is Experimenting with This New Blockchain Messaging App, vice.com, 13.12.2019 https://www.vice.com/en_us/article/v744yy/isis-is-experimenting-with-this-new-blockchain-messaging-app

Grzywotz, Johanna: Virtuelle Kryptowährungen und Geldwäsche, Duncker & Humblot, Berlin 2019

Katsiri, Roy: Bitcoin donations to ISIS soared day before Sri Lanka bombings, Globes (Israel), 2.5.2019 https://en.globes.co.il/en/article-exclusive-isis-funded-sri-lanka-bombings-with-bitcoin-donations-1001284276

Keatinge, Tom / Keen, Florence: Social Media and Terrorist Financing. What are the Vulnerabilities and How Could Public and Private Sectors Collaborate Better?, Global Research Network on Terrorism and Technology: Paper No. 10 (RUSI), London 2019 https://rusi.org/sites/default/files/20190802_grntt_paper_10.pdf

Kirilova, Valentina: CipherTrace conference sheds light on FATF 'Travel Rule' for user info, LeapRate.com, 22.11.2019 https://www.leaprate.com/cryptocurrency/blockchain/ciphertrace-conference-sheds-light-on-fatf-travel-rule-for-user-info/

Klee, Christopher: Durchbruch im Crypto Country: Liechtenstein verabschiedet Blockchain Act, BTC-Echo, 3.10.2019 https://www.btc-echo.de/durchbruch-im-crypto-country-liechtenstein-verabschiedet-blockchain-act/

Koenig, Aaron: Die dezentrale Revolution. Wie Bitcoin und Blockchain Wirtschaft und Gesellschaft verändern, FinanzBuch Verlag, München 2019

Küfner, Robert A.: Das Krypto-Jahrzehnt. Was seit dem ersten Bitcoin alles geschehen ist – und wie digitales Geld die Welt verändern wird, Börsenbuchverlag, Kulmbach 2018

Libra Whitepaper (deutsche Fassung) https://libra.org/de-DE/white-paper

Linver, Henry: FATF AML Regulation: Can the Crypto Industry Adapt to the Travel Rule?, Cointelegraph.com, 10.10.2019 https://cointelegraph.com/news/fatf-aml-regulation-can-the-crypto-industry-adapt-to-the-travel-rule

Middle East Media Research Institute (MEMRI): Defiant Message From ISIS In Response To Campaign Against Its Presence On Telegram, Other Platforms, 2.12.2019 https://www.memri.org/reports/defiant-message-isis-response-campaign-against-its-presence-telegram-other-platforms

Moiseienko, Anton / Isenman, Kayla: From Intention to Action. Next Steps in Preventing Criminal Abuse of Cryptocurrency, RUSI Occasional Paper, September 2019 https://rusi.org/publication/occasional-papers/intention-action-next-steps-preventing-criminal-abuse-cryptocurrency

Mokhniev, Serhii: European AML Regulations Follow the US Path With a Six-Years' Delay, Cointelegraph, 30.11.2019 https://cointelegraph.com/news/european-aml-regulations-follow-the-us-path-with-a-six-years-delay

Policy Department for Citizens' Rights and Constitutional Affairs (Directorate General for Internal Policies of the Union) (Hg.): Virtual currencies and terrorist financing: assessing the risks and evaluating responses, Mai 2018 http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2018)604970

Popper, Nathaniel: Terrorists Turn to Bitcoin for Funding, and They're Learning Fast, The New York Times, 18.8.2019 https://www.nytimes.com/2019/08/18/technology/terrorists-bitcoin.html

Schweizerische Eidgenossenschaft (Hg.): 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), Oktober 2018 https://www.newsd.admin.ch/newsd/message/attachments/56167.pdf

Sexer, Nathan: State of Decentralized Exchanges, 2018 https://media.consensys.net/state-of-decentralized-exchanges-2018-276dad340c79

Smith, Brenna: The Evolution Of Bitcoin In Terrorist Financing, bellingcat.com, 9.8.2019 https://www.bellingcat.com/news/2019/08/09/the-evolution-of-bitcoin-in-terrorist-financing/

Stalinsky, Steven: The Coming Storm – Terrorists Using Cryptocurrency, Middle East Media Research Institute (MEMRI), 21.8.2019 https://www.memri.org/reports/coming-storm-%E2%80%93-terrorists-using-cryptocurrency

United States Department of Justice: Long Island Woman Pleads Guilty to Providing Material Support to ISIS, 26.11.2018 https://www.justice.gov/usao-edny/pr/long-island-woman-pleads-guilty-providing-material-support-isis

Wieczner, Jen: Bitcoin Accounts for 95% of Cryptocurrency Crime, Says Analyst. fortune.com, 24.4.2019 https://fortune.com/2019/04/24/bitcoin-cryptocurrency-crime/

Willmroth, Jan: Der Stapel wächst, Süddeutsche Zeitung, 8.10.2019 https://www.sueddeutsche.de/wirtschaft/zoll-der-stapel-waechst-1.4631795

Wilson, Tom & Williams, Dan: Hamas shifts tactics in bitcoin fundraising, highlighting crypto risks: research, Reuters, 26.4.2019
https://uk.reuters.com/article/us-crypto-currencies-hamas/hamas-shifts-tactics-in-bitcoin-fundraising-highlighting-crypto-risks-research-idUKKCN1S20FA

COUNTER EXTREMISM PROJECT