FRIEDRICH NAUMANN STIFTUNG Für die Freiheit.

BIGS
BRANDENBURGISCHES INSTITUT für GESELLSCHAFT und SICHERHEIT

DARK KRYPTO

Nutzung von Kryptowährungen für illegale Zwecke

Johannes Rieckmann, Tim Stuchtey

ANALYSE

Impressum

Herausgeberin
Friedrich-Naumann-Stiftung für die Freiheit
Truman-Haus
Karl-Marx-Straße 2
14482 Potsdam-Babelsberg

/freiheit.org
/FriedrichNaumannStiftungFreiheit
/FNFreiheit
/stiftungfuerdiefreiheit

Autoren
Dr. Johannes Rieckmann, Senior Research Fellow,
Brandenburgisches Institut für Gesellschaft und Sicherheit (BIGS)
Dr. Tim Stuchtey, Geschäftsführender Direktor,
Brandenburgisches Institut für Gesellschaft und Sicherheit (BIGS)

Redaktion
World Order and Globalization Hub, Washington D.C.
Abteilung Globale Themen, Berlin

Kontakt
Telefon +49 30 220126-34
Telefax +49 30 690881-02
E-Mail service@freiheit.org

Stand
Oktober 2022

Inhalt

EXECUTIVE SUMMARY **4**

1. EINLEITUNG **5**

2. *BLOCKCHAIN* UND KRYPTOWÄHRUNGEN **6**

2.1. Technik blockchain 6

2.2. Kryptowährungen 6

2.3. Transparenz 8

3. VERSCHLEIERUNGSVERFAHREN **9**

3.1. Mixer und Tumbler 9

3.2. Privacy coins 10

3.3. Kryptobörsen 10

4. NUTZUNG FÜR ILLEGALE ZWECKE **11**

4.1. Formen illegaler Geschäfte mit Kryptowährungen 11

4.2. Extremismus- und Terrorismusfinanzierung 12

4.3. Geldwäsche 13

4.4. Staatsnahe Akteure, nationale Sicherheit 13

5. ANSÄTZE ZUR GELDWÄSCHEBEKÄMPFUNG **14**

5.1. Regulierung 14

5.1.1. National 14

5.1.2. Inter- und supranational 15

5.2. Sanktionen 15

5.3. Ermittlung und Strafverfolgung 16

6. HANDLUNGSEMPFEHLUNGEN **17**

7. AUSBLICK **18**

ABKÜRZUNGSVERZEICHNIS **19**

LITERATURVERZEICHNIS **19**

Executive Summary

Die *blockchain*-Technologie und die auf ihr basierenden Kryptowährungen bieten ein erhebliches Innovationspotenzial für Wirtschaft und Gesellschaft. Kryptowährungen sind aber zugleich das Zahlungsmittel der Wahl für bestimmte kriminelle Aktivitäten geworden. In der vorliegenden Studie geben die Ökonomen Johannes Rieckmann und Tim Stuchtey vom BIGS (Brandenburgisches Institut für Gesellschaft und Sicherheit) einen Überblick zur illegalen Nutzung von Kryptowährungen. Sie erklären die Verschleierungs- und Anonymisierungsmethoden mit Hilfe von Mixern sowie die Unterschiede klassischer Kryptowährungen wie Bitcoin und Ether einerseits und anonymisierten Kryptowährungen andererseits, bei denen eine Nachverfolgung von Transaktionen nahezu unmöglich ist. Sie zeigen auf, für welche Straftaten Kryptowährungen innerhalb der *blockchain,* sowie an den Schnittstellen mit der analogen und sonstigen digitalen Welt, missbraucht werden. Sie analysieren bestehende und in Planung befindlicher Regulierungs- und Aktionsansätze.

Auf der Grundlage dieser Analyse sowie von Experteninterviews werden Handlungsempfehlungen abgeleitet, wie der Missbrauch von Kryptowährungen für illegale Zwecke unterbunden und gleichzeitig eine unverhältnismäßige Einschränkung des Innovationspotenzials der Technologie vermieden werden kann. Die bislang im Vergleich zum klassischen Finanzsektor weitgehend unregulierten Kryptowährungen und ihrer Marktplätze werden sich zukünftig Regeln unterwerfen müssen, die eine De-Anonymisierung mit Richtervorbehalt ermöglichen. Diese Regeln müssen für die Nutzer transparent sein, um das Vertrauen in eine Währung und deren Marktplätze nicht zu verlieren. Gleichzeitig kann ein wohl regulierter Markt die legalen Nutzungsoptionen einer Kryptowährung noch deutlich erweitern.

Pläne des Bundes, Ermittlungskompetenzen in einem Bundesfinanzkriminalamt zu bündeln erscheinen schon wegen der notwendigen Fähigkeiten der knappen Mitarbeitenden zielführend zu sein, um Kriminalität, Geldwäsche, Terrorismusfinanzierung und der Sanktionsumgehung einzudämmen. Dabei gilt es, die Verhältnismäßigkeit zu wahren. Ein zentraler Ansprechpartner für alle Themen rund um die Strafverfolgung kann für innovative Unternehmen mit legalen Geschäftsmodellen auch ein attraktiver Standortvorteil sein.

1. Einleitung

Mit dem Auftauchen von Kryptowährungen ist das sonst für die meisten eher langweilige Thema der Geld- und Währungstheorie mit viel Faszination aufgeladen worden. Die Tatsache, dass Kryptowährungen bislang kaum staatlich reguliert sind, übt eine besondere Faszination auf libertär gesinnte Menschen aus. Der oft rasante Preisanstieg und die damit verbundenen Geschichten von Menschen, die binnen kürzester Zeit erhebliche Vermögen erlangt haben, fasziniert Menschen, die eine Kapitalmarktnähe haben. Dass diese Vermögen auch ebenso schnell vergehen können, wie sie geschaffen wurden, aufgrund der hohen Preisschwankungen fasziniert die Skeptiker dieser neuen Währungen und führt vielleicht gar zu Schadenfreude bei manchen. Die potenziellen Anwendungsmöglichkeiten der hinter den Kryptowährungen stehenden *blockchain*-Technologie fasziniert mathematisch gebildete Unternehmensgründer und Innovatoren. Nahezu jeden fasziniert aber auch die dunkle Seite, die mit den neuen Währungen verbunden ist. Die fehlende Regulierung und die schwer nachvollziehbaren Transaktionen mithilfe von Kryptonwährungen hat diese zur Währung der Wahl vieler Krimineller gerade im Bereich der Cyberkriminalität gemacht.

In diesem Beitrag soll geklärt werden

→ warum Kryptowährungen gerade im Bereich des illegalen Handels so gerne zum Einsatz kommen,

→ wie umfänglich dieser Einsatz ist,

→ warum dabei zwischen den verschiedenen Kryptowährungen zu differenzieren ist,

→ welche Möglichkeiten oder Hindernisse sich daraus bei der Kriminalitätsbekämpfung ergeben und

→ ob daraus Regulierungsnotwendigkeiten abzuleiten sind.

Dieser Beitrag soll als Orientierung und thematische Einführung für Leser dienen, die sich aus ordnungspolitischer Perspektive mit der Entwicklung der Technologie und ihrer Einsatzmöglichkeiten im Zahlungsverkehr befassen. Hierbei liegt der Fokus nicht auf den ebenfalls relevanten energie-, umwelt-, industrie- oder geldpolitischen Aspekten, sondern auf sicherheitsbezogenen Gesichtspunkten.

Im Folgenden wird kurz auf die Funktionsweise von Kryptowährungen in ihren verschiedenen derzeitigen Ausprägungen und unter besonderer Berücksichtigung von Verschleierungsverfahren eingegangen. Schwerpunkmäßig wird weiterhin auf die Nutzung durch Kriminelle für Straftaten und illegale Transaktionen, zur Terrorismusfinanzierung und durch staatsnahe Akteure eingegangen. Nationale, europäischen, und internationale Ansätze zur Eindämmung der illegalen Nutzung werden ebenso dargelegt wie sich aus der technischen Entwicklung entstehende Herausforderungen für diese.

2. Blockchain und Kryptowährungen

Digitale Währungen, *blockchain,* Kryptogeld – worum geht es hier eigentlich? Alles nimmt seinen Anfang mit der heute noch bekanntesten digitalen Währung: Dem Bitcoin. Hierbei handelt es sich um ein nicht-staatliches Zahlungsmittel, mit dem analog zu Zahlungen mit Bargeld in der physischen Welt, Transaktionen im digitalen Raum zwischen einzelnen Akteuren möglich wurden, ohne dabei Intermediäre wie Banken oder Zahlungsdienstleister nutzen zu müssen. Die innovative, dieser und allen später folgenden Kryptowährungen zugrunde liegende Technik – die sogenannte *blockchain* – wurde 2008 von einem Programmierer unter dem Pseudonym Satoshi Nakamoto durch Veröffentlichung eines Konzept-Papiers aus der Taufe gehoben.[1] Innovativ war das technische Konzept zum einen deshalb, weil es trotz des Verzichts auf eine zentrale Ausgabe- und Verwaltungsstelle für die digitale Währung sicherstellte, dass jede Geldeinheit vom selben Akteur nur einmal für eine Transaktion verwendet werden kann und damit den Besitzer wechselt, also nicht kopiert werden kann. Zum anderen wurde ein Anreizsystem zur Verwaltung und Fortschreibung „zum Erhalt und zur Pflege einer Datenbank in einem dezentralen Netzwerk"[2] geschaffen.

Kryptowährungen haben ihren Namen von der genutzten Verschlüsselungstechnik, die gemeinsam mit der redundanten Transaktions-Dokumentation im gesamten Netzwerk für Manipulationssicherheit sorgt. Außerdem stellt sie sicher, dass das Geld eines jeden Akteurs auch nur durch diesen – oder genauer, durch den Besitzer seines privaten Schlüssels – gemeinsam mit dem öffentlichen Schlüssel für eine Transaktion genutzt werden kann.[3]

2.1. Technik blockchain

Die Transaktionen werden in Zeitintervallen zu Blöcken zusammengefasst, die zu einer Kette aneinandergereiht werden. Diese Kette aus Blöcken – englisch *blockchain* – ist eine lückenlos aneinanderhängende Folge von Zusammenfassungen elektronischen Signaturen. Im Rahmen des sog. *mining* wird ein ökonomischer Anreiz für die Teilnahme am massenhaften dezentralen Überprüfungsprozess durch eine Belohnung in Form neu geschaffenen Geldes geschaffen, dem sogenannten *block reward.*[4]

Alle anderen Teilnehmer können das Rechenergebnis im mining-Prozess überprüfen und verifizieren.[5] Die fortgeschriebene *blockchain,* auf die sich mittels einer *consensus mechanism* (Konsensmechanismus, ein bekanntes Beispiel ist *proof-of-work*) genannten Technik – nämlich der oben erwähnten Überprüfung der vergangenen Transaktionen – wird dezentral und redundant in einer Art allseits geteilten Kontoregisters (*distributed ledger*) dokumentiert, was Manipulationen bis zur Unmöglichkeit erschweren soll.[6]

Jeder Netzwerkteilnehmer hat also dieselben Informationen vorliegen. So ist die Bitcoin-*blockchain* eine öffentlich einsehbare, fortlaufend gemeinschaftlich gepflegte und geprüfte Datenbank von Transaktionen der Vergangenheit.

2.2. Kryptowährungen

Ob bei den sogenannten Kryptowährungen tatsächlich von Geld gesprochen werden kann, ist umstritten. Von staatlichen Zentralbanken herausgegebenes Geld (sog. Fiat-Geld[7]) zeichnet sich dadurch aus, dass es drei grundlegende Funktionen[8] erfüllt: Es dient als Tauschmittel, als Recheneinheit, und als Wertaufbewahrungsmittel. Welche dieser Funktionen die verschiedenen Arten von Kryptowährungen erfüllen, wird unten kurz angerissen.

Ein bedeutender und für ihr Verwendungspotenzial für illegale Zwecke durchaus bedeutsamer Unterschied von Kryptowährungen zu Fiat-Geld ist der zunächst grundsätzliche Verzicht auf und die Unabhängigkeit von Intermediären beim Abwickeln von Transaktionen im elektronischen Zahlungsverkehr.[9] Wie wir unten beschreiben, gibt es mittlerweile jedoch auch im Universum der Kryptowährungen optional Intermediäre, die unter anderem als Dienstleistung bspw. Depots (sog. *wallets*) verwalten oder Verschleierung von Transaktionswegen anbieten. Der Verzicht auf eine emittierende zentrale Stelle (bei Fiat-Geld wäre das eine Zentralbank) und als Mittler fungierende Finanzinstitutionen (bei Fiat-Geld wären das die Geschäftsbanken) entspricht eigentlich nur dem konsequent weitergedachten Grundgedanken der Österreichischen Schule[10] in der Ökonomie. Eine sich hieraus ergebende Herausforderung ist die Tatsache, dass damit auch in der Bankenwelt übliche Dokumentations-, Kontroll- und ggf. Meldefähigkeiten entfallen, wie sie beispielsweise in Verfahren der Kundenidentifikation (*Know-Your-Customer,* KYC) sowie Geldwäscheverdachtsmeldungen entwickelt wurden.

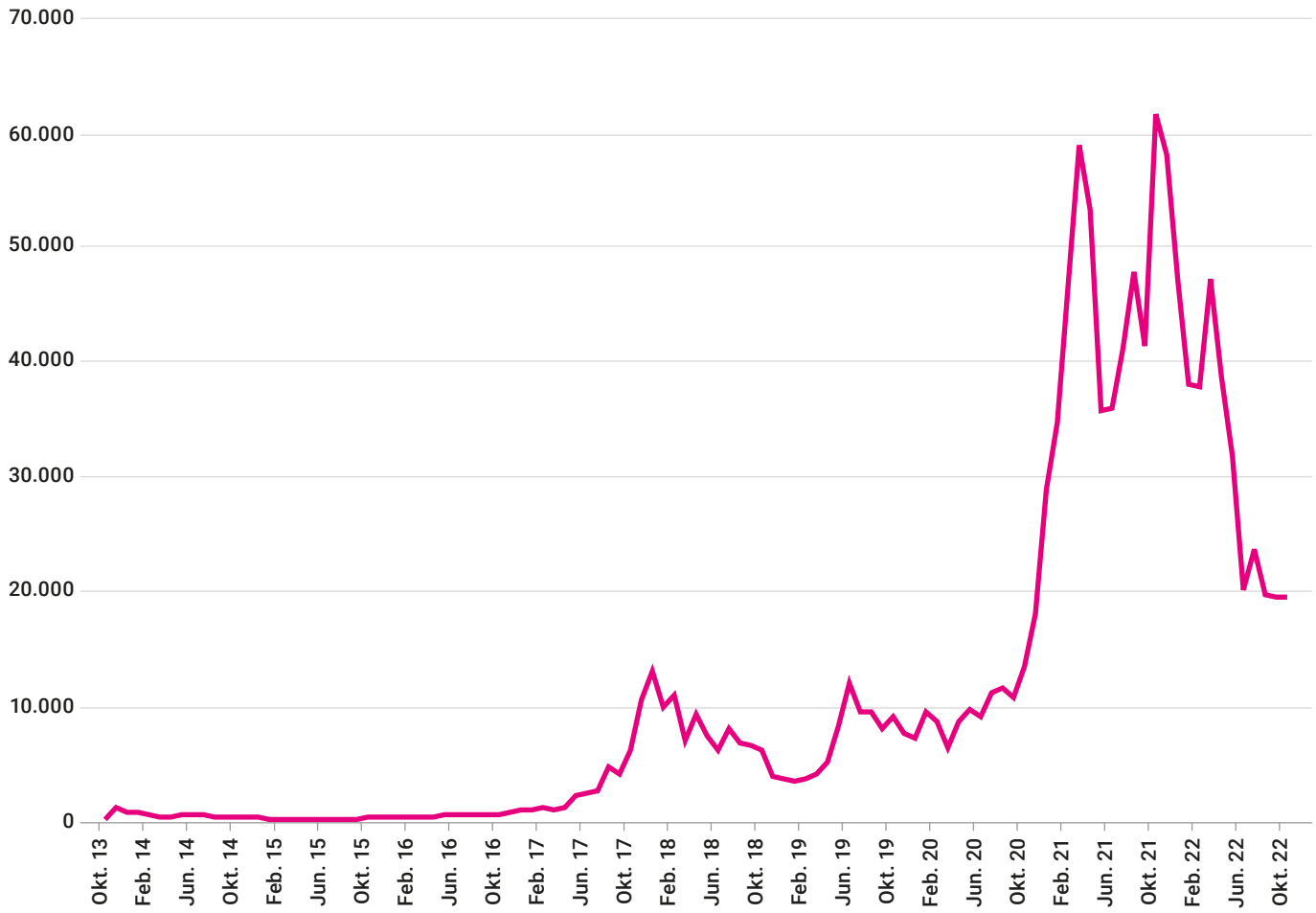
1 Hilgers, Sven & Greilich, K. (2021), S. 10.
2 Ibid., S. 10.
3 Ibid., S. 11.
4 Antonopoulos, A. M. (2017), S. 5.
5 Eine ausführlichere Erläuterung zu Organisation und Funktionsweise sowie Anreizmechanismen der Bitcoin-Blockchain finden Sie in Hilgers, S. & Greilich, K. (2021), S.11 f..

6 Da der *proof-of-work*-Prozess zur Erzielung des Konsenses bezüglich des einheitlichen Datenbank-Inhalts und der gleichzeitigen Schaffung neuer Bitcoins durch *mining* so energieaufwändig ist, die Überprüfung des erfolgreichen *minings* jedoch ein Leichtes, wird sichergestellt, dass das Einschmuggeln gefälschter Transaktion unattraktiv wird – der Aufwand und gleichzeitig die Entdeckungswahrscheinlichkeit und der sofortige Verlust der Beute sind systembedingt sehr hoch. Ein energieschonenderer Mechanismus ist der *proof-of-stake*-Prozess, bei dem an der Überprüfung der Transaktionen und dafür zufällig ausgewählte beteiligte Mitglieder des Netzwerks eine Aufwandsentschädigung, gewissermaßen in Form von Zinsen auf die Währung, erhalten. Der Konsensmechanismus der Ethereum-*blockchain* wurde am 15. September 2022 von *proof-of-work* auf *proof-of-stake* umgestellt.
7 Hierbei handelt es sich um das aus dem Alltag gewohnte Bar- und Buchgeld, das nach dem lateinischen Wort lateinischen Wort fiat (Imperativ, Übersetzung: „Es geschehe") benannt ist.
8 Anderegg, R. (2014), S.19.
9 Bargeld-Transaktionen finden wie die (elektronischen) Kryptowährungs-Transaktionen i.d.R. ohne Intermediäre statt. Dies wirft die Frage auf, was bei der Konzeption von Regulierung als nächstes Äquivalent zu Kryptowährungs-Transaktionen begriffen werden muss – Zahlungen mit Bargeld, oder elektronische Überweisung von Fiat-Geld.
10 Diese wurde im 18. Jahrhundert von Carl Menger gegründet sowie maßgeblich von Ludwig von Mises und Friedrich August von Hayek geprägt, und steht staatlicher Regulierung und zentraler Steuerung wirtschaftlicher Prozesse kritisch gegenüber. Siehe auch Menger, C. (1884), von Mises, L. (1949) sowie Hayek, F. A. (2022).

Durch die Begrenzung der Geldmenge wird z.B. beim Bitcoin versucht, Wertstabilität sicherzustellen. Davon kann allerdings keine Rede sein, wie die nachfolgende Graphik (Abb. 1) deutlich macht, auf der die erheblichen Kursschwankungen des Bitcoins dargestellt sind. Damit muss die Wertaufbewahrungsfunktion als nicht gegeben betrachtet werden. Auch die Geldfunktionen des Tauschmittels und der Recheneinheit sind beim Bitcoin bislang allenfalls eingeschränkt gegeben[11].

11 Hilgers, Sven & Greilich, K. (2021), S. 13.

Abb. 1 | Wertentwicklung des Bitcoins seit 2013 (in US$)



Preisentwicklung Bitcoin in U.S.-Dollar (USD), tägliche Preise, Oktober 2013 bis Oktober 2022.

Quelle: CoinGecko, 2022

Trotz der hohen Schwankungen und der geringen Akzeptanz als Tauschmittel hing dem Bitcoin früh der Ruf einer Währung für Kriminelle an, obwohl er technisch bedingt eine perfekte Transparenz getätigter Transaktionen aufweist. Im Abschnitt 3.4 wird hierauf genauer eingegangen.

Mit der Schaffung der zusätzlich programmierbaren Kryptowährung – anfangs *colored coins* genannt – folgte ab 2011[12] eine Aneignung der zusätzlichen Fähigkeit, die einzelnen Geldeinheiten mit weiteren Informationen zu versehen. Mittlerweile können regelrechte „Softwareprogramme innerhalb des dezentralen Systems"[13] ausgeführt werden, und damit etwa Verträge – sogenannte *smart contracts* – manipulationssicher dokumentiert werden.[14] Die oben genannten Geldfunktionen sind, abgesehen von der Tauschmittelfunktion, auch bei dieser Kategorie von Kryptowährungen nur eingeschränkt gegeben, hinzu tritt die zusätzliche Komplexität je nach Ausprägung der *smart contracts*. Ein prominenter Vertreter dieser Gattung ist die Ethereum-*blockchain*.

Dem Problem der ausgeprägten Wertschwankungen und den damit einhergehenden Einschränkungen vor allem in Bezug auf die Funktionen als Recheneinheit und Wertaufbewahrungsmittel versucht das Konzept der *stablecoins* zu begegnen. Hierzu wird der Wert in Beziehung mit dem einer Fiat-

12 Hilgers, Sven & Greilich, K. (2021), S. 13.
13 Ibid., S. 13.

14 Der Ausschaltung von Intermediären könnte hier der Verzicht beispielsweise auf Notar und Grundbucheintrag bei einem Immobilienkauf entsprechen. Die auf der Blockchain dokumentierbaren zusätzliche Informationen ermöglichen auch die Schaffung neuer Vermögensgegenstände, aufgrund ihrer Nicht-Einheitlichkeit auch non-fungible tokens (NFT) genannt.

Währung (typischerweise den US-Dollar), eines Rohstoffs wie Erdöl oder Gold, Immobilien, oder auch mit dem anderer Kryptowährungen in Beziehung gesetzt. Die Anbindung[15] erfolgt durch Besicherung, also bspw. Hinterlegung einer entsprechenden Menge der Referenzwährung, oder aber durch einen Algorithmus, welcher das Angebot der Nachfrage über die Anbindung an den Wert z.B. einer Fiat-Währung anpasst (ohne diese jedoch als Sicherheit tatsächlich zu hinterlegen). Die Manipulationssicherheit und Geschwindigkeit digitaler Zahlungen bleiben bestehen, hingegen wird die Volatilität des Kurses im Vergleich etwa zum Bitcoin verringert.

Die Besicherung von *stablecoins* muss zentralisiert verwaltet werden, um ihren Wert mit dem der sich im Umlauf befindlichen Währung im Einklang zu halten. Weil ein An- oder Verkauf jeweils auch ein entsprechendes Gegengeschäft mit der hinterlegten Sicherheit mit sich bringt, sind sie systembedingt nicht anonym. Ein Vertreter der Gattung mit Fiat-Geld besicherter *stablecoins* ist Tehter.

Stablecoins kann man aufgrund ihrer relativen Wertstabilität die Eigenschaften einer Recheneinheit und eines Wertaufbewahrungsmittels zuschreiben. Allerdings hat sich bei starken Kursschwankungen anderere Kryptowährungen gezeigt, dass auch *stablecoins* in Mitleidenschaft gezogen werden können, und zwar über die Beeinträchtigungen von Fiat-Währungen durch Inflation hinaus.

Die Zentralbanken etlicher Länder sind bereits mit Prüfungs- und Vorbereitungsphasen für die Entwicklung und Einführung digitaler Währungen befasst. Diese sogenannten *Central Bank Digital Currencies* (CBDC) sollen alle drei Geldfunktionen erfüllen können, und das Bargeld ergänzen. Welche Auswirkungen eine – in diesem Falle notwendigerweise zentral verwaltete – staatliche Kryptowährung auf Privatsphäre einerseits sowie Begehung und Verfolgung von Straftaten andererseits haben wird, ist noch unklar und wird unter anderem auch stark von der jeweiligen Ausgestaltung und politischen Vorgaben abhängig sein.

2.3. Transparenz

Kryptowährungen standen seit ihren Anfängen im Ruf, erstens kompliziert und nur etwas für technikaffine Nutzer zu sein, und zweitens vor allem illegitimen Zwecken zu dienen. Da insbesondere der Bitcoin bereits nach kurzer Zeit von Erpressern für Lösegeldforderungen und für Transaktionen zwischen Kriminellen sowie zur Bezahlung auf Darknet-Plattformen, genutzt wurde, entstand in der breiten Öffentlichkeit bald der Eindruck, dass Transaktionen mit Kryptowährungen nicht nur schnell und jenseits des Internets nicht wahrnehmbar, sondern vor allem auch völlig anonym seien.

Gerade für den Bitcoin – und die Mehrzahl nach ihm entstandener, anderer Kryptowährungen – ist aber genau das nicht der Fall. Tatsächlich ist die gesamte Transaktionshistorie mithilfe von *blockchain explorers* öffentlich einsehbar[16] – wenn auch hiermit nicht gleichzeitig übersichtlich. Statt Anonymität bietet der Bitcoin lediglich Pseudonymität: Das mit einer (für sich allein nichtssagenden) Zahlen- und Buchstabenkombination benannte Depot, auf dem das transferierte Geld sich zur Zeit der Betrachtung befindet, ist durchaus bekannt. Mit anderen Worten, das Depot ist identifizierbar und Transaktionen darüber können beobachtet werden. Solange sich aber nicht eine echte oder juristische Person als Eigentümer zu erkennen gibt, bleibt sie eine graue Eminenz – ähnlich einem Buchautor unter Künstlernamen.

Die Schwierigkeit für Kriminelle besteht in der Wahrung ihres Pseudonyms beim sogenannten *off-ramp,* dem Punkt der Umwandlung von Kryptowährung in Fiat-Geld oder Waren und Dienstleistungen in der analogen Welt. Denn an diesem Punkt muss der Eigentümer des Depots sich oder eine von ihm beauftragte Person exponieren. Daher ist der *off-ramp* auch ein Ermittlungsansatz für Strafverfolgungsbehörden. Kriminelle setzen daher vor und hinter diesem Punkt oft komplexe Verschleierungs- und Geldwäscheverfahren ein, um die Entdeckung, Beschlagnahmung und Strafverfolgung zu verhindern.

Denkbar ist allerdings die Nutzung für Bezahlungen innerhalb der *blockchain* für kriminelle Dienstleistungen, die in der analogen Welt nicht dem Zahlenden zugeordnet werden können. Das könnte bspw. die Bezahlung auf einer *darkweb*-Plattform für einen *crime-as-a-service* anbietenden Dienstleister sein. In diesem Fall hat die Kryptowährung dem ersten Kriminellen bereits als Mittel zum Zweck gedient, wohingegen die Herausforderung der weiteren Verwendung unter Wahrung der eigenen Pseudonymität gewissermaßen an den zweiten Kriminellen weitergereicht wird.

15 Reaume, A. (2022).

16 Stevens, R. (2022).

3. Verschleierungsverfahren

Ähnlich wie beim Bargeld, gibt es Nutzer, die Wert auf die Anonymität ihrer Transaktion legen. Hintergrund kann ein berechtigtes Interesse wie die Wahrung der Privatsphäre sein, jedoch auch unberechtigte, wie die Verdeckung von Straftaten, Geldwäsche, Umgehung von Sanktionen oder Geldbeschaffung für terroristische Organisationen. Hier gilt es also zu prüfen, ob mit einem Markteingriff solch illegale Aktivitäten reduziert werden können. Dabei ergibt sich ein ähnliches Spannungsfeld in der Abwägung, wie auch bei der Nutzung und Regulierung von Bargeld.

Zum Zwecke der Anonymisierung kommen verschiedene Verschleierungsverfahren zum Einsatz, die ein Nachverfolgen des Weges, den das Geld genommen hat, in der Praxis – obschon technisch möglich - bis zur Unmöglichkeit aufwändig macht. Oft kommt sogenanntes *layering* zum Einsatz, also das Hinzufügen von künstlicher Komplexität zu Transaktionen, um die Rückverfolgung von Geldern zu erschweren. Ein systematischer Unterschied zur Fiat-Welt besteht in der Möglichkeit, die Transaktionen sehr schnell, in großer Zahl und sehr kleinteilig vorzunehmen. Dies erschwert die Nachverfolgung und erleichtert das Unterlaufen etwaiger Geldwäscheverdachts-Meldegrenzen. Dies geschieht in der Regel durch sogenannte Mixer und Tumbler.

Gegenstand der Betrachtung in diesem Papier sind dabei nur Verschleierungsverfahren vor dem *off-ramp* (also auf der *blockchain*), da dahinter stattfindende sich nicht von herkömmlichen, aus der Welt der Fiat-Währungen bekannten unterscheiden.

3.1. Mixer und Tumbler

Eine Möglichkeit der Anonymisierung wird von speziellen Dienstleistungsplattformen angeboten: Die Mixer (manchmal auch *tumbler*) genannt werden. Diese vermischen das Geld eines Nutzers mit dem anderer, um anschließend die Summe – ggf. abzüglich einer Dienstleistungsgebühr[17] – wieder auszuzahlen. Die Auszahlung erfolgt allerdings aus anderen Depots, so dass keine logische Verbindung (*on-chain link*) zur Einzahlung mehr besteht und ein Nachvollziehen des Weges, den die Transaktion genommen hat, aufgrund dieser bewussten Abkopplung ohne Zugriff auf die internen Informationen des Mixers nahezu unmöglich ist. Um eine Zuordnung weiter zu erschweren, wird die Auszahlung in Höhe und Zeitpunkten zudem oft zufallsbasiert gestückelt und bisweilen an verschiedene andere Depots des Einzahlenden ausgezahlt.

Eine systematische Schwachstelle teilen die diversen Arten von Mixern allerdings: Die Durchmischung und Abkopplung der Guthaben funktionieren nicht mehr, wenn einzelne Nutzer sehr große Beträge einzahlen, da ein großer Teil dieser Beträge an sie selbst zurückfließt.

Seit 2020 hat die Nutzung von Mixern zunächst stark zugenommen, um sich nunmehr auf hohem Niveau einzupendeln.[18] Ein erheblicher Anteil der Zunahme ist auf Transaktionen von Depots zurückzuführen, deren Verbindung mit illegalen Aktivitäten[19] bereits dokumentiert wurde.[20] Allein deren Anteil an allen von dem auf Blockchain-Analyse spezialisierten Unternehmen Chainalysis beobachteten Transaktionen an Mixer belief sich zu Berichtsschluss[21] am 14. Juli 2022 auf 23 Prozent.

Mixer sind in den meisten Ländern nicht verboten. Ihre Betreiber unterliegen teilweise jedoch rechtlichen Anforderungen, wie klassische Finanzdienstleister, die sie aber in der Regel nicht erfüllen. In letzter Zeit haben Aufsichts- und Strafverfolgungsbehörden verschiedentlich Schritte gegen Mixer unternommen, siehe hierzu Abschnitt 6.2 (Sanktionen).

Die Aktivitäten und Nutzer von Mixern sind nicht nur für die Strafverfolgung und Finanzbehörden von Interesse. Sie haben auch außen- und sicherheitspolitische Bedeutung. So stehen einige cyberkriminelle Gruppen einerseits mit staatlichen Nachrichtendiensten und andererseits mit Darknet-Marktplätzen wie Hydra in Verbindung, und diese wiederum mit Mixern. Hackerangriffe zum Zwecke der Informationsgewinnung, Einflussnahme oder Destabilisierung werden mutmaßlich so in Auftrag gegeben, bezahlt und die Transaktionen verschleiert. Andere Hackerangriffe dienen höchstwahrscheinlich der Erbeutung von Geld in Form von Kryptowährung zwecks Sanktionsumgehung und Mittelbeschaffung[22], auch für Nuklearprogramme.[23] Grundsätzlich wird zwischen zentralisierten und dezentralisierten Mixern unterschieden.

Bei **zentralisierten Mixern** (auch: *custodial*, mit Verwahrfunktion) wird die Dienstleistung von einer Plattform erbracht, die hierfür eine Dienstleistungsgebühr verlangt. Manche Mixer variieren die Höhe dieser Gebühr von Transaktion zu Transaktion, um selbst die Nutzung ihrer Dienstleistung zu verschleiern. Allerdings muss der Nutzer der Plattform und ihrer Bereitschaft zur Wiederauszahlung trauen, da er die Kontrolle über sein Geld zeitweise dieser überlassen muss. Zudem muss die Plattform notgedrungen mindestens bis zum Abschluss der Wiederauszahlung dokumentieren, welche Depots wann wel-

17 Typischerweise liegt diese Gebühr bei ein bis drei Prozent der Transaktionssumme (Allison, I., 2015).

18 Chainalysis (2022a).

19 Hierunter fallen nach Definition von Chainalysis: Terrofinanzierung, Diebstahl, Betrugsmaschen, Belegung mit Sanktionen, Erpressungs-Software (ransomware), Administratoren cyberkrimineller Netzwerke, betrügerischer Online-Handel, Handel im Darknet sowie Kinderpornographie. Quantitativ am bedeutsamsten bei der Nutzung von Mixern sind sanktionierte sowie mit ransomware arbeitende Akteure (Chainalysis, 2022a, Abbildung: Quarterly value sent to mixers from illicit addresses by category). Besonders der russland-basierte Darknet-Marktplatz Hydra sowie die nordkoreansiche Lazarus-Hackergruppe sowie der seinerseits sanktionierte Mixer Blender.io sandten im laufenden Jahr bereits große Geldmengen an Mixer.

20 Chainalysis (2022a).

21 Ibid.

22 Allein im laufenden Jahr 2022 soll die nordkoreanische Hackergruppe Lazarus bereits mehr als eine Milliarde USD in Form von Kryptowährungen erbeutet haben, Ziel waren vor allem dezentralisierte, Blockchain-basierte Finanzmärkte (Decentralized Finance, DeFi). Neben einer Vielzahl kleinerer Diebstähle steckt Lazarus hinter spektakulären Fällen wie 2022 dem Diebstahl von 600 Mio. USD von einer Onlinespiel-Plattform (Berwick, A. & Wilson, T., 2022a) sowie dem Versuch, 2016 die Bank von Bangladesch um fast eine Millarde USD zu bestehlen.

23 United Nations Security Council, (2019), S. 49.

chen Betrag ein- und ausgezahlt bekommen haben, um den Rückfluss des Geldes sowie die Berechnung der Gebühren zu gewährleisten. Erhalten Strafverfolgungsbehörden z. B. durch Beschlagnahme von Servern Zugriff auf diese Daten, kann die Transaktion deanonymsiert werden. Außerdem besteht zumindest theoretisch die Möglichkeit einer Falle seitens staatlicher Ermittlungsstellen (*honeypot*).

Um das Risiko der Deanonymisierung zu verringern, und ggf. aus Misstrauen gegenüber jeglichen Intermediären, kommen alternativ **dezentrale Mixer** (*non-custodial,* ohne Verwahrfunktion) zum Einsatz. Sie verzichten auf eine Plattform als zentralem Intermediär, und funktionieren software-basiert, teilweise auch integriert in Depots. Auch hier existieren wiederum verschiedene Arten. In einem **peer-to-peer-Mixer** werden die Guthaben ohne Intermediär zusammengeführt, vermischt und dann wieder ausgezahlt. **CoinJoin-Mixer,** auch *privacy wallets* genannt, ermöglichen es Nutzergruppen, ihre Guthaben zu durchmischen und in einer Serie von Transaktionen zurückzuerhalten, ohne Verwendung eines zentralen Servers und ohne, dass sie die Kontrolle über die Guthaben anderen überlassen müssen. Diese Variante gewinnt unter kriminellen Nutzern seit Jahren an Beliebtheit.[24] **Smart-Contract-Mixer** bestätigen dem Sender einer Transaktion mit einer kryptierten Quittung seine Urheberschaft. Zu einem beliebigen späteren Zeitpunkt kann dieser von einem anderen Depot eine weitere Transaktion unter Nutzung dieser Quittung an den Mixer schicken, um sein Geld an dieses andere Depot weiterleiten zu lassen. Im Gegensatz zu zentralisierten Mixern existiert hier keine Dokumentation der Transaktionshistorie, die bei Beschlagnahmung der Server bekannt werden könnte. Auch kann keine juristische oder natürliche Person, die als Intermediär fungieren würde, rechtlich belangt oder sanktioniert werden.

3.2. Privacy coins

Neben den eigentlich transparenten klassischen Bitcon und Co. gibt es da auch noch Kryptowährungen, die Anonymisierungstechnik bereits im Code aufweisen. Diese Gruppe wird als *privacy coins* bezeichnet, manchmal auch noch als *dark coin*[25], oder als *Anonymity Enhanced Cryptocurrency* (AEC, Kryptowährung erhöhter Anonymität). Zwei bekannte Vertreter sind Monero und Zcash.

Bei **Monero** kann die Anonymisierungstechnik nicht deaktiviert werden: Sie benutzt Einmal-Adressen sowie Gruppierung mit älteren Transaktionen und eine Technik, die die Betragshöhe verschleiert. Bei **Zcash** ist es möglich, immerhin das Vorhandensein einer Transaktion transparent zu gestalten. Sogenannte *zero-knowledge proofs* – mathematische Prüfrechnungen – können eine Transaktion bestätigen, ohne die verwendeten Depots oder Transaktionsvolumina offenzulegen. Die Kryptowährung **Polkadot**[26] erhält erst durch Kombination mit dem sog. Phala-Netzwerk die Eigenschaft einer privacy coin.

Natürlich kann es auch für die Verwendung von *privacy coins* legitime Gründe[27] geben. Dennoch ist es offensichtlich, dass deren Nutzung auch und gerade durch Kriminelle erfolgt. Da bei diesen Kryptowährungen eine Nachverfolgung der Transaktionen nahezu ausgeschlossen werden kann, haben verschiedene Staaten aus Sorge vor der Nutzung durch das Organisierte Verbrechen deren Nutzung gänzlich verboten (z.B. Japan).[28] In Australien und Südkorea dürfen *privacy coins* nicht durch Handeslplattformen, die einen Umtausch von einer Kryptowährung in eine andere, oder in Fiat-Geld, ermöglichen (sog. *cryptocurrency exchanges,* kurz exchanges), gehandelt werden. Auch auf der technischen Seite reagieren Staaten: Die U.S.-Bundessteuerbehörde (*Internal Revenue Service,* IRS) schrieb beispielsweise 2020 ein Preisgeld[29] in Höhe von 625.000 USD für das Dechiffrieren von Monero-Transaktionen aus. Offensichtlich mit Erfolg, denn mittlerweile sind einige Patente[30] hierauf angemeldet worden.

Bitcoins waren eigentlich das Gegenteil von Privacy coins, da ihre Transaktionen völlig öffentlich und transparent sind. Seit dem Taproot-Update im November 2021 sind "private Lightning Network transactions"[31] mit erweiterten Funktionen möglich, die wie gewöhnliche Transaktionen aussehen. Sie sind dennoch nicht so intransparent wie *privacy coins.*

3.3. Kryptobörsen

Auf Kryptobörsen genannten Tauschplattformen (cryptocurrency exchanges) werden Kryptowährungen gehandelt. Sie können hier gegen andere Kryptowährungen oder gegen Fiat-Währungen getauscht werden. Es gibt sie in zwei Ausführungen, zentralisiert (mit Verwahrfunktion, *custodial,* mit *hosted wallets*) und dezentral (ohne Verwahrfunktion, non-custodial mit self-custody wallets). Erstere verwahren den privaten Schlüssel und haben sowohl Kontrolle über die Gelder der Nutzer (können also auch verdächtige Depots einfrieren) als auch die Verantwortung für deren Schutz gegen Diebstahl durch Hacker. Zweitere überlassen den Nutzern die Kontrolle über ihre Depots, und übernehmen keine Schutzverantwortung.[32]

Aus Perspektive der Kriminalitäts- und Geldwäschebekämpfung sind dezentrale Kryptobörsen eine Herausforderung, da der Handel über Software-Code (smart contracts) organisiert wird und keinerlei zentrale Stelle KYC-Protokolle anwendet. Jedoch können auch zentrale Kryptobörsen effektive Ermittlungen und Strafverfolgung erschweren oder ausschließen, wenn sie nicht kooperieren oder keine KYC-Protokolle einsetzen bzw. Einhalten, also ihre Nutzer nicht kennen. Ein prägnantes Fallbeispiel ist die Kryptobörse Binance, die anfangs keinerlei Identitätsprüfungen durchführte. Firmeninterne Äußerungen[33] des Gründers Zhao im Jahr 2017 warfen die Frage auf, ob dies bewusst zugunsten des Marktanteils geschah.

24 Robinson, T (2020).
25 Die privacy coin Dash hieß bis 2015 Darkcoin.
26 Bylund, A. (2022).
27 Ibid.
28 Seth, S. (2019).
29 SAM.gov (2020).
30 Sinclair, S. (2020).
31 Hertig, A. (2021).
32 Dies schreckt mittlerweile jedoch viele Nutzer nicht mehr ab, da dezentrale Börsen in den letzten drei Jahren enorm an Bedienungsfreundlichkeit gewonnen haben.
33 "Do everything to increase our market share, and nothing else," siehe Berwick, A. & Wilson, T. (2022a).

Für die Einrichtung eines Depots reichte die Angabe einer beliebigen Email-Adresse aus.[34] Die Einführung von Identitätserfassungen erfolgte verzögert und zeitweise in der Durchführung scheinbar mangelhaft.[35] Erst seit August 2021 verlangt Binance, nach Geschäftsverboten in England[36] und Japan[37], von Neukunden die Vorlage eines Ausweisdokuments mit Gesichtsabgleich. Binance handelt unter anderem auch mit *privacy coins* wie monero, und wurde in der Vergangenheit intensiv von Nutzern der Darknet-Plattform Hydra frequentiert.[38] Auch Gelder aus großen Diebstahls- und Betrugsfällen (wie z.B. einem Investmentbetrug zum Schaden zahlreicher Rentner in Deutschland) wurde über Binance gewaschen.[39]

34 bid.
35 Reuters berichtet, dass bspw. in einem Fall die Einreichung dreier identischer Kopien einer Restaurantrechnung als Identitätsnachweis akzeptiert wurde (ibid.).
36 Reynolds, K. (2021).
37 Crawley, J. (2021).
38 Berwick, A. & Wilson, T. (2022a).
39 Ibid.

4. Nutzung für illegale Zwecke

Die auf der *blockchain* basierende Technik und ihre Anwendungen werden zunehmend Bestandteil der allgemeinen Finanzmärkte. Mit zunehmendem Reifegrad der Technik und trotz der hohen Kursschwankungen, steigt die Akzeptanz von Kryptowährungen und diese entwickeln sich scheinbar zu einer eigenständigen Assetklasse für risikofreudige Anleger. Analysten erwarten, dass dieser Trend in Verbindung mit einer verstärkten Beobachtung illegaler Transaktionen trotz des absoluten Wachstums illegaler Transaktionen dazu führt, dass ihr relativer Anteil sinken wird. Illegale Transaktionen machen nach aktuellen Schätzungen nur 0,15 Prozent aller Transaktionen mit Kryptowährungen aus.[40]

4.1. Formen illegaler Geschäfte mit Kryptowährungen

Bei der Nutzung von Kryptowährungen für illegale Zwecke kann grundsätzlich zwischen "*krypto-native crime*", das auf der *blockchain* selbst verübt wird (wie Hacker-Angriffe mit Diebstahl von Krypto-Währung[41]) sowie "off-chain crime" (hier fungiert die Blockchain nur als Zahlungsmittel für illegale Straftaten, z.B. für Lösegeldzahlungen oder Bezahlung einer Drogenlieferung) unterschieden werden. Im Folgenden sind verschiedene Phänomenbereiche krimineller Nutzung jeweils kurz dargestellt.

Schon in den Anfangsjahren der Kryptowährungen wurden diese auf Marktplätzen im *darknet* standardmäßig für Zahlungen verwendet. Silk Road markierte 2011 den Anfang, 2015 trat als weitere sehr bekannte Plattform Hydra dazu.

Mittlerweile nutzen auch Kleinkriminelle und ggf. ihre Kunden für Transaktionen Kryptowährung. Diese ersetzen Fiat-Währungen wie auch im Bereich organisierter und schwerer Kriminalität nicht vollständig[42], jedoch haben nahezu alle Straftatbereiche[43], mit denen sich in irgendeiner Weise Geld verdienen lässt, mittlerweile Berührungspunkte mit Kryptowährungen.

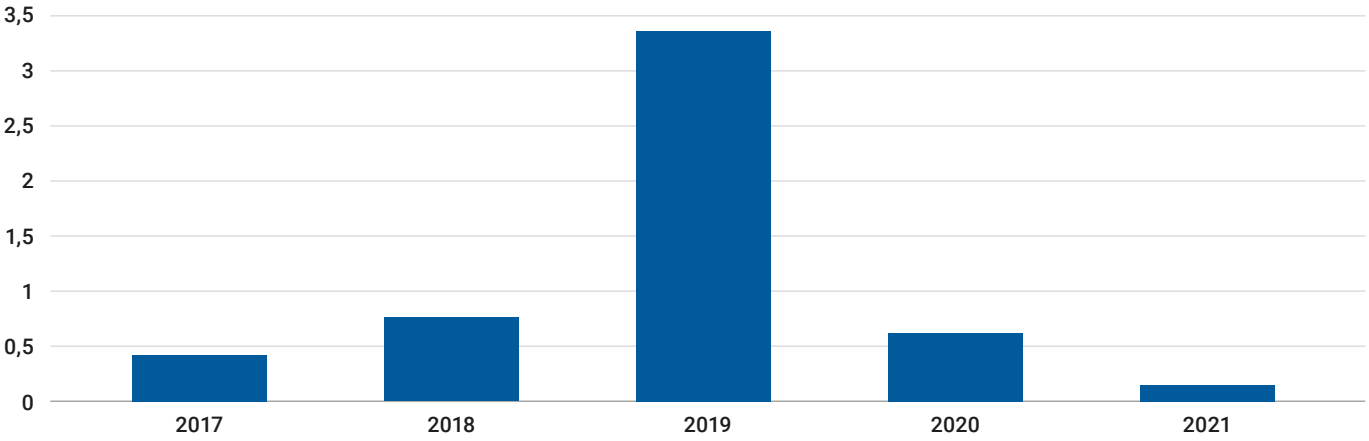
Betrug kann sowohl mit der Kryptowährung selbst erfolgen als auch diese nur als Zahlungsmittel verwenden. So war Betrug besonders im Jahr 2019[44] ein Schwerpunkt-Deliktfeld im Zusammenhang mit Kryptowährungen, und spielt weiterhin eine wichtige Rolle. Einerseits sind Anleger und Nutzer betroffen, die mittels verschiedenster Maschen – sog. *scams* – dazu verleitet werden, Zahlungen zu leisten. Beispielhaft zu nennen sind Schneeballsysteme, bei denen um eine angeblich sehr stark an Wert gewinnenden Währung gezielt Rummel entfacht wird, und erste Anleger Ausschüttungen vom Geld ihnen nachfolgender und unter Umständen von ihnen selbst geworbener Anleger erhalten. Nach einiger Zeit brechen diese Systeme in sich zusammen, die Einnahmen werden von den Initiatoren abgeschöpft, und die Mehrzahl der Anleger verliert das eingesetzte Kapital. Solange werden die Anleger häufig über den Messenger wie Telegram bei der Stange gehalten. Ein weiteres kriminelles Anwendungsfeld sind betrügerische Händlerseiten im Internet, sog. *fraud shops*.[45]

Bei sog. **Ransomware-Attacken** handelt es sich um Hackerangriffe, bei denen sensible Daten der Opfer verschlüsselt und bisweilen gestohlen werden. Die Wiedergabe erfolgt erst nach Zahlung eines Lösegeldes oder gar nicht.[46] Das Lösegeld wird hier zumeist in Form von Kryptowährungen verlangt.

Auf den oben erwähnten Kryptobörsen kommt es immer wieder zu **Diebstählen,** das Jahr 2021 markierte hier den vorläufigen Höhepunkt.[47] Dies betrifft auch den Bereich der *Decentralized Finance* (DeFi) mit ihren dezentralisierten Plattformen, auf denen sich viele Nutzer aufgrund des Verzichts auf verwahrende Intermediäre und angesichts der Transparenz der *blockchain* sicher wähnen. Tatsächlich bereitet aber die

40 Chainalysis (2022b), Chainalysis (2022c), S.4.
41 Inhaber von Kryptowährungen treten durchaus nicht nur auf der Täterseite krimineller Nutzung auf, sondern sind nicht selten Opfer, bspw. von Diebstahl i.Z.m. *hacking* oder Betrug i.Z.m. *scamming*.
42 Europol (2021), S.2.
43 Nach Aussage eines Spezialisten des Bundeskriminalamts in einem Hintergrundgespräch am 08. August 2022 fiel die vermehrte Nutzung durch Kriminelle im zeitlichen Zusammenhang mit der Aufnahme des Themas Kryptowährungen in der breiten medialen Berichterstattung und den sozialen Medien zusammen. So ließe sich ein besonders starker Anstieg in den letzten drei Jahren erkennen. Neben der organisierten Geldwäsche und Cybercrime können sich mittlerweile teilweise aber auch Drogendealer im Straßenhandel in Kryptowährung bezahlen lassen.
44 Chainalysis (2022d).
45 Collins, J. (2022), S. 18.
46 Chainalysis (2022d).
47 Ibid.

Abb. 2 | Anteil illegaler Nutzung an Kryptotransaktionen 2017-2021 (in Prozent)



Quelle: Chainanalysis 2022c

irreversible Natur der *Blockchains* erhebliche Schwierigkeiten, die Beute zurückzuerhalten oder ohne zentrale Intermediäre auch nur einzufrieren.

Im Bereich der Kryptobörsen und *cross-chain bridges* – gewissermaßen Brücken zur Umwandlung von Währungen inkompatibler *Blockchains* – besteht aufgrund komplexer und teilweise nicht ausgereifter Programmierung[48] sich dynamisch entwickelnder Start-up-Unternehmen und FinTechs immer ein Risiko.

Typische Schemata[49] sind sogenannte code exploits, die Fehler in der Programmierung nutzen. Wurden diese Fehler als Hintertüren bewusst seitens der Entwickler eingebaut, spricht man von einem *rug pull* (auch: *exit scam*). Aufgrund der pseudonymisierenden Natur der Transaktionen sind diese nicht ohne Weiteres von anderen Betrugsformen zu unterscheiden. Bei *admin key exploits* werden seitens der Entwickler bewusst eingebaute Hintertüren, die Aktualisierungen der *smart contracts* oder eine Verwaltung der Reserven erlauben soll, aber bei Entdeckung von Kriminellen missbraucht werden kann.

Anders sieht die Ausnutzung von Schwachstellen in der Programmierung bei den sog. *economic exploits* aus. Hier werden seitens der Entwickler unerwartete Eigenschaften vor allem miteinander kombinierbarer *tokens* ausgenutzt, und dann z. B. kurzfristige heftige Wertmanipulationen und Arbitragegeschäfte ermöglichen. Erläuterungen und Fallbeispiele für die verschiedenen Schemata finden sich im DeFi-Bericht der *blockchain*-Analysefirma Elliptic.[50]

Non-fungible tokens[51] (NFT) ermöglichen Formen **Marktmanipulation** zum Schaden anderer Teilnehmer. Ein Beispiel ist eine Form von Scheingeschäft, das sog. *wash trading*[52].

Bei dieser Form der Marktmanipulation befindet sich der Täter sowohl auf der Verkäufer- als auch auf der Käuferseite, täuscht aber Handel mit anderen Teilnehmern vor. Hierdurch entsteht der Eindruck einer hohen Nachfrage und Handelsfrequenz bzgl. des Tokens, was einige Handelsplattformen mit besonderen Anreizsystemen finanziell mit sog. *native tokens* belohnen. Diese wiederum kann der Täter einsetzen (*staking*), um noch mehr Handelsvolumen zu erzeugen. Der Preis des ursprünglichen Tokens wird künstlich aufgebläht. Einerseits erschleicht sich der Täter die Belohnungen des Plattformbetreibers, und andererseits täuscht er anderen Marktteilnehmern eine überhöhte Liquidität des von ihm gehaltenen Tokens vor (und verkauft diesen ggf. zu einem überhöhten Preis). Dieses Schema lohnt sich jedoch nur, wenn die Einnahmen die typischerweise pro Transaktion an den Plattformbetreiber zu zahlenden Gebühren (*gas fees*) übersteigen.[53]

4.2. Extremismus- und Terrorismusfinanzierung

Ein besonders ernstes, wenn auch quantitativ nicht hervorstechendes Feld krimineller Nutzung von Kryptowährungen ist die Finanzierung von terroristischen Gruppen und Anschlägen.[54] Wiederholt haben Terrororganisationen zu Spenden aufgerufen. Zwar ist angesichts dessen, was in den vergangenen Jahren auf der Bitcoin-*blockchain* nachvollzogen werden konnte, davon auszugehen, dass es – verglichen mit anderen Feldern – um jeweils kleinere erzielte Beträge von einigen tausend Euro geht. In den Transaktionsvolumina auf der Bitcoin-*blockchain* waren auch Spendenaufrufen keine größeren Sprünge in den Transaktionsvolumina sichtbar, und seit 2020 gab es keine größeren Beschlagnahmungen. Auch Europol bezeichnet die Fallzahl der Terrorfinanzierung mit Kryptowährungen als überschaubar.[55] Allerdings werden für die Verübung von Anschlägen typischerweise auch keine großen Summen benötigt, wenn Waffen, Sprengstoff, Fahrzeuge oder Reisebewegungen finanziert werden müssen.

48 Elliptic (2021), S. 15.
49 Elliptic (2021), S. 17 f.
50 Elliptic (2021), S. 18 f.
51 Ein NFT ist im Gegensatz zu den Einheiten der jeweiligen Kryptowährung auf der *blockchain* einmalig, nicht austauschbar oder teilbar. Er steht für einen digitalen oder auch physischen Gegenstand. Beispielsweise kann es sich um ein Grundstück in einer virtuellen Welt oder um ein Kunstwerk handeln.
52 Ähnliche Formen der Marktmanipulationen heißen im angelsächsischen Sprachraum *painting the tape* und *churning*.
53 Chainalysis (2022e).
54 Eisermann, D. & Schindler, H.-J. (2020).
55 Europol (2021), S.2.

Genutzt werden Kryptowährungen durch Terrororganisationen für Crowdfunding und Spendenaufrufe sowie für (teilweise legale) Online-Shops. Bereits seit etwa 2017 nutzen extremistische Online-Shops kaum noch klassische Zahlungsdienstleister wie PayPal, Klarna oder Mastercard, sondern sind auf Kryptowährungen ausgewichen. Eine bedeutsame Entwicklung betrifft die Wahl der bevorzugten Kryptowährungen durch Extremisten[56] und Terroristen, die Bitcoin heute viel weniger nutzen als noch vor drei Jahren. Nunmehr bevorzugen sie *privacy coins* wie Monero, Zcash und Dash. Diese können aufgrund ihrer Eigenschaften nicht oder nicht im gleichen Maße von der *blockchain*-Analyseern beobachtet werden wie Bitcoin, Ether und andere etablierte Kryptowährungen.

Wie Chainalysis[57] auflistet, haben in den vergangenen Jahren mindestens zehn terroristische Organisationen Kryptowährungen für ihre Finanzierung verwendet oder dies versucht, darunter auch al Qaida, der sogenannte Islamische Staat oder die Hamas. Um Spenden geworben wird über klassische Soziale Medien wie Facebook und Kanäle in Messenger-Diensten wie Telegram[58]. Sogar Software zur automatischen Generierung von Depot-Adressen fand in der Vergangenheit bei Spendenaufrufen Verwendung.[59]

Handelt es sich bei den verwendeten Währungen nicht um *privacy coins,* können die Gelder jedoch oft rechtzeitig beschlagnahmt werden, bevor sie auf Kryptobörsen in Fiat-Währungen getauscht werden können. Dies gelang[60] etwa in Israel bei Depots mit den Währungen Bitcoin, Ether, Tether, XRP, und anderen.

Zwar sind die Haupteinnahmequellen terroristischer Organisationen vielfältig und bewegen sich eher im *off-chain*-Bereich (Drogenhandel, Extraktion von Rohstoffen, Erpressung, Menschenhandel usw.), jedoch lassen sich die Transaktionen auf *blockchains* sehr viel leichter beobachten und ggf. einfrieren, als eine Einflussnahme in An- und Abbaugebieten usw. umzusetzen ist. Dieser Ansatzpunkt sollte daher zusätzlich und intensiver als bislang genutzt werden.

4.3. Geldwäsche

Für Geldwäsche sind Kryptowährungen trotz der technisch eigentlich lückenlosen, eindeutigen und transparenten Dokumentation der Transaktionshistorie in den diversen *blockchains* von Beginn an interessant. Letztes Jahr wurden geschätzt 8,6 Mrd. USD so gewaschen, 30% mehr als im Vorjahr.[61] Anfangs mag der Grund in der Pseudonymisierung sowie in der scheinbaren Komplexität der neuen Technik gelegen haben. Zusätzlich kann das auch in der analogen Geldwäsche genutzte *layering* im digitalen und kryptierten Transaktionsverkehr ungleich einfacher vervielfacht und die Transaktionen verzweigt werden. Ermittlungsbehörden waren mangels qualifizierten Personals und eigener technischer Fähigkeiten der neuen Aufgabe noch nicht gewachsen.

Mit zunehmender Verbreitung von Kryptowährungen entwickelt sich wie bei jeder auch von Kriminellen adoptierten neuen Technik ein Wettlauf zwischen beiden Seiten. Partnerschaften zwischen Ermittlungsbehörden und spezialisierten Firmen ermöglichen seitdem (mit erheblichem Aufwand) die Anwendung der Strategie *"follow the money"* auch bei vielen Kryptowährungen.

Die Funktionen der *privacy coins* und Mixer heben die technische Herausforderung für Ermittlungsbehörden auf eine neue Stufe, denn die de-facto-Anonymisierung, die diese derzeit ermöglichen, stellt – insofern nicht später und innerhalb der Verjährungsfristen juristisch nutzbare Daten gesammelt und gerichtsfest dokumentiert werden sollten – eine zeitliche Phase der Straffreiheit für Geldwäscher im Prinzip sicher. Dieses Blatt wird sich mit dem Einzug der Quantencomputer mutmaßlich wieder wenden, sollte aber bereits vorher Gesetzgeber sowie Exekutive und Judikative interessieren.

4.4. Staatsnahe Akteure, nationale Sicherheit

Schwieriger liegt der Fall, wenn es sich bei den Kriminellen um sogenannte staatsnahe Akteure handelt. Selbst wenn die Attribution von Hackerangriffen und die Verfolgung von Transaktionen künftig durch Anwendung von Quantencomputern oder andere erweiterte Kompetenzen und Einsatzmittel von Ermittlungsbehörden große Fortschritte machen sollten, so stoßen ihre Möglichkeiten doch oft an Grenzen, sobald sich Täter oder Server mit ermittlungsrelevanten Daten in souveränen Staaten befinden, die nicht mit den deutschen Ermittlungsbehörden kooperieren.

Das Interesse solcher Staaten kann unter anderem in der Instrumentalisierung von nicht im Staatsdienst stehenden, besonders kompetenten und ihre Dienstleistungen an den Höchstbietenden vermietenden Hackern liegen, die im Interesse geopolitischer Interessen entweder für Destabilisierung und hybride Kriegsführung oder Spionage eingesetzt werden. Diese Hacker müssen sicher und möglichst abstreitbar bezahlt werden können.

Insbesondere bei Staaten, die selbst Sanktionen unterliegen, können zwei weitere Motive hinzutreten: Einerseits kann es um die Möglichkeit von Transaktionen mit embargo-brechenden Handelspartnern gehen, wenn entweder für ihre Banken ein Ausschluss aus dem internationalen Finanzsystem besteht (wie dem SWIFT[62]-System) oder wenn trotz der Mög-

56 Diese Entwicklungen sind laut eines erfahrenen Diplomaten und Beraters im außen- und sicherheitspolitischen Umfeld insbesondere in den Phänomenbereichen Rechtsextremismus sowie Islamismus zu verzeichnen, wie er in einem Hintergrundgespräch am 22.08.2022 erörterte. Diese Entwicklung ließe sich bspw. im ransomware-Bereich so nicht beobachten, da hier Lösegeldzahlungen von ansonsten nicht mit derlei Transaktionen vertrauten Unternehmen, Institutionen und Personen verlangt werden. Lösegeldforderungen in Bitcoin lassen sich einfacher im Wert einschätzen, weiterhin ist das Wissen um die technische Umsetzung einer Transaktion verbreiteter als ebi exotischeren und jüngeren Kryptowährungen.
57 Chainalysis (2022) The 2022 Crypto Crime Report, S. 92 ff.
58 Ibid., S.93.
59 Eisermann, D. & Schindler, H.-J. (2020) S.4.
60 Eisermann, D. & Schindler, H.-J. (2020) S.4.
61 BBC (2022).

62 SWIFT steht für die in Belgien ansässige *Society for Worldwide Interbank Financial Telecommunication.* Ein Ausschluss erschwert Transaktionen im Außenwirtschaftsverkehr erheblich. Gegenwärtig sind vor dem Hintergrund des Ukraine-Konflikts russische Banken von einem Ausschluss aus dem SWIFT-System betroffen, vor dem Hintergrund der Nuklearwaffenprogramme ihrer Staaten seit 2018 (und bereits 2012 bis 2016) iranische, seit 2017 nordkoreanische.

lichkeit regulärer Transaktionen eine möglichst intransparente Transaktion gewünscht ist.

Andererseits kann das Motiv in der Beschaffung finanzieller Mittel für die entsprechenden Staaten selbst liegen, wenn diese aufgrund zu geringer Devisenreserven oder der Notwendigkeit, Ausgaben nicht aus kontrollierbaren Haushalten zu bestreiten, nicht in die Staatskasse greifen können.

Sowohl das durch Anwendung kryptowährungsbezogener Verschleierungsverfahren erleichterte unentdeckte Brechen von Embargos durch Verdeckung der handels- und dienstleistungsbezogenen Transaktionen, als auch die verdeckte Geldbeschaffung für solche Transaktionen, stellen unter Umständen auch eine Herausforderung für die nationale und internationale Sicherheit dar. Denn die Mittel können das Forttreiben und Ausweiten von Nuklearwaffenprogrammen finanzieren.

Die Vermutung, dass Kryptowährungen von Staaten oder staatsnahen Akteuren in erheblichen Volumina genutzt werden könnten, um Sanktionen zu umgehen oder finanzielle Mittel zu beschaffen, scheint darüber hinaus bislang zumindest verifizierungsbedürftig zu sein. So gibt es zumindest jenseits von *privacy coins* und Mixern nur in Grenzen Anzeichen dafür, dass etwa mit Sanktionen belegte russische Oligarchen große Summen hierüber bewegen würden.[63] Auch gab es nach dem russischen Angriff auf die Ukraine keine erheblichen hiermit in Verbindung gebrachten Wertentwicklungen bei Kryptowährungen.[64] Der Iran fördert zwar mit Stromsubventionen indirekt das im Land intensiv betriebene *mining* von Kryptowährungen, jedoch reicht das Volumen[65] nicht aus, um die Volkswirtschaft zu stabilisieren.

Nicht vergessen werden darf bei alledem, dass Kryptowährungen, gerade weil sie auf Intermediäre verzichten, eine Möglichkeit schaffen, Dissidenten in totalitären Staaten zu unterstützen oder ihnen hilft, Ihr Vermögen bei der Flucht zu sichern. Die Volksrepublik China hat wohl auch deshalb Transaktionen mit Kryptowährungen im vergangenen Jahr gänzlich verboten,[66] und arbeitet mit dem digitalen Renminbi an einem „weiteren Baustein im digitalen Überwachungsstaat".[67]

63 Nestler, F. (2022).
64 Diese Einschätzung wurde in einem Hintergrundgespräch am 22.08.2022 von einem Spezialisten für Sanktionen und Abwehr von Terrorismusfinanzierung, Dr. Hans-Jakob Schindler, Senior Director Counter Extremism Project, geäußert.
65 Ibid.
66 Wurzel, S. (2021).
67 Hilgers, S. & Greilich, K. (2021), S. 22.

5. Ansätze zur Geldwäschebekämpfung

Geldwäsche im Zusammenhang mit Kryptowährungen wird seit Jahren als wichtige Herausforderung für Regulierer, Behörden und Unternehmen des Finanzsektors betrachtet. Auf nationaler, supra- und internationaler Ebene wurden entsprechende Gesetze und Verordnungen in Kraft gesetzt, deren wichtigste im Folgenden kurz angerissen werden. Weiterhin gibt es erfolgversprechende Entwicklungen im Ermittlungs- und Strafverfolgungsbereich, die bislang bei Mixern, *privacy coins* sowie dezentralen Kryptobörsen derzeit an ihre Grenzen stoßen.

5.1. Regulierung

Regulierung erfolgt über Gesetze und Verordnungen. Diesen können natürliche und juristische Personen unterliegen. Gibt es jedoch, wie im Falle *blockchain*-basierter Transaktionen häufig der Fall, keine Intermediäre wie etwa Banken, Kryptobörsen-Betreiber usw., so kann Regulierung allenfalls die Nutzung der Technik bzw. bestimmte Anwendungen (wie dezentrale Mixer ohne Kunden-Datenbank und KYC-Protokolle, dezentrale Kryptobörsen, oder *privacy coins*) illegalisieren. Zwischen klassischer Regulierung des Finanzsektors und technikbezogener Regulierung, in der neue Wege gesucht werden müssen, besteht also ein Spannungsfeld, das kreative Ansätze erforderlich macht.

Regulierungsbestrebungen bzgl. von Kryptowährungen beziehen sich derzeit einerseits auf den hohen Energiebedarf des *proof-of-work*-Verfahrens, was jedoch nicht Gegenstand dieser Übersicht ist. Andererseits fokussieren sie auf Bekämpfung von Geldwäsche und Terrorismusfinanzierung.

Ein Thema, das sich durch die Regulierungsbestrebungen zieht, ist die Verpflichtung zur Einrichtung und Einhaltung von *Know-Your-Customer*-Protokollen, also der Legitimationsprüfung bei Neukunden inklusive der Erfassung von persönlichen Identifikationsdaten und Geschäftsdaten.

Eine Herausforderung für die Regulierung kann sich aus dem geografischen Standort von Akteuren, und damit Grenzen der Jurisdiktion, ergeben. 2020 war bspw. mehr als die Hälfte[68] aller Kryptobörsen in der Republik Seychellen registriert.

Im Folgenden sollen die derzeit bedeutsamsten Regulierungsaspekte vor allem in Deutschland, der Europäischen Union, und den Vereinigten Staaten thematisiert werden.

5.1.1. National

In den **USA** werden Kryptobörsen mittels des *Bank Secrecy Act* (BSA, 1970) reguliert, was eine Pflicht zur Registrierung der Betreiber beim *Financial Crimes Enforcement Network* (FinCEN)[69] sowie zur Implementierung von Kontrollen bzgl.

68 Ciphertrace (2020).
69 Bei FinCEN handelt es sich um eine Behörde des US-Finanzministeriums, die inländische und internationale Geldwäsche, Terrorismusfinanzierung und andere Finanzverbrechen bekämpft und hierfür Informationen über Finanztransaktionen sammelt und analysiert.

von Geldwäsche (*anti-money laundering,* AML) beinhaltet. Relevant ist zudem der *National Defense Authorization Act* von 2021, NDAA), der den *Anti-Money Laundering Act* von 2020 integriert und Maßnahmen gegen Terrorismusfinanzierung (*counter-terrorist financing,* CTF) reformiert. Mittlerweile muss auch in den USA die *Travel Rule der Financial Action Task Force* (FATF, s.u.) angewandt werden.

Darüber hinaus ist die Regulierung teilweise noch uneinheitlich – so wertet die US-Börsenaufsichtsbehörde (*US Securities and Exchange Commission,* SEC) Kryptowährungen als Wertpapiere, mit entsprechenden Regelungen für Depots und Kryptobörsen. Die US-Regulierungsbehörde für Future- und Optionsmärkte (*Commodities Futures Trading Commission,* CFTC) wertet hingegen Bitcoins als Ware, mit der inklusive ihrer Derivate öffentlich gehandelt werden dürfe.[70]

Aktuell erarbeitet das U.S.-Finanzministerium eine Regulierung von sog. *unhosted wallets,* die offline gehalten werden können und damit schwer kontrollierbar sind. In der Diskussion sind Meldepflichten für Transaktionen über 10.000 USD pro Tag[71] sowie eine Pflicht zur Informationssammlung für Banken bezüglich der beteiligte Transaktionsparteien ab einer Schwelle von mehr als 3.000 USD[72].

In **Deutschland** gilt für Anbieter von Kryptowährungen laut Kreditwesengesetz (KWG), dass sie eine Kryptoverwahrlizenz benötigen, die bei der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) beantragt werden muss.[73] Diese Regelung gilt sowohl für das Verwahrgeschäft als auch für sonstige „Dienstleistungen mit Kryptowerten".[74] Weiterhin ist beim *on-* und *off-ramp* das Geldwäschegesetz (GWG) von Bedeutung, welches in §2 den Kreis der Verpflichteten festlegt. [75]

5.1.2. Inter- und supranational

Die multinationale Organisation FATF gibt Empfehlungen zur Eindämmung von Geldwäsche sowie der Finanzierung von Terrorismus und Proliferation von Massenvernichtungswaffen. Im Jahr 2019 ergänzte die FATF ihre als ***Travel Rule*** bekannte Empfehlung Nr. 16 um den Aspekt, dass auch Anbieter von virtuellen Vermögenswerten die Nutzerdaten von Begünstigten und Auftraggebern während der Übermittlung untereinander und auf Anfrage mit den Strafverfolgungsbehörden austauschen sollen (***Crypto Travel Rule***).

Auf Ebene der Europäischen Union gibt es noch keinen spezifischen Regelungsrahmen[76], aber derzeit zwei Regulierungsinitiativen: Die auf Krypto-Dienstleistungen abzielende *Markets in Crypto-Assets Regulation* (**MiCa**) sowie die **Geldtransferverordnung.** Streitpunkt waren in den vergangenen Monaten dabei Zuständigkeitsfragen, da bislang nicht eindeutig geregelt ist, unter welchen Umständen die europäische Wertpapieraufsicht bzw. nationale Behörden der Mitgliedsstaaten maßgeblich sind. Federführend für die Umsetzung der geplanten MiCA soll jetzt die Europäische Wertpapier- und Marktaufsichtsbehörde ESMA (*European Securities and Markets Authority*) sein, die auch eine schwarze Liste von Kryptowährungsdienstleistern ohne Genehmigung führen und veröffentlichen soll.[77] Vorerst offen bleibt die Regulierung von NFT sowie *Decentralized finance* (DeFi).

Die derzeitige Einigung[78] zur Geldtransferverordnung weitet den Anwendungsbereich bestehender Regelungen auf Kryptowerte aus und bestimmt, dass "Krypto-Plattformen beim Abwickeln von Transaktionen künftig Informationen über Sender und Empfänger ermitteln"[79] müssen, und diese Informationen im Rahmen von Geldwäsche- oder Terrorismusermittlungen mit den Behörden zu teilen haben. Dies gilt voraussichtlich unabhängig von der Betragshöhe, bei unabhängigen Depots (*unhosted wallets*) wird eine Wertgrenze von 1000 Euro erwogen. Ziel ist die Bewältigung der „Risiken der Geldwäsche und der Terrorismusfinanzierung" durch die „Rückverfolgbarkeit von Kryptowertetransfers".[80] Unbetroffen bleiben hingegen „direkte Transfers zwischen Inhabern von plattformunabhängigen Krypto-Geldbörsen oder -Depots".[81]

Auch die aktuelle, 5. **Europäische Geldwäscherichtlinie**[82] sieht vor, dass „Kryptobörsen die Identität ihrer eigenen Kunden verifizieren müssen".[83] In Planung befindet sich zudem eine EU-Anti-Geldwäschebehörde, die die Kontrolle im Falle eines hohen Geldwäscherisikos an sich ziehen können soll.[84]

5.2. Sanktionen

Ein weiteres wichtiges Instrument für die Eindämmung krimineller Nutzung von Kryptowährungen sind Sanktionen. Hiervon waren 2019[85] die Hackergruppe Lazarus, 2020[86] die Bitcoin-Mixer Helix sowie CoinNinja und 2021[87] Bitcoin Fog auf Basis von Registrierungs- und Lizensierungsvorschriften betroffen. Ebenfalls 2021 traf es den in Moskau und St. Petersburg ansässigen Krypto-Händler Suex aufgrund seiner Verbindungen zu Ransomware-Erpressern, Betrug und Darknet-Plattformen.[88] Im Jahr 2022 wurden erstmals Mixer sanktioniert. Der erste[89] war der zentralisierte, verwahrende (*custodial*) Mixer Blender.io. Kurze Zeit später folgte der nicht-verwahrende (*non-custodial*) Ethereum-Mixer Tornado Cash.[90] Dieser wurde unter Spezifizierung von 38 Krypto-Adressen der SDN[91]-Liste des U.S.-amerikanischen *Office of Foreign Assets Control* (OFAC) hinzugefügt.[92] Wie bei Blender.

70 Complyadvantage.com (2022).
71 Thomas, D. & Rossow, A. (2022).
72 Ibid.
73 Huemer, S. (2022).
74 Bundesregierung (2022), S. 2 f.
75 Nicht unproblematisch erscheint angesichts stark schwankender Kryptowerte die Festlegung von Wertgrenzen im Zusammenhang mit Meldepflichten.
76 Europäischer Rat (2022a).
77 Institutional-money.com (2022).
78 Europäischer Rat (2022b).
79 Mussler, W. (2022).
80 Europäischer Rat (2022b).
81 Mussler, W. (2022).
82 Europäische Union (2020).
83 Huemer, S. (2022) Neue Regeln für den Bitcoin.
84 Mussler, W. (2022) Kryptotransfers auf der Spur.
85 Berwick, A. & Wilson, T. (2022a).
86 Durchführende Behörde der Maßnahme: FinCEN (Financial Crimes Enforcement Network, USA).
87 Durchführende Behörde der Maßnahme: DoJ (Department of Justice, USA).
88 Chainalysis (2021).
89 U.S. Department of Treasury (2022).
90 Durchführende Behörde der Maßnahme: OFAC (U.S. Treasury's Office of Foreign Assets Control, USA).
91 Specially Designated Nationals And Blocked Persons List.
92 Durchführende Behörde der Maßnahme: OFAC.

io bestand hier eine Verbindung mit der nordkoreanischen Hackergruppe Lazarus,[93] gestohlene Kryptowerte wurden im großen Stil gewaschen. Dieser Schritt wiederum rief Kritiker auf den Plan und führte zu einer Klage[94] der größten Krypto-Tauschplattform in den USA, da erstmals nicht eine natürliche oder juristische Person, sondern Software das Ziel einer Sanktion war.

Nach Einschätzung eines auf Kryptowährungen spezialisierten Mitarbeiters eines Think Tanks[95] ist die Sanktionierung von Software-Code und -Protokollen - was letztlich einem Nutzungsverbot für Bürger und Unternehmen des sanktionierenden Staates entspricht - jedoch eine weniger direkte Strategie als die Sanktionierung gegenüber natürlichen oder juristischen Personen, für die eine solche Maßnahme mit wirtschaftlichen Nachteilen einhergeht. Da erst kürzlich die erste und einzige derartige Sanktionierung verhängt wurde, muss die Strategie derzeit noch als ungetestet betrachtet werden. Es wird sich über die Zeit zeigen, ob sie sich bewährt. Diese Strategie wirft auch Komplikationen bei der Durchsetzung auf. Erstens gibt es möglicherweise nicht eine einzige lebende Person, die für den täglichen Betrieb des Protokolls verantwortlich ist. Zweitens besteht die heikle Aussicht, es auch mit einer großen Anzahl nicht krimineller Nutzer zu tun zu haben, die mit dem Protokoll oft anonym interagieren.

Ziel von Sanktionen ist zumeist die Behinderung des *off-ramp* durch Isolierung der sanktionierten Einheiten von regelkonformen Finanzdienstleistern. So dürfen U.S.-Bürger und Firmen keine Geschäftsbeziehungen mit derart sanktionierten Einheiten mehr unterhalten, wenn diese auf der SDN-Liste aufgeführt sind.

5.3. Ermittlung und Strafverfolgung

Während die neuen Formen der Tatbegehung und Transaktionen in den Anfangsjahren der kriminellen Nutzung von Kryptowährungen Ermittler noch große Schwierigkeiten bereiteten, hat sich hier mittlerweile viel zum Positiven entwickelt. Vor allem in den Vereinigten Staaten haben sich in Behörden wie dem *Federal Bureau of Investigation* (FBI) und dem Kriminaldienst der Bundessteuerbehörde (*Internal Revenue Service – Criminal Investigation*, IRS-CI) weitreichende Kompetenzen gebildet. Auch die gezielte Zusammenarbeit mit auf *Blockchain*-Analyse spezialisierten Firmen erweist sich als effektiv. Diese Unternehmen[96] sind bislang sämtlich in den USA angesiedelt.

Auch die begünstigenden Bedingungen für Straftaten werden ins Visier genommen: So forderten U.S.-Bundesermittler die weltgrößte Tauschplattform Binance zur Herausgabe weitreichender Informationen bzgl. interner Kommunikation und Prüfverfahren auf. Binance wird aufgrund zunächst fehlender und später laxer KYC-Protokolle ebenfalls mit Geldwäsche im großen Stil in Verbindung gebracht.[97]

In Deutschland befinden sich die Fähigkeiten, beispielsweise beim Bundeskriminalamt, im Aufwuchs. Allerdings sind neben der Anpassung an die internationale Natur des Deliktfelds unklare Zuständigkeiten in der deutschen Behördenlandschaft derzeit noch ein organisatorisches Hemmnis.[98] Nicht nur das Innen-, sondern auch das Finanzressort sind mit Ermittlungen befasst. Bei der zum deutschen Zoll gehörenden Zentralstelle für Finanztransaktionsuntersuchungen (*Financial Intelligence Unit,* FIU) gingen laut Antwort der Bundesregierung[99] auf eine Kleine Anfrage der Linken-Bundestagsfraktion im Jahr 2021 annähernd zehnmal so viele Geldwäsche-Verdachtsmeldungen bzgl. von Kryptowährungen ein, wie 2018.

Diese FIU soll nach den Vorstellungen des Bundesfinanzministeriums in eine eigenständige Behörde, das "Bundesfinanzkriminalamt", überführt werden. In dieser neuen Bundesbehörde sollen die Kompetenzen in vier Säulen gebündelt werden: Erstens ein Fahndungsbereich, der echte Ermittlungsbefugnisse erhalten soll, zweitens die Sanktionskontrolle und -durchsetzung. Drittens soll die Anti-Geldwäsche-Einheit FIU in die neue Bundesbehörde eingegliedert werden. Vierte Säule soll eine Zentralstelle für die Aufsicht über den Nicht-Finanzsektor werden, um Länderzuständigkeiten zu koordinieren und Standards zu definieren.[100] Mit der Schaffung einer solchen zentralen Bundesbehörde sollte auch die Fähigkeit zur Ermittlung von illegalen Aktivitäten mit Hilfe von Kryptowährungen deutlich gestärkt werden.

Es gibt jedoch auch vielversprechende Entwicklungen im privatwirtschaftlichen sowie im technischen Bereich. Eine könnte als "Compliance Plus" bezeichnet werden. So entwickeln innovative Startups[101] Compliance-Strategien und beraten Unternehmen im Finanzsektor bei der Implementierung. Ergänzend zu listenbasierten Kontrollen, Befragung von Kunden und dem Abhaken von Prüfpunkten, was oft nicht zu zeitgerechter Erkennung von Verstößen führt, kommen proaktive Verfahren zum Einsatz. Vor allem FinTechs können aufgrund der Verbundenheit mit dem Internet unter Nutzung offen verfügbarer Teile von Sozialen Medien und anderen Quellen dubiose Verhaltensmuster und gefälschte Identitäten leichter bereits zu einem frühen Zeitpunkt erkennen.[102] Eine weitere könnte sich aus der Entwicklung des Quantencomputings in Verbindung mit der lückenlosen Dokumentation in den *Blockchains* ergeben. Hier könnten zu einem späteren Zeitpunkt gewissermaßen forensische Zeitreisen unternommen werden, um mit den dann vorhandenen Rechnerleistungen alte Schleier zu lüften.

93 Die Lazarus-Gruppe, die mutmaßlich im Auftrag des zum nordkoreanischen Nachrichtendienst gehörenden Büro 121 handelt, steht auch hinter dem Diebstahl auf einer slowakischen Kryptobörse in Höhe von 5,4 Millionen USD (Berwick, A. & Wilson, T. (2022a).
94 Newmyer, T. (2022).
95 Diese wurde in einem Hintergrundgespräch am 30.08.2022 von Yaya J. Fanusie, Adjunct Senior Fellow am Center for a New American Security, geäußert.
96 Die bekanntesten heißen Chainalysis, CipherTrace, Elliptic und TRM Labs, ferner ist Tracer von Coinbase zu nennen.
97 Berwick, A. & Wilson, T. (2022b).
98 Quelle: Hintergrundgespräch 08. August 2022, Gesprächspartner Salih Altuntas.
99 Bundesregierung (2022), S. 5.
100 Bundesfinanzministerium (2022).
101 Ein Beispiel ist die deutsche Beratungsfirma BerFin.
102 Quelle: Hintergrundgespräch am 22.08.2022, Dr. Hans-Jakob Schindler, Senior Director Counter Extremism Project.

6. Handlungsempfehlungen

Regulierung zur Marktgestaltung:

Mit Hilfe der Regulierung von Märkten soll deren Effizienz bei der Allokation knapper Ressourcen sichergestellt werden. Ein wesentlicher Teil für das effiziente Funktionieren von Märkten ist das **Vertrauen** der Marktteilnehmer, dass Transaktionen fair und rechtssicher abgewickelt werden. Der Schutz der Verbraucher und bei Kapitalmärkten der Anlegerschutz sind dabei hohe Güter. Dies gilt ganz besonders für Märkte mit erheblichen Informationsasymmetrien. Gleichzeitig dürfen sie nicht das Feigenblatt für eine unbotmäßige Einschränkung der Konsumentenfreiheit sein.

Wie im klassischen Finanzsektor sind auch im Kryptowährungssektor gewinnorientierte Unternehmen tätig, die aus betriebswirtschaftlichen Gründen möglicherweise bewusst in gewissem Rahmen **Compliance**-Strafen in Kauf nehmen. Gute Um- und Durchsetzung der Regulierung muss dazu beitragen, den Sektor zu einer möglichst weitgehenden Einhaltung zu motivieren.

Ein weiterer Aspekt von Effizienz bei **Finanzmärkten** ist die der Finanzstabilität. Die Finanzkrise von 2008 hat gezeigt, dass Kapitalmärkte ab einer gewissen Größe der Regulierung und Überwachung bedürfen, um keine kaskadierenden Risiken für das gesamte Finanzsystem zu schaffen. Und natürlich regulieren Staaten Märkte, um **Steuerhinterziehung,** Geldwäsche, illegalen Handel und Terrorismusfinanzierung zu verhindern.

Regulierungs-Hopping:

Politik und Regulierer sind in einem Dilemma. Einerseits bedingt die weit verbreitete Nutzung von Kryptowährungen für illegale Geschäfte die Notwendigkeit für eine strenge Regulierung dieses Marktes. Andererseits führt gerade diese Regulierung und die damit verbundenen Kosten dazu, dass solche Plattformen und Unternehmen ihren Sitz außerhalb des Regulierungsbereichs wählen und sich damit gänzlich der Regulierung entziehen (sog. *regulatory arbitrage*). So war vor der Eindämmung von Kryptowährungsaktivitäten Hongkong als Standort beliebt, heute sind unter anderem die Seychellen ein bevorzugtes Sitzland.[103]

Der US-Ansatz, für diesen Fall die Nutzung solcher Institutionen für die eigenen Bürger und US-Unternehmen zu verbieten, ist ein Hilfsmittel, dürfte aber kaum Menschen mit hinreichender krimineller Energie von einer Nutzung abhalten. Effektiv kann ein solcher Ansatz gerade für kleinere Länder nur dann sein, wenn es gelingt, eine weitgehend einheitliche Regulierung der Kryptomärkte international durchzusetzen. Für die USA und die Europäische Union ist es ratsam, das Thema der Regulierung von Kryptowährungen und ihrer Marktplätze zum Thema des gemeinsamen *Trade and Technology Council* (TTC) zu machen. Dieser ist das geeignete Forum, um eine koordinierte Regulierungspolitik der zwei dominanten Wirtschaftsräume zu schaffen und gemeinsam in der Folge durchzusetzen.

Kompetenzbündelung:

Einmal wieder zeigt sich, dass in der digitalen Welt die Bündelung von Kompetenzen und Fähigkeiten an einer Stelle auch in einem ansonsten föderalen Staat wichtig sind. Nicht zuletzt der Mangel an entsprechend qualifiziertem Humankapital auf dem Arbeitsmarkt macht dies unbedingt erforderlich. Der Ansatz des Bundesfinanzministeriums zur Schaffung eines Bundesfinanzkriminalamts ist daher vielversprechend und sollte konsequent umgesetzt werden.

Ein einheitlicher Ansprechpartner kann vielleicht auch helfen, dass sich *Blockchain*-Analyseunternehmen nicht nur in den USA ansiedeln, sondern auch die Nachfrage und den Bedarf in Deutschland sehen. *Blockchain*-Spezialisten fiele es leichter, in Deutschland unternehmerisch tätig zu werden.

Technische Risikobereiche:

Mixer, *privacy coins* und dezentralen Kryptobörsen sowie *unhosted wallets* ermöglichen derzeit weitgehend unbeobachtete Transaktionen. Um den Transparenzforderungen der Europäischen Union zu entsprechen, müssen sie entweder illegalisiert werden, oder aber diesbezügliche Ermittlungsfähigkeiten (auch der öffentlichen Hand) erheblich ausgebaut werden. Ob der zweite Weg ohne eine (nicht wünschenswerte) weitgehende Überwachung des Internetverkehrs überhaupt umsetzbar ist, erscheint fraglich.

Eine Herausforderung wird künftig das Metaverse mit den dort gehandelten NFT. Hier entstehen unregulierte Handelsplätze, auf denen nur mit Kryptowerten gehandelt wird, und die erhebliches Gefahrenpotenzial bezüglich der Geldwäsche bergen.

Terrorismusfinanzierung:

Terrorismusfinanzierung ist, obwohl in der jüngeren Vergangenheit keine großen Transaktionen beobachtet wurden, aufgrund ihrer Wirkung von erheblicher Bedeutung, und muss mit Nachdruck unterbunden und bekämpft werden.

Obwohl die Haupteinnahmequellen terroristischer Organisationen in erster Linie im *off-chain*-Bereich liegen, sollten Eingriffsmöglichkeiten auf der *blockchain* intensiver als bislang genutzt werden.

103 Quelle: Hintergrundgespräch 08. August 2022, Gesprächspartner Salih Altuntas.

KYC:

Zentrale Kryptrobörsen und andere Krypto-Dienstleister müssen zur effektiven Einhaltung von KYC-Protokollen verpflichtet werden. Mit Richtervorbehalt müssen Kundendaten mit Ermittlungsbehörden geteilt werden müssen.

Verhältnismäßigkeit:

Trotz der zuletzt wieder heftigen Kursschwankungen bei den führenden Kryptowährungen steigt der Anteil derer, die Kryptowährungen und die *blockchain*-Technik für innovative und legale Zwecke nutzen. Die *blockchain*-Analysefirma Chainalysis gibt den **Anteil illegaler Transaktionen** mit nur **0,15 Prozent** an.[104] So wichtig es ist, illegale Geschäfte zu verhindern oder zumindest zu verfolgen, so dürfen die Innovationspotentiale der *blockchain*-Technik und der auf ihr basierenden Währungen deswegen nicht unverhältnismäßig gegängelt werden. Aus guten Gründen wird auch das Bargeld nicht verboten, nur weil damit auch illegale Geschäfte bezahlt werden. Und hier dürfte der Anteil sicher deutlich über 0,15 Prozent liegen. Wie beim Internet und vielen anderen Innovationen gilt auch für die *blockchain* das Bonmot, **dass eine Innovation wohl nicht sehr innovativ sein kann, wenn sie nicht von Kriminellen genutzt wird.**

104 Chainalysis (2022b), S.4.

7. Ausblick

Kryptowährungen werden in Zukunft sicherlich stärker reguliert werden – zumindest jene, die aufgrund ihrer Marktkapitalisierung eine gewisse Relevanz für die Stabilität der Finanzmärkte haben. Wenn dies die Volatilität der Kryptomärkte verringert, wird dies die Attraktivität dieser sogar erhöhen.

Staaten werden auf eine Besteuerung von Gewinnen und bestimmten Transaktionen drängen. Allein das setzt eine Deanonymisierung voraus. Kryptowährungen die gerade die Anonymität als Wesensmerkmal aufweisen, werden daher besonders ins Visier der Regulierer und der Ermittlungsbehörden geraten.

Der beste Weg, Kryptogeld zu einem effizienten Zahlungsmittel und Kapitalanlage zu machen, ist die Schaffung einer digitalen Währung durch einen Emittenten, der den Regeln eines liberalen Rechtsstaats unterliegt, Geldwertstabilität sicherstellt und der Deanonymisierung einer Transaktion transparente und hohe rechtstaatliche Hürden voranstellt. Eine so konzipierte Kryptowährung hat erhebliches Potential, im Wettbewerb zum Zahlungsmittel der Wahl für legale Transaktion zu werden. Dies wäre ein positiver Trend für Kryptowährungen, Finanzmärkte und Bemühungen, die grenzüberschreitende organisierte Kriminalität zu bekämpfen.

Falls es aufgrund volatiler Kursverläufe künftig nicht aufgrund unkalkulierbarer finanzieller Risiken und betriebswirtschaftlicher Nachteiligkeit zu einem Austritt legaler Marktteilnehmer kommt – so dass der relative Anteil der aufgrund der Verschleierungsfähigkeiten mutmaßlich verbleibenden unlauteren Nutzer ansteigt –, sollten Regulierer dies im Rahmen einer Rechtsgüterabwägung und Kosten-Nutzen-Analyse im Blick behalten. Nicht zuletzt sollte ein innovationsfreundliches Geschäftsklima im Zuständigkeitsbereich des Regulierers erhalten bleiben.

Auch die Verdrängung von Finanzdienstleistern und Plattformanbietern durch übermäßige Regulierung und Kontrolle aus diesem Zuständigkeitsbereich hinaus kann kontraproduktiv wirken, wenn in Reaktion z.B. Firmensitze an off-shore-Standorte verlegt werden und Strafverfolgungsbehörden keinen Zugriff mehr haben. Andererseits dürfen keine rechtsfreien oder de facto geschützten Räume für Kriminelle geduldet werden, da hier aufgrund des grenzenlosen Charakters des Internets mit einer hohen Konzentrationswirkung zu rechnen wäre, dies in der Öffentlichkeit als Staatsversagen gesehen würde und legale Kryptowährungsdienste in Mitleidenschaft gezogen würden.

Abkürzungsverzeichnis

AEC	*Anonymity Enhanced Cryptocurrency*
AML	*anti-money laundering*
BKA	Bundeskriminalamt
BSA	*Bank Secrecy Act*
CBDC	*Central Bank Digital Currencies*
CFTC	*Commodities Futures Trading Commission*
CTF	*counter-terrorist financing*
DeFi	*Decentralized finance*
ESMA	*European Securities and Markets Authority*
FATF	*Financial Action Task Force*
FBI	*Federal Bureau of Investigation*
FinCEN	*Financial Crimes Enforcement Network*
FIU	*Financial Intelligence Unit*
GWG	Geldwäschegesetz
IRS-CI	*Internal Revenue Service – Criminal Investigation*
KWG	Kreditwesengesetz
KYC	*Know-Your-Customer*
MiCa	*Markets in Crypto-Assets Regulation*
NDAA	*National Defense Authorization Act*
NFT	*non-fungible tokens*
OFAC	*U.S. Treasury's Office of Foreign Assets Control*
SDN	*Specially Designated Nationals And Blocked Persons List*
SEC	*U.S. Securities and Exchange Commission*
SWIFT	*Society for Worldwide Interbank Financial Telecommunication*
USD	U.S. Dollar

Literaturverzeichnis

Allison, I. (2015). Bitcoin tumbler: The business of covering tracks in the world of cryptocurrency laundering. https://www.ibtimes.co.uk/bitcoin-tumbler-business-covering-tracks-world-cryptocurrency-laundering-1487480, zuletzt abgerufen September 2022.

Anderegg, R. (2014). Grundzüge der Geldtheorie und Geldpolitik. In Grundzüge der Geldtheorie und Geldpolitik. Oldenbourg Wissenschaftsverlag, S.19.

Antonopoulos, A. M. (2017). Mastering Bitcoin: programming the open blockchain. Second edition. Sebastopol, CA: O'Reilly.

BBC (2022). Crypto money laundering rises 30%, report finds. https://www.bbc.com/news/technology-60072195, zuletzt abgerufen September 2022.

Berwick, A. & Wilson, T. (2022a). How crypto giant Binance became a hub for hackers, fraudsters and drug traffickers. A Reuters Special Report. https://www.reuters.com/investigates/special-report/fintech-crypto-binance-dirtymoney/, zuletzt abgerufen September 2022.

Berwick, A. & Wilson, T. (2022b). Exclusive: U.S. sought records on Binance CEO for crypto money laundering probe. https://www.reuters.com/technology/exclusive-us-sought-records-binance-ceo-crypto-money-laundering-probe-2022-09-01/, zuletzt abgerufen September 2022.

Bundesfinanzministerium (2022). Finanzkriminalität schlagkräftig bekämpfen: Pressestatement von Christian Lindner. https://www.bundesfinanzministerium.de/Content/DE/Standardartikel/Video-Textfassungen/2022/textfassung-2022-08-24-finanzkriminalitaet-bekaempfen.html, zuletzt abgerufen September 2022.

Bundesregierung (2022). Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Christian Görke, Dr. Gesine Lötzsch, Klaus Ernst, weiterer Abgeordneter und der Fraktion DIE LINKE. Drucksache 20/2531.

Bylund, A. (2022). What Are Privacy coins? https://www.fool.com/investing/stock-market/market-sectors/financials/cryptocurrency-stocks/privacy-coins/, zuletzt abgerufen September 2022.

Chainalysis (2021). Chainalysis in Action: OFAC Sanctions Russian Cryptocurrency OTC Suex that Received Over $160 million from Ransomware Attackers, Scammers, and Darknet Markets. https://blog.chainalysis.com/reports/ofac-sanction-suex-september-2021/, zuletzt abgerufen September 2022.

Chainalysis (2022a). Crypto Mixer Usage Reaches All-time Highs in 2022, With Nation State Actors and Cybercriminals Contributing Significant Volume. https://blog.chainalysis.com/reports/crypto-mixer-criminal-volume-2022/, zuletzt abgerufen September 2022.

Chainalysis (2022b). Crypto Crime Trends for 2022: Illicit Transaction Activity Reaches All-Time High in Value, All-Time Low in Share of All Cryptocurrency Activity, https://blog.chainalysis.com/reports/2022-crypto-crime-report-introduction/, zuletzt abgerufen September 2022.

Chainalysis (2022c). The 2022 Crypto Crime Report.

Chainalysis (2022d). Webcast: Crypto Crime in 2022: Everything You Need to Know Part 2. https://go.chainalysis.com/2022-crypto-crime-part-2.html, zuletzt abgerufen September 2022.

Chainalysis (2022e). Theft, Money Laundering, and NFT Market Manipulation Underline Importance of Safety and Compliance in Web3. https://blog.chainalysis.com/reports/chainalysis-web3-report-preview-safety-compliance-defi/, zuletzt abgerufen September 2022.

Collins, J. (2022). Crypto, crime and control. Cryptocurrencies as an enabler of organized crime. https://globalinitiative.net/wp-content/uploads/2022/06/GITOC-Crypto-crime-and-control-Cryptocurrencies-as-an-enabler-of-organized-crime.pdf, zuletzt abgerufen September 2022.

Complyadvantage.com (2022). Cryptocurrency Regulations Around The World. https://complyadvantage.com/insights/cryptocurrency-regulations-around-world/#:~:text=Cryptocurrency%20exchanges%20are%20legal%20in,submit%20reports%20to%20the%20authorities, zuletzt abgerufen September 2022.

Crawley, J. (2021). Japan's Financial Services Regulator Issues Binance Warning. https://www.coindesk.com/markets/2021/06/25/japans-financial-services-regulator-issues-binance-warning/, zuletzt abgerufen September 2022.

Ciphertrace (2020). 2020 Geographic Risk Report: VASP KYC by Jurisdiction. https://ciphertrace.com/2020-geo-risk-report-on-vasp-kyc/, zuletzt abgerufen September 2022.

Eisermann, D. & Schindler, H.-J. (2020). Cryptocurrencies as Threats to Public Security and Counter Terrorism: Risk Analysis and Regulatory Challenges. https://www.counterextremism.com/sites/default/files/Cryptocurrencies%20as%20Threats%20to%20Public%20Security%20and%20Counter-Terrorism_ENG%20Translation_April%202020.pdf, zuletzt abgerufen September 2022.

Elliptic (2021). DeFi: Risk, Regulation, and the Rise of DeCrime. https://www.elliptic.co/resources/defi-risk-regulation-and-the-rise-of-decrime, zuletzt abgerufen September 2022.

Europäischer Rat (2022a). Digitalisierung des Finanzwesens: Einigung über die europäische Verordnung über Kryptowerte (MiCA). Pressemitteilung. https://www.consilium.europa.eu/de/press/press-releases/2022/06/30/digital-finance-agreement-reached-on-european-crypto-assets-regulation-mica/, zuletzt abgerufen September 2022.

Europäischer Rat (2022b). Bekämpfung von Geldwäsche: Vorläufige Einigung über die Transparenz von Kryptowertetransfers. Pressemitteilung. https://www.consilium.europa.eu/de/press/press-releases/2022/06/29/anti-money-laundering-provisional-agreement-reached-on-transparency-of-crypto-asset-transfers/, zuletzt abgerufen September 2022.

Europäische Union (2020). Directive (EU) 2018/843. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018L0843, letzter Abruf September 2022.

Europol (2021). Cryptocurrencies – Tracing the evolution of criminal finances, Europol Spotlight Report series, Publications Office of the European Union, Luxembourg. https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf, zuletzt abgerufen September 2022.

Hayek, F. A. (2022). Law, Legislation, and Liberty: A New Statement of the Liberal Principles of Justice and Political Economy (Vol. 19). Routledge, Erstausgabe: 1973.

Hertig, A. (2021). Taproot, Bitcoin's Long-Anticipated Upgrade, Has Activated. https://www.coindesk.com/tech/2021/11/13/taproot-bitcoins-long-anticipated-upgrade-activates-this-weekend/, zuletzt abgerufen September 2022.

Hilgers, S. & Greilich, K. (2021). Vier Wellen Digitaler Währungen und die Zukunft des Geldes. Policy Paper. Friedrich-Naumann-Stiftung für die Freiheit, Potsdam.

Huemer, S. (2022). Neue Regeln für den Bitcoin. https://zeitung.faz.net/fas/wert-wohnen/2022-04-24/da7430e0bb876ac575e8baf1c672d39e/?popup=user.lf-ns, zuletzt abgerufen September 2022.

Institutional-money.com (2022). Krypto-Einigung der EU bringt Schwarze Liste, Offenlegungszwang. https://www.institutional-money.com/news/regulierung/headline/krypto-einigung-der-eu-bringt-schwarze-liste-offenlegungszwang-216879/, zuletzt abgerufen September 2022.

Menger, C. (1884). IV. Untersuchungen über die Methode der Sozialwissenschaften und der politischen Ökonomie insbesondere. Jahrbücher für Nationalökonomie und Statistik, 42(1), 353-370.

Mussler, W. (2022). Kryptotransfers auf der Spur. https://www.faz.net/aktuell/finanzen/eu-legt-in-geld-transfer-verordnung-erstmals-regeln-fuer-kryptotransfers-fest-18140664.html?premium=0xdb587ed22210c97da66f86d74aedebf4&GEPC=s5, letzter Abruf September 2022.

Nestler, F. (2022). Die zwei Seiten von Kryptowährungen. https://zeitung.faz.net/faz/finanzen/2022-03-12/e8e10fc85ea38439e177f2dc68655ca2/?GEPC=s9, zuletzt abgerufen September 2022.

Newmyer, T. (2022). Crypto exchange targets Treasury sanctions in national security clash. https://www.washingtonpost.com/business/2022/09/08/coinbase-treasury-sanctions-mixers-/, zuletzt abgerufen September 2022.

Reaume, A. (2022). Stablecoin: What It Is & List Of Top Stablecoins. https://seekingalpha.com/article/4468065-what-are-stablecoins?source=acquisition_campaign_google&internal_promotion=true, zuletzt abgerufen September 2022.

Reynolds, K. (2021). Binance Isn't Allowed to Be Operating in the UK, Watchdog Warns. https://www.coindesk.com/policy/2021/06/27/binance-isnt-allowed-to-be-operating-in-the-uk-watchdog-warns/, zuletzt abgerufen September 2022.

Robinson, T. (2020). "Crime Proceeds being Laundered in Privacy Wallets". https://www.elliptic.co/blog/13-bitcoin-crime-laundered-through-privacy-wallet, zuletzt abgerufen September 2022.

SAM.gov (2020). https://sam.gov/opp/3b7875d5236b47f6a77f64c19251af60/view?index=opp, zuletzt abgerufen August 2022.

Seth, S. (2019). Japan's FSA Bans Private Cryptocurrencies. https://www.investopedia.com/news/japans-fsa-bans-private-cryptocurrencies/#:~:text=Japan%20Imposes%20Ban%20on%20Private,of%20anonymity%2C%20according%20to%20CoinDesk., zuletzt abgerufen September 2022.

Sinclair, S. (2020). CipherTrace Says Homeland Security Work Gave Rise to Monero-Tracking Patent Filings. https://www.coindesk.com/tech/2020/11/23/ciphertrace-says-homeland-security-work-gave-rise-to-monero-tracking-patent-filings/, zuletzt abgerufen September 2022.

Stevens, R. (2022). What Are Privacy coins and Are They Legal?. https://www.coindesk.com/learn/what-are-privacy-coins-and-are-they-legal/, zuletzt abgerufen September 2022.

Thomas, D. & Rossow, A. (2022). U.S. Treasury Department on Track to Regulate Unhosted Wallets. https://beincrypto.com/u-s-treasury-department-on-track-to-regulate-unhosted-wallets/, zuletzt abgerufen September 2022.

United Nations Security Council. "S/2019/171: Report of the Panel of Experts established pursuant to resolution 1874 (2009)," Tech. Rep., 2019, S. 49.

U.S. Department of Treasury (2022). U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats. https://home.treasury.gov/news/press-releases/jy0768, zuletzt abgerufen September 2022.

von Mises, L. (1949). Human Action – A Treatise on Economics.

Wurzel, S. (2021). China verbietet Kryptogeld-Handel. https://www.tagesschau.de/wirtschaft/finanzen/china-kryptowaehrungen-101.html, zuletzt abgerufen September 2022.