Prävention von Straftaten mit Bitcoins und Alt-Coins

Handlungsempfehlung zur Regulierung virtueller Kryptowährungen

im Rahmen des Projekts BITCRIME (Teilprojekt Deutschland)

Bitcoin and Alt-Coin Crime Prevention

A Recommendation for the Regulation of Virtual Cryptocurrencies

in the context of the BITCRIME project (German Subproject)

Januar/January 2017

Executive Summary

Das neue Phänomen virtueller Kryptowährungen wie Bitcoin gewinnt zunehmend an Bedeutung. Neben legalen Nutzern erscheinen die Systeme wegen ihrer dezentralen Organisation auch kriminellen Nutzern attraktiv. Deshalb bedarf es – insbesondere zum Schutz legaler Nutzer und zur Bekämpfung organisierter Finanzkriminalität – eines effektiven Präventionskonzepts für virtuelle Kryptowährungen. Der Vorschlag der Europäischen Kommission, Intermediäre für virtuelle Kryptowährungen in die konventionelle Geldwäscheprävention zu integrieren, erweist sich jedoch sowohl aufgrund praktischer, als auch grundrechtlicher Erwägungen als verfehlt. Angezeigt ist dagegen eine Regulierung auf Grundlage von Transaktionssperrlisten, die einen Umtausch inkriminierter Krypto-Coins in Realwährung bzw. Waren oder Dienstleistungen unterbinden sollen. Der auf virtuelle Kryptowährungen zugeschnittene Ansatz, der sich die Transparenz öffentlicher Blockchains zunutze macht, ist mit einer geringeren Belastung von Grundrechtsträgern verbunden und zugleich effektiver. Eine besonders wirksame präventive Regulierung virtueller Kryptowährungen als globale Systeme erfordert ein internationales Vorgehen.

Virtual cryptocurrencies such as Bitcoin are a new phenomenon that is becoming more and more significant. The decentralised structure of these systems makes them attractive not only to legitimate users but to criminal users as well. An effective prevention strategy for virtual cryptocurrencies is therefore needed – in particular in order to protect legitimate users and to help fight international financial crime. The European Commission's proposal to integrate intermediaries for virtual cryptocurrencies in conventional mechanisms for the prevention of money laundering has, however, turned out to be inappropriate, both for practical reasons and on account of considerations concerning fundamental human rights. An appropriate solution might be a form of regulation based on transaction blacklists, aimed at preventing the exchange of blacklisted cryptocoins into real currencies or real goods and services. An approach geared to cryptocurrencies, which makes use of the transparency of public blockchains, would result in a lesser degree of interference with fundamental rights while at the same time being more effective. An effective preventive regulation of virtual cryptocurrencies as global systems requires an international approach.

Please advance to page 26 for the English translation.

Inhalt

Die Handlungsempfehlung wurde im Rahmen des Projekts BITCRIME (Teilprojekt Deutschland)[1] verfasst von Rainer Böhme, Johanna Grzywotz, Paulina Pesch, Christian Rückert, Christoph Safferling

1 Das Projekt wird vom BMBF im Zuge der Bekanntmachung „Zivile Sicherheit – Schutz vor organisierter Kriminalität“ im Rahmen des Programms „Forschung für die zivile Sicherheit“ der Bundesregierung gefördert. Homepage abrufbar unter https://www.bitcrime.de/deutschland/ (letzter Abruf: 14.10.16).

1. Vorbemerkung

1.1 Problembeschreibung

Virtuelle Kryptowährungen[2] wie Bitcoin sind ein Phänomen, das immer mehr an Bedeutung gewinnt. Sie werden unabhängig von Notenbanken, Staaten und Kreditinstituten direkt zwischen den Nutzern (vermeintlich) anonym gehandelt. Das eröffnet Kriminellen ein hohes Ausnutzungspotential. Eine Analyse von Auswertungsergebnissen des Bundeskriminalamts hat gezeigt, dass virtuelle Kryptowährungen in Deutschland, wenn sie mit Kriminalität in Verbindung stehen, hauptsächlich bei Cybercrime-Delikten im engeren Sinne[3], Erpressungen und betrügerischen Handlungen eingesetzt werden[4]. Darüber hinaus warnen verschiedene Institutionen, wie z.B. die für internationale Geldwäscheprävention zuständige Financial Action Task Force (on Money Laundering) (FATF) oder auch die Europäische Bankenaufsichtsbehörde (EBA) vor der Gefahr der Nutzung zur Geldwäsche und Terrorismusfinanzierung[5]. Ob es wirklich der Fall ist und wenn ja, in welchem Umfang, virtuelle Kryptowährungen zur Terrorismusfinanzierung genutzt werden, ist bislang ungeklärt.[6] Auch die EU sieht Handlungsbedarf. So gab die Kommission im Juli 2016 ihre Pläne bekannt, die vierte Geldwäsche-Richtlinie auch auf virtuelle Kryptowährungen ausweiten zu wollen.[7] Nicht nur an diesen Äußerungen wird deutlich, dass virtuelle Kryptowährungen insbesondere aufgrund ihrer Pseudonymität und Dezentralität besondere Herausforderungen für die Strafverfolgung darstellen. Darüber hinaus ergibt sich jedoch auch die Notwendigkeit der Entwicklung neuer Präventionskonzepte.

1.2 Technischer Überblick über virtuelle Kryptowährungen am Beispiel von Bitcoin

Die Entwicklung solcher Präventionskonzepte erfordert ein Verständnis der grundlegenden Funktionsweise virtueller Kryptowährungen. Diese soll am Beispiel des Bitcoinsystems als bekanntestem Vertreter virtueller Kryptowährungen geschildert werden, bevor der über Bitcoin hinausreichende Anwendungsbereich der vorliegenden Handlungsempfehlung definiert wird.

Das Bitcoinsystem[8] bietet seinen Nutzern die Möglichkeit, Online-Transaktionen vorzunehmen, ohne dass dabei eine zentrale Instanz eingeschaltet wird. In dem dezentralen System werden Bitcoins direkt zwischen den Nutzern transferiert. Bitcoin-Nutzer verfügen über Konten[9], die auf öffentlichen Schlüsseln eines asymmetrischen kryptographischen Systems basieren und von den Nutzern selbst in beliebiger Zahl erzeugt werden können. Jeder Bitcoin im System ist zu jedem Zeitpunkt einem bestimmten Konto zugeordnet. Soll ein Bitcoin, der einem bestimmten Konto zugeordnet ist, überwiesen werden, muss hierzu eine Transaktion erstellt werden, die im Wesentlichen in der Nachricht besteht, dass der Bitcoin einem bestimmten anderen Konto zugewiesen werden soll. Um sicherzustellen, dass nur der Inhaber eines Kontos einen diesem zugewiesenen Bitcoin überweisen kann, muss die Transaktion mit dem zum Konto gehörenden privaten Schlüssel digital signiert werden.[10] Zur Verwaltung von Konten nebst privaten Schlüsseln sowie zum Erstellen und Signieren von Transaktionen wird sog. Wallet-Software genutzt.

2 Dieser Begriff erfasst nur virtuelle, dezentrale kryptographische Währungen. Näher unten 1.2. Zudem wird darauf hingewiesen, dass der Begriff Währung verwendet wird, auch wenn der juristische Währungsbegriff nur staatliche Währungen erfasst, siehe: EBA Opinion on 'virtual currencies', EBA/Op/2014/08, S. 11.

3 Nach der von polizeilichen Gremien erarbeiteten und vom Arbeitskreis II „Innere Sicherheit" genehmigten Definition umfasst „Cybercrime im engeren Sinne" die Straftaten, die sich gegen das Internet, weitere Datennetze, informationstechnische Systeme oder deren Daten richten.

4 Siehe dazu auch: *Grzywotz/Rückert/Köhler*, Cybercrime mit Bitcoins, StV 2016, 753 (756).

5 EBA Opinion on 'virtual currencies', EBA/Op/2014/08, S. 32 f.; FATF Report, Virtual Currencies – Key Definitions and Potential AML/CFT Risks, Juni 2014, S. 9 f.

6 *Grzywotz/Rückert/Köhler*, StV 2016, 753 (756).

7 S. Mitteilung der EU-Kommission an das Europäische Parlament und den Rat vom 02.02.2016 – COM(2016) 50 final.

8 Siehe auch *Böhme/Christin/Edelman/Moore*, Journal of Economic Perspectives, Vol. 29, S. 213 ff.; *Narayanan/Bonneau/Felten/Miller/Goldfeder*, Bitcoin and Cryptocurrency Technologies: A comprehensive Introduction, Princeton 2016; Sorge/Krohn-Grimberghe, DuD 2012, 479 ff.; Zohar, CACM 09/2015, 104 ff.

9 Die Konten werden auch als Adressen bezeichnet.

10 Die Schlüsselpaare des asymmetrischen kryptographischen Systems werden bei Bitcoin für digitale Signaturen genutzt, die der Authentikation dienen. Eine Verschlüsselung zum Zweck der Geheimhaltung von Informationen erfolgt dagegen nicht.

In Ermangelung einer zentralen Instanz, die Transaktionsaufträge entgegennimmt und die Guthaben der Nutzer anpasst, werden Bitcoin-Transaktionen an die Nutzergemeinschaft des Systems verschickt und auch von dieser verarbeitet. Nur durch Prüfung der digitalen Signatur könnten die anderen Nutzer allerdings nicht ausschließen, dass Bitcoins mehrfach ausgegeben werden (sog. Double-Spending), weil sich über jeden Bitcoin eine beliebige Anzahl korrekt signierter Transaktionen erstellen lässt. Um Double-Spending-Versuche festzustellen und durch Nichtverarbeitung der betreffenden Transaktionen zu verhindern, müssen die Nutzer des Bitcoinsystems sämtlicher bereits verarbeiteter Transaktionen des Systems gewahr sein. Dazu werden alle Bitcoin-Transaktionen in einer öffentlichen Datenstruktur, der sog. Blockchain, gespeichert. Die Blockchain ist auf den Rechnern aller Nutzer gespeichert und enthält die gesamte – unverschlüsselte – Transaktionshistorie seit Initialisierung des Bitcoinsystems. Erst, wenn eine Transaktion in die Blockchain aufgenommen worden ist, ist sie erfolgt. Aus der Blockchain ergibt sich, von welchem Bitcoin-Konto wann welcher Bitcoin-Betrag an welches Zielkonto übertragen wurde. So lässt sich für jedermann jeder Bitcoin-Betrag beliebig weit zurückverfolgen.[11]

Die Blockchain wird von den Nutzern des Systems selbst fortgeschrieben, wobei zur Absicherung dieses Prozesses gegen Manipulationen ein Arbeitsnachweis („Proof of Work“) in Form einer Lösung eines mathematischen Problems zu erbringen, also Rechenleistung aufzuwenden ist. Als Anreiz, die damit verbundenen Kosten aufzubringen, werden Nutzern, die die Blockchain fortschreiben, im Gegenzug Bitcoins gutgeschrieben. Die Gutschriften speisen sich aus neu geschöpften Geldeinheiten und gehen nach einem festgelegten Schema im Zeitverlauf auf Gebührenfinanzierung über. Nutzer, die sich an diesem Prozess beteiligen, bezeichnet man als Miner.

Erworben werden können Bitcoins aber insbesondere auch an speziellen Online-Handelsbörsen (Wechselbörsen).[12] Diese sind in der Regel zentral organisiert. Dasselbe ist der Fall bei anderen Angeboten im um das Kernsystem entstandenen Bitcoin-Ökosystem (Abb.). So gibt es etwa Bitcoin-„Zahlungsdienste“, die für Händler „Zahlungen“ in Bitcoin entgegennehmen.[13] Für Nutzer, die ihre Schlüsselpaare nicht auf eigenen Rechnern verwalten möchten, existieren auch Wallet-Dienste, die Schlüsselpaare ihrer Nutzer auf Servern im Internet verwalten.[14] Zudem gibt es sog. Mixing-Dienste, mittels derer Nutzer die Inhaberschaft an Bitcoins verschleiern können.[15]

Neben Bitcoin haben sich zahlreiche alternative Systeme, sog. Alt-Coins gebildet. Die Handlungsempfehlung beansprucht nicht nur für Bitcoin, sondern auch für ähnliche Systeme Geltung. Deshalb werden die folgenden Ausführungen allgemein auf virtuelle Kryptowährungen bezogen. Hiervon erfasst werden sämtliche dezentral kontrollierten virtuellen Währungen, die kryptographisch integritätsgesicherte Transaktionen über von konventionellen Währungen unabhängigen Werteinheiten ermöglichen, die in einer öffentlichen, fortlaufenden, lückenlos nachvollziehbaren Transaktionshistorie verarbeitet werden.[16] Die in den Systemen verwendeten Werteinheiten werden im Folgenden allgemein als Krypto-Coins bezeichnet.

11 *Möser/Böhme/Breuker*, in: Proceedings of the APWG eCrime Researchers Summit, San Francisco, IEEE 2013, S. 2 ff., 12.

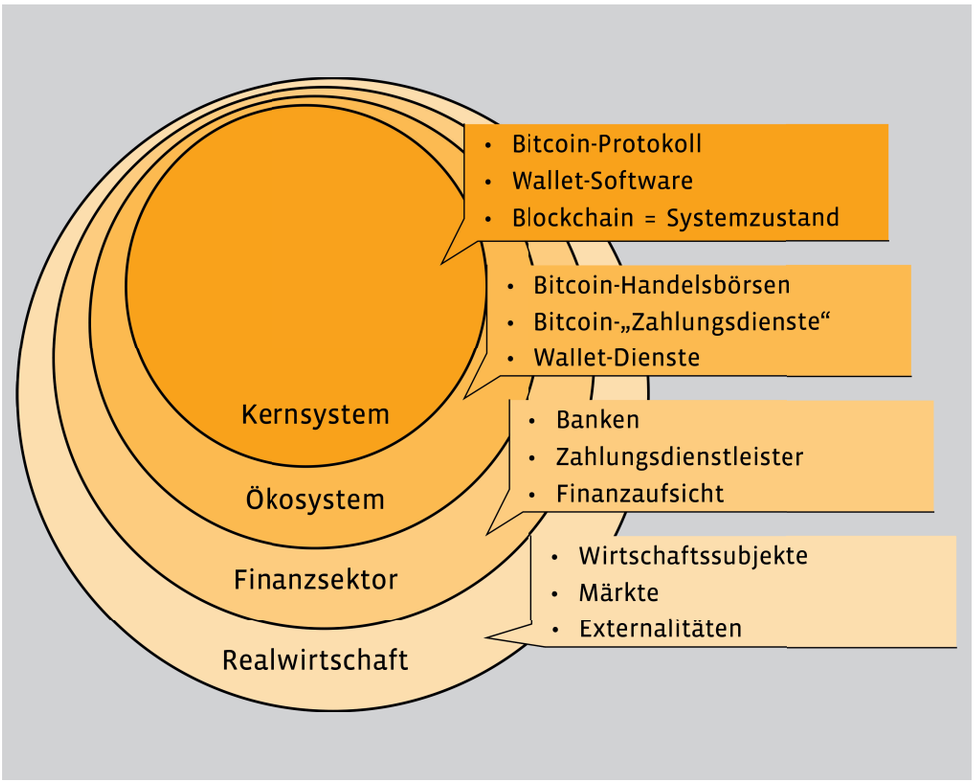
12 Etwa Bitcoin.de, https://www.bitcoin.de/ (letzter Abruf: 16.12.16); Coinbase, https://www.coinbase.com/charts (letzter Abruf: 16.12.16); Kraken, https://www.kraken.com/ (letzter Abruf: 16.12.16).

13 Etwa Bitpay, https://bitpay.com/ (letzter Abruf: 14.10.16); Coinbase, https://www.coinbase.com/merchants (letzter Abruf: 16.12.16); Coinify, https://www.coinify.com/ (letzter Abruf: 16.12.16); GoCoin, https://www.gocoin.com/ (letzter Abruf: 16.12.16).

14 Etwa die Wallets von Blockchain.info, https://blockchain.info/de/wallet/#/ (letzter Abruf: 16.12.2016); Coinbase, https://www.coinbase.com/ (letzter Abruf: 16.12.16); GreenAddress, https://greenaddress.it/ (letzter Abruf: 16.12.16).

15 Die Nutzer generieren hierzu ein neues Konto, teilen dies dem Diensteanbieter mit und überweisen an diesen einen Bitcoin. Der Dienst überweist daraufhin den Bitcoin eines anderen Nutzers an die frisch generierte Adresse. In der Folge können die neu generierte Adresse und der Bitcoin dem Inhaber nicht mehr zuordenbar sein. Näher *Möser/Böhme/Breuker*, in: Proceedings of the APWG eCrime Researchers, Summit (ECRIME 2013), San Francisco, IEEE 2013, S. 1–14, abrufbar unter http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6805780 (letzter Abruf: 19.12.2016).

16 Dem Begriff unterfallen insb. stark an Bitcoin angelehnte sog. Bitcoin-Klone wie z. B. Litecoin, https://litecoin.org/de/ (letzter Abruf: 15.12.2016). Nicht erfasst sind dagegen zentralisierte Systeme mit unter anderem auf Währungsgeld lautenden Verbindlichkeiten wie bei Ripple, https://ripple.com/ (letzter Abruf: 15.12.2016), und anonyme Systeme ohne lückenlos nachvollziehbare Transaktionshistorie wie Zcash, https://z.cash/ (letzter Abruf: 15.12.2016).



1.3 Forschungsorganisatorischer Kontext

Ziel des bilateralen, deutsch-österreichischen Forschungsprojekts BITCRIME war die Entwicklung innovativer, der Natur virtueller Kryptowährungen angemessener und damit praktikabler Ansätze zur Identifikation, Verfolgung und Prävention der organisierten Finanzkriminalität mit virtuellen Kryptowährungen. Im Fokus standen Ansätze, technischer und organisatorischer Art, die effektive kriminalpolizeiliche Ermittlungen ermöglichen, ohne dabei auf pauschalen Verboten (Totalverbot der Nutzung virtueller Kryptowährungen) zu beruhen oder ein erhöhtes Missbrauchspotential im Sinne einer Massenüberwachung (z.B. Vorratsdatenspeicherung im großen Stil) aufzuweisen. Angestrebt wurden im europäischen Raum umsetzbare Lösungen, welche jedoch international übertragbar und anschlussfähig sind.

Das deutsche Teilprojekt beschäftigte sich dabei mit zwei Teilzielen. Im Bereich der Identifikation und Verfolgung wurde ein neuartiges Ermittlungswerkzeug zur besseren Nachvollziehbarkeit von Transaktionen in virtuellen Kryptowährungssystemen entwickelt und auf seine Vereinbarkeit mit geltendem Recht hin untersucht. Das zweite Teilziel bestand in der strategischen Entwicklung einer angemessenen Regulierung des Marktes für virtuelle Kryptowährungen. Diese soll legitime Nutzer schützen, die vom ersten Teilziel verbleibenden Verfolgungslücken schließen und Finanzkriminalität im Bereich virtueller Kryptowährungen bereits präventiv verhindern. Das Ergebnis dieser Arbeit liegt nunmehr in Form der hier gegebenen Handlungsempfehlung vor.

Unter Einbeziehung der technischen Gegebenheiten virtueller Kryptowährungssysteme und unter Wahrung des Schutzes der Grundrechte der an solchen Systemen beteiligten Personen schlagen wir ein Transaktionssperrlistensystem vor, bei dem Intermediären an der Schnittstelle zwischen virtuellem Kryptowährungssystem und Realweltwirtschaft/Realwährungssystem die Annahme und der Umtausch (gegen Waren/Dienstleistungen oder Realwährung) von Transaktionen, die aus einer geldwäschetauglichen Vortat herrühren, gesetzlich verboten wird. Entsprechende Transaktionen sollen mittels einer öffentlich einsehbaren Sperrliste markiert werden.

2. Handlungsempfehlung

2.1 Wirkrichtung: Kriminalitätsprävention/ Geldwäschebekämpfung

Das hier vorgeschlagene Regulierungskonzept betrifft von seiner Wirkrichtung her ausschließlich die Reduzierung der Begehung von Straftaten im Zusammenhang mit virtuellen Kryptowährungen (insbesondere Bitcoin) mit einem Schwerpunkt in der Geldwäscheprävention. Sie steht damit Regelungen wie dem Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäschegesetz – GwG) oder Ziffer 5a des Zweiten Abschnitts des Gesetzes über das Kreditwesen (Kreditwesengesetz – KWG) nahe. Dagegen werden andere durch die besonderen Eigenschaften von virtuellen Kryptowährungen (v.a. die Dezentralität) aufgeworfene Fragestellungen, wie beispielsweise der Verbraucherschutz (z.B. Informationspflichten für Unternehmer) oder die Wertstabilität von Krypto-Coins, ausgeblendet. Diese müssen weiterer Forschung vorbehalten bleiben. Gleiches gilt für möglicherweise eintretende Verdrängungseffekte, wie das Ausweichen krimineller Akteure in alternative virtuelle Kryptowährungssysteme mit anderen technischen Eigenschaften.

2.2 Überblick über Kriminalitätsprävention und Geldwäschebekämpfung bei Realwährungen (Identifizieren, Überwachen, Melden)

Um die besonderen Anforderungen an die Kriminalitätsbekämpfung im Bereich virtueller Kryptowährungen zu verstehen, ist ein kurzer Überblick über bisherige gesetzgeberische Präventionsstrategien im Zusammenhang mit Finanztransaktionen notwendig. Nach Auffassung des deutschen Gesetzgebers soll Geldwäschebekämpfung dreierlei ermöglichen: Den Strafverfolgungsbehörden „müssen Anhaltspunkte für Geldwäschetransaktionen verfügbar gemacht werden“[17]. Ferner sollen sie auf Unterlagen über verdächtige Finanztransaktionen und die daran Beteiligten zurückgreifen können. Schließlich sollen Wirtschaftsunternehmen Vorkehrungen dagegen treffen, dass sie zur Geldwäsche missbraucht werden.[18]

Die Maßnahmen bestehen dementsprechend vorrangig darin, die an Finanztransaktionen beteiligten Akteure (wie z.B. Kreditinstitute, Finanzdienstleister, gewerbliche Händler, Spielbanken, Immobilienmakler)[19] zu Identifizierungs-, Überwachungs-, und Meldemaßnahmen zu verpflichten. So sind die Akteure dazu verpflichtet, ihre Vertragspartner und deren Hintermänner zu identifizieren und die Geschäftsbeziehung (insbesondere die getätigten Finanztransaktionen) zu prüfen, zu überwachen und aufzuzeichnen.[20] Außerdem müssen Verpflichtete sog. Verdachtsmeldungen abgeben, wenn Tatsachen bei einer durchgeführten Transaktion auf Geldwäsche oder Terrorismusfinanzierung hindeuten.[21]

Die Zentrierung der Präventionsstrategien auf private Akteure des Finanzmarkts ist dabei notwendig, weil Finanztransaktionen selbst für Strafverfolgungsbehörden nicht sichtbar und die Aufzeichnungen der privaten Akteure damit einzige Erkenntnisquelle für entsprechende Ermittlungen sind.[22] Ferner wäre eine pauschale staatliche Überwachung aller Transaktionsvorgänge (sofern eine

17 BT-DrS 12/2704, S. 1.

18 Zum Ganzen: BT-DrS 12/2704, S. 1; vgl. auch *Diergarten/Barreto da Rosa*, Praxiswissen Geldwäscheprävention, 2015, 1. Kapitel, Rn 118.

19 § 2 Abs. 1 GwG, § 1 KWG.

20 §§ 3 Abs. 1, 8 GwG; Kreditinstitute müssen hierfür automatisierte Datenverarbeitungsanlagen bereithalten und einsetzen, vgl. § 25h Abs. 2 KWG.

21 Vgl. § 11 Abs. 1 GwG.

22 BT-DrS 12/2704, S. 16.

solche im „normalen“ Geldsystem überhaupt möglich wäre) wegen der großen Streubreite der Maßnahme ein extremer Eingriff in grundrechtlich geschützte Positionen aller Bürger.[23] Für strafrechtliche Ermittlungen müssen Kreditinstitute schließlich eine Kontostammdatendatei bereithalten, die bei Bedarf abgerufen werden kann.[24]

Flankiert werden diese Maßnahmen durch einzelne, teilweise bußgeld- und strafbewehrte Handels- und Transaktionsverbote wie z.B. Terror-Sanktionslisten, mit denen primär Konten von terrorverdächtigen Personen und Gruppierungen sowie von mutmaßlichen Unterstützern eingefroren werden können[25], Handelssanktionen nach dem Außenwirtschaftsgesetz[26] oder das Zertifizierungssystem für Rohdiamanten im Zuge des sog. „Kimberley-Prozesses“[27]. Aus dem Bereich freiwilliger Maßnahmen ist vor allem die – gesetzlich in Deutschland nicht vorgeschriebene – Bestückung von Geldautomaten mit Farbpatronen zu nennen.[28]

Die auf Akteure der Zivilgesellschaft abzielenden Maßnahmen sind bereits für den Bereich der Realwährungstransaktionen wegen ihrer geringen praktischen Wirksamkeit[29] im Vergleich zu den verursachten Kosten und den mit ihnen einhergehenden breit streuenden Grundrechtseingriffen problematisch. Für den Bereich virtueller Kryptowährungen kommt hinzu, dass deren Nutzung nicht von zentralen verwaltenden Stellen abhängig ist. Daher kann eine Verpflichtung von am Markt befindlichen Dienstleistern (z.B. Wechselbörsen) von kriminellen Nutzern wegen der faktischen Grenzenlosigkeit virtueller Kryptowährungssysteme und der Nutzung von Dienstleistern, die Kontakte zwischen Privatpersonen zum Zweck des Tausches virtueller Kryptowährungen in Realwährung herstellen,[30] leicht umgangen werden.[31]

2.3 Darstellung der Handlungsmöglichkeiten bei virtuellen Währungen

2.3.1 Keine (zwingende) Regulierung

Teilweise wird eine (zwingende) Regulierung virtueller Kryptowährungen für nicht erforderlich gehalten. Argumentiert wird etwa mit dem angesichts der geringen Verbreitung virtueller Kryptowährungen niedrigen Gefahrenpotential.[32] Auch wird eine gewisse Selbstregulierung der innovativen, sich schnell entwickelnden Systeme für möglich gehalten.[33] Abseits einer zwingenden Regulierung wäre es möglich, nach dem Vorbild der eIDAS-Verordnung[34] Rahmenbedingungen für Vertrauensdienste zur freiwilligen Zertifizierung von Konten vertrauenswürdiger, identifizierter Nutzer zu regeln.

23 *Diergarten/Barreto da Rosa*, Praxiswissen Geldwäscheprävention, 2015, 1. Kapitel, Rn 122.

24 § 24c KWG; zur Verfassungsmäßigkeit: BVerfG, NVwZ 2008, 547.

25 Vgl. UN-Sicherheitsrat Resolutionen 1373 (2001) und 1390 (2002) sowie EG/EU-Verordnungen Nr. 2580/2001, Nr. 881/2002, Nr. 753/2011 und Nr. 208/2014; Verstöße sind strafbewehrt, vgl. § 18 Abs. 1 Nr. 1b AWG.

26 Vgl. § 4 AWG.

27 Vgl. Verordnung (EG) Nr. 2368/2002.

28 Vgl. http://www.mdr.de/nachrichten/vermischtes/farbpatronen-geldautomaten102.html (zuletzt abgerufen, wie alle nachfolgenden URLs ohne gesonderte Kennzeichnung, am 14.12.2016).

29 So mündeten 2015 nur ca. 2% der Verdachtsmeldungen in Anklagen, Strafbefehlen und Verurteilungen, vgl. FIU Jahresbericht 2015, S. 19.

30 Z.B. *localbitcoins*.

31 Dazu auch 2.3.2.2.

32 *Lerch*, ZBB 2015, 190, 202.

33 *De Filippi*, Bitcoin: a regulatory nightmare to a libertarian dream, abrufbar unter https://policyreview.info/articles/analysis/bitcoin-regulatory-nightmare-libertarian-dream (letzter Abruf: 15.12.2016); *Doguet*, Lousiana Law Review Vol. 73, No. 4, 1119, 1143 ff., abrufbar unter http://digitalcommons.law.lsu.edu/lalrev/vol73/iss4/9 (letzter Abruf: 15.12.2016).

34 Verordnung (EU) Nr. 910/2014.

2.3.2 Regulierung

Möglichkeiten der zwingenden Regulierung reichen theoretisch von einem Totalverbot über eine Integration in die klassische Finanzmarktregulierung bis hin zu spezifischen, auf virtuelle Kryptowährungen zugeschnittenen Ansätzen. Weder Totalverbote noch eine Einbeziehung in die klassische Finanzmarktregulierung ermöglichen jedoch eine sowohl rechtsstaatliche, als auch wirksame Regulierung virtueller Kryptowährungen.

2.3.2.1 (Kein) Totalverbot

Das Projekt BITCRIME hat sich die Entwicklung von Regulierungsansätzen abseits pauschaler Verbote zum Ziel gesetzt. Gründe hierfür sind die Intensität der mit einem Verbot verbundenen Grundrechtseingriffe und zu befürchtende Verdrängungseffekte. Dagegen wird durch eine innovationsfreundliche Regulierungspraxis die internationale Anschlussfähigkeit gewahrt und eine Assoziierung mit nicht demokratischen Staaten mit restriktiver Regulierung virtueller Kryptowährungen[35] vermieden.

2.3.2.2 Unzulänglichkeit der klassischen Geldwäscheprävention

Als unzulänglich ist eine Integration virtueller Kryptowährungen in die klassische Geldwäscheprävention zu bewerten.[36] Deren Identifizierungs- (KYC)[37], Überwachungs- und Meldepflichten[38] auf spezifische Intermediäre auszuweiten, ist nur eingeschränkt möglich und letztlich nicht erfolgversprechend. So sind Anhaltspunkte für Geldwäsche mit konventionellem Geld teils kaum auf virtuelle Kryptowährungen übertragbar, teils ist ihre unbesehene Übertragung auf diese als sachlich verfehlt zu bewerten: Während die Nutzung einer Vielzahl verschiedener Bankkonten ein probater Anhaltspunkt für Geldwäsche sein mag, ist die Nutzung vieler Cryptocoin-Konten durch einzelne Nutzer nicht selten von der genutzten Wallet-Software vorgegeben und auch aus Gründen des Selbstdatenschutzes[39] angezeigt.[40] Ebenfalls aufgrund berechtigter Datenschutzinteressen kann die Nutzung von Anonymisierungsdiensten nicht als Anzeichen für Geldwäsche mit virtuellen Währungen begriffen werden. Im Gegensatz zu klassischen Bankgeschäften handelt es sich bei virtuellen Währungen nicht um ein Verbergen von Informationen vor einem einzigen Finanzintermediär, mit dem man freiwillig eine Geschäftsbeziehung eingegangen ist, sondern um die Ausübung des Grundrechts auf informationelle Selbstbestimmung angesichts einer prinzip-bedingt öffentlichen Transaktionshistorie.

Hinzu kommt, dass die Dezentralität und Pseudonymität der Netzwerke eine effektive Durchsetzung des bestehenden Regulierungsansatzes verhindern. Insbesondere ermöglichen Anonymisierungs-Werkzeuge und private Tauschbörsen eine Umgehung

35 Etwa China, European Parliamentary Research Service, Briefing 11/04/2014, Bitcoin-Market, economics and regulation, Annex B, abrufbar unter http://www.europarl.europa.eu/RegData/bibliotheque/briefing/2014/140793/LDM_BRI(2014)140793_REV1_EN.pdf (letzter Abruf: 13.12.16); Library of Congress, Regulation of Bitcoin in Selected Jurisdictions, abrufbar unter https://www.loc.gov/law/help/bitcoin-survey/#china (letzter Abruf: 13.12.169. Zum regulatorischen Rahmen in Russland *Tereshchenko/Nosova*, A concise history of the bitcoin ban in Russia, abrufbar unter http://www.coinfox.info/news/reviews/5982-a-concise-history-of-the-bitcoin-ban-in-russia (letzter Abruf 15.12.2016).

36 Siehe bereits 2.2 a.E.

37 „Know your customer" = Verpflichtung von Kreditinstituten u.ä. zur Identifizierung ihrer Kunden.

38 Siehe dazu 2.2.

39 Näher zum Recht auf informationelle Selbstbestimmung 2.5.2.2.3.

40 Dazu das Bitcoin-Wiki, Address: „[…] a unique address should be used for each transaction. Most Bitcoin software and websites will help with this by generating a brand new address each time you create an invoice or payment request.", abrufbar unter https://en.bitcoin.it/wiki/Address (letzter Abruf: 15.12.2016).

der Regulierung durch kriminelle Nutzer. Zugleich führt die Übertragung des KYC-Prinzips auf spezifische Intermediäre zur Schwächung des Schutzes personenbezogener Daten der – zumeist legalen – Nutzer, die sich verpflichteter Intermediäre bedienen.[41] Eine klassische Geldwäscheprävention virtueller Kryptowährungen ist damit nicht nur ineffektiv, sondern zugleich mit einer starken Belastung auch legaler Nutzer verbunden.

2.3.2.3 Systematisierung spezifischer Ansätze

Geboten ist vielmehr eine auf die Besonderheiten virtueller Kryptowährungen zugeschnittene Regulierung. Die möglichen Ansätze lassen sich nach dem Adressatenkreis, Ansatz- und Bezugspunkt sowie der näheren Ausgestaltung einer Regulierung differenzieren.

2.3.2.3.1 Mögliche Adressaten

Als Adressaten der Regulierung kommen verschiedene Akteure aus Kern- und Ökosystemen[42] virtueller Kryptowährungen in Betracht: In den dezentralen Kernsystemen stünde als Adressat einer Regulierung nur die Gemeinschaft der Nutzer zur Verfügung. Konkret könnten Miner verpflichtet werden, Transaktionen, die mit kriminellen Vorgängen zusammenhängen, zum Beispiel die Transaktion eines Erpressungsopfers, nicht in der Blockchain zu verarbeiten.[43]

Außerhalb der Kernsysteme kommen als Adressaten einer Regulierung Intermediäre der Ökosysteme in Betracht. Zu den Ökosystemen zählen solche Intermediäre, die spezifische, auf virtuelle Kryptowährungen bezogene Dienste anbieten, z.B. Wechselbörsen, Wallet-Dienste und Anbieter von „Zahlungsdiensten“. Eine Regulierung der Intermediäre ließe sich durch ein Lizenzmodell flankieren.[44]

Denkbar sind schließlich Ansätze zur indirekten Regulierung der Kernsysteme durch Verpflichtung äußerer Akteure. Zu erwägen wäre der Versuch einer Einflussnahme auf die Entwickler der zugrunde liegenden Protokolle, etwa im Rahmen einer internationalen Standardisierung von Blockchain-Technologie.[45] Auch ließe sich Einfluss auf das Miner-Verhalten nehmen, indem Mining-Pools[46] oder die Herstellung von Vorprodukten für das Mining reguliert werden. Dem steht der Ansatz nahe, dass sich der Staat unmittelbar als dominierender Miner betätigt.

Eher abwegig ist dagegen die Vorstellung, dass staatliche Stellen dauerhaft in der Lage sein könnten, kryptographische Verfahren zu brechen und somit die Strafverfolgung zu ermöglichen.

2.3.2.3.2 Ansatz bei legaler oder illegaler Nutzung (Whitelisting/Blacklisting)

Eine spezifische Regulierung der Intermediäre könnte einerseits bei der legalen Nutzung, andererseits bei der illegalen Nutzung ansetzen. Ausgangspunkt der Regulierung kann zunächst die Identifizierung legaler Nutzer sein (Whitelisting). Möglich wäre insbesondere die Erfassung von Konten, deren Inhaber als vertrauens-

41 *Pesch/Böhme*, DuD 2017, 93 (94 f., 98).

42 Zu den Akteuren siehe 1.2. mit Abb.

43 Sog. Redlisting, *Dinesh/Erlich/Gilfoyle/Jared/Richard/Pouwelse*, Operational Distributed Regulation for Bitcoin, 2014, S. 4, abrufbar unter https://arxiv.org/pdf/1406.5440.pdf (letzter Abruf: 14.10.16).

44 Näher zum flankierenden Lizenzmodell 2.5.1.

45 ISO/TC 307 Blockchain and electronic distributed ledger technologies, abrufbar unter http://www.iso.org/iso/home/standards_development/list_of_iso_technical_committees/iso_technical_committee.htm?commid=6266604 (letzter Abruf: 15.12.2016).

46 Mining-Pools sind in der Regel zentral organisierte Zusammenschlüsse von Nutzern, die ihre Rechenleistung für das Mining in Proof-of-Work-Systemen wie Bitcoin bündeln. Zum Proof-of-Work 1.2.

würdig identifiziert worden sind.[47] Auf Grundlage dessen könnten Intermediäre dazu angehalten werden, ihre geschäftlichen Kontakte auf identifizierte andere Nutzer zu beschränken.

Demgegenüber setzen sogenannte Blacklisting-Ansätze bei der Erfassung krimineller Nutzung in sog. Sperrlisten an. Auf deren Grundlage können Intermediäre dazu angehalten werden, Berührungspunkte zu bestimmten kriminellen Vorgängen zu meiden.

2.3.2.3.3 Bezugspunkt von Sperrlisten: Konten oder Transaktionen

Für Sperrlisten kommen verschiedene Bezugspunkte in Betracht. Listen ließen sich einerseits Konten, die im Zusammenhang mit illegalen Aktivitäten stehen, verbunden mit dem Gebot an die adressierten Intermediäre, den gelisteten Konten zugeordnete Krypto-Coins nicht als Leistung zu akzeptieren.

Andererseits wäre die Listung konkreter Transaktionen möglich, verbunden mit dem Gebot an die adressierten Intermediäre, aus diesen Transaktionen herrührende Krypto-Coins nicht als Leistung zu akzeptieren. Erfasst wären davon sämtliche Folgetransaktionen. Möglich wäre es dabei, unter bestimmten Voraussetzungen den Umtausch von Krypto-Coins, die aus gelisteten Transaktionen herrühren, durch lizensierte Intermediäre zuzulassen.[48]

2.3.2.3.4 Sperrlistengrundsätze und Vermischungsproblematik

Knüpfen Sperrlisten an Transaktionen an, stellt sich die Frage, wie mit Transaktionen zu verfahren ist, in denen sich von einer Listung betroffene Krypto-Coins aus inkriminierten Transaktionen mit anderen Krypto-Coins vermischen. Konkret könnte der Umtausch teilweise inkriminierter Krypto-Coins in staatliche Währung bei bestimmten lizensierten Intermediären unter bestimmten Voraussetzungen zugelassen werden.[49] Möglich sind hier verschiedene Policies:[50] Einerseits könnte Konsequenz der Einbeziehung inkriminierter Krypto-Coins stets die Entwertung des gesamten transferierten Betrags sein, sodass ein Umtausch stets ausgeschlossen wäre. Andererseits wäre eine bloß teilweise Entwertung der transferierten Krypto-Coins denkbar. Möglich wäre zunächst eine dem Anteil der in die Transaktion eingehenden inkriminierten Krypto-Coins entsprechende Entwertung (Haircut-Modell). Alternativ könnte die Policy an die Transaktionsstruktur anknüpfen, sodass sich durch Gestaltung der Transaktion eine Risikoaufteilung zwischen Sender und Empfänger realisieren ließe (Senioritätsmodell).[51]

2.3.2.3.5 Einsehbarkeit von Sperrlisten

Für eine Regulierung auf Grundlage von Sperrlisten stellt sich weiterhin die Frage, für welche Akteure die Listen einzusehen sein sollen. Möglich wäre einerseits, die Sperrlisten nur den verpflichteten Intermediären zur Verfügung zu stellen und einfachen Nutzern nur beim Nachweis ihrer Betroffenheit Auskunft zu bestimmten Krypto-Coins zu geben. Andererseits könnten Sperrlisten öffentlich sein, sodass auch einfache Nutzer ohne Weiteres in der Lage sind, zu prüfen, ob bestimmte Krypto-Coins von einer Listung betroffen sind.

47 Etwa durch die unter 2.3.1. genannten Vertrauensdienste.

48 Näher zum Umtausch inkriminierter Krypto-Coins durch lizensierte Intermediäre 2.3.2.3.4. und 2.5.1.

49 Näher zum flankierenden Lizenzmodell 2.5.1.

50 Alle genannten sind beschrieben in *Möser/Böhme/Breuker*, in: Böhme/Brenner/Moore/Smith, Financial Cryptography and Data Security, 1st Workshop on Bitcoin Research (FC 2014), Barbados, Heidelberg u.a. 2014, S. 21 f.

51 Weil sich virtuelle Kryptowährungen bzgl. der Organisation und dem Format von Transaktionen unterscheiden, müsste ein Senioritätsmodell für jede zu regulierende Kryptowährung ausgestaltet werden. Für Bitcoin siehe *Pesch/Böhme*, DuD 2017, 93 (97).

2.4 Vorzugswürdig: Transaktionssperrlisten

Eine Regulierung spezifischer Intermediäre auf Grundlage öffentlicher Transaktionssperrlisten eignet sich am besten zur Prävention auf virtuelle Kryptowährungen bezogener Kriminalität. Zugleich ist mit Transaktionssperrlisten die geringste Belastung legaler Nutzer verbunden und damit das Erfordernis der Verhältnismäßigkeit gewahrt.

2.4.1 Notwendigkeit einer zwingenden Regulierung

Eine zwingende Regulierung ist notwendig. Ansätze zur freiwilligen Selbstkontrolle und -regulierung sind zur Prävention krimineller Transaktionen nicht geeignet. Gerade kriminelle Akteure und auch von ihnen unter Druck gesetzte Opfer – z.B. in Erpressungsfällen – werden eine freiwillige Regulierung im Zweifel nicht beachten.[52] Der Verzicht auf eine Regulierung wegen des derzeit geringen quantitativen Gefahrenpotentials hätte die Perpetuierung nicht effektiv regulierter virtueller Räume zur Folge, in denen legalen Nutzern kein Schutz vor bestimmten Formen der Kriminalität zuteil wird. Insbesondere angesichts gehäuft auftretender Erpressungsfälle[53] ist eine Regulierung dringend angezeigt. Derzeit ist es Tätern möglich, Cryptocoin-Beträge zu erpressen und in konventionelle Zahlungsmittel einzutauschen und dabei das Risiko, zur Verantwortung gezogen zu werden, gänzlich auszuschließen.

2.4.2 Bewertung der spezifischen Ansätze

Weil die Regulierungsansätze jeweils mit Eingriffen in die Grundrechte betroffener Akteure verbunden sind, hängt ihre Bewertung zunächst von ihrer Eignung zur Erreichung des prinzipiell legitimen Ziels der Prävention von Straftaten mit virtuellen Währungen ab; darüber hinaus ist erforderlich, dass es keine milderen ebenso effektiven Regulierungsmöglichkeiten gibt, und der Grundrechtseingriff auch verhältnismäßig im engeren Sinne ist.[54]

2.4.2.1 Adressaten

Erfolg versprechend ist nur eine Regulierung spezifischer Intermediäre aus den Ökosystemen. Die Verpflichtung einfacher Nutzer der Kernsysteme wäre wegen deren Pseudonymität schwerlich durchsetzbar. Dasselbe gilt für eine Regulierung der Entwicklung der Protokolle, die nur maßgeblich sind, soweit sie von den Mitgliedern der jeweiligen dezentralen Nutzergemeinschaft mehrheitlich angewendet werden.[55] Dagegen handelt es sich bei den Intermediären in der Regel um Akteure mit bekannter Identität, denen gegenüber eine sanktionsbewehrte Regulierung effektiv durchsetzbar ist.

Versuche, durch eine Regulierung der Intermediäre indirekten Einfluss auf das Kernsystem zu nehmen, wären allerdings nicht zielführend: Die Durchsetzung von auf das Cryptocoin-Mining bezogenen Ansätzen wäre für Proof-of-Work-[56]basierte virtuelle Kryptowährungen zwar denkbar, weil mit Mining-Pools, am Mining beteiligten Intermediären und den Herstellern von Vorprodukten für das Mining greifbare Intermediäre zur Verfügung stünden. Die Schwäche liegt aber – abseits der damit verbundenen

52 Zur (zweifelhaften) Strafbarkeit der Opfer von Erpressungen mit Ransomware *Salomon*, MMR 2016, 575 ff.

53 *Eikenberg*, Krypto-Trojaner Locky wütet in Deutschland: Über 5000 Infektionen pro Stunde, abrufbar unter http://www.heise.de/security/meldung/Krypto-Trojaner-Locky-wuetet-in-Deutschland-Ueber-5000-Infektionen-pro-Stunde-3111774.html (letzter Abruf: 14.10.16); *McMillan*, In the Bitcoin Era, Ransomware Attacks Surge, abrufbar unter http://www.wsj.com/articles/in-the-bitcoin-era-ransomware-attacks-surge-1471616632 (letzter Abruf: 15.12.2016).

54 *Grzeszick*, in Maunz/Dürig, GG-Kommentar, 78. EL, Art. 20, Rn. 107, 110 ff.; *Jarass*, Charta der Grundrechte der EU, 3. Aufl. 2016, Art. 52, Rn. 34 ff.; *Harris/O'Boyle/Warbrick*, Law of the European Convention on Human Rights, 3. Aufl. 2014, S. 519 f. Eingehend zu grundrechtlichen Aspekten des empfohlenen Sperrlistenansatzes 2.5.2.

55 *Pesch/Böhme*, DuD 2017, 93 (98).

56 Zum Proof-of-Work bei Bitcoin 1.2.

Eingriffe in Informations-[57] und ggfs. Berufsfreiheit[58] – schon praktisch darin begründet, dass sich unschwer alternative virtuelle Kryptowährungen konstruieren lassen, bei denen Mining-Regulierung nicht greift.[59] Damit ließe sich die Regulierung durch eine Änderung des jeweiligen Protokolls oder durch Ausweichen auf ähnliche alternative Systeme umgehen. Dasselbe gilt für eine Regulierung durch eine dominierende Teilnahme staatlicher Stellen als Miner. Eine effektive Regulierung virtueller Kryptowährungen verspricht daher nur eine Regulierung spezifischer Intermediäre, die von technischen Details des jeweiligen Netzwerks weitgehend unabhängig ist.

2.4.2.2 Whitelisting/Blacklisting

Für die Frage, ob für eine Intermediäre adressierende Regulierung Whitelisting- oder Blacklisting-Ansätze als vorzugswürdig anzusehen sind, spielt die jeweilige Eignung eine Rolle: Ansätze, die auf der Erfassung legaler, identifizierter Nutzer beziehungsweise deren Konten beruhen, sind zur Prävention illegaler Nutzung kaum geeignet. Ein Erpressungsopfer wird eine Transaktion an das vom Erpresser genannte Konto ohne Rücksicht darauf veranlassen, dass dieses keiner identifizierten natürlichen Person zugeordnet ist. Weiterhin spricht gegen Whitelisting-Ansätze die Intensität des mit ihnen verbundenen Eingriffs in das Recht auf informationelle Selbstbestimmung von Nutzern.[60] Als vorzugswürdig zu bewerten ist das Blacklisting, also eine Regulierung auf Grundlage von Sperrlisten.

2.4.2.3 Bezugspunkt

Für die Effektivität von Sperrlisten ist die Wahl des Bezugspunkts entscheidend. Die Listung konkreter Konten verspricht keine effektive Regulierung, weil sich Konten in beliebiger Zahl dezentral erzeugen lassen. Kriminelle Nutzer könnten die Listung ihres Kontos durch Erzeugung eines neuen umgehen, ihre Krypto-Coins auf das nicht gelistete, frische Konto übertragen und dann problemlos eintauschen.

Bei der Listung von Transaktionen besteht diese Umgehungsmöglichkeit nicht. Weil sich über die öffentliche Blockchain auch Folgetransaktionen erfassen lassen, lässt sich der Umtausch inkriminierter Krypto-Coins auch nach ihrer Verschiebung auf andere Konten unterbinden.

2.4.2.4 Einsehbarkeit von Sperrlisten

Bei der Frage nach der Einsehbarkeit von Sperrlisten sind die mit der Öffentlichkeit oder Nichtöffentlichkeit verbundenen Nachteile für Betroffene zu berücksichtigen. Zwar können öffentliche Listungen Rufschädigungen auch gutgläubiger Inhaber gelisteter Krypto-Coins zur Folge haben. Dies ist umso problematischer bei Listungen vorläufigen Charakters.[61] Allerdings erlangen bei nicht-öffentlichen Listen einfache Nutzer nicht die Möglichkeit, die Annahme von einer Listung betroffener Krypto-Coins durch Abgleich mit der Sperrliste zu vermeiden. Ein angemessenes Ergebnis ergibt sich im Wege einer Interessenabwägung. Das Interesse an der Vermeidung von Rufschädigungen tritt hinter das Interesse anderer Nutzer am Erhalt nicht von einer Listung betroffener Krypto-Coins zurück. Dabei spielt auch eine Rolle, dass die Listung als

57 Zur europäischen Ebene *Rückert*, Virtual Currencies and Fundamental Rights, S. 26 ff., https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2820634

58 Viele gewerbliche Intermediäre beteiligen sich am Mining. Zur Berufsfreiheit von Intermediären auf europäischer Ebene *Rückert*, Virtual Currencies and Fundamental Rights, S. 23 f., https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2820634

59 Das Fortschreiben von authentisierten Datenstrukturen wie der Blockchain lässt sich auch anders als durch Erbringung eines Arbeitsnachweises absichern, siehe etwa https://en.bitcoin.it/wiki/Proof_of_Stake (letzter Abruf: 14.10.16). Ohne das Erfordernis des für Bitcoin charakteristischen Arbeitsnachweises bedarf rentables Mining weder besonderer Hardware noch der Bündelung von Rechenkapazitäten, sodass es an greifbaren Regulierungsadressaten weitgehend fehlt.

60 *Pesch/Böhme*, DuD 2017, 93 (94 f., 98).

61 Dazu 2.5.2.4.

Zusatzinformation zu den an der Transaktion beteiligten Konten die Personenbeziehbarkeit dieser für Dritte nicht wesentlich erhöht. Damit ist die belastende Auswirkung für den Betroffenen nicht größer, als bei anderen verdachtsbasierten strafrechtlichen Ermittlungsmaßnahmen und Rechtsfolgen einer Verurteilung. Dabei sind sich verständige Nutzer darüber im Klaren, dass sich Transaktionen auf Grundlage der öffentliche Transaktionshistorie durch Verknüpfung mit anderen öffentlichen Informationen mit kriminellen Vorgängen in Verbindung bringen lassen. Umgekehrt ist zu berücksichtigen, dass bei nicht-öffentlichen Sperrlisten eine Instanz nötig ist, die gezielte Abfragen der Sperrlisten durch Berechtigte verarbeitet und die dadurch bereits nach kurzer Zeit Zusatzinformationen über diverse Konten erlangt, deren Inhaber folglich der Gefahr der Identifizierung ausgesetzt sind. Damit wären nicht-öffentliche Sperrlisten mit einer hohen Missbrauchsgefahr verbunden.[62]

2.5 Ausgestaltung einer Regulierung auf Grundlage von Transaktionssperrlisten

2.5.1 Grundlegende Idee/Policy

Empfohlen wird die Einführung von Sperrlisten, die dem Prinzip des Transaktions-Blacklistings folgen, verbunden mit der Verpflichtung spezifischer Intermediäre (z.B. Tauschbörsen, „Zahlungsdiensten“), aus gelisteten Transaktionen herrührende Krypto-Coins nicht anzunehmen. Die Nichtbeachtung dieser Verpflichtung sollte mit straf- oder ordnungswidrigkeitenrechtlichen Folgen sanktioniert werden.

Bei der Vermischung inkriminierter und nicht von einer Listung betroffener Krypto-Coins in einzelnen Transaktionen ist eine bloß teilweise Entwertung des transferierten Betrags vorzugswürdig.[63] Zugelassen werden muss dann der Umtausch von einer Listung bloß teilweise betroffener Krypto-Coins in Währungsgeld. Dies sollte im Sinne einer effektiven Finanzaufsicht allerdings nur bei bestimmten, lizensierten Intermediären zugelassen werden. Die Regulierung durch Sperrlisten ist also durch ein Lizenzmodell zu flankieren.[64]

2.5.2 Rechtliche Rahmenbedingungen und Umsetzung

Der folgende Abschnitt widmet sich den rechtlichen Rahmenbedingungen einer gesetzlichen Umsetzung der Transaktionssperrlistenlösung auf nationaler Ebene. Neben allgemeinen Fragen wie der Gesetzgebungskompetenz des Bundesgesetzgebers (2.5.2.1) und den von der Regelung betroffenen Grundrechten (2.5.2.2) werden vor allem Verhältnismäßigkeitserwägungen angestellt und notwendige Schutzmechanismen abgeleitet (2.5.2.3) und behandelt. Schließlich wird auf die Notwendigkeit der Möglichkeit einer einstweiligen Listung im Ermittlungsverfahren (2.5.2.4) und die Wechselwirkungen des vorgeschlagenen Regulierungskonzepts mit der materiellen Geldwäschestrafbarkeit nach § 261 StGB eingegangen (2.5.2.5).

2.5.2.1 Gesetzgebungskompetenz des Bundes

Die Gesetzgebungskompetenz des Bundes für den hier vorgeschlagenen Lösungsansatz ergibt sich aus Art. 74 Abs. 1 Nr. 11 GG. Danach ist der Bund zuständig für Sicherheitsgesetze, die sich an die Wirtschaft oder an einzelne Wirtschaftszweige richten.[65]

62 Prinzipiell wäre es denkbar, diese Gefahr durch den Einsatz moderner Kryptographie zu reduzieren. Solche Lösungsansätze sind Gegenstand laufender wissenschaftlicher Forschung. Ihr Einsatz in der Regulierungspraxis ist bislang kaum erprobt.

63 Dazu 2.5.2.3.3. und 2.5.2.5.

64 Zur grundlegenden Ausgestaltung einer Lizenzpflicht solcher Intermediäre 2.5.3.

65 BVerfGE 8, 150; Beispiel: Gewerberecht, vgl. BVerfGE 41, 351 f.; dagegen gehört das Spielbankrecht nicht zur Gesetzgebungskompetenz des Bundes, vgl. BVerfGE 28, 146; siehe auch *Maunz*, in: Maunz/Dürig, GG-Kommentar, 77. EL 2016, Art. 74 Rn 151, Rn 44; eine Länderkompetenz ergäbe sich nur für sicherheitsrechtliche Normen, die sich an Jedermann oder an Adressaten außerhalb der Wirtschaft richten, vgl. BVerfGE 3, 433; 8, 150; *Maunz*, in: Maunz/Dürig, GG-Kommentar, 77. EL 2016, Art. 74 Rn 151, Rn 44.

Der vorgeschlagene Sperrlistenansatz verpflichtet die Intermediäre der Cryptocoin-Ökosysteme[66], die gewerblich Krypto-Coins gegen Waren, Dienstleistungen oder Realwährungseinheiten tauschen (ähnlich dem GWG und dem KWG, die ebenfalls sicherheitsrechtliche Normen enthalten).[67] Wegen der faktischen Grenzenlosigkeit virtueller Kryptowährungssysteme und der damit einhergehenden zwingenden möglichst großflächigen Rechtseinheitlichkeit einer Sperrliste sind auch die Voraussetzungen des Art. 72 Abs. 2 GG erfüllt.[68]

Soweit das Gesetz (wie empfohlen) auch straf- und ordnungswidrigkeitenrechtliche Sanktionsnormen zur Durchsetzung der Verbote enthält, ergibt sich die Gesetzgebungskompetenz des Bundes aus Art. 74 Abs. 1 Nr. 1 GG.[69]

Schließlich kommt wegen der vorliegend empfohlenen internationalen Kooperation[70] zur Durchsetzung einheitlicher Sperrlisten eine Gesetzgebungskompetenz nach Art. 73 Abs. 1 Nr. 10 Var. 3 GG (internationale Verbrechensbekämpfung) in Betracht.

2.5.2.2 Grundrechtseingriffe

Die Installation eines Transaktionssperrlistensystems greift in verschiedene grundrechtlich geschützte Interessen der an virtuellen Kryptowährungssystemen beteiligten Personen ein. So tritt durch das Verbot von Annahme und Eintausch von Krypto-Coins, die auf eine gelistete Transaktion rückführbar sind, ein Wertverlust bzgl. dieser Krypto-Coins beim aktuellen Inhaber ein. Dies stellt einen Eingriff in das Eigentumsrecht der Nutzer dar (2.5.2.2.1), während das Verbot der Annahme und des Eintauschs die Berufsfreiheit der Intermediäre betrifft (2.5.2.2.2). Durch die für die Neuberechnung des Sperrzustandes späterer Transaktionen/Krypto-Coins notwendige Erhebung und Verarbeitung von Blockchain-Daten wird in das Recht auf informationelle Selbstbestimmung der betroffenen Nutzer eingegriffen (2.5.2.2.3). Dagegen liegt – eventuell anders als bei einem Totalverbot oder einer Zugangsbeschränkung – kein Eingriff in die Vereinigungsfreiheit vor. Möglich erscheint dagegen ein Eingriff in die Meinungs- und Informationsfreiheit, dieser ist jedoch von untergeordneter Bedeutung (2.5.2.2.4).

2.5.2.2.1 Eigentumsrecht der Nutzer

Die faktische Verfügungsmöglichkeit über Krypto-Coins durch Innehaben des zum jeweiligen öffentlichen Schlüssel zugehörigen privaten Schlüssels ist eine vermögenswerte Position, die dem verfassungsrechtlichen Eigentumsbegriff des Art. 14 Abs. 1 GG unterfällt. Dieser umfasst nach h.M. das Recht einen bestimmten Gegenstand zu haben und zu gebrauchen.[71] Der Eigentumsbegriff umfasst auch privatrechtliche dingliche und obligatorische Rechte.[72] Bei nicht-körperlichen Gegenständen kommt es dabei darauf an, dass sie „nach Art eines Ausschließlichkeitsrechts dem Rechtsträger privatnützig zugeordnet sind, auf Eigenleistungen beruhen und als materielle Grundlagen persönlicher Freiheit dienen“[73]. Diese weite Auslegung erfasst auch Bar- und Buchgeld,

66 Dazu: *Möser/Böhme/Breuker*, in: Böhme/Brenner/Moore/Smith, Financial Cryptography and Data Security, 1st Workshop on Bitcoin Research (FC 2014), Barbados, Heidelberg u.a. 2014, S. 16, (S. 17 f.).

67 Zum GWG: BT-DrS 17/10745, S. 11 f.

68 Vgl. BVerfGE 106, 62 (145 ff.); 110, 141 (174 ff.); 112, 226 (248 f.); 138, 136 (176 ff.); BVerfG NJW 2015, 2399 (2402); vgl. auch BVerfGE 111, 226 (254); 122, 1 (21 f.); 125, 141 (155 ff.); 135, 155 (204); umfassend: *Uhle*, in: Maunz/Dürig, GG-Kommentar, 77. EL 2016, Art. 72 Rn 142, 152 m.w.N.; siehe auch BVerfGE 126, 331 (357), dort wurde im Zusammenhang mit der Verkehrsfähigkeit von Vermögenswerten die Erforderlichkeit einer bundeseinheitlichen Regelung bejaht.

69 Vgl. entsprechend zum GWG: BT-DrS 17/10745, S. 11 f.

70 Dazu 2.6.

71 *Papier*, in: Maunz/Dürig, GG-Kommentar, 77. EL 2016, Art. 14 Rn 8; *Wendt*, in: Sachs, GG-Kommentar, 7. Aufl. 2014 Art. 14 Rn 21 m.w.N.

72 BVerfGE 74, 129 (148); *Hofmann*, in: Schmidt-Bleibtreu/Hoffmann/Hopfauf, Kommentar zum Grundgesetz, 13. Auflage 2014, Art. 14 Rn 14.

73 BVerfGE 97, 350 (371); vgl. auch BVerfGE 40, 65 (82f.); 69, 272 (300); 70, 278 (285); m.w.N. aus der Rechtsprechung.

da eine wesentliche Freiheitsgarantie des Eigentums darin liegt, Geld gegen Sachgüter (und umgekehrt) tauschen zu können.[74] Art. 14 GG gewährleistet allerdings nur die Institution des Geldes und die individuelle Zuordnung, nicht dagegen der Geldwert als solcher, da dieser von vielen – vom Staat nicht kontrollierbaren – Faktoren abhängig ist.[75] Bei vollständigem Entzug der vermögenswerten Position oder deren substantieller Entwertung ist nach der Rechtsprechung des Bundesverfassungsgerichts ein Eingriff hingegen zu bejahen.[76]

Krypto-Coins sind zwar weder Sachen, denn das würde Körperlichkeit voraussetzen, noch sind sie Forderungen,[77] denn das würde eine schuldrechtliche Verbindung von Schuldner und Gläubiger voraussetzen, aus der der Gläubiger vom Schuldner etwas verlangen kann, vgl. § 241 Abs. 1 BGB.[78] Anders als bei Buchgeld (§ 675t Abs. 1 BGB)[79] existieren in Cryptocoin-Netzwerken keine schuldrechtlichen Beziehungen, da keine zentralen, verwaltenden Stellen existieren.[80] Krypto-Coins sind auch keine sonstigen Rechte, denn diese setzen voraus, dass deren Inhaber von einem oder mehreren Schuldnern ein bestimmtes Verhalten (und sei es nur ein Unterlassen) verlangen kann.[81] Der „Inhaber" von Krypto-Coins kann aber von keinem anderen Individuen etwas verlangen.[82] Seine vermögenswerte Position besteht lediglich darin, die alleinige, tatsächliche Verfügungsgewalt über den privaten Schlüssel zu haben, der ihm rein tatsächlich ermöglicht, die Krypto-Coins weiter zu transferieren.[83] Dieser faktischen Verfügungsgewalt weist der Markt zwar einen (schwankenden) Wert zu, ein Recht entsteht deswegen aber nicht.[84]

Allerdings erfüllen Krypto-Coins alle Anforderungen, die für den Einbezug von nichtkörperlichen Gegenständen in den Schutzbereich von Art. 14 GG notwendig sind:[85] Zunächst sind Krypto-Coins exakt abgrenzbare und bestimmbare Gegenstände.[86] Durch die Nachvollziehbarkeit aller Transaktionen in der Blockchain kann zu jedem Zeitpunkt exakt bestimmt werden, welche Krypto-Coins welchem öffentlichen Schlüssel zugeordnet sind. Weiterhin kann der „Inhaber" der Krypto-Coins, die einem bestimmten öffentlichen Schlüssel zugewiesen sind – solange er sicherstellt, dass er über die einzige Kopie des zugehörigen privaten Schlüssels verfügt – alle anderen Personen von der Nutzung der Krypto-Coins ausschließen.[87] Anders als andere virtuelle

74 BVerfGE 97, 350 (371); Papier, in: Maunz/Dürig, GG-Kommentar, 77. EL 2016, Art. 14 Rn. 162; *Hofmann*, in: Schmidt-Bleibtreu/Hofmann/Henneke, GG-Kommentar, 13. Aufl. 2014, Art. 14 Rn 13.

75 Vgl. zum Ganzen: BVerfGE 97, 350 (371); 105, 17 (30); *Hofmann*, in: Schmidt-Bleibtreu/Hofmann/Henneke, GG-Kommentar, 13. Aufl. 2014, Art. 14 Rn 13.

76 BVerfGE 105, 17 (31).

77 *Kütük/Sorge*, MMR 2014, 643 (644); *Boehm/Pesch*, MMR 2014, 75 (77); *Rückert*, MMR 2016, 295 (296).

78 Zum Begriff: *Bachmann*, in: Münchener Kommentar BGB, 7. Aufl. 2016, § 241 Rn 6; *Rückert*, MMR 2016, 295 (296).

79 *Sprau*, Palandt Kommentar BGB, 76. Aufl. 2015, § 675t Rn 4.

80 *Rückert*, MMR 2016, 295 (296).

81 *Grüneberg*, Palandt Kommentar BGB, 76. Aufl. 2015, Einl v § 241 Rn 5.

82 *Rückert*, MMR 2016, 295 (296).

83 *Rückert*, MMR 2016, 295 (296).

84 Zum Ganzen: *Rückert*, MMR 2016, 295 (296).

85 Zu den Voraussetzung in der "Virtual Property"-Debatte (Abgrenzbarkeit, Dauerhaftigkeit, Ausschließbarkeit, Interkonnektivität, Marktwert): *Fairfield*, Boston University Law Review 2005, Vol. 85, p. 1047 (p. 1053); *Erlank*, Potchefstroom Electronic Law Journal 2015, Vol. 18, No.7, p. 2525 (p. 2540 f.); *DaCunha*, Akron Intellectual Property Journal, Vol. 4, No. 1, p. 35 (p. 41 ff.); *Tsukerman*, Berkeley Technology Law Journal 2015, Vol. 30, p. 1128 (p. 1145 ff.); ausführlich für den Eigentumsschutz durch europäische Grundrechte: *Rückert*, Virtual Currencies and Fundamental Rights, S. 20ff., https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2820634.

86 Zum Abgrenzbarkeitskriterium: *Berberich*, Virtuelles Eigentum, S. 108; vgl. auch das "Who owns what" Konzept von *Fairfield*, BitProperty, Southern California Law Review 2015, Vol. 88 (Forthcoming), p. 9, abrufbar unter: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2504710; *Rückert*, Virtual Currencies and Fundamental Rights, S. 22, https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2820634.

87 Zum Ausschließbarkeitskriterium bei virtuellem Eigentum: *Berberich*, Virtuelles Eigentum, S. 107, 224 ff. m.w.N; vgl. auch BVerfG NJW 2005, 589 (Internetdomain); auf europäischer Ebene („exclusive entitlement"): *Wollenschläger*, in: Peers/Hervey/Kenner/Ward (Ed.), The EU Charter of Fundamental Rights, 2014, Art. 17 para. 17(1).16; *Rückert*, Virtual Currencies and Fundamental Rights, S. 22, https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2820634.

Kryptowährungen, die von einem zentralen System/einer zentralen Stelle verwaltet werden (wie z.B. WoW-Gold oder Linden-Dollar), können Krypto-Coins aufgrund der Peer-to-Peer-Struktur des Netzwerks und der öffentlich einsehbaren Blockchain nicht einfach gelöscht werden und verfügen daher auch über eine gewisse Dauerhaftigkeit. Ferner besitzen Krypto-Coins einen Marktwert und ihre Inhaberschaft beruht auf eigener Leistung (Mining oder Erwerb mit eigenen Mitteln). Schließlich erfüllen Krypto-Coins (unabhängig von ihrer exakten einfach-rechtlichen Qualifizierung) in gewissem Maße eine „Geldersatzfunktion" (man kann damit Waren und Dienstleistungen erwerben, sie eintauschen und ihren Wert transportieren oder aufbewahren)[88] und werden von der BaFin als „Rechnungseinheiten" i.S.v. § 1 Abs. 11 Nr. 7 Alt. 2 KWG eingeordnet.[89]

Transaktionssperrlisten würden nicht nur den Tauschwert von Krypto-Coins beeinträchtigen, sondern auch zu einer substantiellen Entwertung führen. Ziel des Ansatzes wäre es, den Umtausch von gelisteten Krypto-Coins in Realwährung oder Waren und Dienstleistungen vollständig zu unterbinden. Hierdurch wären zumindest diejenigen Krypto-Coins, die aus der ursprünglich inkriminierten und dann markierten Transaktion stammen und bevor sie also mit „sauberen" Krypto-Coins durch weitere Transaktionen ggf. vermischt werden, als vollständig entwertet anzusehen. Bei Vermischung mit anderen Krypto-Coins in weiteren Transaktionen liegt – in Abhängigkeit von der gewählten Policy[90] – zumindest eine (substantielle) Teilentwertung vor. Ab welchem Vermischungsgrad nicht mehr von einer substantiellen Vermischung auszugehen wäre, ist eine Frage, die an dieser Stelle nicht abschließend beantwortet werden kann. Dies ist jedoch bei der Beurteilung eines (hypothetischen) Transaktionssperrlistengesetzes nicht notwendig, weil es dabei gerade nicht auf einen konkreten Einzelfall ankommt.

Im Ergebnis ist also ein Eingriff in Art. 14 GG zu bejahen. Für Fälle, in denen die substantielle Entwertungsgrenze unterschritten wird, bleibt (subsidiär) ein Eingriff in Art. 2 Abs. 1 GG, der auch die wirtschaftliche Betätigungsfreiheit und das Vermögen als solches schützt.[91]

Der Eingriff durch Transaktionssperrlisten ist dabei als Inhalts- und Schrankenbestimmung i.S.v. Art. 14 Abs. 1 S. 2 GG zu klassifizieren, denn die Sperrlisten-Regelung legt generell und abstrakt für jedermann gültig die Grenzen des (verfassungsrechtlichen) Eigentums an Krypto-Coins fest.[92] Sie wird auch nicht dadurch zur Enteignung i.S.v. Art. 14 Abs. 3 GG, dass sie konkrete Vermögenspositionen ganz oder zum Teil entzieht.[93] Eine Enteignung wäre nur dann anzunehmen, wenn Transaktionssperrlisten als staatliche Maßnahme zu qualifizieren wäre, deren Zweck in der vollständigen oder teilweisen Entziehung von Eigentumspositionen zur hoheitlichen Güterbeschaffung zur Durchführung konkreter öffentlichen Vorhaben läge.[94] Dies ist offensichtlich nicht der Fall, da die gelisteten Krypto-Coins lediglich ganz oder teilweise entwertet werden, nicht aber der öffentlichen Hand zugutekommen.

88 Zur Gleichwertigkeit von Geld- und Sacheigentum („geprägte Freiheit"): BVerfGE 97, 350 (371).

89 *Münzer* (BaFin), Bitcoins: Aufsichtliche Bewertung und Risiken für Nutzer, https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2014/fa_bj_1401_bitcoins.html; *Auffenberg*, NVwZ 2015, 1184ff.; *Sorge/Krohn-Grimberghe*, DuD 2012, 479 (484).

90 Dazu 2.3.2.3.4.

91 Vgl. BVerfG NJW 1994, 1784; *Di Fabio*, in: Maunz/Dürig, GG-Kommentar, 77. EL 2016, Art. 2 Rn 93 ff. m.w.N. aus Rechtsprechung und Literatur.

92 Vgl. BVerfGE 52, 1 (27f.); 58, 137 (144f.); 58, 300 (330); 70, 191 (200); 72, 66 (76); 100, 226 (240); siehe insbesondere BVerfG NJW 2004, 2073 (2077) zum (erweiterten) Verfall.

93 Vgl. BVerfGE 58, 300 (351); 70, 191 (199f.); 83, 201 (211f.); 100, 226 (240); siehe insbesondere BVerfG NJW 2004, 2073 (2077) zum (erweiterten) Verfall.

94 BVerfGE 52, 1 (27); 58, 300 (330 f.); 70, 191 (199 f.); 74, 264 (280); 79, 174 (191); 83, 201 (211); 102, 1 (15f.); 104, 1 (9); siehe auch *Papier*, in: Maunz/Dürig, GG-Kommentar, 77. EL 2016, Art. 14 Rn 527.

2.5.2.2.2 Berufsfreiheit der Intermediäre

Die Verpflichtung für Intermediäre, keine gelisteten Krypto-Coins einzutauschen, stellt einen Eingriff in deren Berufsfreiheit dar. Beruf i.S.v. Art. 12 Abs. 1 GG ist „jede auf die Dauer berechnete und nicht nur vorübergehende, der Schaffung und Erhaltung einer Lebensgrundlage dienende Betätigung“[95]. Ein Schutz durch Art. 12 GG besteht auch unabhängig von einer etwaigen Erlaubnispflicht, da aus dem Schutzbereich nach neuerer Rechtsprechung nur solche Tätigkeiten ausscheiden, „die schon ihrem Wesen nach als verboten anzusehen sind, weil sie auf Grund ihrer Sozial- und Gemeinschaftsschädlichkeit schlechthin nicht am Schutz durch das Grundrecht der Berufsfreiheit teilhaben können“[96]. Der gewerbliche Handel mit virtuellen Währungen ist daher genauso erfasst, wie der Handel mit Waren oder das Angebot von Dienstleistungen, wenn virtuelle Kryptowährungen als Zahlungsmittel akzeptiert werden.

Die Verpflichtung zur Beachtung der Sperrliste bringt keine Beschränkung der Berufswahl mit sich, sondern stellt lediglich eine Berufsausübungsregel dar.[97]

Beim Erlaubnisvorbehalt im Rahmen eines Lizenzierungsmodells ist zu differenzieren: Soweit es die Zulassung als Dienstleister zum Umtausch von Realwährung in virtuelle Kryptowährungen betrifft, handelt es sich um eine subjektive Berufszulassungsbeschränkung. Dagegen ist der Erlaubnisvorbehalt für Händler, die virtuelle Kryptowährungen als alternatives Zahlungsmittel akzeptieren wollen, formell nur Berufsausübungsregel, weil sie nur eine Bezahlungsmodalität für den gewerblichen Handel regelt. Sie wirkt allerdings faktisch wie eine subjektive Berufszulassungsbeschränkung, da der Händler faktisch einen Teil des von ihm angestrebten Gewerbes (nämlich den Tausch Ware gegen virtuelle Kryptowährung) nicht ohne die Lizenz ausüben kann.

Aus Verhältnismäßigkeitsgesichtspunkten und um eine gewisse Vergleichbarkeit zu den Verpflichteten des GwG und KWG zu gewährleisten, sollte die Notwendigkeit einer Lizenz auf diejenigen Akteure beschränkt werden, die gewerblich Realwährung in virtuelle Kryptowährungen tauschen. Gewerbliche Händler müssen lediglich die Sperrlisten beachten, benötigen aber keine Lizenz.

Weil Wechselbörsen – anders als Banken im Realwährungssystem – in der Regel keine Kundengelder veranlagen, genügt als Lizenzvoraussetzung die allgemeine Zuverlässigkeitsprüfung aus dem Gewerberecht. Zusätzlich muss der Antragsteller lediglich die Implementierung und Verwendung von Datenverarbeitungsanlagen zur Abfrage der Sperrliste nachweisen. Wegen der fehlenden Kundengeldveranlagung erscheint es auch sehr fraglich, ob die bisherige Subsumtion von virtuellen Kryptowährungen unter den Begriff der Rechnungseinheit in § 1 Abs. 11 Nr. 7 Alt. 2 KWG und die daran anknüpfenden umfassenden Erlaubnispflichten mit hohen Anforderungen nach den §§ 32 ff. iVm § 1 Abs. 1, Abs. 1a KWG unter dem Blickwinkel der Berufsfreiheit für (reine)[98] Wechselbörsen-Betreiber verhältnismäßig sind.

2.5.2.2.3 Informationelle Selbstbestimmung der Nutzer

Die Datenerhebung und -verarbeitung durch den (staatlichen) Betreiber des Sperrlistendienstes bei Eintragung von Transaktionen auf der Sperrliste und Fortschreibung des Sperrzustandes von Transaktionen, die auf eine gelistete Transaktion zurückgehen, stellt überdies einen Eingriff in das Recht auf informationelle Selbstbestimmung (RiS) dar.

95 *Scholz*, in: Maunz/Dürig, GG-Kommentar, 77. EL 2016, Art. 12 Rn 29; vgl. auch BVerfGE 7, 377 (397); 9, 73 (78); 13, 97 (106); 14, 19 (22); 16, 147 (163); 50, 290 (362 f.); 68, 272 (281); 97, 228 (252 f.); 105, 252 (265); 110, 141 (156); 111, 10 (28).

96 BVerfG, NJW 2006, 1261 (1262) = BVerfGE 115, 276.

97 Vgl. zur grundlegenden (mittlerweile etwas „aufgeweichten“ Stufensystematik des BVerfG: BVerfGE 7, 377; sowie zur Entwicklung: *Scholz*, in: Maunz/Dürig, GG-Kommentar, 77. EL 2016, Art. 12 Rn 335 ff. m.w.N.

98 Anders ist dies freilich, wenn der Dienstleister tatsächlich Kundengelder veranlagt.

Dieses schützt das Recht des Einzelnen, über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen.[99] Personenbezogene Daten sind gem. § 3 Abs. 1 BDSG Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Zu diesen Daten gehören auch Informationen über Konten und Depots sowie über Zahlungsvorgänge.[100] Dabei kommt es aufgrund der modernen Möglichkeiten der Datenverknüpfung nicht (mehr) auf einen eindeutig personalen Bezug der Daten an.[101] Auch Daten mit auf den ersten Blick geringem Informationsgehalt können durch die Verknüpfung mit anderen Daten eine Gefährdungslage für die Persönlichkeit und Verhaltensfreiheit herbeiführen.[102] Daher erfasst das RiS auch pseudonymisierte Daten jedenfalls dann, wenn aufgrund moderner Verknüpfungsmöglichkeiten mit weiteren Datensätzen eine Auflösung der Pseudonyme[103] möglich ist.

Auch die öffentliche Zugänglichkeit der Daten in der Blockchain schließt einen Eingriff in das RiS nicht von vorherein aus, da die Daten bei der Verarbeitung zur Fortschreibung des Sperrzustandes der Blockchain gezielt zusammengetragen, gespeichert und unter Hinzuziehung weiterer Daten (nämlich derjenigen, aus denen sich eine inkriminierte Herkunft ergibt) ausgewertet werden.[104] Je nach technischer Ausgestaltung der Fortschreibung des Sperrzustandes der Transaktionen in der Blockchain kann es sich sogar um dauerhaftes „Monitoring“ (im Sinne von anhaltsloser und automatisierter Suche nach vorgegebenen Merkmalen oder Auffälligkeiten) oder um Vorratsdatenspeicherung handeln.

Aufgrund der Öffentlichkeit und der Pseudonymität der Daten sowie des Zwecks der Verarbeitung, die gerade nicht auf eine Zuordnung der Daten an einen einzelnen Nutzer gerichtet ist, ist der Eingriff freilich von sehr geringer Intensität.

2.5.2.2.4 Sonstige

Ein Eingriff in eine (bereits in ihrer Existenz und Grundlage umstrittene) virtuelle Vereinigungsfreiheit[105] gem. Art. 9 Abs. 1 GG liegt nicht vor, da weder das System als solches beeinträchtigt ist noch der Zugang für Nutzer erschwert oder vereitelt wird.

Gleiches gilt für einen Eingriff in die Meinungs- und Informationsfreiheit (Art. 5 Abs. 1 GG), weil weder die Verbreitung von Information im Netzwerk noch das Abrufen von Informationen aus dem Netzwerk durch Transaktionssperrlisten berührt wird.[106] Mit dem Schuldprinzip (Art. 1 Abs. 1, 20 Abs. 3 GG) und der Unschuldsvermutung (Art. 20 Abs. 3 GG, Art. 6 Abs. 2 EMRK) gerät die Regelung eines Transaktions-Blacklistings deshalb nicht in Konflikt, weil sie weder eine gerichtliche Schuldzuweisung enthält noch ihr Zweck auf Bestrafung oder strafähnliche Maßnahmen (sondern auf Prävention) gerichtet ist und gegen die betroffenen Personen – soweit es sich um nicht-tatbeteiligte Personen handelt[107] – auch keine Verdachtsmomente zeitigt.[108]

99 BVerfGE 65, 1 (43); 78, 77 (84); BVerfG, NJW 2001, 879 (880); BVerfG, EuGRZ 2001, 249 (252); *Di Fabio*, in: Maunz/Dürig, GG-Kommentar, 77. EL 2016, Art. 2 Rn 175.

100 BVerfG NJW 2007, 2464.

101 BVerfGE 120, 274 (312).

102 BVerfGE 118, 168, 184 f.; BVerfGE 120, 274, 312; siehe auch BVerfGE 65, 1, 45; *Heußner*, BB 1990, 1281, 1282; *Di Fabio*, in: Maunz/Dürig, 75. EL Sept. 2015, Art. 2 Rn 5.

103 Vgl. zu den Begriffen § 3 Abs. 6 und 6a BDSG.

104 Vgl. BVerfGE 120, 274, 345.

105 Vgl. auf nationaler Ebene: *Luch/Schulz*, MMR 2013, 88 (90); *Möhlen*, MMR 2013, 221 (228); auf europäischer Ebene: *Rückert*, Virtual Currencies and Fundamental Rights, S. 25 f., SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2820634 m.w.N.

106 Siehe zu möglichen Einschränkungen durch andere Regulierungsszenarien und zur europäischen Dimension: *Rückert*, Virtual Currencies and Fundamental Rights, S. 26 ff., SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2820634 m.w.N.

107 Für tatbeteiligte Personen kommt ein Eingriff schon deshalb nicht in Betracht, weil deren Schuld in einem ordentlichen gerichtlichen Verfahren unter Geltung der Unschuldsvermutung festgestellt wird, siehe dazu 2.5.2.3.3.

108 Vgl. BVerfG, NJW 2004, 2073 mit ähnlichen ausführlichen Erwägungen zum erweiterten Verfall.

2.5.2.3 Verhältnismäßigkeit und notwendige Schutzmechanismen

2.5.2.3.1 Verhältnismäßigkeit im Vergleich mit anderen Regulierungsmöglichkeiten

Im Vergleich zu anderen Regulierungsmöglichkeiten weist das Transaktions-Blacklisting eine höhere Wirksamkeit bei gleichzeitig geringerer Grundrechtsintervention auf. Ein Totalverbot – welches auch einen nicht hinnehmbaren Innovationsnachteil für den Wirtschafts- und Technologiestandort Deutschland zur Folge hätte – wäre nicht nur schwer bis unmöglich durchsetzbar, es würde auch einen unverhältnismäßigen Eingriff in die oben genannten Grundrechte darstellen. Die Anwendung konventioneller KYC-Maßnahmen wäre zum einen – wegen der Identifizierungspflicht des Kunden und der weiterhin bestehenden öffentlichen Einsehbarkeit aller Finanztransaktionen – ein schwerwiegender Eingriff in das Recht auf informationelle Selbstbestimmung. Zum anderen weist es wegen der leichten Umgehbarkeit einen nur begrenzten Wirkungsgrad auf. Im Vergleich zu Whitelisting-Ansätzen ist das Transaktionsblacklisting deshalb weniger eingriffsintensiv, weil erstere auch – und insbesondere – die legalen Nutzer betreffen und letztlich auf ein Verbot mit Erlaubnisvorbehalt hinauslaufen, während letzteres nur kriminelle Nutzer und einzelne legale Nutzer betrifft.

2.5.2.3.2 Notwendigkeit von Schutzmechanismen zur Wahrung der Verhältnismäßigkeit

Aufgrund der teilweise erheblichen grundrechtseinschränkenden Wirkung, müssen gesetzliche Schutzmechanismen zur Wahrung der Verhältnismäßigkeit gewährleistet werden. Insbesondere die (Teil-)Entwertung von Krypto-Coins bei Nichttatbeteiligten durch eine Fortschreibung des Sperrzustandes für von der gelisteten Transaktion abgeleitete Transaktionen stellt einen schwerwiegenden Eingriff in das Eigentumsrecht der nicht-tatbeteiligten Nutzer dar. Die Erheblichkeit wird dabei noch gesteigert, wenn die inkriminierte Transaktion (wegen der Dauer von Ermittlungen und Strafprozess) erst lange nach ihrer Ausführung und der Weiterüberweisung der betroffenen Krypto-Coins gelistet wird. Das bisherige Instrumentarium zur Entwertung bzw. Entziehung von inkriminierten Vermögensgegenständen – Einziehung und Verfall nach den §§ 73 ff. StGB – ist in seinem Anwendungsbereich auf Gegenstände beschränkt, die dem Täter oder Teilnehmer gehören oder zustehen. Ausnahmen werden nur bei Verschulden des Nicht-Tatbeteiligten (z.B. Gewährung des Gegenstands durch Dritten in Kenntnis der Tatumstände, Handlung des Täters für einen Dritten) oder einer Gefährdung durch den Gegenstand zugelassen. Diese Begrenzungen werden von der Rechtsprechung für die Verfassungsmäßigkeit der Normen als notwendig erachtet.[109] Insofern enthält das Transaktions-Blacklisting eine neue und schwerwiegende Eingriffsdimension. Diese ist zwar angesichts der Beschränkung effektiver Regulierungsoptionen durch die technischen Besonderheiten (v.a. Pseudonymität und Dezentralität) virtueller Kryptowährungssysteme und die deutlich höhere Eingriffsintensität von Totalverbots- und Whitelistingansätzen rechtfertig- und hinnehmbar. Sie nötigt jedoch auch zur Schaffung effektiver Schutzmechanismen zur Wahrung des Verhältnismäßigkeitsgrundsatzes.

2.5.2.3.3 Einzelne Schutzmechanismen

Zunächst müssen die Voraussetzungen, unter denen die Aufnahme einer Transaktion auf der Sperrliste erfolgt, so bestimmt wie möglich gefasst werden. Hier bietet sich ein Rückgriff auf die Norm des § 73 Abs. 1 S. 1 StGB (Verfallsvoraussetzungen) an: „Ist eine rechtswidrige Tat begangen worden und hat der Täter oder Teilnehmer für die Tat oder aus ihr virtuelle Kryptowährungseinheiten (Krypto-Coins) erlangt, so ordnet das Gericht die Aufnahme der Transaktion, durch welche die Krypto-Coins erlangt wurden

109 BGHSt 1, 351 (354 f.); 2, 311 (312 f.); 19, 123 (125 f.); 21, 66 (67 ff.).

oder aus welcher die Krypto-Coins stammen, in die Sperrliste an“. Da eine Aufnahme in die Sperrliste zur Kriminalitätsprävention nur notwendig ist, wenn die erlangten Krypto-Coins beim Täter oder Teilnehmer im Zeitpunkt der Urteilsverkündung nicht abgeschöpft werden können (z.B. weil dieser sie bereits weitertransferiert hat oder sich weigert, die privaten Schlüssel herauszugeben[110]), ist die Aufnahme in die Sperrliste auf diese Fälle zu beschränken bzw. dem Verfall (nicht dem Verfall von Wertersatz, wenn der Täter später noch auf die Krypto-Coins zugreifen kann) ein gesetzlicher Vorrang einzuräumen. Was den Zeitpunkt einer Aufnahme in die Sperrliste anbelangt, so gebieten Rechtsstaatsprinzip und Verhältnismäßigkeit, dass eine solche grundsätzlich erst mit Rechtskraft des Urteils erfolgen darf (insofern also ebenfalls wie in den Fällen von Verfall und Einziehung).[111]

Ferner sollte der sachliche Anwendungsbereich der Transaktionssperrliste (zunächst) auf den Straftatenkatalog des § 261 Abs. 2 StGB beschränkt bleiben. Dies gibt den Strafverfolgungs- und Sicherheitsbehörden einerseits ein effektives Instrument zur Bekämpfung organisierter (Finanz-)Kriminalität und beschränkt andererseits die Eingriffe in die Grundrechte Nicht-Tatbeteiligter in verhältnismäßiger Weise. Eine Ausweitung des Normenkatalogs sollte angesichts der schwerwiegenden Grundrechtseingriffe nur vorsichtig und nur bei empirisch belegbarer Notwendigkeit erwogen werden.

Um die Eingriffsintensität gerade für Nicht-Tatbeteiligte zu reduzieren, ist die öffentliche Einsehbarkeit der Sperrliste für alle Nutzer des jeweiligen virtuellen Kryptowährungssystems erforderlich. So können Nutzer ihr Nutzungsverhalten auf die geänderte Rechtslage einstellen (indem sie Krypto-Coins aus gelisteten Transaktionen und Transaktionen, die auf gelistete Transaktionen zurückgehen, nicht als geschuldete Erfüllung akzeptieren). Eine weitere Reduktion der Eingriffsintensität für Nicht-Tatbeteiligte hat dadurch zu erfolgen, dass das Sperrlistensystem für die Vermischung von inkriminierten mit nicht-inkriminierten Krypto-Coins bei Folgetransaktionen einer Haircut-Policy oder einem Senioritätsmodell folgt.[112]

Schließlich müssen einzelne Betroffene durch Rechtsschutzmöglichkeiten sowie Härtefall- und Entschädigungsklauseln hinreichend geschützt werden. Der Rechtsschutz für den Beschuldigten lässt sich dabei durch den Instanzenzug des Strafverfahrens gewährleisten. Für Nicht-Tatbeteiligte bedarf es eines speziellen Nachverfahrens nach Vorbild von § 439 StPO. Härtefall- und Entschädigungsklauseln müssen insbesondere für Fälle geschaffen werden, in denen (kumulativ) ein Wertverlust größeren Ausmaßes für einen Nicht-Tatbeteiligten droht und dieser die fragliche Transaktion – auch unter Nutzung von ggf. vorhandenen oder entstehenden Risikoanalyse-Dienstleistern – mit allen zumutbaren Maßnahmen auf eine mögliche inkriminierte Herkunft hin überprüft hat.

Um eine missbräuchliche Datenverwendung auszuschließen und die Datenspeicherung auf Vorrat zu rechtfertigen, ist eine Beschränkung des Speicherungs- und Verarbeitungszwecks der Daten auf den Betrieb des Sperrlistensystems notwendig.

110 Vgl. hierzu den Fall von BGH NJW 2015, 3463; dort hatte einer der Angeklagten für einen (großen) Teil der erlangten Bitcoins die Herausgabe der privaten Schlüssel verweigert, sodass nur ein Wertersatzverfall erklärt werden konnte.

111 Zu dennoch notwendigen und möglichen „einstweiligen Listungen“ im Ermittlungsverfahren 2.5.2.4.

112 Dazu 2.3.2.3.4.

Schließlich müssen Datenschutz- und Datensicherheitsstandards beim Betreiber des Sperrlistendienstes und der Data-Provider, welche die Informationen über den Sperrzustand der Transaktionen zur Verfügung stellen, gesetzlich garantiert werden, um missbräuchliche Datenverwendung und Falscheintragungen zu verhindern. Vorbild können hier die vom Bundesverfassungsgericht in seinem Urteil zur Vorratsdatenspeicherung gemachten Vorgaben sein,[113] die in der Neuregelung (§ 113d TKG) vom Gesetzgeber umgesetzt wurden. Außerdem muss technisch sichergestellt sein, dass die Informationen über den Sperrzustand in nicht diskriminierender Weise (also ohne Ermöglichung eines Informationsvorsprungs einzelner Marktteilnehmer) zur Verfügung gestellt werden. Hier bietet sich eine Regelung an, die feste Zeitpunkte für die Aktualisierung vorgibt. Angesichts der sehr geringen Eingriffsintensität in das Recht auf informationelle Selbstbestimmung erscheint es derzeit möglich, die Sperrliste durch staatliche Behörden verwalten zu lassen.

2.5.2.4 Einstweilige Listung im Ermittlungsverfahren

Schließlich sollte die Transaktionssperrlisten-Regelung um die Möglichkeit einer einstweiligen Listung durch die Staatsanwaltschaft im Ermittlungsverfahren bei Vorliegen eines Tatverdachts ergänzt werden. Eine solche Regelung würde die Sicherstellungsregeln für Vermögenswerte nach §§ 111b ff. StPO für Fälle ergänzen, in denen eine Sicherstellung nach diesen Vorschriften (bei denen im Übrigen rechtlich umstritten ist, ob und wie diese auf die Sicherstellung von Krypto-Coins anwendbar sind[114]) mangels Herausgabe des privaten Schlüssels und sonstiger Zugriffsmöglichkeiten faktisch nicht durchführbar ist. Besonders notwendig erscheint die Möglichkeit einer einstweiligen Listung in Fällen, in denen noch kein konkreter Verdächtiger zu einer verdächtigen Transaktion ermittelt werden konnte (dies ist z.B. in den praktisch sehr relevanten Fällen der CryptoLocker-Erpressungen[115], also bei „Lösegeldzahlungen“ häufig der Fall). Hierdurch würde die Präventionswirkung deutlich erhöht, wenn kriminelle Akteure damit rechnen müssten nicht erst, wenn sie als Tatverdächtige ermittelt sind oder sogar erst mit rechtskräftigem Abschluss des Strafverfahrens ihre Krypto-Coins „zu verlieren“, sondern bereits bei Verdachtsmomenten *allein die Transaktion* betreffend, eine Entwertung durch Aufnahme in die Sperrliste möglich ist. Gleichzeitig verringert sich das Risiko legaler Nutzer, von einer späteren Listung betroffen zu sein, da auch die einstweiligen Listungen öffentlich einsehbar wären. Hierdurch würde der erhebliche Eingriff in Art. 14 Abs. 1 GG deutlich abgemildert. Um die (möglicherweise) rufschädigende Wirkung einstweiliger Listungen zu begrenzen, sollte die einstweilige Listung als solche erkennbar sein.

Die schnellere Information der Nutzer darüber, welche Transaktionen möglicherweise mit kriminellen Handlungen in Verbindung stehen, wirkt sich jedoch negativ auf die Austrocknung von Mixing-Diensten[116] und damit auf einen Teil der erhofften Präventionswirkung aus. Denn hierdurch wird das Risiko, einer später eintretenden (Teil-) Entwertung durch Listung einer im Mixing-Vorgang verwendeten Transaktion für die Beteiligten verringert.[117] Dieser Nebeneffekt ist aber angesichts der oben beschriebenen vorteilhaften Wirkungen hinnehmbar.

113 Vgl. BVerfGE 125, 260 (325 ff.); ähnlich auch EuGH, Urteil vom 21.12.2016, C-203/15 und C-698/15, Rn 109, 122.

114 Vgl. *Rückert*, MMR 2016, 295; *Goger*, MMR 2016, 431; Heine, NStZ 2016, 441; *Greier*, wistra 2016, 249.

115 Vgl. z.B.: http://www.sueddeutsche.de/bayern/unterfranken-dettelbach-zahlt-loesegeld-nach-cyberangriff-1.2892279; http://www.zeit.de/digital/datenschutz/2016-02/it-sicherheit-ransomware-erpressung-krankenhaus-los-angeles-neuss.

116 Dazu 1.2.

117 Für Details: *Abramova/Schöttle/Böhme*, Mixing Coins of Different Quality: A Game-Theoretic Approach (noch nicht veröffentlicht).

Die Intensität des Eingriffs in Art. 14 Abs. 1 GG durch eine einstweilige Listung wird – im Vergleich zur endgültigen Listung nach Rechtskraft des Urteils – noch dadurch erhöht, dass diese lediglich auf einer Tatverdachtsbasis erfolgt (ähnlich zu §§ 111b ff. StPO). Zur Wahrung der Verhältnismäßigkeit sind daher Rechtsschutz- (z.B. Antrag auf gerichtliche Entscheidung nach dem Vorbild von § 98 Abs. 2 S. 2 StPO oder sogar ein präventiver Richtervorbehalt), Höchstfrist- (z.B. nach Vorbild von § 111b Abs. 3 StPO) und Entschädigungsvorschriften (durch eine Aufnahme der Maßnahme in den Katalog von § 2 Abs. 2 StrEG, z.B. als Nr. 4a) notwendig. Als Regelungsstandort für die einstweilige Listung wird eine Ergänzung der §§ 111b ff. StPO vorgeschlagen.

2.5.2.5 Wechselwirkung mit Geldwäschestrafbarkeit

Die Sperrlistengrundsätze werfen ihrerseits Fragen hinsichtlich des Verhältnisses zur Strafbarkeit wegen Geldwäsche nach § 261 StGB auf. Eine große Rolle spielt dabei die Vermischung legaler und illegaler Krypto-Coins. Eine solche Vermischung kommt zwar auch bei Bar- und Buchgeld (und das wohl sogar alltäglich) vor.[118] Im Regelfall scheitert eine Strafbarkeit wegen Geldwäsche hier jedoch an der fehlenden Kenntnis der Herkunft der Gelder aus einer Katalogtat. Mit Einführung einer Transaktionssperrliste kann die damit verbundene (mögliche) Kenntnis der inkriminierten Herkunft bei Benutzung der gelisteten Krypto-Coins jedoch Vorsatz begründen. Der Frage der Auswirkung einer Transaktionssperrliste auf den Vorsatz kommt insbesondere vor dem Hintergrund der „Vermischungsproblematik“ und der damit verbundenen Gefahr der „Infizierung“ legaler Krypto-Coins große Bedeutung zu. Dies ist auf die Rechtsprechungspraxis des BGH zur Vermischung illegaler und legaler Gelder auf einem Konto zurückzuführen.[119] Eine „Totalkontamination“, d.h. Vergiftung aller an der Vermischung beteiligten Gelder, soll immer dann gegeben sein „*sofern der illegale Anteil als nicht lediglich völlig unerheblich*“ zu bewerten ist, was zumindest bei einer Bemakelungsquote von 5,9 % bis 35 % angenommen werden soll.[120]

Wird nun diese Rechtsprechung konsequent auf virtuelle Kryptowährungen übertragen, so besteht die Gefahr einer fortschreitenden Vergiftung des gesamten Systems.[121] Zwar würde durch eine einstweilige Listung die Problematik insofern abgemildert werden, dass später endgültig gelistete Transaktion von den Nutzern nicht mehr unbekümmert weitertransferiert werden. Jedoch ist unabhängig davon eine Übertragung der vom BGH vertretenen Totalkontaminationslehre auf virtuelle Kryptowährungen mehr als fraglich. Dies gilt insbesondere vor dem Hintergrund der bereits aufgeworfenen Frage der Auswirkung einer Transaktionssperrliste auf den Vorsatz, was damit zusammen hängt, dass der Straftatbestand der Geldwäsche nach deutschem Recht weit gefasst ist und die Handlungsebene der Geldwäsche bei einem dezentralen, pseudonymen und grenzüberschreitenden System (noch) schnell(er) erfüllt ist. Für Annahme von Vorsatz hinsichtlich des Herrührens aus einer Katalogtat ist die Kenntnis der Herkunft aus irgendeiner in § 261 Abs. 1 StGB gelisteten Tat ausreichend, d.h. der Vorsatz muss sich nicht auf eine spezifische Katalogtat beziehen.[122] Im Rahmen des Leichtfertigkeitstatbestandes des § 261 Abs. 5 StGB reicht es sogar schon aus, wenn sich eine solche Herkunft aufgedrängt hat, dies jedoch aus grober Unachtsamkeit oder Gleichgültigkeit nicht erkannt wurde.[123]

118 So eindrücklich: *Fischer*, Woher haben Sie dieses Geld?, Zeit Online v. 13.10.2015, S. 4.

119 BGH, Beschl. v. 20.05.2015 – 1 StR 33/15, NJW 2015, 3254.

120 Der BGH legt sich hier jedoch ausdrücklich nicht auf eine bestimmte Mindestquote fest.

121 Erste Schätzungen, die unter der Prämisse standen, dass durch die Listung inkriminierter Transaktionen keine Verhaltensänderungen stattfinden haben ergeben, dass nach nur 500 Blöcken (ca. 3.5 Tage) im Mittel bereits 1% aller sich im Umlauf befindlichen Bitcoins vergiftet wären.

122 BGH, Urt. v. 28.01.2003 – 1 StR 393/02 = BeckRs 2003, 01885 mit Verweis auf BGHSt 43, 158 (165); BGH, Beschl. v. 10.11.1999 – 5 StR 472/99 = StV 2000, 67.

123 BGHSt 43, 158 (168); 50, 347 (351); BT-DrS 12/989, S. 28.

Es ist somit festzuhalten, dass die Anwendung der Totalkontaminationslehre auf virtuelle Kryptowährungen bei Etablierung einer Transaktionssperrliste für Nutzer die Gefahr der Geldwäschestrafbarkeit enorm erhöht.

Nicht nur deshalb ist die Totalkontaminationslehre im Bereich virtueller Kryptowährungen als unverhältnismäßig abzulehnen. Dies lässt sich erstens damit begründen, dass sich der vom BGH intendierte Abschreckungseffekt durch die Annahme der Totalvergiftung bei Vermischungskonstellationen auf virtuelle Kryptowährungen als solche beziehen würde. Zweitens divergiert der Ablauf der Vermischung bei virtuellen Kryptowährungen erheblich im Vergleich zur Vermischung auf einem Konto. Dies ist zum einen auf die öffentliche Einsehbarkeit aller Konten und damit einhergehend die öffentliche Einsehbarkeit des Transaktionsverlaufs sowie zum anderen auf die Tatsache zurückzuführen, dass bei vielen virtuellen Kryptowährungen keine Vermischung von Krypto-Coins auf Basis von Konten erfolgt. Die Ausgangsvoraussetzungen unterscheiden sich somit erheblich von denen bei Vermischung legaler und illegaler Gelder auf einem Konto, sodass zwingende Gründe bestehen, bei virtuellen Kryptowährungen nicht grundsätzlich an der Totalkontaminationslehre festzuhalten. Eine Transaktionssperrliste stellt folglich ein milderes, gleichzeitig aber auch effektiveres Mittel der Geldwäscheprävention dar.

2.5.3 Ausgestaltung eines flankierenden Lizenzmodells

Für die Ausgestaltung eines flankierenden Lizenzmodells sind einige grundlegende Aspekte zu bedenken: Um Innovationen im Bereich virtueller Kryptowährungen nicht unverhältnismäßig zu erschweren und eine Abwanderung von Intermediären aus dem europäischen Wirtschaftsraum zu vermeiden, sollte der Kreis erlaubnispflichtiger Intermediäre möglichst gering gehalten werden. Empfohlen wird eine Erlaubnispflicht nur für solche Intermediäre, die teilweise von einer Listung betroffene Krypto-Coins in Währungsgeld umtauschen. Andere Intermediäre, die von einer Listung betroffene Krypto-Coins nicht annehmen, sollten dagegen von einer Erlaubnispflicht ausgenommen werden. Weiterhin sind die Besonderheiten virtueller Kryptowährungen zu berücksichtigen. Insbesondere besteht bei Cryptocoin-Intermediären kein Kreditinstituten vergleichbares Kreditrisiko, sodass insbesondere geringere Anforderungen an das Anfangskapital (vgl. § 33 Abs. 1 Nr. 1 KWG) der Intermediäre und die fachliche Eignung der Geschäftsleitung (vgl. §§ 33 Abs. 1 Nr. 4, 25c KWG) zu stellen sind.

Durch das Lizenzmodell muss im Wesentlichen sichergestellt werden, dass der Verpflichtete bekannt, erreichbar und hinreichend zuverlässig ist.

2.5.4 Technische Aspekte

Das vorgeschlagene Sperrlistensystem lässt sich effizient realisieren, wenn es von Beginn an mit einem verlässlichen und redundant implementierten informationstechnischen System unterstützt wird. Dieses System sollte den Prinzipien geringer Entwurfskomplexität folgen und entsprechend den Anforderungen der Sperrlistenverwaltung entwickelt werden. Entwicklung und Betrieb müssen dem Stand der Technik entsprechen und Weiterentwicklungen zeitnah berücksichtigen. Dies gilt besonders mit Blick auf die Integrität der Sperrliste, der Autorisierung von Schreibzugriffen und der Vertraulichkeit von nicht-öffentlichen Informationen wie bspw. die Umstände einer vorläufigen Listung (verantwortliche Stelle, Verdachtsmoment, Aktenzeichen etc.). Die Abfrage von Informationen muss datensparsam, bestenfalls anonym möglich sein. Dem Gebot der Zweckbindung folgend, ist es nicht angebracht, aus etwaigen praktischen oder wirtschaftlichen Erwägungen die Sperrlistenfunktionalität als Erweiterung bestehender Systeme zu realisieren. Angesichts der Neuheit und Besonderheiten virtueller Kryptowährungen dürfte der Integrationsaufwand in bestehende Systeme ohnehin erheblich höher sein als der zu erwartende Nutzen. Die Identifikation von

gelisteten Transaktionen sollte – soweit bei dezentralen Systemen technisch möglich – eindeutig sein und muss für jede unterstützte virtuelle Kryptowährung definiert werden. Zweckmäßig ist eine Orientierung an den in den jeweiligen Kernsystemen gebräuchlichen Kennzeichen.

Besondere Anforderungen an die Verfügbarkeit und Skalierbarkeit des Systems ergeben sich aus der Tatsache, dass verpflichtete Intermediäre erwartungsgemäß jede beabsichtigte Transaktion vorab mit der Sperrliste abgleichen müssen und es plausibel ist, dass virtuelle Kryptowährungen deutlich an Popularität zunehmen. Mögliche Zeitverzögerungen bei der Beantwortung von Anfragen aufgrund von Überlast sind zu vermeiden, da sie zu einer Ungleichbehandlung von Intermediären und mittelbar Nutzern führt, welche dadurch finanzielle Nachteile erleiden können. Zudem erhöht unzureichende Skalierbarkeit die Wahrscheinlichkeit für erfolgreiche DDoS-Attacken.[124]

Um pseudonymen Nutzern Rechtsschutz bei fälschlicher Listung zu gewährleisten, sind technische Schnittstellen und Prozesse zum Nachweis der Betroffenheit nötig (z.B. durch Nachweis über den Besitz der Zugangsinformationen eines von einer gelisteten Transaktion betroffenen Kontos). Ist der Nachweis erfolgt, sind dem Betroffenen Informationen über den Vorgang zuzustellen, der zur Listung geführt hat.

Zur Erhöhung der Rechtssicherheit für verpflichtete Intermediäre wäre es wünschenswert, wenn die Auskunft (insbesondere auch negative) über Sperrlisteneinträge mit Zeitstempel digital signiert erteilt würde. So können diese später nachweisen, dass sie ihrer Pflicht nachgekommen sind.

2.6 Europäische und internationale Anschlussfähigkeit der empfohlenen Handlungsweise

Die Transaktionssperrliste weist eine hohe internationale Anschlussfähigkeit auf, da sie technisch mit überschaubarem Aufwand und auf Basis erprobter Technologien umsetzbar ist und nicht an besondere nationale rechtliche Gegebenheiten anknüpft.

2.6.1 Einheitliche Sperrliste innerhalb der EU

Innerhalb der EU ist eine einheitlich geführte und verwaltete Transaktionssperrliste aufgrund der faktischen Grenzenlosigkeit virtueller Kryptowährungssysteme und der Einheitlichkeit des EU-Binnenmarktes erstrebenswert. Grundlage für eine entsprechende Verordnung können Art. 75, 114 AEUV sein. Als verwaltende Behörde kommt Europol in Betracht, da dort bereits umfassende Datenverarbeitungskompetenzen vorhanden sind. Alternativ ist eine neue Behörde zu schaffen (ähnlich OLAF[125]).

2.6.2 Internationale Sperrliste über völkerrechtliche Verträge

Um (faktisch naheliegende) Umgehungsstrategien und Verdrängungseffekte zu unterbinden, empfiehlt es sich außerdem, eine internationale Zusammenarbeit anzustreben, idealerweise in Form verbindlicher völkerrechtlicher Übereinkommen über die Führung internationaler Transaktionssperrlisten und die Verpflichtung der jeweiligen nationalen Akteure durch die Unterzeichnerstaaten. Als Nahziel sollte zumindest die international einheitliche Kriminalisierung von kryptowährungsbezogenen Straftaten angestrebt werden (z.B. im Rahmen einer „neuen“ Cybercrime Convention), um eine einheitliche Rechtsbasis für die Aufnahme inkriminierter Transaktionen in nationale bzw. EU-weite Sperrlisten bei grenzüberschreitendem Zahlungsverkehr mit virtuellen Kryptowährungen zu ermöglichen.

124 Der Sperrlistenansatz wird in der Nutzergemeinschaft kontrovers diskutiert, siehe nur Bitlegal.io, Bitcrime to undermine fungibility of bitcoin, abrufbar unter http://bitlegal.io/2016/05/25/bitcrime-to-undermine-fungibility-of-bitcoin/ (letzter Abruf: 15.12.2016). Zugleich sind DDoS-Attacken in Teilen der Nutzergemeinschaft ein übliches Mittel des Protests, dazu *Vasek/Thornton/Moore*, in: Böhme/Brenner/Moore/Smith, Financial Cryptography and Data Security, 1st Workshop on Bitcoin Research (FC 2014), Barbados, Heidelberg u.a. 2014, S. 57 ff.

125 http://ec.europa.eu/anti-fraud//home_en.

Content

The recommendation was written in the context of the BITCRIME project (German Subproject)[1] by *Rainer Böhme, Johanna Grzywotz, Paulina Pesch, Christian Rückert, Christoph Safferling and subsequently translated from the German original.*

1 The project is sponsored by the BMBF (German Federal Ministry of Education and Research) in the context of the call "Civil Security – Protection against Organised Crime" in the framework of the programme "Research for Civil Security" of the German Federal Government. Website https://www.bitcrime.de/deutschland/ (last access: 14.10.16).

1 Introductory Remarks

1.1 Outline of the Problem

Virtual cryptocurrencies[2] such as Bitcoin are a phenomenon of growing significance. They are traded anonymously (so it is said), independently of central banks and of states and credit institutes and the trading is done directly between users. This creates major potential for abuse by criminals. An analysis of evaluation results from the Federal Criminal Police Office showed that, in Germany, virtual cryptocurrencies, when they are linked to crime, are mainly used in cybercrimes in the narrower sense,[3] in blackmail and in fraudulent activities.[4] In addition, various institutions – such as the Financial Action Task Force (on Money Laundering), FATF, which is responsible for the prevention of international money laundering, and the European Banking Authority (EBA) – have issued warnings about the use of these currencies for money laundering and financing of terrorism.[5] Whether this is really the case, and if so, to what extent virtual cryptocurrencies are used for the financing of terrorism, remains to be established.[6] The EU too sees the need for further action. Thus in July 2016 the Commission announced plans to extend the fourth Money Laundering Directive to encompass virtual cryptocurrencies.[7] These and other pronouncements make it clear that virtual cryptocurrencies with their pseudonymity and decentralisation pose a particular challenge for criminal prosecution. In addition, however, there is also a need to develop a new crime prevention strategy.

1.2 Technical Overview of Virtual Cryptocurrencies, using Bitcoin as an Example

The development of such a crime prevention strategy presupposes an understanding of the basic functioning of virtual cryptocurrencies. This will be described in the following by reference to the Bitcoin system, as the best-known example of a virtual cryptocurrency. Then the area of application of this present recommendation, which extends beyond Bitcoin, will be set out.

The Bitcoin system[8] offers its users the possibility to undertake online transactions without using central authorities as intermediaries. In this decentralised system bitcoins are transferred directly between users. Bitcoin users have accounts[9] which are based on public keys of an asymmetric cryptographic system and which can be generated by the users themselves in arbitrary numbers. Each Bitcoin in the system is allocated to a specific account at any one time. If a bitcoin allocated to a specific account is to be transferred, a transaction has to be generated which basically consists of the message that the bitcoin is to be allocated to another specific account. In order to ensure that only the owner of an account is able to transfer a bitcoin allocated to this account, the transaction has to be digitally signed using the private key belonging exclusively to this account.[10] So-called wallet software is used for administering accounts and their private keys and for generating and signing transactions.

2 This term only comprises virtual, decentralised cryptographic currencies. Cf. 1.2 below. In addition, it must be pointed out that the term currency is used, although legal definitions of currency only comprise state-issued currencies. Cf. EBA Opinion on 'virtual currencies', EBA/Op/2014/08, p. 11.

3 According to the definition worded by police bodies and approved by working group II "Inner Security", "cybercrime in the narrower sense" comprises all crimes against the internet, other data networks, IT systems or data stored thereon.

4 Cf. also: *Grzywotz/Rückert/Köhler*, Cybercrime mit Bitcoins, StV 2016, 753 (756).

5 EBA Opinion on 'virtual currencies', EBA/Op/2014/08, pp. 32; FATF Report, Virtual Currencies – Key Definitions and Potential AML/CFT Risks, June 2014, pp. 9 f.

6 *Grzywotz/Rückert/Köhler, StV 2016, 753 (756).*

7 Cf. Communication by the EU Commission to the European Parliament and to the Council of 02.02.2016 – COM(2016) 50 final.

8 Cf. also Böhme/Christin/Edelman/Moore, Journal of Economic Perspectives, Vol. 29, pp. 213 ff.; Narayanan/Bonneau/Felten/Miller/Goldfeder, Bitcoin and Cryptocurrency Technologies: A comprehensive Introduction, Princeton 2016; Sorge/Krohn-Grimberghe, DuD 2012, pp. 479 ff.; Zohar, CACM 09/2015, pp. 104 ff.

9 The accounts are also called addresses.

10 The key pairs of the asymmetric cryptographic system are used as digital signature for Bitcoin transactions, which serves as a means of authentication. However, there is no encryption for purposes of keeping information secret.

In the absence of a central authority which receives the transaction instructions and adjusts the balances of the users, Bitcoin transactions are sent to the system's user community and are also processed by this community. It would not, however, be possible for other users to exclude the possibility that the same individual bitcoins were used in multiple transactions (what is known as double-spending) simply by checking the digital signature, because for each bitcoin any number of correctly signed transactions may be generated. In order to identify attempts at double-spending and to prevent them by blocking the processing of the respective transactions, the users of the Bitcoin system must be aware of all system transactions which have been processed thus far. To this end all Bitcoin transactions are stored in a public data structure, the so-called blockchain. The blockchain is stored on the computers of all users and contains the entire – non-encrypted – transaction history dating from the initialisation of the Bitcoin system. Any transaction is only considered to have been executed after it has been added to the blockchain. The blockchain provides the information as to which bitcoin amount was transferred when and from which Bitcoin account to which target account. In this way everybody can trace back any bitcoin amount to any time in the past.[11]

The blockchain is continually updated by the system users. In order to protect these processes against manipulation, so-called "proof of work" in the form of a solution of a mathematical problem must be furnished, i.e. computing power must be expended. As an incentive for accepting the cost involved in this, users who update the blockchain are credited with bitcoins. The credits come from newly created money units, and after a defined fixed pattern in the timeline are converted to user-pays financing. Users participating in this process are called miners.

But bitcoins may also be bought in special online trading places (exchange platforms).[12] These exchange platforms are usually centrally organised. This is also the case for other offers in the Bitcoin ecosystem that has developed around the core system (cf. fig.). For example, there are Bitcoin "payment services" which accept "payments" in bitcoins on behalf of traders.[13] For users who do not want to administer their key pairs on their own computers there are also wallet services which administer the key pairs of their users on web-based servers.[14] In addition there are so-called mixing services with which users can disguise the ownership of bitcoins.[15]

In addition to Bitcoin numerous alternative systems, so-called Alt-Coins have been established. This present recommendation claims to be valid not only for Bitcoin but also for other similar systems. The following, therefore, refers generally to "virtual cryptocurrencies". This comprises all decentralised virtual currencies which enable cryptographically integrity-assured transactions via value units which are independent of conventional currencies and which are processed in a public, continuous, completely traceable transaction history.[16] The value units used in the systems will all be referred to as cryptocoins in the following.

11 *Möser/Böhme/Breuker*, in: Proceedings of the APWG eCrime Researchers Summit, San Francisco, IEEE 2013, pp. 2 ff., p. 12.

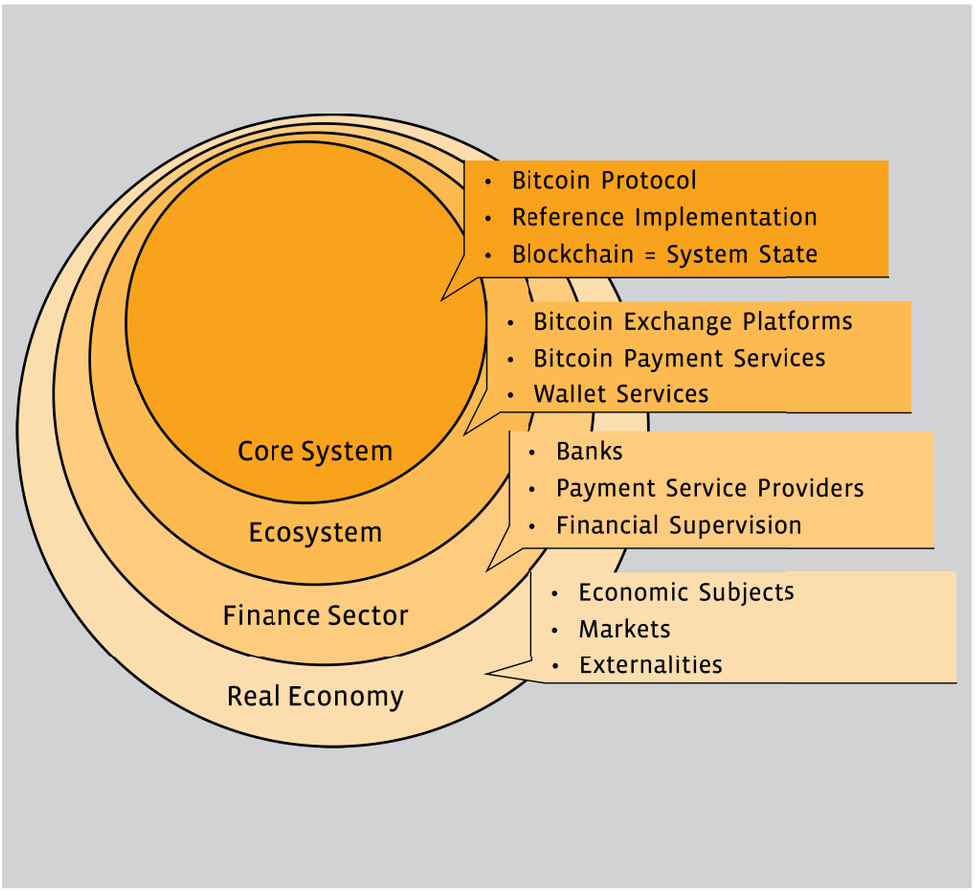
12 Such as Bitcoin.de, https://www.bitcoin.de/ (last access:16.12.16); Coinbase, https://www.coinbase.com/charts (last access: 16.12.16); Kraken, https://www.kraken.com/ (last access: 16.12.16).

13 Such as Bitpay, https://bitpay.com/ (last access: 14.10.16); Coinbase, https://www.coinbase.com/merchants (last access: 16.12.16); Coinify, https://www.coinify.com/ (last access: 16.12.16); GoCoin, https://www.gocoin.com/ (last access: 16.12.16).

14 Such as the wallets of Blockchain.info, https://blockchain.info/de/wallet/#/ (last access: 16.12.2016); Coinbase, https://www.coinbase.com/ (last access: 16.12.16); GreenAddress, https://greenaddress.it/ (last access: 16.12.16).

15 For this the users generate a new account, inform the service provider about it, and transfer a bitcoin to the provider. The service then transfers another user's bitcoin to the newly generated address. As a consequence, it might not be possible to allocate the newly generated address and the bitcoin to the owner. More in *Möser/Böhme/Breuker*, in: Proceedings of the APWG eCrime Researchers, Summit (ECRIME 2013), San Francisco, IEEE 2013, pp. 1–14, accessible under http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6805780 (last access: 19.12.2016).

16 This term comprises in particular so-called Bitcoin clones which are strongly influenced by Bitcoin, such as Litecoin, https://litecoin.org/de/ (last access: 15.12.2016). It does not, however, comprise centralised systems in which obligations are traded, such as Ripple, https://ripple.com/ (last access: 15.12.2016), and anonymous systems without completely traceable transaction history, such as Zcash, https://z.cash/ (last access: 15.12.2016).



1.3 Organisational Context of Research

The aim of the bilateral German-Austrian research project BITCRIME was to develop innovative approaches appropriate to the nature of virtual cryptocurrencies and therefore capable of being implemented to identify, prosecute and prevent organised financial crimes involving virtual cryptocurrencies. The focus was on approaches, of both a technical and an organisational kind, which enable effective criminal investigation without being based on blanket bans (complete ban on the use of virtual cryptocurrencies) and without presenting an increased potential for abuse in the sense of mass surveillance (e.g. massive retention of data). The project aimed at finding solutions which could be implemented in Europe but which could be transferred and linked internationally.

The German subproject dealt with two sub-goals. In the field of identification and prosecution, a new type of investigative tool enabling better traceability of transactions in virtual cryptocurrencies was developed and checked with a view to compliance with current legislation. The second sub-goal was the strategic development of suitable regulation of the virtual cryptocurrency market. This was to protect legitimate users, to close off any prosecutable gaps remaining from the first sub-goal and to prevent financial crime in the field of cryptocurrencies. The result of this work is presented in the form of this recommendation.

Taking into account the technical realities of virtual cryptocurrencies and observing the need to protect the fundamental rights of all persons involved in such systems, we propose a system of transaction blacklists where intermediaries at the interface between the virtual cryptocurrency system and the real economy / real currency system are prohibited by law from accepting or exchanging (for goods/services or real currencies) transactions which are derived from predicate offences to money laundering. Relevant transactions are to be marked up in a publicly accessible blacklist.

2 Recommendation

2.1 The Area of Application: Crime Prevention/ Fight against Money Laundering

The regulatory framework proposed here has as its main area of application the reduction of crime committed in the context of virtual cryptocurrencies (in particular Bitcoin) with a special focus on the prevention of money laundering. It is, therefore, close to regulations such as the legislation on tracing profits from serious criminal activities (GwG – Money Laundering Act) or clause 5a of the second section of the legislation on banking (KWG – Banking Act). By contrast, other questions arising from the special characteristics of virtual cryptocurrencies (mainly its decentralised organisation), such as consumer protection (e.g. information requirements for businesses) or the value stability of cryptocoins are not addressed. These remain a subject for further research. The same applies to possible displacement effects, such as the switching of criminal agents to alternative virtual cryptocurrency systems with other technical characteristics.

2.2 Overview of Crime Prevention and the Fight against Money Laundering for Real Currencies (Identifying, Monitoring, Reporting)

In order to understand the special crime fighting requirements in the field of virtual cryptocurrencies a brief overview of previous legislative prevention strategies in the context of financial transactions is necessary. In the German legislator's view the fight against money laundering is supposed to make three things possible: law enforcement authorities "must be provided with evidence for money laundering transactions"[17]. Furthermore they must be enabled to have access to documentation about suspicious financial transactions and those involved in them. And finally companies should apply anti-money-laundering provisions.[18]

These measures, therefore, consist mainly in requiring the actors in financial transactions (such as financial institutions, finance services providers, commercial dealers, casinos, real estate agents)[19] to implement identification, monitoring and reporting measures. The actors are thus required to identify their contractual partners and the backers of these latter, and to check, monitor and document their business relationship (in particular any financial transactions).[20] In addition, obligated parties must make so-called suspect notifications, if the facts of an implemented transaction would suggest money laundering or terrorist funding.[21]

It is necessary to focus the prevention strategies on private actors in the finance market, because financial transactions themselves are invisible to law enforcement authorities and private actors are thus the only source of information for relevant investigations.[22] Furthermore, any blanket state surveillance of all transaction activities (if this were even possible in a "normal" money system) would, due to the broad scope of such a measure, constitute extreme interference with all citizens' legal positions as protected by fundamental rights.[23] And finally, for criminal investigations, financial institutions must keep available a file with account master data which may be called up as required.[24]

17 BT-DrS 12/2704, p. 1.

18 For entire topic: BT-DrS 12/2704, p. 1; cf. also *Diergarten/Barreto da Rosa*, Praxiswissen Geldwäscheprävention, 2015, chapter 1, marginal note 118.

19 § 2 section 1 GwG, § 1 KWG.

20 §§ 3 section 1, 8 GwG; financial institutions must provide and use automated data processing systems for this purpose, cf. § 25h section 2 KWG.

21 Cf. § 11 section 1 GwG.

22 BT-DrS 12/2704, p. 16.

23 *Diergarten/Barreto da Rosa*, Praxiswissen Geldwäscheprävention, 2015, chapter 1, marginal note 122.

24 § 24c KWG; about compliance with the constitution: BVerfG, NVwZ 2008, 547.

These measures are accompanied by individual bans on trading and transactions, some of them subject to administrative fines or punishable in law, such as terror sanction lists, used primarily for freezing the accounts of individuals or groups suspected of terrorism and their suspected supporters[25], trade sanctions according to the German Foreign Trade and Payments Law[26] or the certification system for uncut diamonds in the context of the so-called "Kimberley Process"[27]. Special reference should be made to one of the voluntary measures, something that is not legally required in Germany: fitting ATMs with dye packs.[28]

The measures aimed at actors in civil society as regards real currency transactions are already problematic because of their low level of practical effect[29] as compared with the costs arising and also on account of the concomitant widespread interference with fundamental rights. An additional factor, when looking at the field of virtual cryptocurrencies, is that their use does not depend on centrally organised bodies. Hence any requirement made of service providers in the market (e.g. exchange platforms) may be easily circumvented by criminal users due to the de facto limitless character of virtual cryptocurrency systems and the use of service providers who establish contact between private persons for the purpose of the exchange of virtual cryptocurrencies into real currencies[30].

2.3 Presentation of Possible Actions for Virtual Currencies

2.3.1 No (Mandatory) Regulation

Some parties do not think that a (mandatory) regulation of virtual cryptocurrencies is necessary. They argue, for example, that there is a low danger potential due to the low-level distribution of virtual cryptocurrencies.[31] A certain self-regulation of the innovative, rapidly developing systems is also thought to be possible.[32] Apart from mandatory regulation, it might be possible to regulate a framework for trust services for a voluntary certification of accounts belonging to trustworthy, identified users, modelled on the eIDAS Regulations[33].

2.3.2 Regulation

Theoretically, the possibilities for mandatory regulation comprise everything from a blanket ban to the integration into the classical regulations of the financial markets and right through to specific approaches geared to virtual cryptocurrencies. However, neither a blanket ban nor integration into classical regulations for the financial markets facilitates an efficient regulation of cryptocurrencies which is both compliant with the rule of law and effective.

25 Cf. UN Security Council Resolutions 1373 (2001) and 1390 (2002) as well as EC/EU Regulations No. 2580/2001, No. 881/2002, No. 753/2011 and No. 208/2014; infringements are punishable, cf. § 18 section 1 No. 1b AWG.

26 Cf. § 4 AWG.

27 Regulation (EC) No. 2368/2002.

28 Cf. http://www.mdr.de/nachrichten/vermischtes/farbpatronen-geldautomaten102.html (last access, as all following URLs which are not specially marked: 14.12.2016).

29 So in 2015 only about 2 per cent of the suspect notifications led to charges, summary punishment or sentences, cf. FIU Jahresbericht 2015, p. 19.

30 E.g. *localbitcoins*, https://localbitcoins.com/; cf. also 2.3.2.2.

31 Lerch, ZBB 2015, 190, 202.

32 *De Filippi*, Bitcoin: a regulatory nightmare to a libertarian dream, accessible at https://policyreview.info/articles/analysis/bitcoin-regulatory-nightmare-libertarian-dream (last access: 15.12.2016); *Doguet*, Lousiana Law Review Vol. 73, No. 4, 1119, pp. 1143 ff., accessible at http://digitalcommons.law.lsu.edu/cgi/viewcontent.cgi?article=6425&context=lalrev (last access: 15.12.2016).

33 Regulation (EU) No. 910/2014.

2.3.2.1 (No) Blanket Ban

The BITCRIME Project has set itself the task of developing regulatory approaches which go beyond blanket bans. The reasons for this are the intensity of the accompanying interference with fundamental rights and the displacement effects which are then to be expected. In contrast, any regulation practice which remains innovation-friendly will maintain the possibility of international links and will avoid any association with non-democratic states which operate restrictive regulation of virtual cryptocurrencies[34].

2.3.2.2 Inadequacy of Classical Money Laundering Prevention

The integration of virtual cryptocurrencies into the classical prevention method of money laundering is considered to be inadequate.[35] It would only be partially possible, and not very promising in the long run, to extend the classical system's identification (KYC)[36], monitoring and reporting requirements[37] to specific intermediaries. On the one hand evidence for money laundering with conventional money can hardly be transferred to virtual cryptocurrencies and, on the other hand, transferring such evidence without hesitation to virtual cryptocurrencies must be considered factually inappropriate: while the use of many different bank accounts may be an appropriate indication of money laundering, the use of many cryptocoin accounts by individual users is often even specified by the wallet software used and also advisable for reasons of personal data protection.[38] [39] Likewise for justified data protection reasons the use of anonymisation services cannot be seen as a sign of money laundering with virtual currencies. In contrast to classical banking activities, with virtual currencies this is not a case of disguising information from an individual financial intermediary with whom you have voluntarily entered into a business relationship, but the exercise of the fundamental right to informational self-determination in view of a transaction history which is public in principle.

In addition to this the decentralisation and pseudonymity of the networks prevent any effective implementation of existing regulatory approaches. In particular, anonymisation tools and private exchange platforms facilitate the circumvention of regulations by criminal users. Likewise the transfer of the KYC principle to specific intermediaries leads to a weakening of the protection of personal data of the – mostly – legitimate users who use the services of obligated intermediaries.[40] Applying classical prevention measures for money laundering to virtual cryptocurrencies is therefore both ineffective and places a heavy burden on legitimate users.

34 Such as China. European Parliamentary Research Service, Briefing 11/04/2014, Bitcoin—Market, economics and regulation, Annex B, accessible at http://www.europarl.europa.eu/RegData/bibliotheque/briefing/2014/140793/LDM_BRI(2014)140793_REV1_EN.pdf (last access: 13.12.16); Library of Congress, Regulation of Bitcoin in Selected Jurisdictions, accessible at https://www.loc.gov/law/help/bitcoin-survey/#china (last access 13.12.2016).
On regulatory framework in Russia *Tereshchenko/Nosova*, A concise history of the bitcoin ban in Russia, accessible at http://www.coinfox.info/news/reviews/5982-a-concise-history-of-the-bitcoin-ban-in-russia (last access 15.12.2016).

35 Cf. end of 2.2.

36 "Know your customer"= obligation of banking and similar institutions to identify their customers.

37 Cf. 2.2.

38 More on the right to informational self-determination 2.5.2.2.3.

39 On this cf. Bitcoin-Wiki, Address: „[…] a unique address should be used for each transaction. Most Bitcoin software and websites will help with this by generating a brand new address each time you create an invoice or payment request.", accessible at https://en.bitcoin.it/wiki/Address (last access: 15.12.2016).

40 *Pesch/Böhme*, DuD 2017, 93 (94 f., 98).

2.3.2.3 Systematisation of Specific Approaches

What is required is a form of regulation geared to the specific characteristics of virtual cryptocurrencies. Possible approaches may be differentiated according to the regulation's target groups, to starting and reference points as well as by the regulation having more precisely detailed terms.

2.3.2.3.1 Possible Target Groups

Various actors from the core and ecosystem[41] of virtual cryptocurrencies may be considered as possible target groups for regulation: in the core of decentralised systems the target group for regulation could only be the community of users. In concrete terms, miners may be obligated not to process any transactions in the blockchain which are linked to criminal activities, e.g. transactions of a victim of blackmail.[42]

Outside the core systems, the intermediaries of the ecosystems can be considered as the target group for regulation. The ecosystem comprises intermediaries who offer specific services relating to virtual cryptocurrencies, e.g. exchange platforms, wallet services and "payment services" providers. Regulation of intermediaries might by accompanied by a licence model.[43]

Finally, a system of approaches for indirect regulation of the core systems where external agents are enlisted is conceivable. Consideration could be given to an attempt to exert influence on the developers of the protocols on which the systems are based, for example by way of an international standardisation of blockchain technologies[44]. Equally, influencing miner behaviour might be possible by regulating mining pools[45] or by creating precursor products for mining. Another approach is close to this: proposing that the state acts directly as the dominant miner.

However, the idea that state bodies might be permanently able to break cryptographic algorithms and thus enable criminal prosecution, must be considered rather absurd.

2.3.2.3.2 Starting Point at Legal or Illegal Use (Whitelisting/Blacklisting)

Any specific regulation of intermediaries could either take legal or illegal use as its starting point. One starting point for regulation could be the identification of legitimate users (whitelisting). In particular, this could list accounts whose owners had been identified as trustworthy.[46] On this basis intermediaries could be urged to limit their business contacts to identified users.

In contrast to this are the approaches that start with the listing of criminal use in blacklists. On this basis intermediaries may be urged to avoid contact with specific criminal activities.

2.3.2.3.3 Reference Point for Blacklists: Accounts or Transactions

Various reference points may be considered for blacklists. On the one hand, accounts may be listed which are connected to illegal activities, linked to the requirement that intermediaries addressed should not accept the cryptocoins allocated to the listed accounts (as payment).

41 On agents cf. also 1.2. with fig.

42 So-called Redlisting, *Dinesh/Erlich/Gilfoyle/Jared/Richard/Pouwelse*, Operational Distributed Regulation for Bitcoin, 2014, p. 4, accessible at https://arxiv.org/pdf/1406.5440.pdf (last access: 14.10.16).43

43 More on flanking license model in 2.5.1.

44 ISO/TC 307 Blockchain and electronic distributed ledger technologies, accessible at http://www.iso.org/iso/home/standards_development/list_of_iso_technical_committees/iso_technical_committee.htm?commid=6266604 (last access: 15.12.2016).

45 Mining-pools usually are centrally organised associations of users who pool computer power for mining in proof-of-work systems such as Bitcoin. On Proof of Work cf. 1.2.

46 For example by the trust services named in 2.3.1.

On the other hand, it might be possible to list concrete transactions, linked to the requirement that intermediaries addressed should not accept the cryptocoins coming from these transactions (as payment). This would also capture all follow-up transactions. It would be possible in this case to admit the exchange of cryptocoins originating from listed transactions by licensed intermediaries subject to certain specified conditions.[47]

2.3.2.3.4 Blacklist Principles and Mixing Issues

If blacklists start from transactions, the question arises how one should deal with transactions where cryptocoins from incriminated transactions affected by a blacklisting are mixed with other ("clean") cryptocoins. In concrete terms, the exchange of partly incriminated cryptocoins into state currency could be permitted for specific licensed intermediaries, subject to specific conditions.[48] Various policies are possible in this context:[49] On the one hand, the inclusion of incriminated cryptocoins could always result in the invalidation of the entire amount transferred so that an exchange would always be made impossible. On the other hand, a part invalidation of the amount of cryptocoins transferred might be possible. One option would be to devaluate all cryptocoins transferred in the transaction proportionally to the amount of incriminated cryptocoins (the haircut model). Alternatively, the policy could be tied to the transaction structure so that by designing the transaction in a particular way the risk could be shared between sender and recipient (the seniority model).[50]

2.3.2.3.5 Accessibility of Blacklists

For a regulation based on blacklists the further question arises as to which actors should be able to access the lists. On the one hand, it would be possible only to provide the blacklists to the obligated intermediaries, and to provide information about specific cryptocoins to individual users only upon proof that they are personally concerned. On the other hand, blacklists could be public so that individual users could simply check whether specific cryptocoins are affected by a blacklisting.

2.4 Preferable: Transaction Blacklists

A regulation of specific intermediaries based on public transfer blacklists is best suited for the prevention of crime linked to virtual cryptocurrencies. At the same time transaction blacklists place the least burden on legitimate users and thus the requirement of proportionality is fulfilled.

2.4.1 Necessity of Mandatory Regulation

Mandatory regulation is necessary. Approaches based on voluntary self-control and regulation are not suitable for the prevention of criminal transactions. Criminal actors in particular, and also the victims pressurised by them – e.g. in blackmail cases – are not likely to pay much attention to merely voluntary regulations.[51] Waiving a regulation because of the currently quantitatively low level of potential danger would lead to a perpetuation of virtual spaces without effective regulation where legitimate users are not protected against specific forms of crime. In particular in

47 More on the exchange of incriminated cryptocoins by licensed intermediaries in 2.3.2.3.4. and 2.5.1.

48 More on the flanking license model in 2.5.1.

49 All named policies are described in *Möser/Böhme/Breuker*, in: Böhme/Brenner/Moore/Smith, Financial Cryptography and Data Security, 1st Workshop on Bitcoin Research (FC 2014), Barbados, Berlin et al. 2014, pp. 21 f.

50 Because virtual cryptocurrencies differ in organisation and in transaction format, a seniority model would have to be designed for each cryptocurrency to be regulated. For Bitcoin cf. *Pesch/Böhme*, DuD 2017, 93 (97).

51 On the (doubtful) criminality of victims of blackmail with ransomware cf. *Salomon*, MMR 2016, pp. 575 ff.
Eikenberg, Krypto-Trojaner Locky wütet in Deutschland: Über 5000 Infektionen pro Stunde, accessible at http:/www.heise.de/security/meldung/Krypto-Trojaner-Locky-wuetet-in-Deutschland-Ueber-5000-Infektionen-pro-Stunde-3111774.html (last access: 14.10.16); McMillan, In the Bitcoin Era, Ransomware Attacks Surge, accessible at http://www.wsj.com/articles/in-the-bitcoin-era-ransomware-attacks-surge-1471616632 (last access: 15.12.2016).

view of the frequency of blackmail cases[52] regulation is urgently required. Currently perpetrators can extort cryptocoin sums and exchange them for conventional currencies while completely avoiding any risk of being called to account.

2.4.2 Evaluation of Specific Approaches

Because all regulatory approaches involve possible interference with the fundamental rights of affected actors, their evaluation depends primarily on their suitability for achieving the basic legal goal of preventing virtual currency criminality; in addition it is necessary that there not be any more lenient, but equally effective, regulatory methods and that interference with fundamental rights be proportionate, also in the narrower sense.[53]

2.4.2.1 Target Groups

The only promising regulation is one that addresses specific intermediaries from the ecosystems. Obligating ordinary core system users would be difficult to enforce due to their pseudonymity. The same applies for a regulation of the development of the protocols which are only relevant if they are used by the majority of the members of the specific decentralised user community.[54] In contrast, the intermediaries are generally actors with a known identity against whom regulation underpinned by sanctions can be effectively enforced.

Attempts to indirectly influence the core system by regulating the intermediaries would, however, not be expedient. It would indeed be conceivable to enforce approaches relating to cryptocoin mining for cryptocurrencies based on proof of work[55] because, in the case of mining pools, the intermediaries involved in mining and the producers of precursor products for mining, concrete intermediaries would be available. But the weakness of this approach – over and above concomitant interference with freedom of information[56] and possibly with freedom of profession[57] – lies in the practical reason that it is not difficult to design alternative virtual cryptocurrencies where mining regulations are not effective.[58] Thus the regulation could be circumvented by changing the respective protocols or by switching to similar alternative systems. The same applies to regulation via dominant participation of state bodies as miners. Effective regulation of virtual cryptocurrencies can therefore only be assured by the regulation of specific intermediaries, which is largely independent of the technical details of the respective networks.

2.4.2.2 Whitelisting/Blacklisting

For the question as to whether blacklisting or whitelisting approaches are preferable for a regulation targeting intermediaries the respective suitability of each type of approach must be considered: approaches based on documenting legitimate,

52 The requirements at EU level in concrete terms in Guideline ECB (EU) 2016/680.

53 *Grzeszick*, in Maunz/Dürig, GG-Kommentar, 77. EL, Art. 20, marginal notes. 107, 110 ff.; Jarass, EU Charter of Fundamental Rights, 2nd edition, 2013, art. 52, marginal notes 35 ff.; *Harris/O'Boyle/Warbrick*, Law of the European Convention on Human Rights, 3rd edition 2014, pp. 519 f. In-depth treatment of the fundamental rights aspects of the recommended approach using blacklists 2.5.2.

54 *Pesch/Böhme*, DuD 2017, 93 (98).

55 About Proof-of-Work for Bitcoin cf. 1.2.

56 For the European level Rückert, Virtual Currencies and Fundamental Rights, pp. 26 ff., https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2820634.

57 Many commercial intermediaries are involved in mining. On the freedom of profession of intermediaries on a European level *Rückert*, Virtual Currencies and Fundamental Rights, pp. 23 f, https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2820634.

58 Updating of authenticated data structures such as the blockchain may also be secured in other ways than by stipulating a proof of work, cf. https://en.bitcoin.it/wiki/Proof_of_Stake (last access: 14.10.16). Without the stipulation of the proof of work characteristic for Bitcoin, profitable mining needs neither special hardware nor pooling of computer power so that there are hardly any tangible targets for regulation.

identified users or their accounts are hardly suitable for preventing illegal usage. A blackmail victim will always initiate a transaction to the account named by the blackmailer irrespective of whether this account is linked to an identifiable natural person or not. A further argument against whitelisting approaches is the intensity of the accompanying interference with the users' right to informational self-determination.[59] Blacklisting, i.e regulation using blacklists, is preferable.

2.4.2.3 Reference Point

The choice of the point of reference is decisive for the effectiveness of blacklists. Listing concrete accounts does not make for effective regulation because any amount of accounts may be generated in a decentralised manner. Criminal users could circumvent the listing of their account by generating a new one, transferring their cryptocoins to the non-listed new account and then exchanging them without any difficulty.

But when transactions are blacklisted this loophole does not exist. Because the public blockchain provides the possibility of documenting follow-up transactions, the exchange of incriminated cryptocoins may still be prevented after transfer to other accounts.

2.4.2.4 Accessibility of Blacklists

The question as to whether or not blacklists should be publicly accessible must be decided with consideration of the disadvantages arising for the people concerned both as regards public and non-public access. On the one hand, public blacklisting could entail damage to the reputations of bona fide owners of listed cryptocoins. This is even more problematic for provisional listings.[60] On the other hand, whenever blacklists are not public, ordinary users will not have the opportunity to avoid accepting listed cryptocoins by comparing them with a blacklist. A consideration of competing interests is helpful here. The interest in avoiding damage to reputations is secondary to the interest of other users receiving cryptocoins which are not affected by a blacklisting. In this context it is also material that blacklisting, as additional information about the accounts involved in the transaction, does not significantly increase the danger that third parties may link this (transaction) to any individual person. Thus the burden on the persons involved is no higher than it is with any other criminal investigation based on suspicions and the legal consequences of a conviction. Reasonable users are thus aware of the fact that transactions may be linked to criminal activities on the basis of the public transaction history by linking them to other public information. Conversely it must be taken into account that in the case of non-public blacklists there would need to be an authority which would process specific blacklist enquiries by entitled persons and which thus after a short time would possess additional information about various accounts whose owners would then be exposed to the danger of being identified. Thus non-public blacklists would be associated with a high risk of abuse.[61]

2.5 Design of a Regulation Based on Transaction Blacklists

2.5.1 Basic Principle/Policy

What is recommended is the introduction of blacklists following the principle of transaction blacklisting, accompanied by the obligation of specific intermediaries (such as exchange platforms, "payment services") not to accept cryptocoins originating from listed transactions. Violation of this obligation should be sanctioned as a criminal or administrative offence.

59 *Pesch/Böhme*, DuD 2017, 93 (94 f., 98).

60 Cf. 2.5.2.4.

61 In principle, it would be thinkable to reduce this risk by using modern cryptography. Such approaches are subject to current academic research. Their use in regulatory practice has hardly been tested so far.

Whenever incriminated and non-blacklisted cryptocoins are mixed in one transaction it would be preferable to only partially invalidate the transferred amount.[62] The exchange of only partially incriminated cryptocoins into real currency must then be permitted. In the interest of effective financial supervision this should, however, only be possible with specific licensed intermediaries. Regulation via blacklists must, therefore, also be accompanied by a licensing model.[63]

2.5.2 Legal Framework and Implementation

The following section is concerned with the legal framework of legislative implementation of the solution using transaction blacklists on a national level. In addition to general questions such as the legislative power of the federal legislator (2.5.2.1) and the fundamental rights affected by the regulation (2.5.2.2), considerations of the proportionality principle will be looked at and the necessary protection mechanisms (2.5.2.3) arising will be addressed. Finally the necessity of a possible provisional blacklist in investigative procedures (2.5.2.4) and the interaction between the suggested regulation concept and material money laundering offences according to § 261 StGB (German Criminal Code) will be addressed (2.5.2.5).

2.5.2.1 Legislative Competence of the Federal Legislator

The legislative competence of the federal legislator for the approach suggested here stems from article 74 section 1 No. 11 GG (German Basic Law). According to this the federal legislator is responsible for security legislation which addresses the economy or individual sectors of the economy.[64] The suggested blacklist approach obligates those intermediaries of the cryptocoin ecosystems[65] who commercially exchange cryptocoins for goods, services or real currency units (similar to the GWG – Money Laundering Act] and the KWG (German Banking Act) which also contain statutory security requirements).[66] Because virtual cryptocurrency systems are unbound and because, therefore, any blacklists must be as widely uniform as possible, the preconditions of article 72 section 2 GG are fulfilled.[67]

Insofar as the law (as recommended) also contains sanctions from criminal and administrative law with which to enforce its prohibitions, the legislative competence of the federal legislator as per article 74 section 1 no. 1 GG.[68] obtains.

Finally, because of the international cooperation as recommended here[69] for the enforcement of uniform blacklists, legislative power obtains on the basis of article 73 section 1 no. 10 var. 3 GG (international fight against crime).

62 Cf. 2.5.2.3.3. and 2.5.2.5.

63 On the basic design of a licensing obligation for such intermediaries cf. 2.5.3.

64 BVerfGE 8, 150; Example: Trade Law, cf. BVerfGE 41, pp. 351 f; in contrast, the legislation regulating casinos is not within the legislative power of the federal legislator, cf. BVerfGE 28, 146; cf. also *Maunz*, in: Maunz/Dürig, GG-Kommentar, 77. EL 2016, Art. 74 marginal note 151, marginal note 44; the federal states would only have the power to legislate for security legislation addressing all and sundry or target groups outside the economy, cf. BVerfGE 3, 433; 8, 150; *Maunz*, in: Maunz/Dürig, GG-Kommentar, 77. EL 2016, article 74 marginal note 151, marginal note 44.

65 On this: *Möser/Böhme/Breuker*, in: Böhme/Brenner/Moore/Smith, Financial Cryptography and Data Security, 1st Work shop on Bitcoin Research (FC 2014), Barbados, Berlin et al. 2014, p. 16, (pp. 17 f.).

66 On GWG: BT-DrS 17/10745, pp. 11 f.

67 Cf. BVerfGE 106, 62 (pp. 145); 110, 141 (pp. 174); 112, 226 (pp. 248); 138, 136 (pp. 176); BVerfG NJW 2015, 2399 (2402); cf. also BVerfGE 111, 226 (p. 254); 122, 1 (pp. 21); 125, 141 (pp. 155); 135, 155 (p. 204); comprehensively: *Uhle*, in: Maunz/Dürig, GG-Kommentar, 77. EL 2016, article 72 marginal notes 142, 152 with further references; cf. also BVerfGE 126, 331 (357), here in the context of the tradability of assets, the requirement of a uniform regulation for the Federal Republic was affirmed.

68 For correspondence to GWG cf.: BT-DrS 17/10745, pp. 11 f.

69 On this cf. 2.6.

2.5.2.2 Interference with Fundamental Rights

Installation of a system of transaction blacklists interferes with various constitutionally protected interests of persons participating in virtual cryptocurrency systems. Thus by prohibiting the acceptance and exchange of cryptocoins which can be traced back to a listed transaction, the actual owner will experience a value loss respective to these cryptocoins. This constitutes an interference with the property rights of the user (2.5.2.2.1), while prohibiting the acceptance and exchange affects the freedom of profession of the intermediaries (2.5.2.2.2). The collection and processing of blockchain data which is necessary for the recalculation of the blacklist state of subsequent transactions / cryptocoins interferes with the affected users' right to informational self-determination (2.5.2.2.3). However – and this might be different in the case of a complete ban or a restriction of access – there is no interference with the freedom of association. An interference with freedom of expression and information seems possible, however, but is of secondary importance (2.5.2.2.4).

2.5.2.2.1 Property Rights of Users

The de facto possibility of disposing of cryptocoins when in possession of the private key linked to the respective public key is an asset covered by the constitutional concept of property as in article 14 section 1 GG. According to prevailing opinion, this comprises the right to possess and use a specific object.[70] The concept of property also comprises real rights and rights *in personam* under private law.[71] In the case of intangible assets it is decisive that they are "due the holder of the right in the nature of an exclusive right, based on his own efforts and serving as the material basis for personal freedom"[72]. This comprehensive interpretation also comprises cash and bank deposit money, since an essential guarantee of freedom of property is constituted by the freedom to be able to exchange money against material goods (and vice versa).[73] Article 14 GG, however, only guarantees the institution of money and its individual assignment, not the value of the money as such, since this latter is subject to factors outside state control.[74] In the case of the complete deprivation of an asset or of this asset's substantial devaluation the Federal Constitutional Court has ruled that an interference with this right is to be affirmed.[75]

Cryptocoins are neither goods, because this would presuppose their physicality, nor are they receivables,[76] for this would presuppose a legal transaction between debtor and creditor governed by the law of obligations, from which the creditor can demand something from the debtor, cf. § 241 section 1 BGB.[77] In contrast to bank deposit money (§ 675t section 1 BGB)[78] there are no *in personam* relationships in

70 *Paper*, in: Maunz/Dürig, GG-Kommentar, 77. EL 2016, article 14 marginal note 8; *Wendt*, in: Sachs, GG-Kommentar, 7th edition 2014, article 14 marginal note 21 with further references.

71 BVerfGE 74, 129 (148); *Hofmann*, in: Schmidt-Bleibtreu/Hoffmann/Hopfauf, Kommentar zum Grundgesetz, 13th edition 2014, article 14 marginal note 14.

72 BVerfGE 97, 350 (371); cf. also BVerfGE 40, 65 (pp. 82); 69, 272 (300); 70, 278 (285); with further references to court decisions.

73 BVerfGE 97, 350 (371); *Paper*, in: Maunz/Dürig, GG-Kommentar, 77. EL 2016, article 14 marginal note 162; *Hofmann*, in: Schmidt-Bleibtreu/Hofmann/Henneke, GG-Kommentar, 13th edition 2014, article 14 marginal note 13.

74 For the entire topic cf.: BVerfGE 97, 350 (371); 105, 17 (30); *Hofmann*, in: Schmidt-Bleibtreu/Hofmann/Henneke, GG-Kommentar, 13th edition 2014, article 14 marginal note 13.

75 BVerfGE 105, 17 (31).

76 *Kütük/Sorge*, MMR 2014, 643 (644); *Boehm/Pesch*, MMR 2014, 75 (77); *Rückert*, MMR 2016, 295 (296).

77 On the concept: *Bachmann*, in: Münchener Kommentar BGB, 7th edition 2016, § 241 marginal note 6; *Rückert*, MMR 2016, 295 (296).

78 *Sprau*, Palandt Kommentar BGB, 76th edition 2015, § 675t marginal note 4.

cryptocoin networks since there are no central administrative bodies.[79] Neither do cryptocoins constitute any other rights, since these presuppose that the owner can demand a specific behaviour (even if only refraining from a specific action) from one or several debtors.[80] But the "holder" of cryptocoins cannot demand anything from any other individual.[81] His asset consists solely in the de facto power of use of the private key which in actual fact enables him to transfer cryptocoins.[82] However, while the market assigns a (fluctuating) value to this de facto power of disposition, no right arises from this.[83]

But cryptocoins do indeed fulfil all the requirements necessary for the integration of intangible assets into the scope of protection under article 14 GG[84]: First of all, cryptocoins are accurately definable and identifiable objects.[85] Due to the traceability of all transactions in the blockchain, at any one time, it is possible to determine exactly which cryptocoins are assigned to which public key. Furthermore, the "holder" of the cryptocoins which are assigned to a specific public key – as long as he makes sure that he has the only copy of the corresponding private key – can exclude all other persons from using these cryptocoins.[86] In contrast to other virtual currencies which are administered by a centralised system / a central location (such as e.g. WoW Gold or Linden-Dollar) cryptocoins, due to the peer-to-peer structure of the network and the publicly accessible blockchain, cannot be simply deleted and thus have a certain permanence. Furthermore, cryptocoins have a market value and their ownership is based on personal input (mining or purchase with one's own funds). Finally, cryptocoins (independently of their exact but purely legal qualification) do to a certain extent fulfil the function of "money replacement" (you can purchase goods and services with them, exchange them and transport or store their value)[87] and are considered as "units of account" by the BaFin (Federal Financial Supervisory Authority) in the sense of § 1 section 11 no. 7 alt. 2 KWG.[88]

Transaction blacklists would not only impair the exchange value of cryptocoins, they would also result in a substantial devaluation. The goal of this approach would be to completely prohibit the exchange of listed cryptocoins to real currency or goods and services. This would mean that at least those cryptocoins originating from the originally incriminated and then marked-up transaction are to be considered

79 *Rückert*, MMR 2016, 295 (296).

80 *Grüneberg*, Palandt Kommentar BGB, 76.th edition 2015, statement of § 241 marginal note 5.

81 *Rückert*, MMR 2016, 295 (296).

82 *Rückert*, MMR 2016, 295 (296).

83 On the entire topic: *Rückert*, MMR 2016, 295 (296).

84 On the preconditions in the "Virtual Property" debate (definability, permanence, excludability, interconnectivity, market value): *Fairfield*, Boston University Law Review 2005, Vol. 85, p. 1047 (p. 1053); *Erlank*, Potchefstroom Electronic Law Journal 2015, Vol. 18, No.7, p. 2525 (pp. 2540 f); *DaCunha*, Akron Intellectual Property Journal, Vol. 4, No. 1, p. 35 (pp. 41 ff.); *Tsukerman*, Berkeley Technology Law Journal 2015, Vol. 30, p. 1128 (pp. 1145 ff.); comprehensive treatment for protection of property through European fundamental rights: *Rückert*, Virtual Currencies and Fundamental Rights, pp. 20 ff., https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2820634.

85 About the criterion of definability: *Berberich*, Virtuelles Eigentum, p. 108; cf. also the "Who owns what" concept of Fairfield, BitProperty, Southern California Law Review 2015, Vol. 88 (Forthcoming), p. 9, accessible at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2504710; Rückert, Virtual Currencies and Fundamental Rights, p. 22, https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2820634.

86 About the criterion of definability: *Berberich*, Virtuelles Eigentum, p. 108; cf. also the "Who owns what" concept of *Fairfield*, BitProperty, Southern California Law Review 2015, Vol. 88 (Forthcoming), p. 9, accessible at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2504710; *Rückert*, Virtual Currencies and Fundamental Rights, p. 22, https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2820634.

87 On the equal value of money and tangible property: ("coined liberty"): BVerfGE 97, 350 (371).

88 *Münzer* (BaFin), Bitcoins: Aufsichtliche Bewertung und Risiken für Nutzer, https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2014/fa_bj_1401_bitcoins.html; *Auffenberg*, NVwZ 2015, 1184ff.; *Sorge/Krohn-Grimberghe*, DuD 2012, 479 (484).

as completely invalidated before they might be mixed with "clean" cryptocoins in further transactions. In the case of mixing with other cryptocoins in further transactions then – depending on the policy chosen[89] – there would at least be a (substantial) partial devaluation. The question as to above which degree of mixing this mixing would no longer be considered "substantial" cannot be definitively answered here. This is, however, not necessary for assessing a (hypothetical) transaction blacklist law, precisely because this would not address concrete cases.

The conclusion is, therefore, that interference with article 14 GG must be affirmed. For cases below the substantial devaluation limit, there remains the (subsidiary) interference with article 2, section 1 GG which also protects the freedom of economic activity and property as such.[90]

Interference through transaction blacklists must be classified here as a "substantive and boundary definition of property", in the sense of Article 14 section 1 sentence 2 GG, since regulation via blacklists determines the boundaries of (constitutionally guaranteed) ownership of cryptocoins in a general and abstract manner and is valid for all persons.[91] It does not become an expropriation in the sense of article 14, section 3 GG by deprivation of concrete assets, either completely or partially. Expropriation could only be posited if the transaction blacklists were to be qualified as a state measure with the purpose of complete or partial deprivation of property for public acquisition for implementation of concrete public goals.[93] This is obviously not the case, since the listed cryptocoins are only invalidated, either completely or in part, but are not benefiting the state sector.

2.5.2.2.2 Freedom of profession for Intermediaries

The obligation of intermediaries not to exchange listed cryptocoins constitutes an interference with their freedom of profession. An occupation in the sense of article 12n section1 GG is "any permanent and not merely temporary activity serving the creation and maintenance of a livelihood"[94]. Protection under article 12 GG is also independent of any possible obligation to obtain authorisation, since, according to recent court decisions, only such activities are excluded "which by their very nature must be considered prohibited, because due to their harmful effect on society and community they must absolutely not enjoy protection by the fundamental right of the freedom of profession"[95]. Thus commercial trading with virtual currencies is covered, as is trading with goods or the provision of services, when virtual cryptocurrencies are accepted as the means of payment.

The obligation to comply with the blacklist does not entail any limitation of the choice of occupation, but merely constitutes a regulation concerning the practice of a profession.[96]

89 On this cf. 2.3.2.3.4.

90 Cfl. BVerfG NJW 1994, 1784; *Di Fabio*, in: Maunz/Dürig, GG-Kommentar, 77. EL 2016, article 2 marginal note 93 ff. with further references to case law and literature.

91 Cf. BVerfGE 52, 1 (27f.); 58, 137 (pp. 144); 58, 300 (330); 70, 191 (200); 72, 66 (76); 100, 226 (240); cf. in particular BVerfG NJW 2004, 2073 (2077) on (extended) forfeit.

92 Cf. BVerfGE 58, 300 (351); 70, 191 (199 f.); 83, 201 (211 f.); 100, 226 (240); cf. in particular BVerfG NJW 2004, 2073 (2077) on (extended) forfeit.

93 BVerfGE 52, 1 (27); 58, 300 (330 f); 70, 191 (199 f); 74, 264 (280); 79, 174 (191); 83, 201 (211); 102, 1 (pp. 15 f); 104, 1 (9); cf. also paper in: Maunz/Dürig, GG-Kommentar, 77. EL 2016, article 14 marginal note 527.

94 *Scholz*, in: Maunz/Dürig, GG-Kommentar, 77. EL 2016, article 12 marginal note 29; cf. also BVerfGE 7, 377 (397); 9, 73 (78); 13, 97 (106); 14, 19 (22); 16, 147 (163); 50, 290 (362 f); 68, 272 (281); 97, 228 (252 f); 105, 252 (265); 110, 141 (156); 111, 10 (28).

95 BVerfG, NJW 2006, 1261 (1262) = BVerfGE 115, 276.

96 On the basic (meanwhile slightly "eroded") systematic tiers defined by the BVerfG cf.: BVerfGE 7, 377; as well as on development cf. *Scholz*, in: Maunz/Dürig, GG-Kommentar, 77. EL 2016, article 12 marginal note pp. 335 with further references.

As far as the obligation to obtain authorisation in the context of a licensing model is concerned a differentiated approach is called for: insofar as the authorisation to provide a service for the exchange of real currency into virtual cryptocurrencies is concerned, this constitutes a subjective restriction of professional licensing. In contrast the obligation to obtain an authorisation for traders who want to accept virtual cryptocurrencies as an alternative means of payment is only formally a subjective regulation concerning the practice of a profession, because it merely regulates the payment modalities for commercial trade. De facto, however, it has the same affect as a subjective restriction of professional licensing, since the trader de facto will not be able to exercise a part of the occupation sought by him (i.e. the exchange of goods for virtual cryptocurrencies) without this licence.

From considerations of the proportionality principle and in order to safeguard a certain comparability to the persons obligated by the GWG (Money Laundering Act) and KWG (Banking Act) the necessity of a licence should be limited to those actors who commercially exchange real currencies for virtual cryptocurrencies. Commercial traders would merely have to comply with the blacklists, but not need a licence.

Because exchange platforms – unlike banks in the real currency system – do not as a rule invest customer money, the requirement of a general credibility check as stipulated in commercial law is considered sufficient. In addition, the applicant must merely give proof of the implementation and use of data processing systems for access to the blacklist. Because no customer money is invested it also seems very doubtful whether the previous subsumption of virtual cryptocurrencies under the concept of "units of account" in § 1 section 11 no. 7 alt. 2 KWG and the ensuing comprehensive needs for licences with high requirements according to §§ 32 ff. in conjunction with § 1 section 1, section 1a KWG are proportionate from the perspective of the freedom of occupation for (mere)[97] providers of exchange platforms.

2.5.2.2.3 Informational Self-Determination of Users

Data collection and processing by the (state) operator of the blacklist services while entering transactions on the blacklist and updating the blacklist state of transactions going back to a listed transaction furthermore constitutes an interference with the rights to informational self-determination (RiS). This protects the right of individuals to determine which of their personal data are disclosed and used.[98] According to § 3 section 1 BDSG (German Federal Data Protection Act) personal data are particulars about personal or factual circumstances of a specific identified or identifiable natural person. These data also include information about accounts and deposits as well as about payment transactions.[99] In this context, due to modern possibilities of data linkage, an unambiguous personal reference is not (or no longer) necessary.[100] Data which may at first sight have very little information content can, by linkage to other data, result in a concrete danger to personal rights and the freedom of conduct.[101] Therefore, the RiS also covers pseudonymised data, particularly when, because of modern possibilities of linkage with further data sets, it might be possible to decipher pseudonyms.[102]

97 This is, of course, different if the service provider actually invests customer money.

98 BVerfGE 65, 1 (43); 78, 77 (84); BVerfG, NJW 2001, 879 (880); BVerfG, EuGRZ 2001, 249 (252);*Di Fabio*, in: Maunz/Dürig, GG-Kommentar, 77. EL 2016, article. 2 marginal note 175.

99 BVerfG NJW 2007, 2464.

100 BVerfGE 120, 274 (312).

101 BVerfGE 118, 168, 184 f; BVerfGE 120, 274, 312; cf. also BVerfGE 65, 1, 45; *Heußner*, BB 1990, 1281, 1282; *Di Fabio*, in: Maunz/Dürig, 75. EL Sept. 2015, article 2 marginal note 5.

102 For concepts cf. § 3 sections 6 and 6a BDSG.

Neither does the public accessibility of data in the blockchain preclude interference with the RiS from the start, since for the processing to update the blacklisted state of the blockchain, data are specifically collected, stored and evaluated using further data (those from which an incriminated origin may be derived).[103] Depending on the technical design of the updating of the blacklisted state of the transactions in the blockchain this might even turn out to be a permanent "monitoring" (in the sense of a non-indicated and automated search according to given characteristics or conspicuous features) or data retention.

Because the data are publicly accessible and pseudonymous and because of the purpose of processing, which is precisely not aimed at allocating the data to an individual user, this interference will, of course, be of a very low intensity.

2.5.2.2.4 Other

There is no interference with the freedom of virtual association (whose existence and basis in itself is rather controversial)[104] according to article 9 section 1 GG, since neither the system as such is affected nor is user access frustrated or blocked.

The same applies to interference with the freedom of expression and information (article 5 section 1 GG), because neither the circulation of nor access to information from the network is affected by transaction blacklists.[105] There is no conflict between a regulation via transaction blacklists and the fault principle (article 1 section 1, 20 section 3 GG) and the presumption of innocence (article 20 section 3 GG, article 6 section 2 ECHR), because it neither contains a judicial ascription of guilt nor is its purpose aimed at punishment or measures of a punitive character (but rather at prevention) and does not result in allegations[106] against the persons involved – unless they are involved in criminal activity.[107]

2.5.2.3 Proportionality and Necessary Protective Mechanisms

2.5.2.3.1 Proportionality in Comparison with Other Regulatory Possibilities

In comparison with other regulatory possibilities transaction blacklisting has a higher level of effectiveness while at the same time resulting in less interference with fundamental rights. A blanket ban – which would also result in an unacceptable innovation disadvantage for Germany as an economic and technological location – could be difficult, if not impossible, to enforce; it would also constitute a disproportionate interference with the fundamental rights named above. Application of conventional KYC measures on the one hand – because of the customers' obligation to identify themselves and due to continued public accessibility of all financial transactions – would constitute a serious interference with the right to informational self-determination. On the other hand, they are easy to circumvent and thus have only limited efficiency. In comparison to whitelisting approaches transaction blacklisting is less invasive, because the former also – and in particular – affect legitimate users and, in the end, come down to a ban subject to authority approval, while the latter would only concern criminal users and individual legitimate users.

103 Cf. BVerfGE 120, 274, 345.

104 On a national level cf.: *Luch/Schulz*, MMR 2013, 88 (90); *Möhlen*, MMR 2013, 221 (228); on a European level cf. *Rückert*, Virtual Currencies and Fundamental Rights, pp. 25 f, SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2820634 with further references.

105 On possible restrictions by other regulation scenarios and on the European dimension cf.: *Rückert*, Virtual Currencies and Fundamental Rights, pp. 26 ff., SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2820634 with further references.

106 For accomplices this constitutes no interference for the simple reason that their guilt will be ascertained in a proper trial under the application of the presumption of innocence, cf. 2.5.2.3.3.

107 Cf. BVerfG, NJW 2004, 2073 with similar, detailed considerations on extended forfeit.

2.5.2.3.2 Necessity of Protective Mechanisms to Safeguard Proportionality

Due to partly substantial restrictions of fundamental rights, legal protection mechanisms must be guaranteed to safeguard proportionality. In particular the (partial) devaluation of virtual cryptocurrency units for non-accomplices in any criminal activity by continuation of the blocking state to transactions originating from a listed transaction constitutes a serious restriction of the property rights of non-accomplice users. The relevance is further increased if the incriminated transaction (due to the duration of investigations and the legal process) is only blacklisted long after its implementation and the further transfer of the respective cryptocoins. Existing tools for invalidating or expropriating incriminated assets – expropriation and forfeit according to §§ 73 ff. StGB (German Criminal Code) – is limited in its scope of application to objects which the perpetrator or participant owns or is entitled to. Exceptions are only granted in cases of culpability of the non-accomplice (e.g. granting the object by third parties in full cognizance of the facts, perpetrator acting for a third party) or if a risk results from the object. These limitations are considered necessary by the courts in order for norms to be compliant with the constitution.[108] In this respect transaction blacklisting comprises a new and serious dimension of interference. This is indeed justifiable and acceptable in view of the limited nature of effective regulatory options due to the special technical characteristics (mainly pseudonymity and decentralisation) of virtual cryptocurrencies and the significantly more serious interferences caused by blanket ban and whitelisting approaches. But it does necessitate the creation of effective protection mechanisms to safeguard the proportionality principle.

2.5.2.3.3 Individual Protective Mechanisms

First of all, the conditions for blacklisting a transaction must be worded as specifically as possible. Here reference to the norm of § 73 section 1 sentence 1 StGB (conditions for forfeit) would suggest itself: "If a criminal act was committed and the perpetrator or accomplice has received virtual cryptocurrency units (cryptocoins) for or from this act, the court shall rule that the transaction through which the cryptocoins were received, or from which they originate, shall be included in the blacklist." Since inclusion in the blacklist for crime prevention is only necessary if the cryptocoins received cannot be levied from the perpetrator or accomplice at the time of sentencing (e.g. because they have already transferred them on or because they refuse to surrender the private keys[109]), inclusion in the blacklist must be limited to these cases or the forfeit (not the forfeit of value replacement if the perpetrator can later access the cryptocoins) must be given legal priority. As far as the timing of an inclusion in a blacklist is concerned, the principle of the rule of law and the proportionality principle would demand that in principle this must only be effective when the final judgement comes into force (similarly, that is to say, as in cases of forfeit and expropriation).[110]

Furthermore, the material scope of application of the transaction blacklist should (initially) remain limited to the list of offences in § 261 section 2 StGB. On the one hand this gives criminal investigation and security authorities an effective tool

108 BGHSt 1, 351 (354 f); 2, 311 (pp. 312 f); 19, 123 (125 f); 21, 66 (pp. 67 ff.).

109 On this cf. the case of BGH NJW 2015, 3463; here, one of the defendants had refused to surrender the private keys for a (large) share of the bitcoins received so that only a forfeit of value replacement could be declared.

110 On "provisional" listings in investigative procedures which are nevertheless necessary and possible cf. 2.5.2.4.

for fighting organised (financial) crime and on the other hand it limits interference with the fundamental rights of non-accomplices, in compliance with the proportionality principle. In view of the serious nature of interference with fundamental rights, any extension of the set of standards should be undertaken only after careful consideration and only in cases of empirically proven necessity.

In order to reduce the intensity of interference, particularly for non-accomplices, it is necessary to make the blacklist publicly accessible for all users of the respective cryptocurrency system. Thus users may adapt their user behaviour to the changed legal situation (by not accepting cryptocoins from listed transactions or from transactions originating from listed transactions, as fulfilment of an obligation). A further reduction of the intensity of the interference for non-accomplices must be achieved by ensuring that the blacklisting system applies a haircut policy or a seniority model for mixing incriminated and non-incriminated cryptocoins in follow-up transactions.[111]

Finally, individuals concerned must be sufficiently protected by legal remedies as well as hardship and indemnity clauses. Legal remedies for the defendants can here be safeguarded by the procedural rules of the criminal trial. For non-accomplices special subsequent proceedings modelled on § 439 StPO (Criminal Procedure Code) are required. Hardship and indemnity clauses must be created in particular for all cases where (cumulatively) a significant loss in value is impending for a non-accomplice and the latter has used all reasonable measures to check the transaction in question for a possible incriminated origin – including using risk analysis providers, both existing or to be established.

In order to exclude data misuse and to justify data retention it will be necessary to limit the storage and processing purpose of data to the operation of the blacklisting system.

Finally, data protection and data security standards at the operator of the blacklisting service and at the data providers which provide information about the blacklisting state of transactions must be guaranteed by law in order to avoid data misuse and false entries. This could be modelled on the legal requirements stipulated by the Federal Constitutional Court in its verdict concerning data retention[112] which were put into effect by the legislator in the revision of the Telecommunication Act (§ 113d TKG German Telecommunication Act). In addition there must be technical safeguards to ensure that information about the blacklisting state is made available in a non-discriminatory manner (i.e. without creating an information advantage for individual market participants). Here a form of regulation would suggest itself which specifies fixed times for updating. In view of the very minor level of intensity of interference with the right to informational self-determination, it seems currently possible to have the blacklist administered by state authorities.

2.5.2.4 Provisional Listing in Investigative Procedures

Finally, the transaction blacklist regulation should be supplemented by the possibility of a provisional listing established by the public prosecutor's office in investigative procedures in cases of suspicion. This regulation would supplement

111 Cf. 2.3.2.3.4.

112 Compare BVerfGE 125, 260 (pp. 325 ff.).

the regulations on asset recovery according to §§ 111b ff. StPO for those cases where a recovery following those regulations (for which, incidentally, there is no legal consensus as to whether and how they may be applied to the recovery of virtual cryptocurrency units[113]) is de facto impossible because of a refusal to surrender private keys or other means of access. The possibility of provisional listings seems to be particularly necessary in cases where no concrete suspect has been identified for a suspicious transaction (as e.g. in the practically very relevant cases of CryptoLocker blackmail[114], i.e. for "ransom payments" where this is often the case). It would significantly increase the preventive effect if criminal actors have to expect to "lose" their cryptocoins not only once they were identified as suspects or even on the legally binding conclusion of the criminal procedure, but if devaluation were possible through blacklisting on the grounds of a suspicion regarding *merely the transaction*. At the same time this decreases the risk for legitimate users to be affected by a subsequent blacklisting, since the provisional blacklist would also be publicly accessible. This would significantly lessen the serious interference with article 14 section 1 GG. In order to limit any (possible) damage to reputation by provisional blacklisting, any provisional listing should be recognisable as such.

Faster information for users about which transactions might be linked to criminal activities will, however, have a negative impact on the drying up of mixing services[115] and thus to a part of the desired preventive effect. For this reduces the risk for all parties involved that there will be subsequent (part) devaluation by blacklisting of transactions used in a mixing process.[116] However, this side-effect is acceptable in view of the advantageous effect described above.

The intensity of the interference with article 14 section 1 GG through provisional listing is further increased – in comparison to the final listing after a final verdict – by the fact that this is only implemented on the grounds of a suspicion (similar to §§ 111b ff. StPO). To comply with the proportionality principle legal remedies are needed (e.g. request for a court decision modelled on § 98 section 2 sentence 2 StPO or even preventive requirement of a court decision), a maximum duration (e.g. modelled on § 111b section 3 StPO) and compensation rules (by including the measure in the catalogue of § 2 section 2 StrEG (Law on Compensation for Wrongful Prosecution), e.g. as No. 4a). The appropriate location for the regulation on provisional blacklisting would be suggested as a supplement to §§ 111b ff. StPO.

2.5.2.5 Interaction with Money Laundering Offences

The blacklisting principles themselves raise questions concerning their relationship to money laundering offences as per § 261 StGB. Here the mixing of legal and illegal cryptocoins plays a major role. This type of mixing does indeed also occur with cash and deposit money (and most likely on a daily basis).[117] In such cases, however, the authorities usually fail to establish a punishable offence of money laundering because of an absence of knowledge about the origin of the moneys

113 Vgl. *Rückert*, MMR 2016, 295; *Goger*, MMR 2016, 431; *Heine*, NStZ 2016, 441; *Greier*, wistra 2016, 249.

114 Compare e.g.: http://www.sueddeutsche.de/bayern/unterfranken-dettelbach-zahlt-loesegeld-nach-cyberangriff-1.2892279; http://www.zeit.de/digital/datenschutz/2016-02/it-sicherheit-ransomware-erpressung-krankenhaus-los-angeles-neuss.

115 On this cf. 1.2.

116 For details: *Abramova/Schöttle/Böhme*, Mixing Coins of Different Quality: A Game-Theoretic Approach (unpublished).

117 Impressively in: *Fischer*, Woher haben Sie dieses Geld?, Zeit Online of 13.10.2015, p. 4.

from a catalogued offence. By introducing a transaction blacklist the accompanying (possible) knowledge of an incriminated origin when using listed cryptocoins can, however, establish premeditation. Seen, in particular, against the backdrop of the "mixing issue" and the accompanying risk of "infecting" legal cryptocoins the question of the effect of a transaction blacklist on premeditation acquires major significance. This must be referred back to the juridical practice of the Federal Court of Justice (BGH) concerning the mixing of legal and illegal moneys in one account.[118] A "total contamination", i.e. the poisoning of all moneys in the mixing is only to be said to exist "*if the illegal share has to be assessed as not merely completely insignificant*", which is to be assumed to be the case at a poisoned share of 5.9 to 35 per cent.[119]

If such a legal ruling is consistently transferred to virtual cryptocurrencies, there is the danger of a progressive poisoning of the entire system.[120] A provisional blacklisting would indeed mitigate the problem insofar as, at a later date, definitively blacklisted transactions will no longer be readily transferable by the users. But independently of this, a transfer of the total contamination doctrine, as advocated by the BGH, to virtual cryptocurrencies is more than questionable. This is particularly true against the backdrop of the question, which has already been raised, of the effect of a transaction blacklist on premeditation, which is linked to the fact that the offence of money laundering is defined in wide terms in German law, and that the action level of money laundering is (even more) readily fulfilled in a decentralised, pseudonymised and cross-border system. For the assumption of premeditation as regards origin from a catalogued offence, it is sufficient to have knowledge of the moneys originating in any action listed in § 261 section 1 StGB, i.e. the premeditation does not need to be linked to a specific catalogued offence. In the context of the offence of carelessness as per § 261 section 5 StGB it would even be sufficient for such an origin to have suggested itself but to have remained unrecognised due to gross negligence or indifference.[122]

It must, therefore, be stated that any application of the total contamination doctrine to virtual cryptocurrencies in establishing a transaction blacklist would massively increase the risk of a money laundering offence for users.

This is not the only reason why the total contamination doctrine must be rejected as disproportionate in the field of virtual cryptocurrencies. First, this can be justified by the fact that the deterrent effect intended by the BGH assuming total poisoning in mixed constellations would refer to virtual cryptocurrencies as such. Secondly, the process of mixing virtual cryptocurrencies differs significantly from mixing (real) moneys in an account. This is due, on the one hand, to the fact that all (crypto) accounts, and hence the course of transactions, are publicly accessible; on the other hand it is due to the fact that for many virtual cryptocurrencies there is no mixing of cryptocoins based on accounts. The starting conditions are thus significantly different from those for mixing legal and illegal (real) moneys in an

118 BGH, decision of 20.05.2015 – 1 StR 33/15, NJW 2015, 3254.

119 However, the BGH explicitly does not commit to a specific minimum share.

120 First estimates presupposing that the blacklisting of incriminated transactions would not bring about a change in behaviour had the result that after only 500 blocks (about 3.5 days) an average of 1 per cent of all bitcoins in circulation would be poisoned.

121 BGH, verdict of 28.01.2003 – 1 StR 393/02 = BeckRs 2003, 01885 with reference to BGHSt 43, 158 (165); BGH, decision of 10.11.1999 – 5 StR 472/99 = StV 2000, 67.

122 BGHSt 43, 158 (168); 50, 347 (351); BT-DrS 12/989, p. 28.

account so that there are compelling reasons for not absolutely adhering to the total contamination doctrine for virtual cryptocurrencies. A transaction blacklist, therefore, constitutes a milder but at the same time more effective means of preventing money laundering.

2.5.3 Design of a Flanking Licensing Model

Some fundamental aspects need to be taken into account in the design of a flanking licensing model: in order not to hinder innovation in virtual cryptocurrencies to a disproportionate extent and to avoid an exodus of intermediaries from the European economic region, the group of intermediaries who are obliged to obtain authorisation should be kept as small as possible. The recommendation is to have an obligation to obtain authorisation only for those intermediaries who exchange partially blacklisted cryptocoins into real currency. By contrast, other intermediaries who do not accept blacklisted cryptocoins should be exempt from the obligation to obtain authorisation. Furthermore, the special characteristics of virtual cryptocurrencies must be taken into account. In particular, the credit risk for cryptocoin intermediaries is not comparable to that for banking institutions. Thus a lower level of requirements concerning intermediaries' starting capital (cf. § 33 section 1 no. 1 KWG) and professional competence of management (compare §§ 33 section 1 no. 4, 25c KWG) is called for.

Essentially the licensing model has to safeguard that the obligated person is known, accessible and sufficiently reliable.

2.5.4 Technical Aspects

The blacklisting system suggested may be efficiently implemented if, right from the start, it is supported by a reliable and redundantly implemented IT system. This system should be organised according to the principles of low design complexity and be developed to fulfil the requirements of blacklist administration. Development and operation must be state-of-the-art and must timeously take account of future developments. This applies particularly to the integrity of the blacklist, the authorisation of writing access and the confidentiality of non-public information such as, for example, the circumstances of a provisional listing (responsible authority, suspicion, file reference etc.). Information retrieval must require minimum data use and ideally be anonymous. Following the principle of purpose limitation, it is not advisable to implement the blacklisting function by extending existing systems, either for possible practical or economic considerations. In view of the novelty and the special characteristics of virtual cryptocurrencies the effort required to integrate them into existing systems might anyway be significantly higher than the expected benefit. Identification of listed transactions should – as far as technically possible in decentralised systems – be unambiguous and must be separately defined for each supported virtual cryptocurrency. Orientation on the identifiers used in the respective core systems would be appropriate.

Special requirements for the availability and scalability of the system arise from the fact that obligated intermediaries are expected to check each intended transaction against the blacklist in advance, and that it is plausible that virtual cryptocurrencies will considerably increase in popularity. Possible time lags in answering requests due to overload must be avoided, since they would lead to unequal treatment of intermediaries and indirect users who thus might suffer

financial disadvantages. In addition, insufficient scalability would increase the probability of successful DDoS attacks.[123]

In order to ensure that pseudonymous users have legal protection in the event of erroneous blacklisting, technical interfaces and processes are needed to prove that they were involved (e.g. by proof of ownership of the private key for an account affected by a listed transaction). Once this proof is furnished, the person concerned must be provided with information about the process which resulted in the listing.

To increase legal certainty for obligated intermediaries, it would be desirable for the information (particularly also negative information) about entries in the blacklist to be issued with a time stamp and digital signature. Thus the intermediaries could later prove that they fulfilled their obligations.

2.6 European and International Applicability of the Recommended Action

The transaction blacklist has high international applicability since it may be implemented with a manageable degree of technical effort, on the basis of tried and tested technologies and since it is not based on special national legal circumstances.

2.6.1 Uniform Blacklist within the EU

Given the de facto unbounded nature of virtual cryptocurrency systems as against the uniformity of the EU internal market, a uniformly kept and administered transaction blacklist for the EU is desirable. Respective directives could be based on article 75, 114 TFEU. Europol would be the choice of an administering authority since it already disposes of comprehensive data-processing competence. Alternatively a new authority could be created (similar to European Anti-Fraud Office OLAF[124]).

2.6.2 International Blacklist via International Treaties

In order to block (actual and likely) circumvention strategies and displacement effects it is also recommended to aim at international cooperation. This would ideally take the form of binding international agreements on the keeping and updating of international transaction blacklists and would make respective national actors obligated by the signatory states. As a short-term objective the minimum aim should be the internationally uniform criminalisation of offences linked to cryptocurrencies (e.g. in the context of a "new" Cybercrime Convention), in order to make possible a uniform legal basis for the inclusion of incriminated transactions in national or EU-wide blacklists for cross-border payment transactions with virtual cryptocoins.

123 The blacklisting approach is controversially discussed by the user community, cf. Bitlegal.io, Bitcrime to undermine fungibility of bitcoin, accessible at http://bitlegal.io/2016/05/25/bitcrime-to-undermine-fungibility-of-bitcoin/ (last access: 15.12.2016). At the same time, DDoS attacks are considered a common means of protest in parts of the user community, cf. *Vasek/Thornton/Moore*, in: Böhme/Brenner/Moore/Smith, Financial Cryptography and Data Security, 1st Workshop on Bitcoin Research (FC 2014), Barbados, Berlin et al. 2014, pp. 57 ff.

124 http://ec.europa.eu/anti-fraud//home_en.